Process Risk and Reliability Management

Process Risk and Reliability Management

Second Edition

Ian Sutton

ELSEVIER

AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO
Gulf Professional Publishing is an imprint of Elsevier

G P
P

Gulf Professional Publishing is an imprint of Elsevier
The Boulevard, Langford Lane, Oxford, Kidlington, Oxford, OX5 1GB

First edition 2010
Second edition 2015

Notice
No responsibility is assumed by the publisher for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions or ideas contained in the material herein. Because of rapid advances in the medical sciences, in particular, independent verification of diagnoses and drug dosages should be made

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Catalog Number
A catalog record for this book is available from the Library of Congress

ISBN: 978-0-12-801653-4

For information on all Gulf Professional publications visit our website at books.elsevier.com

Typeset by MPS Limited, Chennai, India
www.adi-mps.com

Printed and bound in the United States of America

15 16 17 18 19   10 9 8 7 6 5 4 3 2 1

Preface

The first version of this book was published in the year 1997 with the title *Process Safety Management* (Sutton, 1997). At that time process safety regulations in the United States had been in force for just a few years, so most companies in the process industries were developing and implementing the programs needed to address the new regulations. The book aimed to help managers and technical specialists with the design and implementation of Process Safety Management (PSM) programs.

Since those early days, the management of safety on process facilities has matured and improved dramatically. Also PSM is now typically seen as being part of the bigger picture of risk management, covering not just safety but also environmental performance, quality, production, and productivity. Therefore, in the year 2010 the book was greatly expanded and renamed *Process Risk and Reliability Management.*

But time marches on and the PSM world continues to expand. Hence the current edition. Virtually all of the content of the book has been expanded, revised, and updated. And many new sections have been added. These include:

- The impact of resource limitations on the process industries in general and process safety programs in particular
- A review of some of the major incidents that have affected the process industries
- Thoughts to do with the impact of the on-going crisis at the Fukushima-Daiichi nuclear power complex
- The value of storytelling as a means of conveying process safety values and principles
- The impact of the proposed changes to the OSHA PSM standard.

In addition to the developments of this book, other books in the same series have been published. *Offshore Safety Management* is now in its second edition and focuses on regulations, management systems, and technical issues to do with the offshore oil and gas business. *Plant Design and Operations* covers detailed topics, as can be seen from the chapter titles.

1. Operations
2. Maintenance
3. Energy Control Procedures
4. Occupational Safety
5. Personal Protective Equipment
6. Health and Industrial Hygiene
7. Human Factors
8. Contractors
9. Security
10. Safety in Design
11. Equipment
12. Piping and Valves
13. Instrumentation and Control Systems

14. Transportation
15. Layout
16. Common Hazards
17. Project Management.

This edition of *Process Risk and Reliability Management* is organized into four sections with a total of 20 chapters, as shown below:

Sections	Chapters
Risk	1. Risk Management 2. Compliance and Standards 3. Culture and Participation
Management Elements	4. Technical Information 5. Hazard Identification 6. Operating Procedures 7. Training and Competence 8. Prestartup Reviews 9. Asset Integrity 10. Management of Change 11. Incident Investigation and Root Cause Analysis 12. Emergency Management 13. Audits and Assessments
Analysis Techniques	14. Consequence Analysis 15. Frequency Analysis 16. Reliability, Maintainability, Availability
Management	17. Managing a Risk Program 18. Project Management 19. Contractors 20. The Risk Management Professional

- The first section—Risk (Chapters 1−3)—provides an overview of the concepts of risk and safety culture. It also covers compliance and case studies.
- The second section—Management Elements (Chapters 4−13)—provides guidance on the specifics of a process risk management program. The chapter titles are basically the same as the elements of a typical PSM program.
- The third section—Analysis Techniques (Chapters 14−16)—describes some of the technical tools that are used to understand, calculate, and manage risk.
- The fourth section—Management (Chapters 17−20)—provides guidance to do with the management of a risk program, including project management and the attributes of a professional working in the process safety business.

CHAPTER

RISK MANAGEMENT

1

CHAPTER OUTLINE

INTRODUCTION

Facilities in the process industries typically handle large quantities of hazardous materials. The consequences of an incident involving these materials can be very serious, so it is critical that management in those industries develop and implement risk management programs. The contents of this book provide guidance as to how this can be done. Risk management covers a broad range of issues, including technical analysis, the development and use of management systems, and human behavior, so the scope of this book is broad. And the goals of risk management programs go beyond safety—which is why the title of this book was changed from *Process Safety Management*

Process Risk and Reliability Management. DOI: http://dx.doi.org/10.1016/B978-0-12-801653-4.00001-1

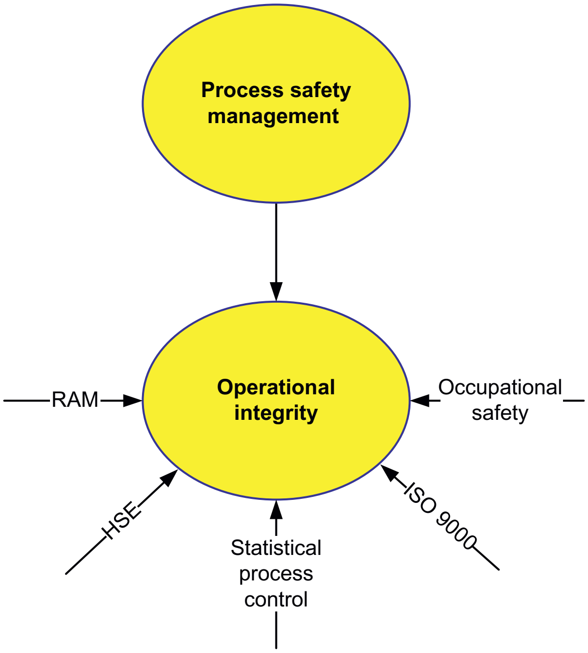


FIGURE 1.1

Operational integrity management programs.

to *Process Risk and Reliability Management*. An effective risk management program considers not just safety, but also environmental impacts, economic losses, and more nebulous topics such as company reputation.

Risk management is part of the larger topics of Operational Integrity and Operational Excellence. A facility which has a high level of operational integrity is one that performs as expected in an atmosphere of "no surprises." The facility exhibits integrity in all aspects of its operation. These programs incorporate not just process safety but also many other technical initiatives that companies have been pursuing during the last two decades in order to improve safety, environmental performance, and profitability. A partial list of such initiatives includes:

1. RAM (reliability, availability, and maintainability) programs that focus on achieving maximum profitability.
2. HSE programs covering the broad spectrum of Health, Safety, and Environmental (HSE) work.
3. Statistical process control.
4. Quality standards such as ISO 9000.
5. Occupational and behavior-based safety programs that help improve the actions and behaviors of individuals.

Each of these topics—along with many others not listed above—can be thought of as contributing toward the overall discipline of operational integrity, as illustrated in Figure 1.1.

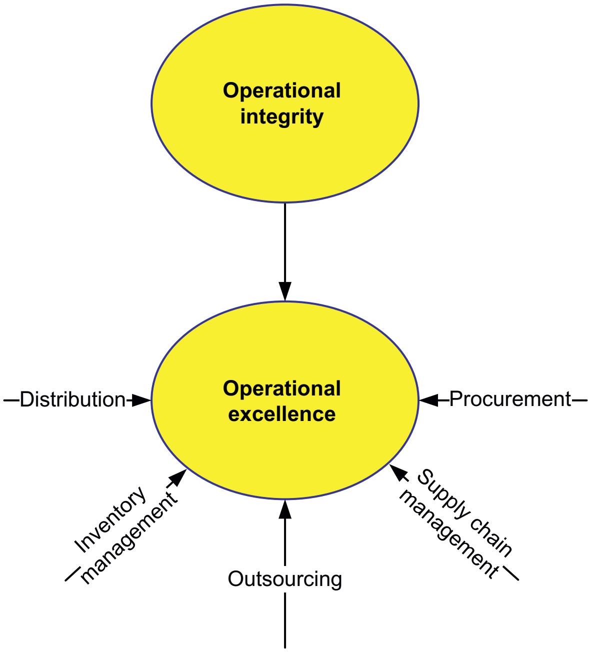


FIGURE 1.2

Operational integrity to operational excellence.

In addition to the incorporation of a wide range of management techniques that are shown in Figure 1.1, operational integrity can be applied to a much wider variety of industries than is the case with process safety management. Operational Integrity Management (OIM) can be used not only in chemical facilities and refineries, but also in transportation, pipelines, and offshore oil and gas.

Many companies are also developing operational excellence programs. The manner in which these can relate to operational integrity is shown in Figure 1.2. Operational integrity is made up of technical initiatives; operational excellence incorporates nontechnical management systems that can affect safety and operability. These include distribution, inventory management, outsourcing, supply chain management, and procurement.

TECHNICAL, PROCESS, AND OCCUPATIONAL SAFETY

The word “safety” has many different interpretations and is used in many different contexts. For those managing risk in the process industries, it is useful to distinguish between three types of safety: technical safety, process safety, and occupational safety. There is considerable overlap between them, but the broad characteristics of each are as follows:

- *Technical* safety is mostly to do with quantitative analysis and often involves very high-consequence events. The calculation of blast overpressures, the dispersion of gas clouds,

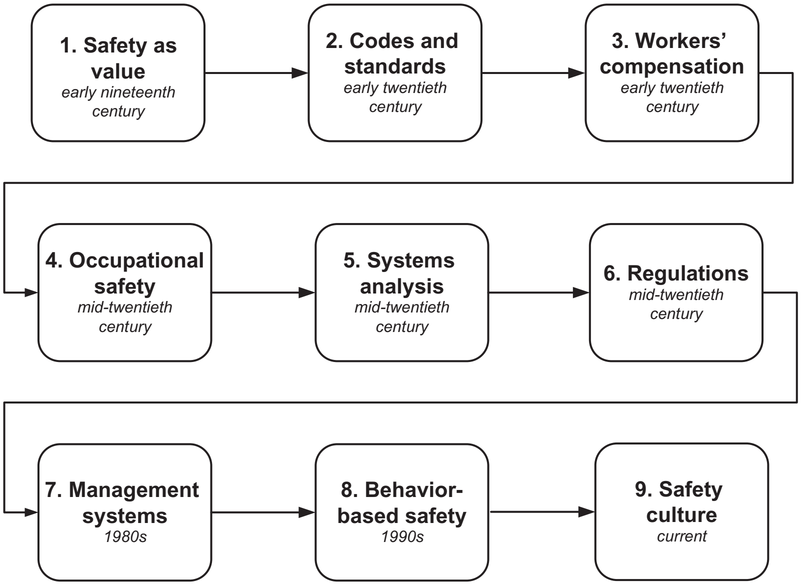


FIGURE 1.3

Developments in safety systems.

and the design of fire ring mains would all fall into this category. Technical safety would also include quantitative risk analysis and decisions to do with levels of acceptable risk. Formal safety assessments, as generally applied to offshore work, are mostly to do with technical safety.

- *Process* safety incorporates elements of technical safety, but its focus tends to be on operations and the role of people on facilities that are already in operation. Process safety is also concerned with process-oriented issues such as runaway chemical reactions, corrosion, and the inadvertent mixing of hazardous chemicals. The impact of such events can lead to major incidents such as explosions, large fires, and the release of toxic gases.
- *Occupational* safety, sometimes referred to as "hard-hat" safety, covers topics such as vessel entry, vehicle movement, protective clothing, and tripping hazards.

HISTORICAL DEVELOPMENT

Safety and risk management programs have always been an integral part of the process industries. Initially such programs were quite crude and basic, but they have become much more sophisticated as standards have risen and as processes have become more complex.

Figure 1.3 provides an overview of some of the major changes and advances that have been made in the last 150 years or so.

1. SAFETY AS A VALUE

People working in the process industries now take it for granted that safety is a value, even when their own organization has a poor safety record—no one ever says, “Safety doesn’t matter.” However, such an attitude was not the norm 200 years ago. In his novel *Hard Times*, published in the year 1854, Charles Dickens satirically condemned the industrialists who failed to acknowledge that safety and clean air were values, in and of themselves.

> They [the industrialists] were ruined when they were required to send labouring children to school; they were ruined when inspectors were appointed to look into their works; they were ruined, when such inspectors considered it doubtful whether they were quite justified in chopping people up with their machinery; they were utterly undone, when it was hinted that perhaps they need not always make quite so much smoke...

The weapon that Dickens and his fellow authors used was satire. This weapon has now fallen out of use—modern professional safety workers rarely attempt the use of irony (although some of what is written in Chapter 3 in the section to do with Warning Flags represents a feeble attempt to follow in Dickens’ footsteps).

2. CODES AND STANDARDS

By the beginning of the twentieth century, the number of industrial accidents had risen to unacceptably high levels. For example, between the years 1870 and 1910, at least 10,000 boiler explosions occurred in North America. By the year 1910, the rate of such explosions had reached approximately 1,400 per year.

In response to this unacceptable situation, industrial societies (particularly the American Society of Mechanical Engineers) started publishing what has since become a very wide range of codes and standards. The first boiler code was published in 1914.

3. WORKERS’ COMPENSATION

Worker’s compensation programs were introduced around the start of the twentieth century in various nations. These programs are a no-fault insurance system in which an injured worker receives medical and compensation benefits regardless of the causes of the job-related accident. If the injury or illness is job related, the injured worker receives medical benefits and, if eligible, temporary compensation for loss of earning power. In some cases, the injured worker may also receive permanent compensation and job retraining. In return, lawsuits against the employer, except under very limited circumstances, are not permitted.

The cultural impact of workers’ compensation was to make it clear that there is liability to do with accidents; some of that liability lies with the employer, and some with the worker, and that both parties need protection.

4. OCCUPATIONAL SAFETY

In the mid part of the twentieth century, increasing emphasis was placed on occupational safety issues such as training, working conditions, and the use of PPE (personal protective equipment).

5. SYSTEMS ANALYSIS

Toward the end of the Second World War, systems techniques such as fault tree analysis were introduced in order to predict the reliability and performance of military airplanes and missiles. The use of such techniques led to the formalization of the concept of probabilistic risk assessment (PRA). The publication of the Reactor Safety Study (NRC, 1975)—often referred to as the Rasmussen Report after the name of principal author, or by its subtitle WASH 1400—demonstrated the use of such techniques in the fledgling nuclear power business. Although WASH 1400 has since been supplanted by more advanced analysis techniques, the report was groundbreaking in its approach to system safety.

Systems analysis was also an integral part of the U.S. nuclear navy. The stringent standards imposed by Admiral Rickover to do with both nuclear safety and personnel selection have been a critical factor in the navy's continuing record of zero reactor accidents.

Systems analysis techniques are used only to a limited extent in the process industries for two reasons. First, such techniques are not generally effective at predicting human behavior (e.g., WASH 1400 did not anticipate the Three Mile Island accident). Yet human performance is a very important component of safety performance in the process industries. Second, the use of PRA methodologies is generally time-consuming and expensive—particularly when used in the chemical industries where there is so much difference from facility to facility.

A modified method of quantifying risk through the use of systems analysis has been adopted by the process industries. The technique is known as LOPA (layers of protection analysis) provides an order of magnitude estimation of risk (details of the method are provided in Chapter 15).

In spite of its limitations, the use of systems analysis has helped modify the culture of the process industries. By developing quantified analyses, risk professionals are able to move to a more objective approach in the management of process safety and operational integrity. There is less "I think/You think," and more "Here is what the numbers are telling us."

6. REGULATIONS

Regulation of the process industries has increased steadily, particularly since the early 1960s. In the United States, the catalyst for the environmental movement was the publication of Rachel Carson's *Silent Spring* in the year 1962. Although her book focused on the hazards of DDT on birds of prey, it also created a broader challenge to technological progress and set the stage for the modern environmental movement.

Of particular importance to process industries in the United States was the creation of OSHA (Occupational Safety and Health Administration) in the year 1970 by the Nixon administration.

7. MANAGEMENT SYSTEMS

During the 1980s, a series of bad accidents in the process industries, both onshore and offshore, demonstrated that a new approach to management safety was needed. Examples of these new approaches were the development of Process Safety Management (PSM) in the United States and the introduction of the Safety Case Regime in Europe. In the United States, process safety legislation requirements were included in the amendments to the Clean Air Act of 1992. This legislation directed the OSHA and the Environmental Protection Agency (EPA) to each develop, implement, and enforce process safety standards in order to protect both workers and the public. Some states also introduced their own process safety regulations.

Similar programs were introduced in the same time frame in many other nations and industries. For example, regulations covering the offshore industry in the North Sea were introduced following the Piper Alpha disaster of 1988. In addition, industry organizations such as the American Petroleum Institute (API) and the American Chemistry Council (through the Responsible Care® program) developed their own process safety standards that were generally not adopted into law but that typically provided good practical guidance regarding the implementation and management of process safety systems.

Considerable progress to do with the implementation of process safety programs has been made in the 15 years since the early 1990s—particularly with respect to regulatory compliance. For example, prior to the early 1990s, few companies had a formal Management of Change program; now such programs are part of the furniture in almost all process facilities. This is not to say that further improvements cannot be made. Indeed, in the words of one facility manager, "There is always news about safety, and some of that news will be bad." Moreover, there have been greater improvements in occupational safety than there have been in process safety (Whipple and Pitblado, 2008).

And such data as exist would seem to confirm that progress with process safety has not been as good as for occupational safety. For example, Figure 1.4, which is based on data provided by Pitblado (2008), showed that there has been a steady improvement in occupational safety in the process industries—(the overall trend line, which is built on data from many large companies, demonstrates an order of magnitude improvement in occupational safety in the 12-year period covered.

The same paper states, however, that "there is no clearly visible overall decline in major accident process safety events observed in either the United States or European Union, although the data is noisy and some successes do exist—notably the U.K. Sector of the North Sea reduction in major leak events." In other words, the significant improvements that have occurred in occupational safety in the last decade are not being repeated with regard to process safety. One suggested technique for improving process safety performance is to manage technical safety barriers in real time, i.e., to implement a system to ensure that all safety systems and devices are fully functioning at all times.

In addition, new concerns—such as the increased shortage of experienced employees—have come to the fore as challenges to continued improvement in process safety performance process. Nevertheless, the process industries (including the regulators) can take a great deal of credit for having made substantial strides in process safety during the course of the last two decades.

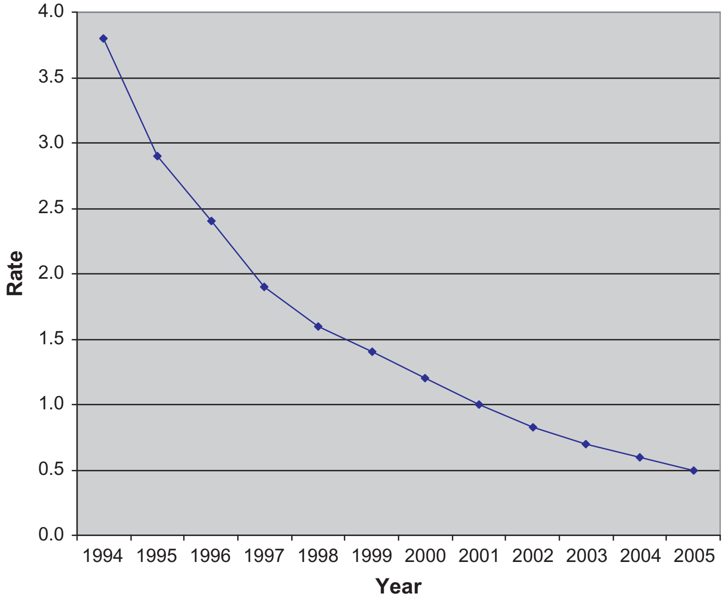


FIGURE 1.4

Occupational injury trends.

8. BEHAVIOR-BASED SAFETY

In recent years, many companies have invested in behavior-based safety (BBS) programs. BBS is a process that helps employees identify and choose a safe behavior over an unsafe one. It also encourages employees to work with their colleagues on improving their mutual understanding of effective and ineffective behaviors as they apply to safety.

The first step in the BBS process is to observe employees performing their routine tasks. Both safe and unsafe behaviors are noted and recorded (with personal information omitted). The observer provides positive feedback on safe behaviors and nonthreatening feedback on unsafe behaviors. Employees are provided with suggestions on correcting the unsafe or at-risk behaviors. The employees are not reprimanded or disciplined for at-risk behaviors, nor are any findings reported to management. Employees are encouraged to comment on the observations; their comments are included with observations themselves, along with any suggestions for improvement.

Results from the observation records are gathered and compiled in a single database. Reports from the database indicate which types of at-risk behavior are most prevalent and in which locations they are taking place. Based on the insights generated during the review and analysis phase, recommendations for improvement can be made.

BBS should be a part of the company way of life. This means that if any employee notes that a colleague is demonstrating an at-risk behavior then he or she is encouraged to talk to the colleague and suggest ways of eliminating that behavior. Similarly, behaviors that are particularly good should receive commendation.

9. SAFETY CULTURE

The final box in Figure 1.3 is to do with the concept of safety culture—a topic that is the focus of much current discussion and development. This topic is discussed in Chapter 3.

MAJOR EVENTS

Many of the improvements in safety and risk management have resulted from changes made following a major incident. A summary of some of them is provided in Table 1.1.

Table 1.1 Some Major Process Incidents

Year	Location	Brief Description
1974	Flixborough, England	Rupture of a temporary pipe bypass led to a large release of cyclohexane gas, followed by a massive explosion. 28 deaths; 89 injuries (workers and public)
1976	Seveso, Italy	Release of highly potent toxin, TCDD. Approximately 250 community injuries.
1979	Three Mile Island, PA	Partial core meltdown in a nuclear power plant. There was no significant release of radioactive materials to the environment, nor was anyone injured. Nevertheless, the event leads to a virtual moratorium on the construction of new nuclear power plants in the United States for a generation.
1984	Bhopal, India	Addition of water to a tank containing a hazardous chemical led to a release of isocyanate vapors. More than 2,500 deaths in the local community, and many more serious injuries.
1988	Piper Alpha, North Sea	Release of hydrocarbons led to an explosion and destruction of the offshore platform. 165 deaths.
1989	Pasadena, TX	Release of ethylene/propylene led to a massive explosion 23 deaths and about 130 injuries.
1990	Channelview, TX	Explosion of storage tank. 21 deaths.
2005	Texas City, TX	Fire and explosion. 15 deaths.
2010	Deepwater Horizon/ Macondo, Gulf of Mexico	Explosion and fire leading to nine fatalities, a massive environmental spill, and enormous financial loss.
2011	Fukushima–Daiichi Nuclear Power Plant Complex, Japan	Earthquake and tsunami leading to ongoing release of radioactive materials and enormous financial loss.

Table 1.2 Elements of HSE

Element	Covers	Timeline
Environmental/sustainability	All life forms	Years, possibly decades
Health	Public and workers	Months to years
Safety	Workers	Short term or instantaneous

HEALTH, SAFETY, AND ENVIRONMENTAL PROGRAMS

Most companies in the process industries have Health, Safety, and Environmental (HSE) departments, which are also referred to by the letters SHE, HES, and EHS—the sequence of the letters is not important. (In the United Kingdom, the letters "HSE" generally refer to the regulatory agency, the Health and Safety Executive.) The term "loss prevention" is also used to describe HSE activities; it is also the title of the well-known three-volume series *Loss Prevention in the Process Industries* (Lees, 2004).

Although HSE activities are often grouped together and are often directed by a single manager, the three topics are actually quite distinct from one another. Table 1.2 gives who or what is covered by each of the elements of HSE and outlines the geographical scope and timeline for each of those elements.

ENVIRONMENTAL/SUSTAINABILITY

Environmental programs are broad in scope; in principle, they cover all living creatures and all parts of the globe. A facility's environmental performance affects not only the communities in which they are located, but also the public in general, and—when issues such as global climate change are considered—the future of the planet itself. Increasingly, environmental professionals are using the term "sustainability" rather than "environmentalism." The earth is viewed as having finite resources. Therefore, society's long-term goal should be not only to have as little long-term impact on the environment as possible but to replace resources that have been used.

Environmental issues can take a long time to develop or to understand. For example, the issue of global warming and its consequences was identified in the late 1970s. But, even now, very little action is being taken to address this problem.

Environmental performance is largely driven by regulations because no company is big enough to address such issues alone. Also, whereas PSM programs are nonprescriptive, environmental work is generally driven by detailed, prescriptive rules and standards.

In one respect, the legal framework in which environmental professionals work is unusual. In most other types of legal process, a person is assumed to be innocent unless proven guilty beyond all reasonable doubt. It is up to the prosecution to establish guilt—not to the defendant to establish innocence. In the case of environmental work, the opposite applies. Industries are generally assumed to be creating an unacceptable level of pollution—the onus is on them to demonstrate that they are not.

HEALTH

Health issues generally affect only the workers at a facility and people living in the immediate neighborhood of that facility. The timeline for health concerns is likely to be considerably shorter than for environmental issues—typically weeks or months rather than years (although some poorly understood health issues may take longer than that to diagnose and understand).

Health and environmental concerns often overlap. For example, if a company is discharging a toxic gas such as sulfur dioxide (SO_2) on a routine basis, then the company will have to be concerned about meeting the environmental rules to do with SO_2 emissions. Going beyond mere regulatory compliance however, the company may then elect to conduct analyses to determine what impact the SO_2 may be having on the health of the local community, or of workers at the facility. The results of such a study may encourage the company management to implement control measures that are more stringent than what is legally required.

Whereas environmental compliance is typically driven by legislation, many health programs such as asbestos abatement are propelled by litigation, particularly in the United States. In other words, standards are developed through the use of lawsuits rather than government mandates.

SAFETY

Safety is primarily concerned with sudden, catastrophic incidents that could result in serious injury or death. Safety generally affects only facility workers. (There are exceptions to this statement; sometimes an industrial accident can impact public safety. For example, the Bhopal tragedy led to the death of thousands of people in the local community). In general, the timeline in which safety events take place is short, often covering just a fraction of a second.

PRESCRIPTIVE/NONPRESCRIPTIVE

Risk management programs can be divided into two broad categories: prescriptive and nonprescriptive. Prescriptive standards, in which a set of detailed standards are developed, usually by a regulator or industry standards-setting body, are what most people think of when safety is discussed, are often associated with traditional occupational safety standards. To pick an example almost at random, OSHA has the following rule to do with ladders:

> All rungs shall have a minimum diameter of three-fourths inch for metal ladders, except as covered in paragraph (b)(7)(i) of this section and a minimum diameter of 1 1/8 inches for wood ladders.

A statement such as that is quite clear and uncompromising; it is also easy to follow. A person installing a ladder at an industrial site need not think about the basic principles of ladder design or use. Nor does that person have to carry out any type of risk analysis. He or she simply has to follow the rule as written.

Another example of prescriptive standards for offshore facilities regarding the design of systems to prevent overpressure of vessels comes from API Recommended Practice 14C which states

> The safety system should provide two levels of protection to prevent or minimize the effects of an equipment failure.

Although more nuanced than the OSHA rule to do with ladders, the above sentence is also prescriptive. It does, however, allow for some nonprescriptive judgment. For example, the standard does not specify the types of protection. Most designers will protect against overpressure using a combination of safety instrumentation and a mechanical device such as a pressure relief valve, but this approach is not actually a requirement of the standard.

The other style of risk management is nonprescriptive. Companies are not provided with specific and detailed rules regarding what to do; instead managers at these companies take the appropriate actions needed to keep their facilities safe. The basic idea behind this approach is that the companies that operate sophisticated facilities such as offshore platforms and drilling rigs are the ones who know the process and equipment the best, so they are the best qualified to decide what needs to be done to achieve safe operations. It is up to the managers, technical experts, and the operations/maintenance personnel to determine how this should be done. A nonprescriptive rule states, "do whatever it takes on your facility not to have accidents." It is up to the managers and employees to determine how this should be done. There are no universally "correct answers" as to what needs to be done to achieve a safe operation. What is appropriate in one location may or may not be appropriate in another. All that is required is that programs be in place, and that they be adhered to. (In this regard, PSM is similar to ISO 9000 and other quality standards, which also require that companies set their own standards, and then adhere to them.)

An important benefit of the nonprescriptive/performance-based approach is that an industry can immediately capture what has been found by experience or test to work well—there is no need for the regulators to catch up with the latest technology.

The nonprescriptive approach can be illustrated by the following quotation from OSHA's PSM standard to do with the topic of Mechanical Integrity. It states

> The employer shall establish and implement written procedures to maintain the ongoing integrity of process equipment.

The standard provides no specific requirements regarding the amount of detail or the content of those procedures. One consequence of this approach is that the overall PSM standard is only about 10 pages long.

Nonprescriptive standards are, of necessity, performance-based because there is no external specific standard against which they can be assessed. Also, it is never possible to be "in compliance." Ultimately, the only measure of success is success. Consequently, from a theoretical point of view, it is impossible to achieve "compliance." The only truly acceptable level of safety is perfection. Yet, no matter how well run a facility may be a zero accident rate is a theoretically unattainable goal. Risk can never be zero. Indeed, if a facility operates for long enough, it is certain—statistically speaking—that there will be an accident. Therefore, management has to determine a level for "acceptable safety." And because risk can never be zero, there are always ways of improving safety and operability.

SAFETY MANAGEMENT PROGRAMS

In practice, all actual safety management programs combine a mix of prescriptive and nonprescriptive approaches. For example, many offshore Safety Cases make reference to the API's Recommended Practice 14C, a prescriptive standard. On the other hand, judgment will always be required when prescriptive standards are being applied—no rule or standard can cover every possible situation. It would be invidious to state that one approach is better than the other.

Nevertheless there is a trend toward adopting nonprescriptive approaches for the following reasons:

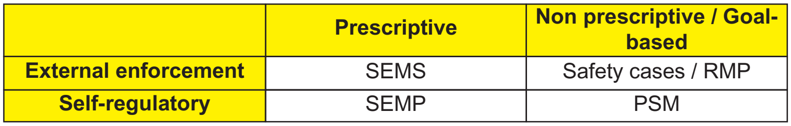
- It is difficult for a regulator or standards body to keep up with new developments in technology in rapidly changing areas such as deepwater drilling. This difficulty was illustrated when, following the *Deepwater Horizon* catastrophe, BOEMRE—the agency responsible for offshore safety in the Gulf of Mexico at the time—quickly issued new standards to do with blowout preventers. The technology to do with these devices had advanced but the regulations had not kept up.
- The causes of major events are typically complex and involve a series of low-probability events. It is very difficult to write standards and regulations to cover all such complex trains of events.
- The operation of modern process facilities involves the use sophisticated management systems. Once more, it is difficult to write prescriptive standards to address all the nuances of such systems.

In spite of the trend toward nonprescriptive approaches, there is a balance, and sometimes the pendulum can swing the other way, as illustrated with the problems that Boeing had with the batteries on its 787 airplane (Henderson, 2013).

REGULATIONS

Figure 1.5 illustrates the different regulatory approaches that can be followed. (There is considerable overlap between the categories.) Also shown are safety management programs that are representative of each approach.

- In the top right-hand corner are rules that are largely nonprescriptive and that are enforced by an external agency, usually a government regulator. The Safety Case approach is an example. The EPA's risk management program is similar.



	Prescriptive	Non prescriptive / Goal-based
External enforcement	SEMS	Safety cases / RMP
Self-regulatory	SEMP	PSM

FIGURE 1.5

Regulatory strategies.

- An example of the nonprescriptive but self-enforced category (the bottom right corner) is OSHA's PSM standard. Companies have to have a PSM program, but they do not need to share it with OSHA unless they are asked for it.
- SEMP (the voluntary standard for offshore safety) is quite prescriptive because it refers to a large number of prescriptive standards. It is also self-regulated, and so is in the bottom left square.
- SEMS is basically the same as SEMP except that it has been incorporated into law and therefore is prescriptive, thus putting it into the top left square.

THE REGULATOR'S DILEMMA

Regulators face a dilemma with regard to goal-setting, nonprescriptive safety management systems (SMS). Facility owners and operators develop their own safety programs that are designed to meet their specific circumstances. If a regulator approves those programs, then he or she has implicitly stated that the program is satisfactory. If, later on, a deficiency is found with the program (either during an audit or an incident investigation), then the regulator must take some responsibility and the owner/operator can claim that the incident is not all his fault.

PROCESS SAFETY MANAGEMENT

PSM is a program oriented toward the management and control of processes that handle large quantities of hazardous and flammable chemicals. The focus of PSM is on the prevention of major incidents in facilities that typically employ very sophisticated technology.

The nature of PSM can be understood by examining its component words.

- The first word is *process*. PSM is concerned with process issues such as fires and the release of toxic gases, as distinct from *occupational* safety issues, such as trips and falls.
- The second word is *safety*. Although an effective PSM program improves all aspects of a facility's operation, the initial driving force for most PSM programs was the need to meet a safety regulation and to reduce safety incidents related to process upsets and hazardous materials releases.
- The third word is *management*. In this context, a manager is taken to be anyone who has some degree of control over the process, including operators, engineers, and maintenance workers. Effective control of an operation can only be achieved through the application of good management practices.

The Center for Chemical Process Safety (CCPS, 2007) provides guidance as to what constitutes a PSM event:

- It must involve a chemical or have chemical process involvement.
- It must be above a minimum reporting threshold.
- It must occur at a process location.
- The release must be acute, i.e., it must occur over a short period of time.

PSM is not new; indeed, it has always been an integral part of the process industries. Companies have always carried out activities such as the writing of procedures, planning for

Table 1.3 OSHA Elements of PSM

1. Employee Participation
2. Process Safety Information
3. Process Hazards Analysis
4. Operating Procedures
5. Training
6. Contractors
7. Prestartup Safety Review
8. Mechanical Integrity
9. Hot Work
10. Management of Change
11. Incident Investigation
12. Emergency Planning and Response
13. Compliance Audits
14. Trade Secrets

emergencies, training of operators, and the investigation of incidents. But it was in the late 1980s and early 1990s that PSM programs became more formalized and regulated.

Although industry tended to resist these new regulations, they did force companies to complete their process safety work promptly. Prior to the regulation, there was a tendency to put off tasks such as the writing of operating procedures "until we have time." OSHA required that most of the elements be implemented immediately. The standard put managers' feet to the fire.

Figure 1.1 shows that PSM is an integral component of operational integrity management. Therefore, it is useful to review the elements of PSM because they are so foundational to risk and reliability management work. Different companies and regulatory agencies have different approaches to the topic; some of them are discussed below.

The PSM standard (OSHA, 1992) promulgated by the U.S. OSHA is widely followed, not only in the United States, where it is the law, but in other countries that use it on a voluntary basis. Large companies can use it to set up a uniform system for all their international operations, largely because the creation of the standard involved considerable input from the leading operating companies of the time.

OSHA divided process safety into 14 elements listed in Table 1.3.

As companies have gained more experience with the implementation of PSM, they have found that the list in Table 1.4 has some limitations. A modified list published by the Center for Chemical Process Safety is given in Table 1.4.

Some of the elements in Table 1.4, such as Management of Change, are identical to those in Table 1.3. Others are modified—e.g., Prestartup Safety Review becomes Operational Readiness. But some of the elements in Table 1.4, such as Measurements and Metrics, are completely new. One of the topics in the original OSHA list—Trade Secrets—has been removed.

In addition to the systems shown above, many other organizations, such as the API and the American Chemistry Council, have offered their own methods for organizing PSM programs. Many larger companies also have their own systems. What is important is to recognize that the systems are generally quite similar to one another; a company that meets the requirements of one system is likely to have little trouble addressing other systems.

Table 1.4 CCPS Elements of PSM

1. Process Safety Culture
2. Compliance
3. Competence
4. Workforce Involvement
5. Stakeholder Outreach
6. Knowledge Management
7. Hazard Identification and Risk Management
8. Operating Procedures
9. Safe Work Practices
10. Asset Integrity/Reliability
11. Contractor Management
12. Training/Performance
13. Management of Change
14. Operational Readiness
15. Conduct of Operations
16. Emergency Management
17. Incident Investigation
18. Measurement and Metrics
19. Auditing
20. Management Review

DEFINITION OF PSM

The definition for PSM provided by the Center for Chemical Process Safety (CCPS, 1994) is:

> The application of management systems to the identification, understanding, and control of process hazards to prevent process-related injuries and incidents.

Some of the fundamental features of a successful PSM program are discussed in the sections below. Based on these discussions, the following alternative definition is offered:

> Process Safety Management is an ongoing process, involving all managers, employees and contract workers that aims to minimize uncontrolled change from design and/or operating intent and to keep the process within its safe limits.

SAFE LIMITS

The safe limits for each process variable must be defined quantitatively. For example, the safe temperature range for a certain reaction may be 125–150°C. If the actual temperature deviates outside of that range, then that reaction is—by definition—out of control and potentially unsafe; action *must* be taken to bring the temperature back into the correct range. The fact that the process has deviated outside the safe range does not mean that an emergency situation exists—management and the operators may have plenty of time to react. But they must do something because the facility must always be operated within its safe limits. The option of doing nothing is not an option.

Once the safe range has been defined, management must determine how to operate their facility so that it stays within that range. In the case of the reaction temperature example, instrument set

Table 1.5 Examples of Safe Limits

Item	Parameter	Units	Safe Upper Limit	Safe Lower Limit
T-100	Level	%	95	10
	The high limit is based on operating experience; it has been found that upsets rarely cause the level to deviate more than 2% or 3%. Therefore, keeping the level at 95% or less should minimize the chance of tank overflow. Minimum flow protection for the pumps, P-101 A/B, is not provided so a minimum level in the tank must be maintained to prevent pump cavitation leading to seal leaks.			
P-101 A/B	Flow	kg/h	N/A	500
	The upper limit for flow is set by the capacity of the pumps. In this case, even when they are pumping at maximum rates, no hazardous condition is created. Therefore, no meaningful value for a safe upper limit of flow exists. Below the prescribed minimum flow rate, the pumps may cavitate.			
V-101	Pressure	bar(g)	12 (at 250°C)	0
	The upper pressure limit is set by code. V-101 is not vacuum rated, and there is uncertainty about lower pressure limit, so 0 barg (1 bar abs) has arbitrarily been set as the lower limit.			
V-101	Temperature	°C	250	−10
	The upper temperature limit is defined by code. Stress cracking may occur below the lower safe limit value.			

points must be adjusted and operators trained so as to achieve the 125−150°C range. All the people involved in running or maintaining the unit must know how to identify an out-of-control situation, what its consequences might be, and how they should respond to it. If it is management's intention to operate outside the prescribed range, then the Management of Change program should be implemented in order to ensure that the new conditions are safe, that new limits have been set, or that new safeguards have been installed.

When a facility is new, the safe limits are defined by its designers. As operating experience is accumulated, new safe limit values will be implemented—often through use of the hazards analysis and management of change processes.

Table 1.5 provides some examples for safe limit values for the first standard example (Figure 1.17) that is provided at the end of this chapter. It can be seen that the selection of a numerical value for a safe limit is supported by some discussion.

Some safe limits may have no meaningful value. For example, if a pressure vessel is designed for full vacuum operation, then that vessel has no safe lower limit for pressure. Similarly, in Table 1.5, no value for a safe upper limit for high flow is provided because the system is safe even when the pumps are running flat-out with all control valves wide open.

Another type of safe limit is to do with the mixing of incompatible chemicals. Mixing tables such as that given in Table 1.6 are commonly used to ensure that only compatible chemicals

Table 1.6 Mixing Scenarios and Safe Limits

	A	B	C	D	E
A	–				
B	‡	–			
C	√	√	–		
D	X	X	‡	–	
E	N/A	√	√	√	–

are mixed with one another. (The information to do with the inadvertent mixing of two chemicals will often be developed during a process hazards analysis when discussing the parameters "reverse flow" and "misdirected flow.")

Table 1.6 lists five chemicals: A–E. It shows which chemicals can and cannot be mixed with one another safely.

The symbols in Table 1.6 have the following meanings:

√	No known problems with the mixing of these two chemicals in any range
‡	Problems in certain mixing ranges
X	Mixing creates unsafe conditions in any range of concentration
N/A	Information not available

Mixing tables generally consider only binary mixtures. The consequences associated with simultaneously mixing three or more materials are not usually known.

For those mixing scenarios where only certain ranges are hazardous, a chart such as that shown in Figure 1.6 can be used. The range in which chemical X has a concentration of 30–60% is considered to be unsafe for that particular temperature and pressure.

Not much information to do with safe mixing values is available. The U.Ss Coast Guard does provide a publicly available database (Coast Guard, 2001).

SET POINT VALUES

Figure 1.7 shows the relationship between safe limit and set point values for the temperature in a reactor. The safe upper limit for the temperature is 150°C. Given that the control system allows a swing of ±3°, the set point value has to be 147°C.

During the 1980s and 1990s, many process facilities installed Distributed Control Systems (DCS). One of the justifications for the use of these systems is that they reduce the amount of fluctuation in the process operation. Hence, it is possible to operate the facility closer to its safe operating limits—as illustrated in Figure 1.8 which shows that the set point has been raised from 147–149°C. This tighter control is good from an operational point of view because it means that more production can be squeezed out of the same equipment without creating a safety problem. It also leads to significant improvements in energy efficiency.

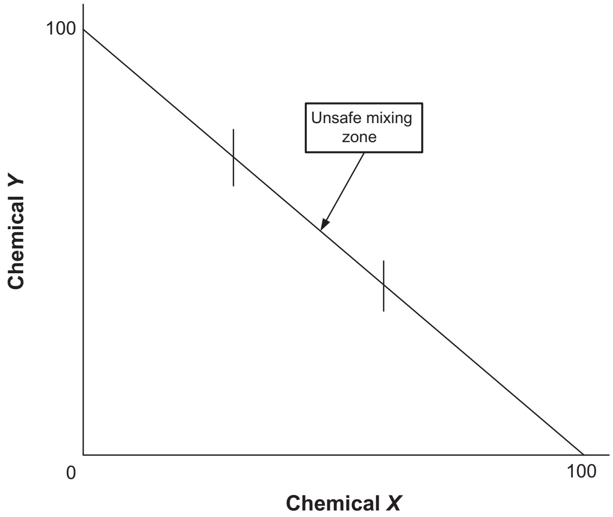


FIGURE 1.6

Unsafe mixing range.

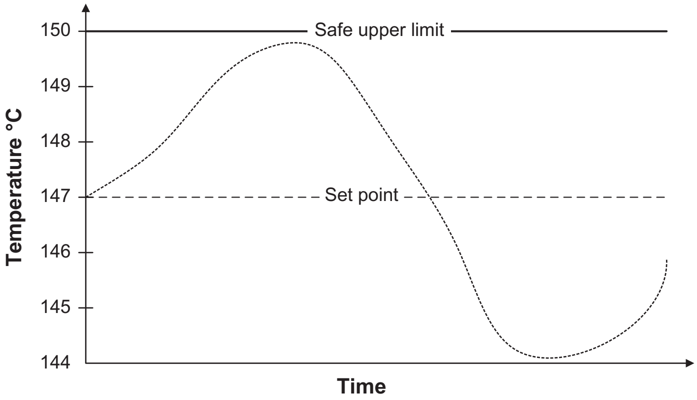


FIGURE 1.7

Safe limit and set point values.

OPERATING, SAFE, AND EMERGENCY LIMITS

The concept of safe limits can be extended to include operating and emergency limits, as illustrated in Figure 1.9, which shows values for a process variable such as pressure, temperature, level, or flow rate.

The innermost range of Figure 1.9 shows the *optimum* value for this particular parameter. In this case, it is 239–240. This optimum point may change as target conditions to do with production rates, yields, or product quality change.

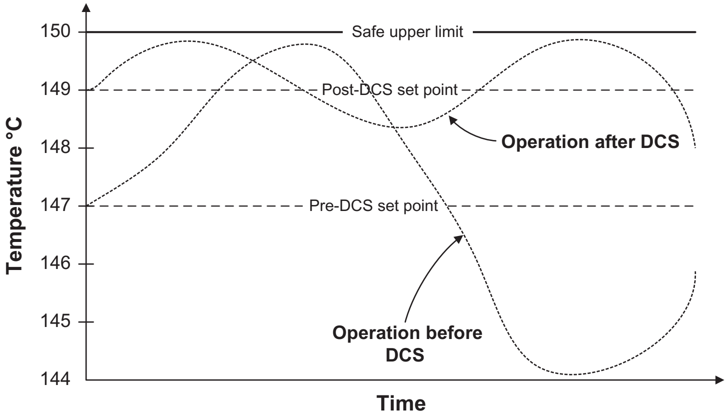


FIGURE 1.8

Effect of DCS on set point values.

The *operating range* represents the upper and lower limits for that variable's normal value. Supervision is free to move the variable to any point within that range in order to achieve production and quality goals. In Figure 1.9, the operating range is 235–245.

If operating conditions are allowed to move outside the operating limits, but within the safe limits, then the facility is said to be in trouble, i.e., there are no safety issues to worry about, but the system is operating inefficiently. Troubleshooting efforts to bring the value back into the operating range will save money. Indeed, much of management's attention will be directed toward troubleshooting because addressing difficulties in this area will often lead to a significant improvement in profitability for relatively little expenditure. Examples of "trouble" include:

- Excessive energy consumption
- Product quality problems
- Unusually high use of spare parts
- Low production rates.

The operating limit values are often quite fuzzy. As the system moves away from optimum operation, it will start to exhibit symptoms of unusual operation which will eventually lead into the troubleshooting range.

The next range is defined by the *safe limit* values. In the case of Figure 1.9, if the parameter allowed to exceed 275 or go below 210, then the system is in an unsafe condition and action must be taken to bring that value back into the safe range.

The final set of values is the *emergency limits*. If the process parameter goes beyond one of these limits, then an emergency situation has been created. Immediate action is required; generally the safety instrumentation and safety equipment (such as pressure relief valves) will be activated. In Figure 1.9, the upper emergency limit is 310; there is no lower emergency limit. The relationship between operating, safety, and emergency limits is given in Table 1.7.

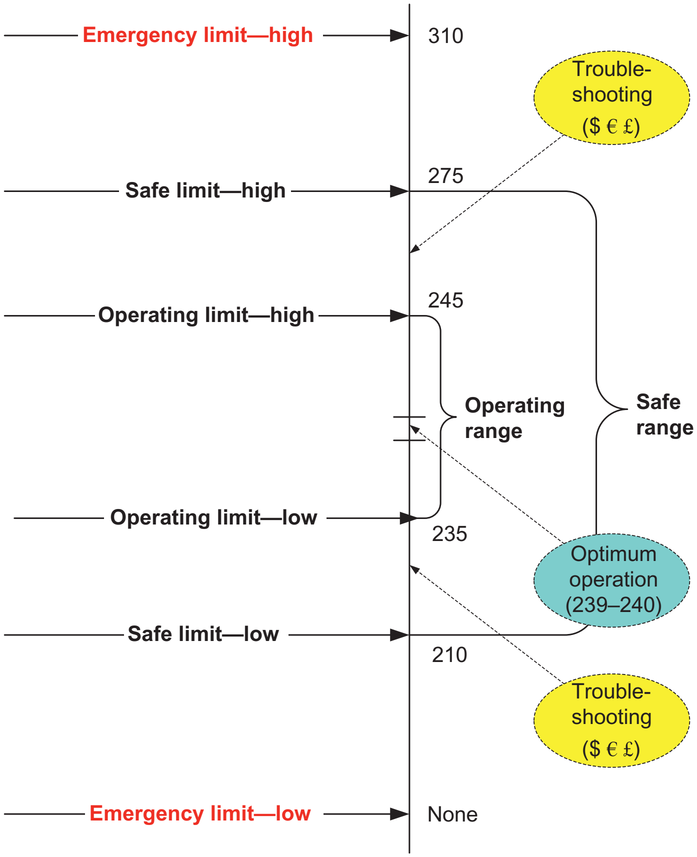


FIGURE 1.9

Operating, safe, and emergency limits.

MEASUREMENT STRATEGIES

An effective risk management program requires that progress be measured quantitatively. Objective goals and tools must be provided for determining how much progress has been made toward achieving those goals. Trends in occupational safety can be measured through the use of parameters such as recordable injuries. It is much more difficult to measure trends and progress with regard to process safety because large process-related accidents occur only rarely. Also, no consistent measurement techniques for process safety are available, and elements such as Workforce and Stakeholder Involvement are inherently difficult to quantify.

A common strategy for evaluating incidents and for identifying root causes is to use the incident pyramid or triangle shown in Figure 1.10, a concept introduced in the year 1931 by H.W. Heinrich. The basic idea behind the triangle is that serious events such as fatalities, large environmental spills, and serious financial losses occur only rarely. By contrast, near-misses and low-consequence

Table 1.7 Types of Nonstandard or Abnormal Situation

Operational Deviation	Safety Deviation	Emergency Operation	Emergency Response
Limit Values			
The operation stays within the safe limits.	Some operating parameters move outside their safe limits, but not at the emergency level. Time is not of the essence.	The emergency limits are exceeded; emergency operations and/or automated instrument response are required.	The emergency has spread to other units.
Severity of Consequences			
The consequences of the problem are primarily economic, although failure to address the situation may lead to a safety problem eventually.	The consequences resulting from the deviation are that worker safety is jeopardized and/or a major environmental problem may result.	The deviation is very serious. There is immediate danger of a fatality or of a major environmental release.	The situation has deteriorated such that an entire facility is threatened, not just one operating unit. The public may also be affected.
Response Time			
Usually there is time to review what needs to be done.	Action must be taken since safety standards have been violated. However, there may be plenty of time to evaluate what needs to be done.	Speed is essential.	Speed is essential.
Operating Procedures Requirements			
A troubleshooting guide is needed. The instructions can be quite lengthy, discursive, and complex, if necessary. Different points of view can be presented because there may be different causes that generate the same symptoms and because more than one solution may be viable. The instructions take the form of guidance or suggestions; there is no absolutely correct or incorrect way of addressing the situation.	The instructions can be reasonably detailed, and they can offer options. However, they must be unambiguous and they must be followed as written. However, there is room for interpretation and judgment.	The instructions must be short in number, simple, and easy to execute. Absolutely no ambiguity is permitted.	The instructions will provide guidance to a trained emergency response team.

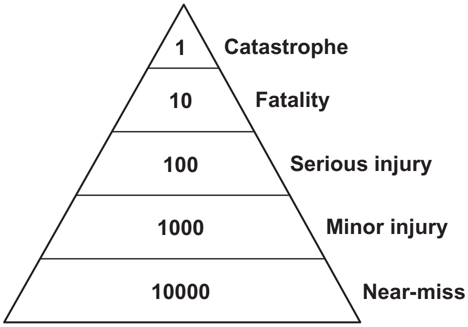


FIGURE 1.10

Incident triangle—1.

events are much more common and can be seen as being precursors to the more serious events. If a relationship exists between the two types of event, then programs that reduce the number of near-misses and minor injuries will, it is argued, lead to a corresponding reduction in the number of catastrophes.

Figure 1.10, which uses created data, shows five levels of seriousness to do with worker safety (similar categories can be used for environmental and economic loss). Single order of magnitude steps are used. Hence it is estimated that, for every 10,000 near-misses, there will be a 1,000 minor injuries, a 100 serious injuries, 10 fatalities, and 1 catastrophic event.

Various studies report on actual ratios. For example, Mannan et al. (2005) give the following ratios.

Fatalities:	1
Serious injury:	7
Minor injury:	44
No injuries:	300.

The assumption underpinning the incident pyramid is that the causes for all types of event are the same. In fact, this assumption is only partially correct because the root causes of minor events are different from those that lead to process safety events. Therefore, improving “day-to-day” safety will not necessarily reduce the number of serious incidents. Minor events are typically caused by *occupational* problems such as trips and falls, lack of proper PPE, and improper use of machinery. Major events, however, are more often caused by *process* safety problems such as incorrect instrument settings, corrosion, or mixing of incompatible chemicals. Hence a program that leads to improvements in occupational safety will not necessarily help reduce the frequency of process-related events. Indeed, improvements in the occupational safety record may induce a false sense of confidence regarding the potential for a major event. (It is probable, however, that a poor performance in occupational safety will correlate positively with a poor performance in process safety.)

The lack of a simple correlation between occupational safety and process safety was highlighted in the Baker report to do with the 2005 explosion at BP’s Texas City refinery (Baker, 2007), one section of which states:

> BP's executive management tracked the trends in BP's personal safety metrics, and they understood that BP's performance in this regard was both better than industry averages and consistently improving. Based upon these trends, BP's executive management believed that the focus on metrics such as OSHA recordables... were largely successful. With respect to personal safety, that focus evidently was effective. BP's executive management, however, mistakenly believed that injury rates, such as days away from work case frequency and recordable injury frequency, were indicators of acceptable process safety performance... it was not until after the Texas City accident that management understood that those metrics do not correlate with the state of process safety.

The reason that good occupational safety performance does not necessarily correlate with the frequency of serious accidents is that occupational accidents tend to have simple causes. For example, if a worker traps his or her fingers in a piece of moving machinery, some likely recommendations that result from such an event are:

- Ensure that that item of machinery, and all others like it, is properly guarded.
- Ensure that all affected personnel are properly trained in the use of that type of machine.
- Issue better PPE.

However, a thorough incident investigation into such an apparently simple accident could lead to the discovery of significant and subtle deficiencies in the overall management program that could, in turn, lead to ways of improving process safety.

Figure 1.10 can therefore be modified as shown in Figure 1.11. A disconnect is shown between the large number of occupational injuries and the much smaller number of catastrophic events that are process related.

Evidence as to whether an opposite, top-down effect may apply is hard to come by, i.e., whether improvements in process safety lead to matching improvements in occupational safety. Many process safety professionals feel that such a trend does exist although it is difficult to prove.

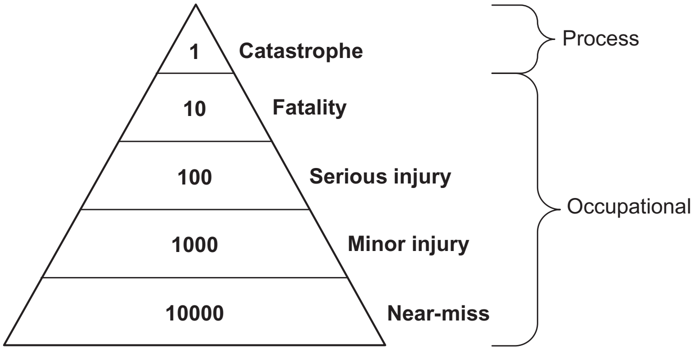


FIGURE 1.11

Incident triangle—2.

INVOLVEMENT

Process safety is not a management program that is handed down by management to their employees and contract workers; it is a program that involves everyone: designers, operators, maintenance technicians, managers, and senior executives. The key word is *involvement*—which is much more than just *communication*. All managers, employees, and contract workers are responsible for the successful implementation of the program. Management, who must provide determined and committed leadership, must organize and lead the initial effort, but the employees must be fully involved in its implementation and improvement because they are the people who know the most about how a process really operates, and they are the ones who have to implement recommendations and changes. Specialist groups, such as staff organizations and consultants, can provide help in specific areas, but process safety is fundamentally a line responsibility.

THOROUGHNESS

PSM regulations also require thoroughness. For example, a company may have a good training program, but one person may have missed part of it because he or she was on vacation. Management will have to make sure that this person is trained and that his or her personnel files are updated appropriately.

HOLISTIC

The elements of process safety have strong interaction with one another—it is not possible to meet the requirements of one of the elements without considering its effect on the others.

The interconnectedness of the elements can be illustrated by considering the development of an Emergency Response Plan, in which the following sequence of actions—involving seven of the elements shown in Table 1.4—may occur.

1. The writing of the *Emergency Response Plan* (element 16) requires a knowledge of which hazards have to be addressed.
2. Consequently a *Hazards Analysis* (element 7) is required to identify the hazards.
3. In order to be able to carry out the hazards analysis, information from sources such as P&IDs and material safety data sheet (MSDS) is needed. Much of this information is included in the *Knowledge Management* program (element 6).
4. Once the Emergency Response Plan has been developed, it will be necessary to *train* everyone in its use (element 12).
5. The Emergency Response Plan has to be *audited* on a regular basis (element 19).
6. During the training process, those being trained will come up with ideas that will improve the quality of the Emergency Response Plan. This is *Workforce Involvement* (element 4).
7. After going through the *Management of Change* step (element 13), these ideas can be used to upgrade the emergency manual.

When considered in isolation, many of the elements appear to be the “most important.” For example, *Workforce Involvement* could be considered to be the key element because, if the employees do not participate in the process safety program, then that program will not function properly. But *Management of Change* could be considered the "most important" because the root cause of all incidents is uncontrolled change. On the other hand, all of the elements require a solid base of up-to-date, comprehensive information. Therefore, *Knowledge Management* is the "most important." But then it could be argued that *Incident Investigation and Root Cause Analysis* is what really matters because incidents reveal what is really going on in the organization.

In a discussion to do with Due Diligence and Process Safety (Einolf et al., 2007), the following elements of PSM were identified as being particularly important:

- Process Hazards Analysis
- Mechanical Integrity
- Management of Change
- Operating Procedures
- Auditing.

The real point, of course, is that they are all important and necessary, and that they all rely on one another to be effective.

ENVIRONMENT

Environmental risks are normally controlled by rules and regulations rather than an analysis of risk. They are also assessed and controlled through the use of Environmental Impact Assessments, which are rather like Safety Cases (Chapter 2) in that they require the facility management to account for environmental values in their decisions and to justify those decisions in light of detailed environmental studies and public comments on the potential environmental impacts (Holder, 2004).

QUALITY MANAGEMENT

Companies in the process industries have typically implemented a wide range of quality management programs in recent years. In many cases, there is a strong overlap between quality management, OIM, and PSM. A brief discussion of some of the quality techniques that are used in the process industries is provided below.

STATISTICAL PROCESS CONTROL

Statistical process control (SPC) involves using statistical techniques to measure and analyze and control the variation in processes. SPC will not improve the quality of a poorly designed facility, but it can be used not only to maintain the consistency of how the product is made but also to improve equipment reliability.

ISO 9000/14001

May quality programs are organized using the ISO 9000 system. It provides management with an infrastructure on which to build a workable, manageable quality system based on the following points.

- It clearly defines "how we do things around here." Both responsibilities and authority are defined.
- It requires the implementation of a continuous improvement system through the use of feedback and corrective action.
- It helps ensure that chronic problems are addressed properly, rather than with "firefighting" every time when they occur.

A company that implements ISO 9000 does four things:

1. It writes down what it is going to do.
2. It trains everybody to follow the standards that have been set.
3. It implements an audit program.
4. It suggests means for improving the present operation.

ISO standards are typically quite similar to those for process safety and operational integrity. Companies set their own performance targets based on general guidance and then work toward achieving those targets.

The first major release—ISO 9000:1994—was built around the concept of "Document what you do, do what you document, and be prepared to prove it". Its replacement—ISO 9000:2000—is based on a management model that can be summarized as "Plan, Do, Check, Act." The updated standard also incorporates customer needs and feedback and a continual improvement process.

ISO 14001 is similar to ISO 9000 except that it focuses on environmental compliance. It incorporates, but goes beyond, legal requirements on environmental issues.

SIX SIGMA

The Six Sigma process is a technique used in the design of a new product or technology, or for measuring how an existing process is performing. The process allows for a 3.4 defects per million opportunities and is organized into five steps: Define, Measure, Analyze, Design, and Verify. Like all statistical approaches to quality, Six Sigma aims to move process understanding from art to science. Events should have a complete explanation—with supporting facts.

The Six Sigma process does not lead to invention because it is a designed experimental program that does not allow deviation from plan. This approach conflicts, for example, with the approach of a process hazards analysis team leader who is skilled at getting people to "think the unthinkable." Nor does the Six Sigma method necessarily help identify underlying causes—which is at the heart of any successful incident investigation and analysis program, for example.

RISK

The word "risk" has a wide range of meanings. In the context of process plant management, and of the structure of this book, risk can be categorized into one of three ways.

The first type of risk is to do with catastrophic events—some of which are listed in Table 1.1. Although such events are rare, their impact can be profound. Not only do they often lead to a totally unacceptable loss of life, major environmental problems, huge economic shortfalls, very bad public relations, civil litigation, and even criminal prosecution. These events also frequently have a major impact on the development of management systems and regulations.

The second type of process risk is to do with troubleshooting. In such situations, the facility suffers from ongoing operating problems that eat away at profits and take up the time of key personnel. The causes of the problem are often hard to identify.

Examples of "trouble" are:

- A critical pump breaks down on numerous occasions.
- Steam consumption is up 10%, and no one seems to know why.
- The quality of the final product is erratic.

The risk associated with troubleshooting situations is primarily economic. However, if such situations are not taken care of promptly, unsafe conditions can develop, not least because the additional maintenance puts workers at risk.

The third type of risk is to do with what is referred to as RAM. This topic, which is discussed in detail in Chapter 20, is related to troubleshooting but implies a higher degree of predictability. Based on historical records, the failure rates and repair times of equipment items can be predicted and maintenance schedules can be set up so as to preemptively address potential problems. Management systems such as Risk-Based Maintenance and Risk-Based Inspection are often integrated with the RAM program. Investments in availability improvement programs are often very attractive because such investments have a disproportionate effect on profitability.

The management systems used to control these different types of risk have much in common. But they are not identical, particularly when it comes to the prevention of catastrophic events. One of the lessons learned from the Texas City refinery event of 2005 is that the management was not using the proper types of SMS.

COMPONENTS OF RISK

Risk, which always implies some type of negative outcome, is made up of three components:

1. Hazards
2. The consequences of the hazards
3. The predicted frequency (likelihood) of occurrence of the hazards.

These three terms can be combined as shown in Eq. (1.1).

$$\text{Risk}_{\text{Hazard}} = \text{Consequence} * \text{Predicted Frequency} \tag{1.1}$$

Equation (1.1) shows that risk can never be zero—a truth not always grasped by members of the general public or the news media. Hazards are always present within all industrial facilities. Those hazards always have undesirable consequences, and their likelihood of occurrence is always finite. The magnitude of the consequence and likelihood terms can be reduced, but they can never be eliminated. The only way to achieve a truly risk-free operation is to remove the hazards altogether (or, with respect to safety, to remove personnel from the site).

HAZARDS

The first component in Eq. (1.1) is the hazard. A hazard is a condition or practice that has the potential to cause harm, including human injury, damage to property, damage to the environment, or some combination of these. The key word in the definition is "potential." Hazards exist in all human activities but rarely result in an incident. For example, walking down a staircase creates the hazard of "falling down stairs," with the consequence of an injury, ranging from minor first aid to a broken limb or even death. However, most people, most of the time, manage to negotiate a flight of stairs without falling.

Some of the potential hazards associated with the second standard example are listed below.

- Tank T-100 is pumped dry.
- Tank T-100 overflows.
- P-101A seal leaks.
- V-101 is overpressured.
- Liquid flows backward from V-101 into T-100.
- Other.

One of the greatest challenges to do with practical risk analysis is defining the scope of the hazard term. For example, with respect to the second hazard in the above list—an overflow of T-100—more detail is needed. Clearly there is an enormous disparity between having a few drops spill into a closed drain system and having thousands of liters of the chemical pour on to the ground and then flow into the local waterways.

Similarly, with regard to the fifth hazard—"Liquid flows backward from V-101 into T-100"—there is a world of difference between a reverse flow of a few milliliters of RM-12 lasting for a few seconds and a reverse flow of thousands of kilograms of material lasting for an hour or more.

The final hazard in the list is "other." This term is included as a reality check. No risk analysis team, no matter how well qualified the members may be or how much time they spend, can ever claim to have identified all hazards. Throughout this book, the "other" term is used in all types of analysis in order to keep everyone on their toes and thinking creatively as to "what might be."

CONSEQUENCE

Once the hazards associated with a process have been defined, the corresponding consequence and likelihood values can be determined. The consequence of an event usually falls into one of three categories:

1. Safety
2. Environmental
3. Economic.

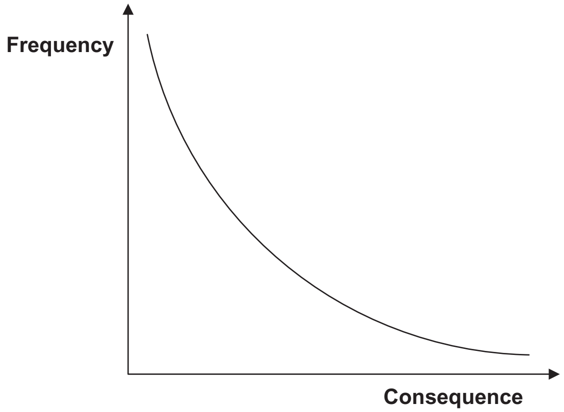


FIGURE 1.12

Frequency vs. consequence.

For many companies, safety tends to be the driver; their managers reason that, if they can avoid people being hurt, then the environmental and economic performance will follow along.

PREDICTED FREQUENCY

Each event has a predicted frequency of occurrence, such as once in a 100 years. The word "predicted" is used to point out that the future frequency of an event is not the same as its historical frequency, particularly if the risk management program is effectively reducing the chance of a failure from occurring.

Frequency is not the same as probability. An item has a frequency of failure measured in inverse time units such as once in a 100 years. The consequences of that event may be mitigated by a safeguard, which has a (dimensionless) probability of occurrence. For example, high level in a tank may occur once every 2 years. However, the tank has level control instruments that detect high level and stop the flow of liquid into the tank. These instruments may have a probability of failure of 0.01 or 1%. Therefore, the likelihood of a system failure is 0.005 year^{-1}, i.e., once in 200 years.

Figure 1.12 shows that an inverse relationship generally exists between consequence and frequency. For example, in a typical process facility, a serious event such as the failure of a pressure vessel may occur only once every 10 years, whereas trips and falls may occur weekly.

SAFEGUARDS

A safeguard is a device that either reduces the likelihood of an event occurring or minimizes the consequences of that event. Examples of safeguards are:

- Pressure safety relief valves that blow down excess pressure in equipment or piping and thus reduce the likelihood of an explosion.

- Hard hats that reduce the severity of head injuries if someone is struck by a falling object.
- A safety interlock on a tank that shuts down the pump feeding the tank when high level is detected.

The essential feature of safeguards is that they are dedicated to safety and play no other role in plant operations. Therefore, normal operating procedures are not safeguards—even though they can help minimize the chance of an event occurring.

PRESENCE OF PERSONS

One factor that radically affects the safety risk associated with a hazard is the presence of persons in the area of the event. For example, the consequence of a seal failure from P-101 A/B could be a fire. If no one is present, the safety impact is zero. The economic loss may be great but no one will be hurt. However, if someone is present, they could be killed. Yet it can be very difficult for a risk analyst or for a risk management team to forecast whether or not someone will be present at the time of the event.

In some cases, the probability of someone being present is higher than would normally be anticipated because those people are there to work on what appears to be a relatively minor problem. For example, at a chemical facility in Texas, a tank exploded killing 17 workers. The area in which the explosion occurred was normally deserted; but the workers were there to correct the conditions that led to the explosion. On another occasion, a refinery in west Texas experienced a major explosion and fire. Many major equipment items were destroyed, and the smoke from the fire was so great that an adjacent freeway had to be closed down. If a risk management team had modeled the event ahead of time they would surely have postulated multiple fatalities and serious injuries. In fact, no one was hurt.

Management must be particularly cautious when sending operators and maintenance workers into a hazardous situation in order to correct problems. It is likely that additional safeguards and precautions will be needed.

In other situations, it may be found that the presence of a hazardous situation actually reduces the number of people at risk. For example, in the Gulf of Mexico during the period 2003−2005, some 164 offshore platforms were either lost or seriously damaged due to hurricanes. The economic loss was high, yet the number of fatalities and serious injuries associated with the storms was zero; the reason being that, whenever a hurricane is brewing in the general location of a platform, the crew is evacuated. In this case, the probability of workers being present was much *less* than would have been anticipated by a risk management team.

In other cases, the people may be located close to a hazard for reasons that no risk analyst could reasonably foresee. Probably the best known example of this occurred at the Texas City refinery explosion in the year 2005. Adjacent to the site of the release were temporary trailers used for project workers. All of the fatalities were to people working in those trailers (CSB, 2007).

Another example of the unexpected presence of people at an incident site occurred at a facility in the southern United States. A high-pressure, high-capacity pump that had just been brought on line for the first time was exhibiting serious mechanical problems. About half a dozen people, including some senior managers, were gathered in the area to find out what was going on. Suddenly the pump's seal failed, shooting out a large jet of a high-temperature caustic liquid.

Fortunately the direction of the failure was away from the personnel. The liquid caused some environmental damage but none of the people in the area were hurt. They were lucky—they could have been seriously burned had the jet been directed toward them. Once more, no risk analysis could have reasonably anticipated that a large number of people would be present and that the jet would point the way it did.

In the long term, one of the best means of improving safety is to develop systems that are so automated that very few humans are required to be in the vicinity of operating equipment so that they are not exposed to hazards.

SINGLE CONTINGENCY EVENTS

When a facility is being designed, the single risk concept is typically applied. It specifies that only one emergency (or group of interrelated emergencies) will occur at one time. The probability that multiple unrelated incidents would occur simultaneously is so low that it is not a credible consideration. Therefore, when designing a facility, it is normal to design a safety device to handle the largest single risk. For example, pressure vessels can be subject to overpressure for a number of separate causes such as external fire, pump pressure, and internal chemical reactions. The safety relief valve will be designed for the worst of the identified cases. Multiple unrelated incidents are examined through the use of common cause–effect analysis and with techniques such as fault tree analysis, as described in Chapter 6. When it is plausible that a relief device could be called upon to handle multiple releases, such as may occur during a cooling water failure, capacity should be provided for this emergency.

ECONOMIES OF SCALE

Processing facilities are often very large in order to take advantages of economies of scale. Such economies usually derive from the "two thirds rule." Using the simplest three-dimensional shape—a sphere—as an example, the volume increases with the cube of the diameter, whereas the surface area (which governs the cost of the object) increases with the square of the diameter. The same principle can be applied to more complex shapes and structures. The general rule is that the cost of an item follows the equation:

$$C = k \cdot P^n \tag{1.2}$$

where C is the capital cost, k is a constant, P is the capacity, and n is a scale-up index, usually having a value in the range 0.6–0.7. Equation (1.2) is the driving force for creating larger and larger single-train facilities.

However, large facilities pose a greater risk—particularly with regard to catastrophic events. For example, a vessel that contains larger quantities of flammable or toxic materials poses a greater threat than two or three smaller vessels that have the same total capacity because it is not likely that all of the smaller vessels will experience the same accident at the same time. Therefore, the size of the release or fire is likely to be much greater. Indeed, the safety issues to do with the development of "jumbo" facilities were one of the reasons for the development of loss prevention systems (Davenport, 2006).

COMMON CAUSE EVENTS

A common cause event causes two separate, supposedly independent systems to fail simultaneously. For example, solid materials in a liquid system may cause both a pressure controller instrument and the high-pressure shutdown system to be blocked at the same time. The normal control and the interlock are not independent of one another.

Common cause events negate the value of an AND gate in a fault tree (Chapter 15).

FUKUSHIMA–DAIICHI

A particularly noteworthy common cause scenario occurred at the Fukushima–Daiichi nuclear power complex in Japan. On March 11, 2011, north eastern Japan was devastated by the Tōhoku subsea earthquake—the most powerful ever to have hit Japan since records have been kept. The earthquake was followed about 50 minutes later by a tsunami of 14 meters in height. It is estimated that the earthquake and tsunami together resulted in 15,883 deaths, with many others injured or missing. Up to 1 million buildings were destroyed or damaged.

The earthquake caused extensive damage to the structures of the Fukushima–Daiichi power plant and knocked out the pump systems that supply cooling water to the reactors and the spent fuel pools. This is known as a Loss of Coolant Accident (LOCA) takes place.

The tsunami then overwhelmed the facility's inadequate 5.5 meter seawall and, most important from a process safety point of view, it knocked out the safety systems designed to keep the reactors cool. Consequently the cores of the reactors overheated leading to partial meltdowns and follow-on problems, such as the generation of hydrogen gas that exploded. A considerable amount of radioactive material leaked to the ground, the sea, and the air—and those leaks appear to be ongoing.

EXAMPLES

The following are examples of common cause events that frequently crop up.

Utility Failure

Problems with utility systems are probably the most prevalent of common cause effects, as already illustrated with the electrical power event in the fault trees shown above. Utilities such as electrical power, cooling water, steam, and plant air are typically used throughout a facility. Should they fail, many other systems are likely to fail at the same time.

Instruments on Manual

If instruments are placed on manual, particularly emergency instruments, then a common cause event has been created. For example, one of the contributing factors in the Piper Alpha disaster was that both firewater pumps were on manual. They had been placed in that state to ensure that any divers in the water were not sucked into the firewater intake in the event of an automatic start of the pumps. Unfortunately, the fire on the platform prevented operators from getting to the pumps to turn them on. The lack of firewater capability materially contributed to the magnitude of the disaster.

Instrument Pluggage

If solids materials enter a system that is meant to contain only liquid or gas, all of the instruments may be plugged, thus canceling out perceived redundancy.

Vibration

High vibration can cause multiple equipment and instrument items to fail, particularly those that are on standby.

External Events

External events include earthquakes, floods, hurricanes, and freezing weather. Any of these can cause multiple failures.

Maintenance Availability

A subtle, but very important, common cause effect concerns the availability and quality of maintenance personnel and of replacement parts. If a facility has only one crew that can repair pumps and both P-101A and P-101B were to fail at the same time, then the repair times provided in the example would be overly optimistic.

Human Error/Untrained Personnel

Human error is frequently the source of common cause problems. It is also very difficult to quantify. On one chemical plant, for example, the material balance around a large reactor did not balance. The instruments showed that more material was going in than coming out, yet all other indicators showed that there were no problems. The follow-up investigation showed that an instrument technician had installed all the orifice plates the wrong way round. As soon as that error was corrected, the flows balanced perfectly. The technician's lack of training (or lack of attention to detail, or errors in the instrument data sheets) was the common cause error in this example.

Airlines use a second pilot to serve as a backup in the event that the first pilot is incapacitated during the flight for any reason. Management aims to eliminate common cause events where possible. For example, the pilots may be required to eat different types of meals so that, if one type of meal is contaminated, only one of the pilots is affected.

SUBJECTIVE NATURE OF RISK

> A truth ceases to be a truth as soon as two people perceive it.
>
> **Oscar Wilde, 1854–1900**

What Oscar Wilde meant by the above quotation is that facts are never truly objective; each person has their own perception of what they perceive to be the same reality. His insight also suggests that there is no such entity as "common sense"—no two people have a truly common view of the world so they cannot share a "common sense."

This observation regarding different truths applies to hazards analysis and risk management work. Each person participating in a hazards analysis has his or her own opinions, memories, attitudes, and overall "world view." Most people are—in the strict sense of the word—prejudiced, i.e., they prejudge situations rather than trying to analyze the facts rationally and logically. People jump to preconceived conclusions, and those conclusions will often differ from those of other people who are looking at the same information with their own world view. With regard to risk management, even highly trained, seasoned experts—who generally regard themselves as being governed only by the facts—will reach different conclusions when presented with the same data. Indeed, Slovic (1992) states that there is no such thing as "real risk" or "objective risk." His point is that if risk can never be measured objectively then objective risk does not exist at all.

In his book *Bad Science*, the author Ben Goldacre has a chapter entitled "Why Clever People Believe Stupid Things" (Goldacre, 2008). Many of his insights can be fairly applied to risk assessment and management in the process industries. He arrives at the following conclusions:

1. We see patterns where there is only random noise.
2. We see causal relationships where there are none.
3. We overvalue confirmatory information for any given hypothesis.
4. We seek out confirmatory information for any given hypothesis.
5. Our assessment of the quality of new evidence is biased by our previous beliefs.

The subjective component of risk becomes even more pronounced when the perceptions of nonspecialists, particularly members of the public, are considered. Hence successful risk management involves understanding the opinions, emotions, hopes, and fears of many people, including managers, workers, and members of the public.

Some of the factors that affect risk perception are discussed in the following sections.

DEGREE OF CONTROL

Voluntary risks are accepted more readily than those that are imposed. For example, someone who believes that the presence of a chemical facility in his community poses an unacceptable risk to himself and his family may willingly go rock-climbing on weekends because he feels that he has some control over the risk associated with the latter activity, whereas he has no control at all over the chemical facility, or of the mysterious odors it produces. Similarly, most people feel safer when driving a car rather than riding as a passenger, even though half of them must be wrong. The feeling of being in control is one of the reasons that people accept highway fatalities more readily than the same number of fatalities in airplane crashes.

The desire for control also means that most people generally resist risks that they feel they are being forced to accept; they will magnify the perceived risk associated with tasks that are forced upon them.

FAMILIARITY WITH THE HAZARD

Most people understand and accept the possibility of the risks associated with day-to-day living, but they do not understand the risk associated with industrial processes, thus making those risks less acceptable. A cabinet full of household cleaning agents, for example, may actually pose more danger to an individual than the emissions from the factory that makes those chemicals. But the perceived risk is less.

Hazards that are both unfamiliar and mysterious are particularly unacceptable, as can be seen by the deep distrust that the public feels with regard to nuclear power facilities.

DIRECT BENEFIT

People are more willing to accept risk if they are direct recipients of the benefits associated with that risk. The reality is that most industrial facilities provide little special benefit to the immediate community apart from offering some job opportunities and an increased local tax base. On the other hand, it is the community that has to take all of the associated risk associated with those facilities, thus creating the response of NIMBY ("Not in My Backyard").

PERSONAL IMPACT

The effect of the consequence term will depend to some degree on the persons who are impacted by it. For example, if an office worker suffers a sprained ankle, he or she may be able to continue work during the recovery period; an outside operator, however, may not be able to work at his normal job during that time. Or, to take another example, the consequence of a broken finger will be more significant to a concert pianist than to a process engineer.

NATURAL VS. MAN-MADE RISKS

Natural risks are generally considered to be more acceptable than man-made risks. For example, communities located in areas of high seismic activity understand and accept the risks associated with earthquakes. Similarly people living in hurricane-prone areas regard major storms as being a normal part of life. However, these same people are less likely to understand or accept the risks associated with industrial facilities.

RECENCY OF EVENTS

People tend to attribute a higher level of risk to events that have actually occurred in the recent past. For example, the concerns to do with nuclear power facilities in the 1980s and 1990s were very high because the memories of Chernobyl and Three Mile Island were so recent. This concern is easing given that these two events occurred decades ago, and few people have a direct memory of them.

PERCEPTION OF THE CONSEQUENCE TERM

The risk Eq. (1.1) is linear; it gives equal value to changes in the consequence and frequency terms, implying a linear trade-off between the two. For example, according to Eq. (1.1), a hazard resulting in one fatality every 100 years has the same risk value as a hazard resulting in 10 fatalities every 1,000 years. In both cases, the fatality rate is one in a 100 years, or 0.01 fatalities year^{-1}. But the two risks are not *perceived* to be the same. In general, people feel that high-consequence events that occur only rarely are less acceptable than more frequent, low-consequence accidents. Hence, the second of the two alternatives shown above is perceived as being worse than the first.

The same way of looking at risk can be seen in everyday life. In a typical large American city, around 500 people die each year in road accidents. Although many efforts are made to reduce this fatality rate, the fact remains that this loss of life is perceived as a necessary component of modern life, hence there is little outrage on the part of the public. Yet, were an airplane carrying 500 people to crash at that same city's airport every year, there would be an outcry. Yet the fatality rate is the same in each case, i.e., 500 deaths per city per year. The difference between the two risks is a perception rooted in feelings and values.

To accommodate the difference in perception regarding risk, Eq. (1.1) can be modified so as to take the form of Eq. (1.3):

$$\text{Risk}_{\text{Hazard}} = \text{Consequence}^{n} * \text{Likelihood} \tag{1.3}$$

where $n > 1$

Equation (1.3) shows that the contribution of the consequence term has been raised by the exponent n, where $n > 1$. In other words, high-consequence/low-frequency accidents are assigned a higher *perceived* risk value than low-consequence/high-frequency accidents.

Since the variable "n" represents subjective feelings, it is impossible to assign it an objective value. However, if a value of say 1.5 is given to "n," then Eq. (1.3) for the two scenarios just discussed—the airplane crash and the highway fatalities—becomes Eqs. (1.4) and (1.5), respectively.

$$\text{Risk}_{\text{airplane}} = 500^{1.5} * 1 = 11,180 \tag{1.4}$$

$$\text{Risk}_{\text{auto}} = 1^{1.5} * 500 = 500 \tag{1.5}$$

The 500 auto fatalities are perceived as being equivalent to over 11,000 airplane fatalities, i.e., the apparent risk to do with the airplane crash is 17.3 times greater than for the multiple automobile fatalities.

In the case of hazards that have very high consequences, such as the meltdown of the core of a nuclear power facility, perceived risk rises very fast as a result of the exponential term in Eq. (1.3), thus explaining public fear to do with such facilities. Over the years, managers and engineers in such facilities have reduced the *objective* risk associated with nuclear power plants to an extremely low value, largely through the extensive use of sophisticated instrumentation systems. However, since the worst-case scenario—core meltdown—remains the same, the public remains nervous and antagonistic. In such cases, management would be better advised to address the consequence term rather than the likelihood term. With regard to nuclear power, the route to public acceptance is to make the absolute worst-case scenario one of low consequence.

The subjective and emotional nature of risk is summarized by Brander (1995) with reference to the changes in safety standards that were introduced following the Titanic tragedy.

> They [scientists and engineers] tend to argue with facts, formulas, simulations, and other kinds of sweet reason. These don't work well. What does work well are shameless appeals to emotion—like political cartoons. Like baby seals covered in oil. And always, always, casualty lists. Best of all are individual stories of casualties, to make the deaths real. We only learn from blood.

COMPREHENSION TIME

When people are informed that a significant new risk has entered their lives, it can take time for them to digest that information. For example, when a patient is informed by a doctor that he or she has a serious medical condition, the doctor should not immediately launch into a discussion of possible treatments. He should allow the patient time to absorb the news before moving on to the next step. So it is with industrial risk. If people—particularly members of the public—are informed of a new risk associated with a process facility, then those people need time to grasp and come to terms with what has been said. There is a difference between having an intellectual grasp of risk and of subjectively understanding how things have changed.

RANDOMNESS

Human beings tend to create order out of a random series of events. People have to do this in order to make sense of the world in which they live. The catch is that there is a tendency to create order, even when events are statistically independent of one another.

For example, psychologists gave test subjects a set of headphones and then played a series of random beeps. The subjects were told to imagine that each beep corresponded to an automobile going by. They were then asked if the beeps were coming in batches, such as would occur when cars were leaving a red traffic light, or whether the cars were spaced randomly, such as would happen on a freeway. The subjects generally said that the beeps were in groups, even though they were in fact occurring at random.

Therefore, it is important for those working in process risk management not to create patterns and order out of randomly occurring events. For example, if two or three near-miss incidents can be attributed to a failure of the Management of Change system, this does not necessarily mean that the Management of Change system is any more deficient than the other elements of the process safety program.

REGRESSION TO THE MEAN

Related to the above discussion concerning the tendency to create nonexistent order out of random events, people will also create causal relationships where there are none, particularly when a system was regressing to the mean anyway.

For example, a facility may have suffered from a series of serious incidents. In response to this situation, management implements a much more rigorous PSM program than they had before. The number of incidents then drops. It is natural to explain the improvement as a consequence of the new PSM program. Yet, if the serious events were occurring randomly, then it is likely that their frequency would have gone down anyway because systems generally have a tendency to revert to the mean.

BIAS TOWARD POSITIVE EVIDENCE/PRIOR BELIEFS

People tend to seek out information that confirms their opinions and they tend to overvalue information that confirms those opinions. It is particularly important to recognize this trait when conducting incident investigations. As discussed in Chapter 12, it is vital that the persons leading an investigation listen to what is being said without interjecting with their own opinions or prejudices.

We also tend to expose ourselves to situations and people that confirm our existing beliefs. For example, most people will watch TV channels that reinforce their political opinions. This can lead to shock when it turns out in an election that those beliefs did not constitute a majority opinion.

AVAILABILITY

People tend to notice items which are outstanding or different in some way. For example, someone entering their own house will not see all of the items of furniture, but she will notice that the television has been stolen or that a saucepan has boiled dry. Similarly anecdotes and emotional descriptions have a disproportionate impact on people's perceptions (as illustrated in the discussion to do with the *Titanic* tragedy provided earlier in this chapter).

Goldacre (2008) notes that, as information about the dangers of cigarette smoking became more available, it was the oncologists and chest surgeons who were the first to quit smoking because they were the one who saw the damage caused to human lungs by cigarettes.

QUANTIFICATION OF RISK

> There are two kinds of people: those who can count and those who can't count.

Where possible, risk should be quantified. Doing so allows managers and regulators to have an objective understanding as to how well they are doing and how they compare with other facilities and companies.

MATHEMATICAL TERMS

Analysis of system risk involves the use of mathematical terms that are used in statistical analysis and probability theory. Since some of these terms are also used by the public in a more general sense it is necessary to provide a precise definition for them. In particular, as has already been discussed, the words frequency, probability, and likelihood tend to be used interchangeably in normal conversation, yet, strictly speaking, they are different, and risk professionals should use them correctly.

Frequency

The number of times that an event occurs over a period of time represents its frequency rate. For example, the failure frequency rate for Pump, P-101A, is once in 2 years, or 0.5 year^{-1}. The distinction between frequency and probability has already been discussed.

Frequency can also be expressed as a likelihood of failure per operating cycle or per mission. For example, in a batch process, the failure rate of a reactor dump valve may be 0.01 batch^{-1}. In other words, the valve is expected to fail once in every 100 cycles.

Predicted Frequency

Frequency values are obtained from historical data. Yet most risk analyses look into the future. Analysts are generally concerned with the predicted failure rate of an event, not with what has happened in the past. However, historical rate data does not always provide a good forecast of future failure rates. For example, one refinery had a set of block valves in critical service that frequently leaked. Therefore, the reported failure rate for these valves was very high. The problem was so severe that management decided to cut out all the offending valves and replace them with valves from a different manufacturer. The new valves turned out to be much more reliable. Hence the historical database to do with these block valves would have been extremely misleading to anyone not aware of the strategic change that had been made.

The use of Bayes' theorem to show how historical data can be used to upgrade probability estimates is discussed in Chapter 15.

Probability

Probability terms are dimensionless and are usually associated with safeguards. Hence the word probability in the context of risk studies usually refers to the probability of failure on demand as distinct from the likelihood of failure over a period of time. For example, with regard to P-101B, the predicted probability of the spare pump not starting on demand is 0.1 (1 in 10 times).

Probability terms are often combined with equipment failure rates to come up with a system failure rate. P-101A has a failure rate of 0.5 year^{-1}; the probability that P-101B will not start on demand at the time P-101A fails is 0.1; therefore, the overall failure rate for the pump system becomes (0.5*0.1) year^{-1}, or once in 20 years.

Another example could be to do with high pressure in V-101. The vessel may reach its maximum allowable working pressure (MAWP) say once in 10 years; thus the frequency of this event is 0.1 year^{-1}. If the relief valve on the vessel has a probability of failure on demand of one in 50, or 0.02, then the predicted failure rate for the vessel is 0.002 year^{-1}, or once in 500 years.

It is often very difficult to estimate the failure rate of backup systems and standby devices because they are typically very reliable and they are not often used. If no failure rate data is available, the failure time is often assumed to be one-half of the test interval.

Likelihood and Failure Rate

Likelihood is a catchall term that can be applied to either frequency or probability. The symbol λ (lambda) is used for the mathematical expression of the overall failure rate.

Error/Statistical Significance Confidence

Statisticians use the word 'error' to measure uncertainty. Engineers generally use the word to refer to inaccuracies in measurements and calibration (they use the word 'precision' when talking about uncertainty).

Statistical confidence is the probability that a particular confidence interval (as calculated from sample data) covers the true value of the statistical parameter.

Failure/Fault

The terms "failure" and "fault" have specific meanings in the context of risk management. "Failure" refers to the nonfunctioning of a specific item of equipment; "fault" refers to the nonfunctioning of a system or subsystem. For example, Pump P-101A may *fail* to operate. If the backup pump P-101B does not start, then a *fault* exists with the pumping system. (In practice, it is unusual for this semantic distinction to be scrupulously followed.)

Independence and Randomness

There are two forms of independence: physical and statistical. In the example, the two pumps, P-101A and B, are physically independent of one another. Two events are statistically independent of one another if the probability of one of either event occurring is not affected by the occurrence or nonoccurrence of the other event.

Physical independence does not always equate to statistical independence. Although P-101A and P-101B are physically independent of one another, they are not completely statistically independent of one another due to common cause effects such as electric power failure (if power fails, then the electrically driven pump will stop and the steam-driven pump will also stop also because the loss of electricity leads to a shutdown of the boilers that generate steam).

Every event, failure, variation, and uncertainty has a cause. However, it is not always possible to determine the cause, in which case the event is said to occur at random.

FN CURVES

Total risk is generally obtained by calculating the risk value for each hazard, and then adding all the individual risk values together. The result of this exercise is sometimes plotted in the form of an FN curve as shown in Figure 1.17 in which the ordinate represents the cumulative frequency (*F*) of fatalities or other serious events, and the abscissa represents the consequence term (usually expressed as *N* fatalities). Figure 1.13 projects that the organization will have a fatality about once every 50 years, whereas a major event (say more than 10 fatalities) will occur every 1,000 years or so. Saraf (2009) provides an example of an FN curve for the frequency of fatalities in the process industries during the years 1911–1995.

Because the values of *F* and *N* typically extend across several orders of magnitude, both axes on an FN curve are logarithmic. (More sophisticated analyses will actually have multiple curves with roughly the same shape as one another. The distribution of the curves represents the uncertainty associated with predicting the frequency of events.) The shape of the curve itself will vary according to the system being studied; frequently a straight line can be used.

FN curves are generally used when making industry-wide decisions; they would not generally be calculated for individual process facilities. However, if two types of technology are being considered, their respective FN curves can be compared, as illustrated in Figure 1.14, which compares two technologies: A and B.

LIMITATIONS

Although the quantification of risk provides invaluable insights, particularly with regard to the prioritization of resources, it does have limitations.

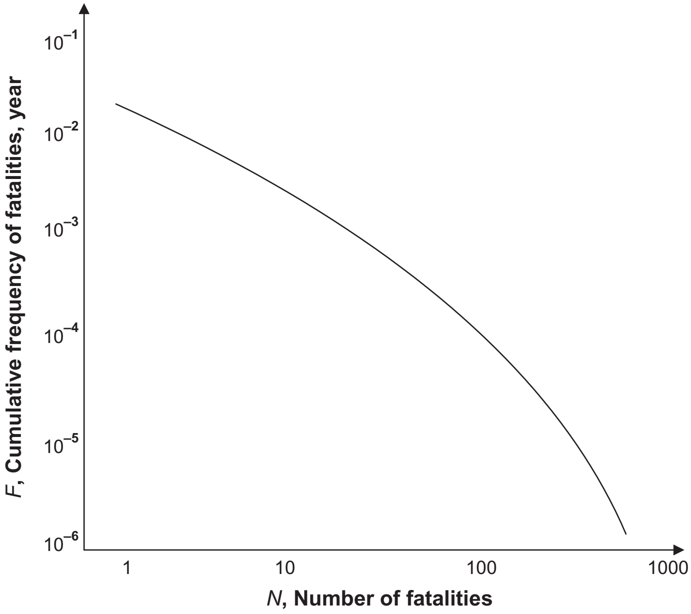


FIGURE 1.13

Representative FN curve.

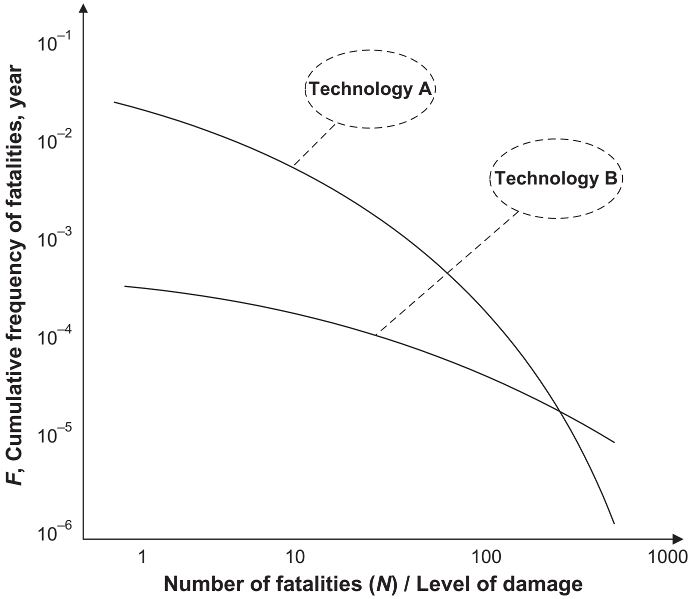


FIGURE 1.14

Comparative FN curves.

One limitation is to do with the selection of data to achieve desired goals. The paper to do with the offshore SEMS rule (Transportation Research Board, 2012) discusses this issue.

> With quantitative risk calculation, it was found that discussions on the risk requirements for approving new developments on the Norwegian Continental Shelf quickly became pure number-crunching exercises. That, in turn, meant it was easy for statisticians to document that the various risks in such projects were within the acceptable limits.

ACCEPTABLE RISK

A fundamental aspect of understanding culture is to have a clear understanding as to what levels of risk are acceptable. Given that risk is basically subjective, it is not possible to dispassionately define what level of risk is acceptable and what is not. After all, if a facility operates for long enough, it is *certain*—statistically speaking—that there will be an accident. Yet, given that real-world targets are needed for investing in PSM, a target for "acceptable safety" is needed. This is tricky. Regulatory agencies in particular will never place a numerical value on human life and suffering because any number that they develop would inevitably generate controversy. Yet working targets have to be provided, otherwise the facility personnel do not know what they are shooting for.

The difficulty with attempting to identify an acceptable level of risk is that, as discussed in the sections above, the amount of risk people are willing to accept depends on many, hard-to-pin down factors. Hence no external agency, whether it be a regulatory body, a professional society, or the author of a book such as this can provide an objective value for risk. Yet individuals and organizations are constantly gauging the level of risk that they face in their personal and work lives, and then acting on their assessment of that risk. For example, at a personal level, an individual has to make a judgment as to whether it is safe or not to cross a busy road. In industrial facilities, managers make risk-based decisions regarding issues such as whether to shut down an equipment item for maintenance or to keep it running for another week. Other risk-based decisions made by managers are whether or not an operator needs additional training, whether to install an additional safety shower in a hazardous area, and whether a full Hazard and Operability Analysis (HAZOP) is needed to review a proposed change. Engineering standards, and other professional documents, can provide guidance. But, at the end of the day, the manager has a risk-based decision to make. That decision implies that some estimate of "acceptable risk" has been made.

One company provided the criteria given in Table 1.8 for its design personnel.

Table 1.8 Example of Risk Thresholds

	Fatalities Per Year (Employees and Contractors)
Intolerable risk	$>5 \times 10^{-4}$
High risk	$<5 \times 10^{-4}$ and $>1 \times 10^{-6}$
Broadly tolerable risk	$<1 \times 10^{-6}$

Their instructions were that risk must never be in the “intolerable” range. High-risk scenarios are “tolerable,” but every effort must be made to reduce the risk level, i.e., to the “broadly tolerable” level.

THE THIRD LAW

The Third Law of Thermodynamics states that it is impossible for any system to reduce its entropy to zero in a finite number of operations. A safety incident is an example of a system that is not in a zero entropy state, i.e., one that is not perfectly ordered. And it makes sense. No person is perfect, no organization is perfect. No matter how much time, effort and money and goodwill we spend on improving safety, incidents will occur. Indeed, the data shown in Figure 1.15 suggest that safety trends offshore have reached an asymptote. The data, which were published by the United States Bureau of Safety and Environmental Enforcement (BSEE), show a steady improvement from the mid-1990s to the year 2008. But since then there seems to have been a leveling out. Whether this trend will continue is to be seen, but it does suggest that some type of limit may have been reached.

Looked at in this light, perfect safety can never happen. Nevertheless we should strive toward it because otherwise we accept that people will be injured—which is something that none of us want or accept, and we certainly do not want to quantify (although a goal of zero incidents over a specified time frame may be achievable).

PERFECTION AS A SLOGAN

Although perfect safety may not be theoretically achievable, many companies will use slogans such as *Accidents Big or Small, Avoid them All*. The idea behind such slogans is that the organization should strive for perfect safety, even though it is technically not achievable.

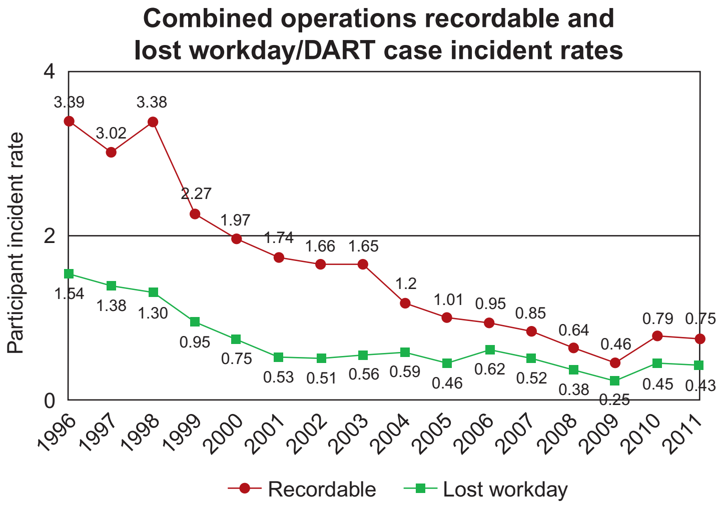


FIGURE 1.15

Offshore safety trends (United States).

Whether such slogans have a positive effect is debatable. Many people view them as being simplistic and not reflecting the real world of process safety. They seem to oversimplify a discipline that requires dedication, hard work, education, imagination, and a substantial investment. For example, a large sign at the front gate of a facility showing the number of days since a lost-time injury is not likely to change the behavior of the workers at that facility. Indeed, it may encourage them to cover up events that really should have been reported. Or to be cynical about the reporting system.

AS LOW AS REASONABLY PRACTICAL

Some risk analysts use the term "as low as reasonably practical (ALARP)" for setting a value for acceptable risk. The basic idea behind this concept is that risk should be reduced to a level that is as low as possible without requiring "excessive" investment. Boundaries of risk that are "definitely acceptable" or "definitely not acceptable" are established as shown in Figure 1.16, which is an FN curve family. Between those boundaries, a balance between risk and benefit must be established. If a facility proposes to take a high level of risk, then the resulting benefit must be very high.

Risk matrices (discussed below) can be used to set the boundaries of acceptable and unacceptable risk. The middle squares in such a matrix represent the risk levels that are marginally acceptable.

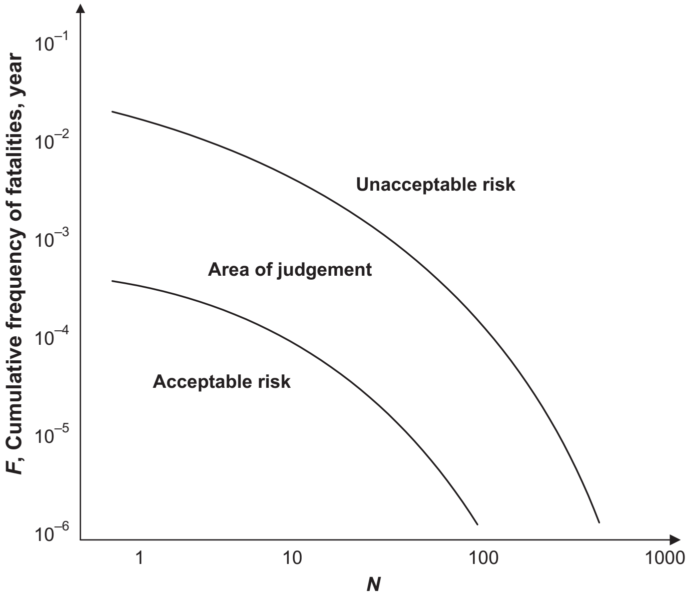


FIGURE 1.16

Risk boundaries.

One panel has developed the following guidance for determining the meaning of the term “ALRP.”

- Use of best available technology capable of being installed, operated, and maintained in the work environment by the people prepared to work in that environment.
- Use of the best operations and maintenance management systems relevant to safety.
- Maintenance of the equipment and management systems to a high standard.
- Exposure of employees to a low level of risk.

The fundamental difficulty with the concept of ALARP is that the term is inherently circular and self-referential. For example, the phrase “best available technology” used in the list above can be defined as that level of technology which reduces risk to an acceptable level—in other words to the ALARP level. Terms such as “best operations” and “high standard” are equally question-begging.

Another difficulty with the use of ALARP is that the term is defined by those who will not be exposed to the risk, i.e., the managers, consultants, and engineers who work safely in offices located a long way from the facility being analyzed. Were the workers at the site be allowed to define ALARP, it is more than likely that they would come up with a much lower value.

Realistically, it has to be concluded that the term “ALARP” really does not provide much help to risk management professionals and facility managers in defining what levels of risk are acceptable. It may be for this reason that the U.K. HSE chose in the year 2006 to minimize its emphasis to do with ALARP requirements from the Safety Case Regime for offshore facilities. Other major companies have also elected to move away from ALARP toward a continuous risk reduction model (Broadribb, 2008).

DE MINIMIS RISK

The notion of *de minimis risk* is similar to that of ALARP. A risk threshold is deemed to exist for all activities. Any activity whose risk falls below that threshold value can be ignored—no action needs to be taken to manage this *de minimis* risk. The term is borrowed from common law, where it is used in the expression of the doctrine *de minimis non curat lex*, or, “the law does not concern itself with trifles.” In other words, there is no need to worry about low-risk situations. Once more, however, an inherent circularity becomes apparent: for a risk to be *de minimis* it must be “low,” but no prescriptive guidance as to the meaning of the word “low” is provided.

CITATIONS/“CASE LAW”

Citations from regulatory agencies provide some measure for acceptable risk. For example, if an agency fines a company say $50,000 following a fatal accident, then it could be argued that the agency has set $50,000 as being the value of a human life. (Naturally, the agency’s authority over what level of fines to set is constrained by many legal, political, and precedent boundaries outside their control, so the above line of reasoning provides only limited guidance at best.) Even if the magnitude of the penalties is ignored, an agency’s investigative and citation record serve to show which issues are of the greatest concern to it and to the community at large.

RAGAGEP

With regard to acceptable risk in the context of engineering design, a term that is sometimes used is "Recognized and Generally Accepted Good Engineering Practice" (RAGAGEP). The term is described in Chapter 9—Asset Integrity. The concept has also been proposed as part of the updated OSHA process safety standard (Chapter 2).

INDEXING METHODS

Some companies and industries use indexing methods to evaluate acceptable risk. A facility receives positive and negative scores for design, environmental and operating factors. For example, a pipeline would receive positive points if it was in a remote location or if the fluid inside the pipe was not toxic or flammable (Muhlbauer, 2003). Negative points are assigned if the pipeline was corroded or if the operators had not had sufficient training. The overall score is then compared to a target value (the acceptable risk level) in order to determine whether the operation, in its current mode, is safe or not.

Although indexing systems are very useful, particularly for comparing alternatives, it has to be recognized that, as with ALARP, a fundamental circularity exists. Not only has an arbitrary value for the target value to be assigned, but the ranking system itself is built on judgment and experience, therefore it is basically subjective. The biggest benefit of such systems, as with so many other risk-ranking exercises, is in comparing options. The focus is on relative risk, not on trying to determine absolute values for risk and for threshold values.

RISK MATRICES

Risk is commonly analyzed and managed through the use of a system of three risk matrices. They are:

1. Consequence matrix
2. Frequency matrix
3. Risk matrix.

The approach has been used in various standards, including Military Standard 882C and AS/NZS 4360:1999.

CONSEQUENCE MATRIX

A representative consequence matrix is given in Table 1.9. The matrix has four levels of consequence covering worker safety, public safety, the environment, and economic loss. There are no rules as to how many levels should be selected, nor does any major regulatory body insist on a particular size of matrix. However, many companies choose four levels; three levels does not provide sufficient flexibility and differentiation, but five levels imply a level of accuracy that is probably not justified. The steps in Table 1.9, from "low" to "very severe," are roughly in

Table 1.9 Consequence Categories

	Worker Safety	Public Safety	Environment	Economic (Annual)
Low, 1	Reportable or equivalent.	None.	Limited impact that is readily corrected.	$10,000 to $100,000
Moderate, 2	Hospitalization or lost-time injury.	Minor medical attention.	Report to agencies and take remedial action.	$100,000 to $1 million
Severe, 3	Single disabling injury.	Hospitalization or serious injury. Some local reporting.	Irreversible damage to low-quality land, or clean-up of environmentally sensitive areas required.	$1 million to $10 million
Very severe, 4	Fatality or multiple serious injuries.	Fatality or multiple serious injuries. Massive negative publicity.	Months of clean-up work needed in environmentally sensitive areas.	≥ $10 million

orders of magnitude, i.e., each increased level is about 10 times more serious than the one before it.

Worker Safety

The first of the consequence columns given in Table 1.9 is worker safety—the topic that usually receives the most attention during risk analyses. Indeed many risk analysts will elect to consider this item only, which is why it has been shaded. If the workers are safe, it is argued, then the other consequence terms will probably be acceptable also.

Public Safety and Health

Incidents that affect members of the public usually attract a good deal of attention. Hence the values for public safety, which are provided in the third column of Table 1.11, are an order of magnitude higher than for worker safety. (It could be argued that all people have the same value, and that a member of the public is not "more valuable" than a worker. However, because risk is fundamentally a subjective topic, incidents that affect the public are perceived as being worse than those involving just workers. Such incidents become even less acceptable if they affect children.)

Related to public safety and health is the topic of negative publicity, particularly those major events that "make the newspapers."

Environmental Impact

Environmental risks are given in Table 1.9. In practice, environmental issues are normally controlled by rules and regulations rather than an objective analysis of risk.

The Norwegian offshore industry uses the values given in Table 1.10 to categorize the consequences of environmental incidents.

Table 1.10 Environmental Consequences—Offshore Norway

Minor	Recovery time: 1 month to 1 year
Moderate	Recovery time: 1 to 3 years
Significant	Recovery time: 3 to 10 years
Serious	Recovery time: more than 10 years

Table 1.11 Economic Loss Categories

Minor	1 to 7 days
Moderate	7 days to 1 month
Significant	1 month to 3 months
Serious	More than 3 months

Economic Loss

The final consequence category in Table 1.9 is economic loss. All process incidents generate losses in one or more of the following areas:

- Damaged or destroyed equipment
- Lost production
- Off-quality product
- Litigation
- Clean-up.

Economic loss can either be one time (say the destruction of a piece of equipment) or ongoing, in which case the value given in Table 1.11 represents an annual loss. The cost associated with a safety event can be derived from incident data. For example, one company has reported that the cost of a serious incident is in the range $2−$10 million, whereas the cost of a lost-time incident is $150,000.

The difficulty with using the "economic loss" column in a risk-ranking matrix is that it effectively assigns a financial value to human life and suffering. For example, Table 1.9 suggests that a single, disabling injury is "worth" from $1 to $10 million. As already discussed, such statements, being entirely subjective, can be controversial and almost impossible to defend. A similar critique can be made about insurance payments—it is not possible to truly assess the cost of a fatality or an injury.

FREQUENCY MATRIX

Once the consequences associated with an incident have been identified, the next step is to estimate the frequency with which the incident may occur. A representative frequency matrix is given in Table 1.13. As with the consequence matrix, four value levels are provided. The use of just three levels is probably too coarse, but five levels or more implies a degree of accuracy that probably could not be justified (precision is not the same as accuracy).

Table 1.12 Frequency Matrix

	Frequency	**Comments**
Low, 1	<1 in 1,000 years	Essentially impossible: “Once in a blue moon” or “meteor falling out of the sky.”
Moderate, 2	1 in 100 years to 1 in 1,000 years	Conceivable—has never happened in the facility being analyzed but has probably occurred in a similar facility somewhere else.
High, 3	1 in 10 years to 1 in 100 years	Might happen in a career.
Very high, 4	>1 in 10 years	It is likely that the event has occurred at the site if the facility is more than a few years old.

Table 1.13 Risk Ranking Matrix

		Consequence			
Frequency		Low, 1	Moderate, 2	Severe, 3	Very severe, 4
	Low, 1	D	D	C	C
	Moderate, 2	D	C	C	B
	High, 3	C	C	B	A
	Very high, 4	C	B	A	A

As with the consequence matrix, the steps in Table 1.12 are roughly an order of magnitude greater than the one before it.

In practice, the most difficult judgment to make is between the “high” and “moderate” values. Events in this range have probably not been observed by the workers at the site, yet they are plausible.

One way of helping people visualize and estimate the frequency of very unlikely events is to examine the overall industry record. For example, if a certain event has an estimated frequency of 1 in 100 years, it is not likely that anyone on the facility will have witnessed that event. However, if there are 100 similar facilities worldwide, then that event should be occurring about once a year somewhere in the world. (Because shared information can be so useful, many companies choose to tell others about their safety difficulties, in spite of potential trade secrets and other legal issues.)

RISK MATRIX

Having determined consequence and frequency values to do with a particular hazard, the overall risk is determined using a third matrix such as that given in Table 1.13, which shows four levels of risk.

The risk values will usually line up diagonally, with all the values in any one diagonal being the same.

The meaning of the four letters in Table 1.13 is given in the following sections.

A—(Red) Very High

This level of risk requires prompt action; money is no object, and the option of doing nothing is not an option. An "A" risk is urgent. On an operating facility, management must implement Immediate Temporary Controls (ITC), while longer-term solutions are being investigated. If effective ITCs cannot be found, then the operation must be stopped. During the design phases of a project, immediate corrective action must be taken in response to an "A" finding, regardless of the impact on the schedule and budget.

B—(Orange) High

Risk must be reduced, but there is time to conduct more detailed analyses and investigations. Remediation is expected within, say, 90 days. If the resolution is expected to take longer than this, then an ITC must be put in place.

C—(Yellow) Moderate

The risk is significant. However, cost considerations can be factored into the final action taken, as can normal scheduling constraints such as the availability of spare parts or the timing of facility turnarounds. Resolution of the finding must occur within, say, 18 months. An ITC may or may not be required.

D—(Green) Low

Requires action but is of low importance. In spite of their low-risk ranking, "D" level risks must be resolved and recommendations implemented according to a schedule; they cannot be ignored. (Some companies do allow very low-risk-ranked findings to be ignored on the grounds that they are within the bounds of acceptable risk.)

If the hazard is associated with a change to an existing process, it is not always necessary to conduct a full risk ranking, particularly if the change does not make a fundamental alteration to the process itself. In these cases, it is enough just to check that the risk value does not shift form one square to another. If it does not then no further evaluation is needed.

Other Categories

In addition to the four letters given in Table 1.13, the following types of risk response can be used:

- O—*Operational*

  Sometimes the risk associated with a hazard is purely economic; it has neither safety nor environmental implications. Use of the letter "O" tells management that they do not have to respond to the finding for safety reasons, but they may choose to do so in order to improve profitability. Use of this term also means that a hazards analysis team will probably not use the economic consequence column in Table 1.14. Instead, all economic findings will be placed in the "O" category, regardless of their magnitude.
- S—*Standards*

  Some risks represent a violation of regulations, industry consensus standards/codes or company policy. It is difficult to assign frequency and consequence values to this type of risk, but professional practice suggests that something should be done (and if the issue is a code or regulatory violation, then something must be done). One option is to arbitrarily assign a B-level risk to regulatory and code violations, and a C-level risk to nonconformance to consensus standards.

- L—*Low-Hanging Fruit*

  This term is obviously written tongue-in-cheek, yet many times it is unnecessary to dwell on the development of recommendations; what needs to be done is simple, straightforward, effective, quick, cheap, and noncontroversial. In such cases, there is little point in conducting a risk assessment—it is better simply to fix the problem. For example, if an operating procedure is not up to date, it is better just to rewrite it rather than worrying about the risk associated with use of the present procedure. Similarly, if a safety sign is unreadable, it should simply be replaced. (Although problems such as the above can be addressed right away, management may consider the implications of why these minor problems existed in the first place. For example, an improperly formatted operating procedure is not a major issue, but it may point to a fundamental difficulty with the way in which procedures are written. Similarly, an illegible safety sign may indicate deeper problems regarding the occupational safety and housekeeping programs.)

LIMITATIONS OF RISK MATRICES

In spite of their widespread use, risk matrices do have limitations, some of which are described below:

- “A”-level/Red Square risks occur only very rarely—in most cases such hazards have already been identified and addressed. Therefore that part of the matrix is not of much practical use.
- A similar argument applies to “D”-level/Green Square sections of the matrix. Although there are many hazards as this level they are generally of low enough consequence that they do not need to be analyzed or discussed.
- High-consequence/low-frequency events also tend to be ignored. For example, a hazards analysis team may briefly consider the scenario of an airplane crashing into their facility, but decide that it is not worth further discussion.
- Estimate of frequency and consequences are unreliable and subjective. The value that people assign to the likelihood of an event occurring varies enormously and is particularly dependent on whether they have actually experienced such an event. A related difficulty, particularly when matrices with many rows and columns are used, is the potential for confusing precision with accuracy.

The scientific basis for these matrices has also been challenged. For example, Thomas et al. (2013) state,

> The perceived benefit of the RM is its intuitive appeal and simplicity. RMs are supposedly easy to construct, easy to explain, and easy to score. They even might appear authoritative and intellectually rigorous. Yet, the development of RMs has taken place completely isolated from scientific research in decision making and risk management. This paper discusses and illustrates how RMs produce arbitrary decisions and risk management actions.

In practice, therefore, a risk matrix does not provide as much guidance as may be anticipated. An alternative approach is to group hazards as follows.

Low-Hanging Fruit

Many hazards can be removed quickly and easily. Examples include writing a missing operating procedure or painting a yellow line around a hazardous area. Some of these items may be quite costly, but the response is the same. For example, on one refinery, the block valves in a highly corrosive service were chronic leakers. The solution was simple but not cheap: replace all the valves with those from another manufacturer that were known to be effective.

Prepare for the Worst Case

There is no need to analyze rare, catastrophic events such as the airplane crash. But it important to make sure that the facility has the necessary response systems in place to handle worst-case scenarios such as explosions, leaks of toxic gas, or blowouts.

Expensive Good Ideas

For most of the “B” and “C” items management has neither the funds nor the people to do them all at once. Each item develops its own life and trajectory. Realistically the ones selected are those that have the strongest support or champions. The necessary decisions as to which items will be acted upon will be made without consulting the matrix.

BLACK SWAN EVENTS

In his best-selling book *Black Swan* Nissam Taleb (2007) discusses those rare events that cannot be forecast but that have a major impact. Many of his examples are from the world of finance, but the concept certainly applies to the risks associated with process facilities.

The following are features of *Black Swan* events:

- They are a surprise and were not forecast by the risk models in use.
- They have a major impact.
- After their occurrence, those involved rationalize what happened.

In order to minimize the impact of such events, Taleb says, “Avoid Optimization, Learn to Love Redundancy.” However, he notes that most managers are rewarded on short-term gains rather than preparing for a rare event that cannot be defined or explained and that may not happen for a very long time.

Taleb used his web page to note that the Japanese Nuclear Commission had, in the year 2003, set the following goal:

> The mean value of acute fatality risk by radiation exposure resultant from an accident of a nuclear installation to individuals of the public, who live in the vicinity of the site boundary of the nuclear installation, should not exceed the probability of about 1×10^6 per year (that is, at least 1 per million years).

Just 8 years later, the reactors at the Fukushima nuclear power plant catastrophe released enough radioactivity that it is plausible that some of the people in the nearby communities will sicken, and some of them will die.

He then goes on to state,

> I spent the last two decades explaining (mostly to finance imbeciles, but also to anyone who would listen to me) why we should not talk about small probabilities in any domain. Science cannot deal with them. It is **irresponsible** to talk about small probabilities and make people **rely** on them, except for natural systems that have been standing for 3 billion years (not man-made ones for which the probabilities are derived theoretically, such as the nuclear field for which the effective track record is only 60 years).

He is equally scathing about estimates of consequence. He believes that the consequences of events such as Deepwater Horizon or Fukushima–Daiichi will always be much more serious that estimated in the risk management models.

DIFFERENT INDUSTRIES

In any industry, there is a tendency for specialists to believe that only they can address the problems of their particular business. They do not readily accept that people from other industries can make a contribution. The response of in-house experts to an outsider is, "But we're different, you know—we don't think that you can help us."

With regard to process risk management, this attitude is generally misleading. Certainly there are differences between industries; but those differences are relatively minor compared to the concepts and programs that they share. The elements of process safety given in Table 1.3 can be used in all process industries.

Some of the distinctive features of the following industries with regard to risk and PSM are discussed in this section:

- Oil refineries
- Onshore oil and gas
- Offshore oil and gas
- Pipelines.

OIL REFINERIES

Oil that comes from the ground is a mixture of many hydrocarbons, ranging from light components such as butane to heavy, tar-like materials. (The composition will vary considerably depending on the source of the crude oil. Crude from Saudi Arabia, for example, has a high fraction of light components whereas crude from Venezuela is much heavier.)

In its raw form, crude oil has very little value; it has to be split into its various components in an oil refinery. Examples of its products include:

- Gasoline for automobiles
- Fuel oil (bunker fuel) for ships
- Butane gas for backyard barbeques.

Some of the products from refineries, such as naphtha, are termed intermediates; they are not used directly; instead they are sold to chemical plants which use them to make a wide range of chemical products, such as plastics and motor fuel additives. Refineries use physical separation processes, particularly distillation, to separate the various components. However, the ratio of components in crude oil is rarely what is desired by the market. For example, a representative barrel of crude contains something like 15% of gasoline components. But the demand for gasoline as a fraction of the total barrel is much higher than that. Therefore, refineries use a wide range of chemical processes to achieve the desired ratios. Examples include:

- Alkylation to combine C_4 molecules to make C_8 molecules (octanes), thereby producing more gasoline.
- Catalytic cracking to break down larger molecules so as to create lighter components.

Refineries are flexible in the way in which they operate and in the way in which they can structure their processes. They work with constantly changing feedstocks and product slates. Partial turnarounds are quite common, and they can often handle multiple operations with the same equipment.

Refineries and chemical plants generally handle large quantities of flammable and toxic materials, often at high pressure and temperature. In this respect, they are like offshore platforms. The general technical similarity between offshore and onshore technologies means that the safety and process safety standards and rules for each bear strong similarities to one another. (There are, however, some important technical differences between onshore and offshore safety. For example, in an emergency, it is usually possible to evacuate employees at a refinery or chemical plant to a safe location that is distant from the plant itself; offshore evacuation is much more difficult and time-consuming. On the other hand, many chemical facilities use highly toxic and specialized chemicals that require the use of special precautions—such is not the case offshore.)

- The operations of oil refineries are flexible because they need to change product profiles depending on market demands and the crude oil feedstocks that they are using. This flexibility can create hazardous situations. (During a HAZOP, one senior operator claimed that he could put gasoline in the refinery manager's coffee cup just by opening and closing valves.)
- Although workers at a refinery can be exposed to high hazard situations, it is unusual for incidents to "go over the fence" and to affect members of the public (although HF and H2S can provide exceptions to this statement).

OFFSHORE OIL AND GAS

The offshore business does not have to address most of the above problems. For example, offshore platforms use various chemicals such as methanol and monoethylene glycol for hydrate removal. Although these chemicals are toxic and flammable, they do not compare to some of the chemicals found in a typical chemical plant or refinery. Moreover, the quantities used offshore are quite small as compared with a typical onshore facility. Generally, the chemicals are supplied in tote tanks that are offloaded from a supply boat and stored at a dedicated section of the deck.

In addition, operating conditions on offshore platforms tend to be less severe than those in chemical plants and refineries. Temperatures and pressures are usually quite low, and the process steps consist mainly of the physical separation of oil, water, and gas. Even if there is a chemical processing step, such as the removal of hydrogen sulfide from the gas stream, the process is likely to be fairly simple—certainly when compared to onshore chemical plants.

Finally, offshore platforms, unlike onshore pipelines, are pretty much out of the public eye. Unless a platform or rig has a very serious spill, offshore events are not likely to directly impact members of the public.

Nevertheless, the offshore business also has its own special safety issues. They include the following:

- Lack of escape routes
- Persons on board
- Cyclones/hurricanes
- Downers and leaners
- Blowouts
- Hydrogen sulfide
- Dropped objects
- Helicopters
- Ship collision.

These topics are discussed below.

Lack of Escape Routes

On an onshore facility such as a refinery or chemical plant workers at the site can, in the event of a major release or fire, escape from the scene (once they have secured the equipment for which they are responsible, and assuming that they are not part of the emergency response team). On one refinery, for example, an operator was drenched in light hydrocarbons that leaked from a failed filter housing. He was surrounded by fired heaters, so he simply ran away. A major fire did erupt, and much of the equipment was seriously damaged, but no one was injured ("If a man's not there, he can't be killed"). His actions were correct; he could have stayed in the region of the fire—had he done so he would have died, and the resulting damage would have been no less.

Offshore, however, there is nowhere to run or to hide. Platforms are typically very congested so there is no "outside." If someone wishes to "run away" his or her only option is to enter the sea, preferably by TEMPSC or life raft. (Going into the water directly may be feasible in warm locations such as the Gulf of Mexico or Angola, but jumping into the North Sea or the ocean off the coast of Labrador, particularly in winter, is likely to be a death sentence. Even in warm waters, hitting the surface of the sea can cause serious injuries, and there is no guarantee that a person will not hit part of the steel structure before landing in the water.)

Platforms will always have a designated Temporary Refuge (TR) area which serves as a muster point in the event of an emergency. The TR will be protected against fire, blast, and smoke ingress, and will be provided with means of communicating with the rescue and support services. In many cases, the facility's Living Quarters are also the primary TR.

Persons on Board

On onshore facilities, the people who are not actually at work go home. Therefore, in the event of a serious accident, they cannot be killed—the number of affected people is limited to those who are on duty. For example, the explosion at the chemical plant in Flixborough, England, in the year 1974 was very bad: 28 men died. But the accident occurred on a weekend; had it occurred during the middle of a working day the death toll would have been higher—much higher. (The number of deaths could have been zero had the men operating the plant realized that they had “lost it,” and they needed to get away. As it was, they stayed in the control room for more than 20 minutes following the initial release, and they paid for that decision with their lives.)

On an offshore platform, however, the persons who are not on duty are still present, and they may be killed or injured. Many of the deaths on the Piper Alpha platform, for example, were of off-duty crew who were sleeping, and who could not escape from the Living Quarters. By contrast, 25 years later, when the explosion and fire occurred on the Deepwater Horizon platform, 11 men died instantly, but the other 135 persons on board survived the blast and subsequent fire. This is an indication that the safety measures that have been designed into platforms in the years following Piper have had a positive effect on safety improvement.

Cyclones/Hurricanes

Cyclones (hurricanes/typhoons) develop over warm bodies of water and create high winds and thunderstorms. Many offshore oil and gas facilities, particularly in the Gulf of Mexico, are vulnerable to the effects of cyclones. Tropical storms and tropical depressions have the same causes as cyclones but generally do not generate such high winds—although they can create considerable rainfall.

Some of the consequences of hurricanes in the GoM in recent years—Ivan, Katrina, and Rita—have had the following consequences:

- Sustained wind speeds were 175 mph (Katrina), 180 mph (Rita). These are record values. Ivan was narrower but generated mud slides. One platform is now buried under 50 feet of mud.
- Of the 4,000 platforms in the GoM around 3,050 were in the path of at least one of the storms.
- One hundred and thirteen platforms went down; 52 were seriously damaged (therefore about 95% of the platforms made it through the storms without significant damage).
- Twenty-two of the downed platforms were less than 10 years old.

Downers and Leaners

When a platform is destroyed during a hurricane, it usually remains in place—in a severely damaged condition. If it sinks and rests on the seabed then it is a “downer.” If it partially collapses, with some structure showing above the sea surface, then it is a “leaner.”

These damaged platforms have to be removed because they pose a hazard to shipping. However, their removal can be time-consuming and expensive. One operator has already spent over $1 billion on clearing out some of these platforms. Also, some insurers are dropping coverage for nonproducing wells. The cost of decommissioning a well after the platform is down is estimated to be 10 times greater than if it is done in a planned manner.

Even when the water is shallow, it is not safe to send divers down because the structure may collapse while the diver is in the water. Moreover, if the wellhead has not been properly secured, a gas blowout could occur at any time—once more posing a great risk to divers in the vicinity. This means that ROVs (remotely operated vehicles) have to be used. (One estimate is that 85% of the remediation work is done by divers, the rest by ROVs.) Explosives are rarely used because of the potential impact on turtles and other marine creatures. Chemicals, including diesel fuel, that were on board the facility at the time of the platform collapse pose an environmental hazard and can be a safety hazard for divers in the area.

It is often difficult to get construction information about older platforms. Either the information is missing or there has been a lot of "midnight engineering," i.e., undocumented changes. In some cases, the only records were on the platform that went down.

The "Reef in Place" program allows some platforms to be used as potential reefs. However, they must be at least 90 feet below the water line, and regulatory permission is required. Some companies are relocating their damaged platforms to other reefs in place locations.

Blowouts

As the recent *Deepwater Horizon/Montara* event has demonstrated so dramatically, blowouts can be very dangerous and environmentally destructive. They are also very expensive, both in terms of destroyed equipment and wasted production. Therefore, any SMS for a drilling rig must pay particular attention to the avoidance of blowouts.

A blowout occurs when the pressure of the hydrocarbons in a formation exceeds the pressure of the column of mud in the annulus of the drill string. Oil and gas rises very quickly up the string (with the gas expanding as it goes). When they reach the deck of the drill rig, they can ignite and/or create a major spill.

To prevent blowouts from occurring, the SMS has to ensure (a) that the density of drilling mud is sufficiently high and (b) that the blowout preventer is functioning properly.

Hydrogen Sulfide

Hydrogen sulfide (H_2S) is a highly toxic, colorless, flammable gas with a pungent odor at low concentrations. (Most texts state that H_2S smells like rotten eggs, but, with modern refrigeration, it is probably more appropriate to state that rotten eggs smell like H_2S.) The gas is often found in crude oil—sometimes in the form of mercaptans, which break down to form H_2S. Potential exposure to H_2S is an issue of most refineries and many offshore facilities.

Exposures to H_2S at concentrations as low as 600 parts per million (ppm) can cause death in a matter of minutes due to paralysis of the respiratory system. Because H_2S oxidizes rapidly in the body, there are normally no permanent effects from acute exposure if the victim is rescued promptly and resuscitated before experiencing prolonged oxygen deprivation.

Hydrogen sulfide can also cause corrosion of stainless steels such as 316 and 410 stainless in the form of sulfide stress cracking. Copper alloys corrode rapidly in H_2S service. Upper limit values have been developed by the National Association of Corrosion Engineers (NACE MR-0175 NACE 2008). In the gas phase, a stream is sour if the H_2S partial pressure exceeds 0.05 psia. If a single phase liquid is in equilibrium with a gas phase, where the gas phase H_2S partial pressure exceeds 0.05 psia, then that liquid is also considered to be sour.

Dropped Objects

Dropped objects (usually from deck cranes) are a major hazard on offshore platforms. If they fall on the deck, they can hurt workers and/or seriously damage equipment (with the potential for a catastrophic event). If the dropped object is heavy and it falls into the sea, it can be traveling quite fast by the time it reaches the seabed, especially in deepwater. Consequently the dropped object can cause substantial damage to subsea equipment—with the potential for causing a serious environmental problem.

At the annual meeting of the Offshore Operators Committee held in December 2010, it was noted that 19.5% of offshore accidents are due to crane movement (closely associated with dropped objects events) and that the number of accidents in this area has not been improving. The favorable trend shown in Figure 1.11 does not apply to such accidents. For this reason, the OOC working the BOEMRE is researching the causes of such accidents so that actions can be taken to reduce their number.

Helicopters

Helicopters are used to transport personnel and light freight to and from offshore platforms. They are also used for the emergency evacuation of injured personnel (but cannot be used, of course, if the platform itself is sinking or on fire). The crash of a helicopter is almost always a very serious event—often leading to fatalities and serious economic loss.

Ship Collision/Mooring Failure

Offshore platforms can be hit by ships—usually the service boats that provide equipment and supplies. Sometimes these impacts can be very serious. In the case of the Mumbai High incident, for example, a large support vessel approached the platform to evacuate an injured man. The boat had problems with its computer-assisted azimuth thrusters so she was brought in stern-first under manual control. The helideck on the support vessel hit a riser, which started leaking. The leak resulted in a fire that leads to approximately 22 fatalities and total loss of the platform and of the vessel.

Spill Response

If the worst happens, and there is a big release of oil or gas to the ocean, industry needs to be able to respond quickly and effectively. The Deepwater Horizon incident demonstrated that such a response capability was not in place—it took industry 3 months to cap the leak from the damaged well head and to direct the flow of oil to a safe location. The National Commission report to the President (discussed in detail in the next chapter) says the following about that event.

Just as the events of April 20, 2010, exposed a regulatory regime that had not kept up with the industry it was responsible for overseeing, the events that unfolded in the subsequent weeks and months made it dismayingly clear that neither BP nor the federal government was prepared to deal with a spill of the magnitude and complexity of the Deepwater Horizon disaster.

PIPELINES

Pipelines are used to transport process chemicals and hydrocarbons, often over very long distances. Some distinctive issues to do with pipelines include the following:

- They are very much in the public domain. Chemical plants, refineries, and onshore oil and gas facilities are mostly located in a relatively small area that is fenced off, often with tight security. Offshore oil and gas facilities are usually out of sight of the public. But pipelines are almost entirely in public areas, with the exception of terminals and pumping stations. Also many pipelines are buried so detecting a leak can be difficult, particularly if the pipe is not designed to handle smart pigs.

- From a process point of view they are quite simple. They do not feature chemical reactions, and process conditions are generally quite constant, apart from the pressure drop that naturally occurs between pumping stations.
- The biggest hazards associated with pipelines are usually to do with corrosion—particularly corrosion inside the pipe. It is often difficult to detect such corrosion, particularly when the pipeline is buried.

The risks associated with pipelines are generally put into one of three categories: low, medium, and high.

- A *low-risk* pipeline is one that is transporting benign materials, such as drinking water and/or is located in a remote environment. Operators and contractors are well experienced in the design, construction, and operation of this type of pipeline.
- A *medium-risk* pipeline passes through a region where moderate restrictions regarding environmental compliance apply.
- A *high-risk* pipeline transports materials that are corrosive and/or are located in a region with severe environmental mandates. If the pipeline is technically innovative or if the consequences of a leak are very serious, then it would be considered to be high risk.

EXAMPLES

Throughout this, book the examples shown below are used to illustrate the concepts and ideas that are presented. They are referenced at the appropriate points of succeeding chapters, and they are provided at http://www.stb07.com/process-industry-examples.html.

EXAMPLE 1—FACILITY DESIGN

A process consists of four operating units and a utilities section. A schematic of the system is shown in Figure 1.17.

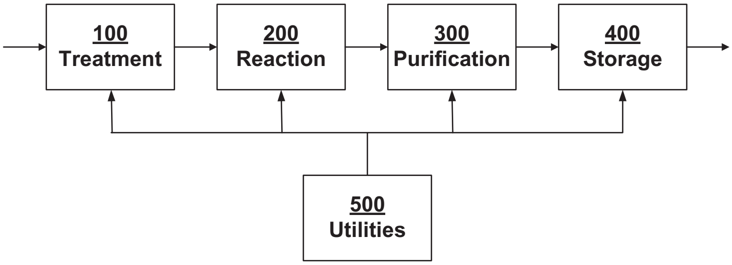


FIGURE 1.17

Process units.

EXAMPLE 2—PROCESS FLOW

Figure 1.18 shows part of Unit 100 from Figure 1.17. Liquid flows into an atmospheric tank, T-100. The liquid, which is both flammable and toxic, is called Raw Material Number 12—abbreviated to RM-12. From T-100, RM-12 is pumped to pressure vessel, V-101, using Pump P-101A or P-101B, either of which can handle the full flow (A is normally in service, with B being on standby). The pumps are driven by a steam turbine and an electric motor respectively.

The flow of liquid both into and out of T-100 is continuous. The incoming flow varies according to upstream conditions and is outside the control of the operators responsible for the equipment shown. The flow rate from T-100 to V-101 is controlled by FRC-101, whose set point is cascaded from LRC-101, which measures the level in T-100. The level in T-100 can also be measured with the sight glass, LI-100.

V-101 is protected against overpressure by safety instrumentation (not shown) that shuts down both P-101 A/B, and by the relief valve, PSV-101.

Failure and repair times for the pumps are provided in Table 1.14.

Summarizing Table 1.14 in words:

- P-101A (which is the pump that is normally in operation) is expected to fail twice a year. It takes 8 hours to repair.
- When P-101A stops working, P-101B is started. It is expected that P-101B will fail to start on demand once in 10 times. If P-101B does not start immediately, its anticipated repair time is 3 hours.

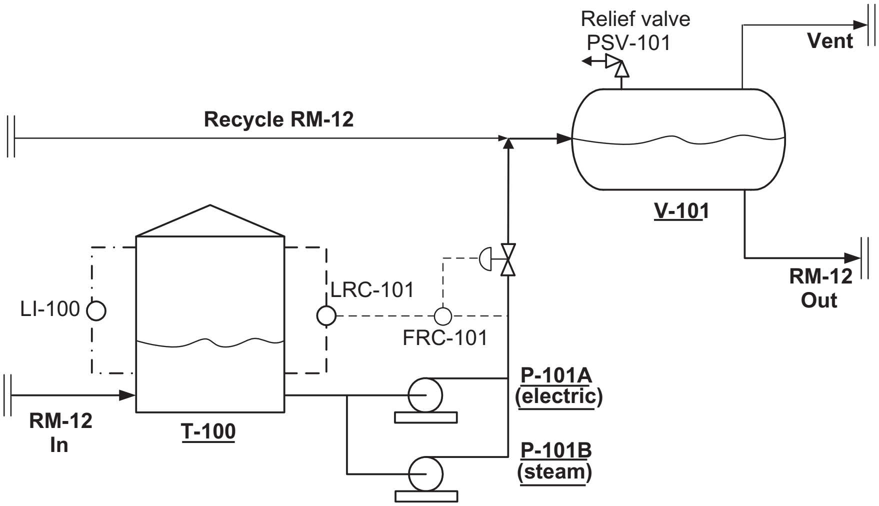


FIGURE 1.18

Process flow example.

Table 1.14 Failure and Repair Times

Item	Failure Rate, year^{-1}	Failure Rate, hour^{-1}	Probability of Failure on Demand	Mean Downtime (MDT), hour
P-101A	0.5	0.000057077	–	8
P-101B	–	–	0.1	3

EXAMPLE 3—HEAT EXCHANGER

Figure 1.19 shows a shell and tube heat exchanger. Hydrocarbon vapors enter the exchanger on the shell side where they are condensed by cooling water which runs through two passes of tubes. The pressure relief valve and the drain and vent valves on the shell side are shown.

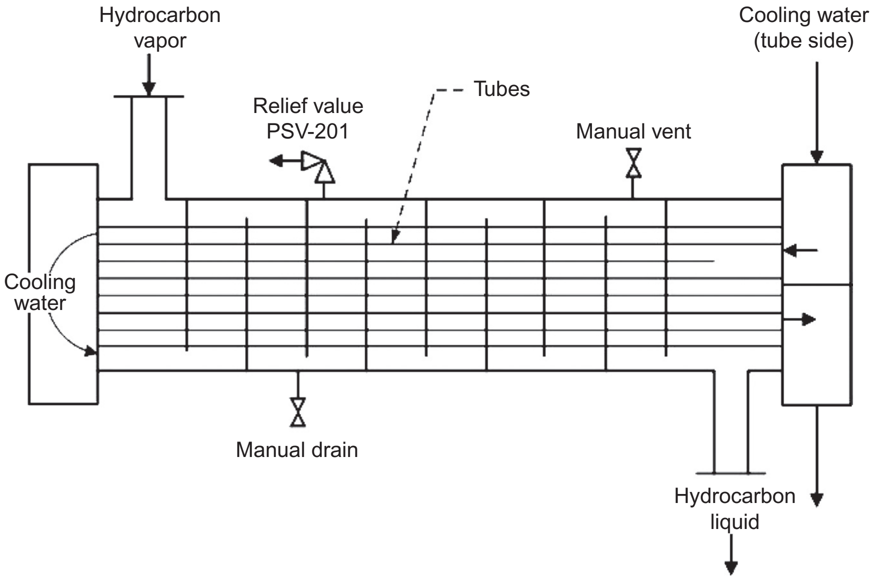


FIGURE 1.19

Heat exchanger example.

EXAMPLE 4—RISK MANAGEMENT WORKFLOW

The third example is used for discussions of the management of risk. Figure 1.20 illustrates the major steps in the development of a representative risk management program.

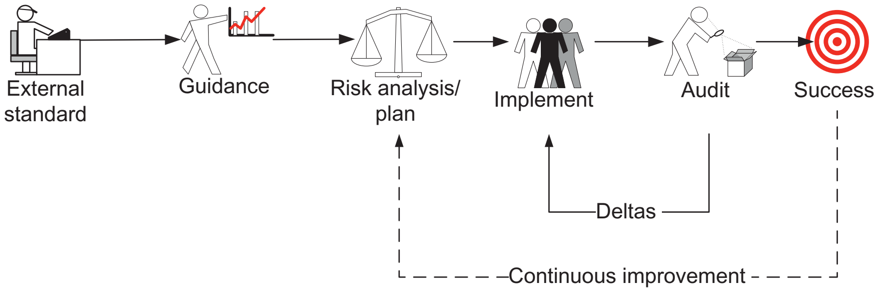


FIGURE 1.20

Risk management workflow example.

External Standard

The first step in the development of a risk management program is to check for the existence of standards from an external agency—generally either a government regulator or a company's own corporate group). Regulations are broad in scope. Corporate standards are likely to be more specific because they focus on just those operations that the company carries out.

Guidance

Because external standards do not generally provide enough detail to actually develop and run a risk management program additional nuts-and-bolts guidance is needed. Such guidance can be internally generated or it can be provided by outside experts and consultants.

Risk Analysis Plan and Implement

The next step is to conduct a risk analysis that will help determine what risks exist, how those risks can be mitigated, and how resources should be prioritized. Planning is followed by implementation.

Audit/Deltas

No management program is perfect. Gaps between goals and reality always exist. In order to systematically identify the gaps, audits are needed. If the audit finds deficiencies or gaps, the process recycles to the implementation step. (The word "delta" is sometimes used to describe the difference between plan and performance because it sounds less critical than words such as "deficiency" or "failure.")

Success/Continuous Improvement

Ideally, once the plan is implemented and has been audited, management can declare that they have successfully implemented their risk management program. However risk can never be low enough; improvements can always be made. Therefore, once the program has been completed, management should start the whole process over again—usually at the risk analysis and planning steps—in order to achieve even higher levels of safety and economic performance.

EXAMPLE 5: SIGNIFICANT POTENTIAL INCIDENT

This example is loosely based on an actual event that occurred at a process facility. Fortunately, the incident did not result in a major loss, but it does provide some opportunities for lessons learned.

A cone-roof, atmospheric storage tank stores a nonflammable, low-vapor-pressure inorganic liquid. The vapor space above the chemical is air; the tank breathes in and out through a simple vent line. A small, steady stream of the inorganic liquid is pumped from the tank into the process, which contains light hydrocarbons at moderately high pressure. One of the facility's private roads is located close to the tank. A small but steady stream of vehicles uses the road.

On a number of occasions the pump stopped operating, the check valve failed to hold and light hydrocarbons flowed backward from the process into the tank. A layer of hydrocarbons formed on top of the inorganic liquid, as shown in Figure 1.21. No instrumentation was installed to warn of the occurrence of this event.

The tank is refilled with the inorganic liquid about once a month from a truck. As the level in the tank rose during the truck unloading process, vapors from the hydrocarbon layer came out of the vent. A hydrocarbon detector located about 100 meters from the tank detected the presence of flammable vapors and sounded an alarm.

The incident was a near-miss—the vapors did not light off, and no one was hurt. (There were, however, economic costs associated with cleaning out the tank safely.) However, the potential for a serious event was high—the vapors could have ignited at a vehicle engine or exhaust manifold. The flame front could then have entered the tank and caused a large explosion.

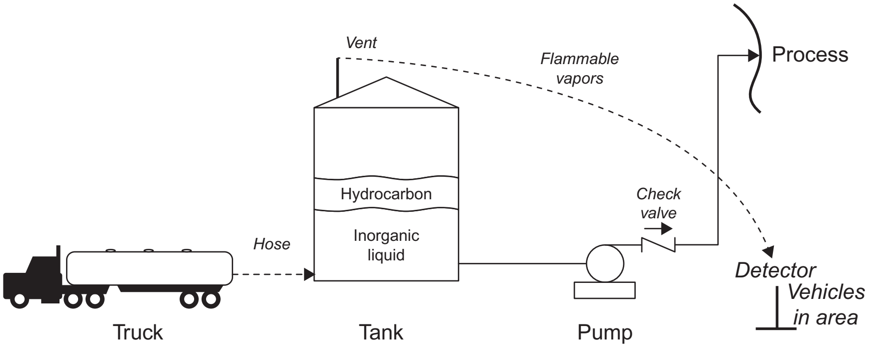


FIGURE 1.21

Reverse flow to tank.

CHAPTER

COMPLIANCE AND STANDARDS

2

CHAPTER OUTLINE

This chapter discusses regulations and standards. Detailed information to do with industry standards from organizations such as the American Petroleum Institute (API), the International Organization for Standardization (ISO), the American Society of Mechanical Engineers (ASME) and the Institute of Electrical and Electronics Engineers (IEEE). The application of these standards to specific design is discussed in the book *Plant Design and Operations.*

Process Risk and Reliability Management. DOI: http://dx.doi.org/10.1016/B978-0-12-801653-4.00002-3

INTRODUCTION

In Chapter 1, it was noted that the Process Safety Management (PSM) regulations are oriented toward helping managers achieve high levels of safety, environmental performance, and profitability—in other words, they are performance based. Nevertheless PSM regulations do exist, and they have to be addressed. This chapter outlines general regulatory and compliance issues to do with PSM, particularly with regard to the United States OSHA (Occupational Safety & Health Administration) standard.

In principle, there should be no need for external rules and regulations—managers should strive to achieve process safety goals because they provide their own inherent reward. In practice, regulations are needed. Concerns to do with liability do influence behavior. Even in those facilities where management has the best of intentions, there is always the temptation to put off safety and environmental work "until we have time." A regulation will management's feet to fire. If a plant has been running safely for many years, it is tempting to defer the rectification of hazards on the grounds that they have never been a problem in the past. Expenditures to correct these hazards do not lead to an immediate return on investment—they merely make an already low probability number even lower.

Regulations put all companies and facilities on the same basis—those companies which have traditionally invested heavily in safety and environmental improvement are no longer at a short-term financial disadvantage. Regulations also provide a justification for mid-level managers and PSM professionals to carry out those activities that they had always wanted to do, but for which they had had trouble finding the necessary funding. For example, an operations manager may have always wished to increase the amount of training that his operators receive but may have had trouble in justifying the expense. However, if a regulation requires that operator training be carried out, that manager can demand that the training program be funded because it is now a legal requirement.

From a technical point of view, the requirements of various process safety regulations are generally quite similar; if a company develops a PSM program to meet one standard, it is likely that it has gone most of the way toward addressing the others. However, in the regulatory world, there can be very substantial differences between standards in nontechnical areas such as community communication, reporting procedures, and the lists of covered chemicals. For example, the original OSHA and EPA (Environmental Protection Agency) regulations to do with process safety have basically the same technical structure. However, the coverage and reporting requirements vary considerably from one another.

Figure 2.1 shows how regulations, codes, standards, and guidance link to one another. They are shown in descending order of priority: regulations carry more authority than codes, which in turn have more authority than industry consensus standards and professional guidance.

The boundaries between the categories shown in Figure 2.1 are fuzzy—a good deal of overlap exists between them. For example, some regulations incorporate codes and industry standards into their language, thus effectively giving those "voluntary" standards the force of law.

REGULATIONS

The first level in Figure 2.1 is "Regulations." The different types of regulatory strategy are discussed below. Information to do with specific process safety regulations is provided later in this chapter.

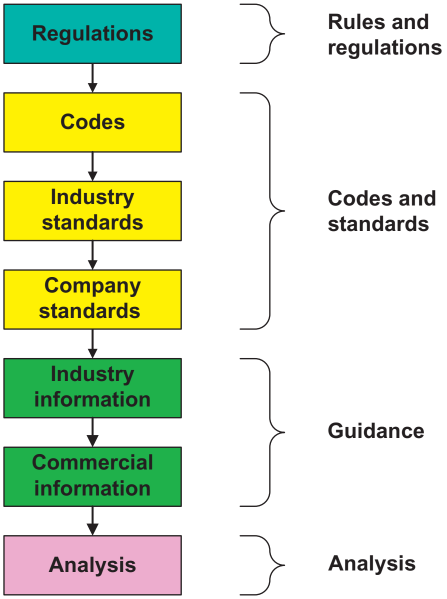


FIGURE 2.1

Rules/codes/guidance.

Figure 2.2 outlines the types of regulatory and compliance strategies that are used in the process industries, along with examples of that particular approach. (In practice, all regulations contain elements of both approaches—however, a sharp distinction between them is made here in order to illustrate the concepts being discussed.)

Regulations are sometimes supplemented by guidance and/or by examples provided by the pertinent regulatory authority. Regulatory guidance does not possess the authority of a regulation or rule; guidance does not have to be followed. In practice, the guidance provided by regulators is often too general in nature to be of much practical benefit in day-to-day situations.

RULE-BASED APPROACH

The left-hand column of Figure 2.2 shows the rule-based approach, which is similar to the prescriptive strategies discussed in Chapter 1. The regulatory agency provides explicit instructions as to what has to be done; then inspectors from the agency check that the rule is being followed. An example of this approach is the American Petroleum Institute (API)'s Recommended Practice (RP) 14C as adopted into law by the Minerals Management Service (MMS) for offshore oil and gas production facilities. Many environmental regulations are rule based. They define exactly how much of a certain chemical can be discharged to the atmosphere or ground water over a certain period of time.

The great advantage of a rule-based system is its simplicity. Everyone involved—the facility's managers, the auditors, and the regulators—knows what is to be done and can readily check to see

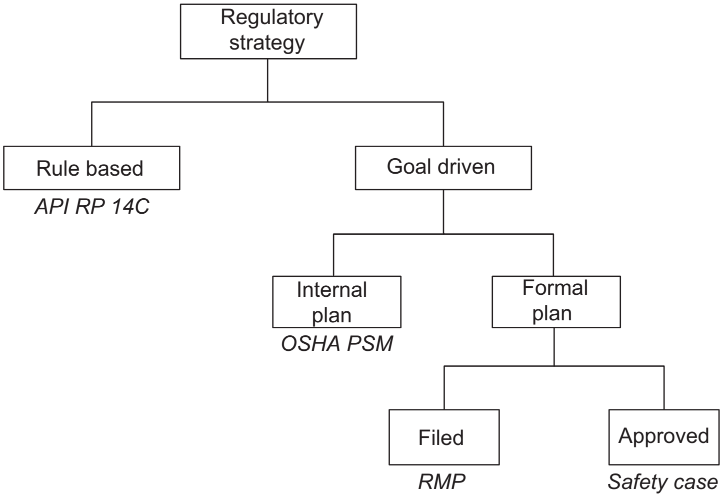


FIGURE 2.2

Regulatory strategies.

if it is being done. For example, a rule may require that handrails must “not be more than 37 in. (94 cm) high nor less than 30 in. (76 cm) from the upper surface of the handrail to the surface of the tread.” It is then quite simple to check all the handrails in the facility to ensure that they meet this rule.

Compliance can also be relatively speedy and economical because the company will often purchase off-the-shelf solutions to address its operational and engineering issues.

GOAL-DRIVEN APPROACH

In the 1970s to the 1980s, it became increasingly evident that the rule-based approach to industrial safety possessed a number of serious limitations. In particular, as industrial processes became increasingly complex, sophisticated regulators find that they lack the knowledge and insights to write and enforce rules that were pertinent to the new technology. Therefore, there was a move toward goal-driven or performance-based standards. Such standards are nonprescriptive in nature.

Nonprescriptive standards provide few specific details as to how a facility is to be designed or operated. These standards rely on management and the company professionals taking the right actions to ensure that process safety goals are met. Such an approach is particularly appropriate when the facility is complex, possesses unique technology, or uses very sophisticated processes. In a nonprescriptive environment, each facility or company develops its own standard for its own operations. The only measure of success is success. If the facility operates cleanly, safely, and profitably, then the standards are effective and vice versa.

Unlike detailed rule-based rules, goal-driven regulations tend to be nonspecific. For example, OSHA’s PSM standard to do with Mechanical Integrity procedures merely states “The employer shall establish and implement written procedures to maintain the ongoing integrity of process equipment." There are no specific requirements regarding the amount of detail or the content of those procedures.

An important benefit of a performance-based approach is that an industry can immediately capture what has been found by experience or test to work well—there is no need for the regulators to catch up with the latest technology (which will have moved on by the time they have done so).

Figure 2.2 shows that a goal-driven approach can be managed with either an internal or a formal plan that can be evaluated and reviewed by external parties. OSHA's process safety standard is an example of an internal plan. Companies are not required to submit anything to OSHA. Only if they are inspected, they will have to share their plans with the regulators.

A formal plan is written according to a format and outline provided by the regulator. In some cases, for example, the EPA's RMP, the plan is filed but no action is taken by the agency. In other cases, e.g., safety cases in the United Kingdom, the plan is not only filed, but it is also approved by the agency (the Health, Safety and Environment (HSE)).

PROCESS SAFETY REGULATIONS

Table 2.1 summarizes the major state and federal process safety regulations in the United States in the chronological order in which they were promulgated.

The first regulation to be applied nationally was the OSHA PSM standard, 29 CFR 1910.119, in 1992. Consequently, it is this standard that has drawn most attention. Its development had started in the late 1980s. During that decade, there had been a number of serious accidents in process plants in the United States. Industry executives from various chemical companies recognized that the introduction of a process safety regulation in the United States was inevitable. Therefore, senior managers from these companies, working with the Organization of Resource Counselors, set about developing standards that would serve both society's and industry's needs. Published in 1988, this

Table 2.1 Process Safety Regulations (United States)

Region	Year	Title
California	1988	Risk Management Prevention Program (RMPP), Assembly Bill 3777 Article 2, Section 25531, et seq. of Chapter 6.95 of the Health and Safety Code
New Jersey	1989	Toxic Catastrophe Prevention Act (TCPA), N.J.S.A. 13:1K-19 et seq.
Delaware	1989	Extremely Hazardous Substances Risk Management, Delaware Code, Title 7, Chapter 77
Nevada	1991	Nevada Senate Bill No. 641
United States and Territories	1992	Process Safety Management of Highly Hazardous Chemicals, Occupational Safety & Health Administration (OSHA), 29 CFR 1910.119
	1996	Risk Management Program (RMP), Environmental Protection Agency (EPA), 40 CFR 68
	2013	Proposed expansion of 29 CFR 1910.119

report was entitled "Recommendations for Process Hazards Management of Substances with Catastrophic Potential." This document served as the basis for API 750 and 29 CFR 1910.119.

One of the most important consequences of having a standard developed by industry was that the resulting regulations were nonprescriptive and performance based. The companies who drafted the standard were trying to avoid the problem of having a large number of lengthy, highly prescriptive, detailed regulations such as are to be found in the environmental and nuclear power businesses. This was important because there is such a wide variety of processes and technologies, and the development of detailed standards for all of them would have been very time consuming and inefficient.

CODES AND STANDARDS

Some years ago, a Process Safety Manager at a large petrochemical facility said "My plant is old but my engineers are young." His statement was not intended as a compliment. He recognized that, although his young engineers were well educated and enthusiastic, they lacked the knowledge and experience that he felt was needed to ensure that the plant ran safely. His particular concern was that the various reduction-in-force programs that companies such as his had undergone meant that valuable engineering experience had been lost and was not being replaced.

One way of overcoming this knowledge and experience gap is through the use of engineering standards. Standards represent a distillation of years of the knowledge and experience of some of the best minds in the area being covered. Therefore, by carefully following the appropriate codes and standards, a facility greatly increases its chances of avoiding an accident.

The International Organization for Standardization (ISO) defines standards as follows:

> Documented agreements containing technical specifications or other precise criteria to be used consistently as rules, guidelines, or definitions of characteristics, to ensure that materials, products, processes and services are fit for their purposes.

ISO also states that standards are developed according to the following principles:

- *Consensus*

  The views of all interests are taken into account: manufacturers, vendors and users, consumer groups, testing laboratories, governments, engineering professions, and research organizations.
- *Industry wide*

  Global solutions to performance based.
- *Voluntary*

  International standardization is market driven and therefore based on voluntary involvement of all interests in the market place.

Standards can be categorized as codes, RPs, or guidance. Codes are generally perceived to be a requirement—often having legal standing. Indeed, the use of codes is frequently mandated by regulators such as the U.S. EPA. Even those standards that are not considered to be codes—such as RPs from the API—are very authoritative and often have considerable standing in a court of law.

Codes and standards are usually prepared by professional bodies such as the ASME (American Society of Mechanical Engineers), the NFPA (National Fire Protection Association), and the API. These organizations generally receive their funding from industrial sponsors, the sale of journals and seminars, and the membership fees of engineers and other technical professionals. Generally, the standards are developed by committees made up of professionals who have many years of experience in the pertinent specialist area.

Regulatory agencies frequently refer to the standards developed by professional societies. However, they cannot delegate rulemaking to an outside nongovernmental agency without review, and without announcing its intention in the Federal Register and allowing the required opportunity for public comment.

Codes and standards provide two important benefits. First, they provide practical guidance to operational integrity professionals. Whereas regulations mostly say that a company *must* do something, standards often provide practical suggestions as to *how* to do it. Hence, design decisions can be made more quickly and efficiently than if the engineers or managers had to work from first principles. A second benefit of codes and standards is that they provide a legal defense in the event that an accident does occur. If a manager or Operational Integrity Management (OIM) professional can demonstrate that he or she conformed to an external professional standard, then he or she has an excellent defense in law.

Codes and standards provide a foundation for most of the design work. Generally, they summarize the knowledge and experience of hundreds of highly experienced engineers and other specialists. Not to use such experience would be foolish (and probably in violation of rules and regulations in many locations).

There are, however, a number of potential drawbacks with regard to the use of engineering standards. These limitations include the following:

- Standards look backward in time. They address technical issues from the past, and so may not be up to date with regard to the latest technology and management systems. Moreover, standards cannot provide guidance for future developments and technologies.
- Standards are generic. They are written for any location, company, and vendor. They may not address site-specific concerns.
- Most standards are developed through a process of consensus. This means that they are likely to provide only minimum acceptable design conditions.

Codes and standards should, therefore, be used to provide a foundation for a safe and reliable design. But their use is not enough—PSM and inherent safety principles should also be applied if the final facility is to meet high standards of safe and reliable operations.

DEVELOPMENT OF A STANDARD

Standards are usually developed by nongovernmental not-for-profit agencies. These agencies have committees that create detailed design, inspection, installation, and operating requirements, often for narrowly defined equipment items such as pressure vessels, instruments, and rotating equipment.

In the United States, standardization work is usually done under the auspices of the American National Standards Institute (ANSI). In its own publication (ANSI, 2005), the organization has this to say about the standardization process.

> . . .the U.S. standardization system reflects a market-driven and highly diversified society. It is a decentralized system that is naturally partitioned into industrial sectors and supported by independent, private sector standards developing organizations (SDOs). It is a demand-driven system in which standards are developed in response to specific concerns and needs expressed by industry, government, and consumers. And it is a voluntary system in which both standards development and implementation are driven by stakeholder needs.

Standardization encompasses a broad range of considerations—from the actual development of a standard to its promulgation, acceptance, and implementation. Also included are the methods of evaluating conformance to a standard—issues such as laboratory accreditation; certification of products, processes, systems, services, and personnel; metrology and measurement; testing and sampling; and more. Standardization has become the key to market access and is inherently essential to a sound national economy and to the facilitation of global commerce.

The costs for developing and implementing a voluntary standard are borne by those who will derive benefit from that document. Certain expenses are borne by the entity responsible for facilitating development of the standard and others by the parties—the subject matter experts and those who employ or support them—who participate in its creation. The end user bears the cost of purchase, if applicable, and assumes responsibility for implementation expenditures. The equitable distribution of expenses incurred during the standardization life cycle helps to mitigate the risk that any single group will attempt to exercise undue influence because it has borne an inordinate share of the expenses.

STANDARDS ORGANIZATIONS

Some of the professional organizations that provide process industry standards are listed in Table 2.2.

A very brief description of some of these organizations is provided below.

American Chemistry Council/Responsible Care®

The American Chemistry Council (ACC) was formally known as the Chemical Manufacturers Association (CMA). It represents the interests of the chemical industry. One of its activities is to research ways to minimize risks to employees and to the environment from chemical facilities. Activities include communicating with the government and the public in the areas of taxation, environmental and workplace safety regulations, and engineering and safety standards.

In the period 1985–1988, the Association launched its Responsible Care® program to improve the industry's responsible management of chemicals. Participation in the initiative, which is based on the work of the Canadian Chemical Producers Association, is a requirement of association membership.

At the heart of the Responsible Care approach to managing risk is an assumption of responsibility by those companies that manufacture and transport hazardous chemicals. Rather than working in isolation from their communities, these companies work with and communicate with everyone who may have a concern to do with the safety and environmental impact of the chemical industry.

Table 2.2 Standards Organizations

Abbreviation	Name
ACC	American Chemistry Council
API	American Petroleum Institute
ANSI	American National Standards Institute
ASCE	American Society of Civil Engineers
ASHRAE	American Society of Heat, Refrigeration, Air Conditioning Engineers
ASME	American Society of Mechanical Engineers
ASTM	American Society of Testing Materials
AWWA	American Water Works Association
AWS	American Welding Society
BOCA	Building Officials & Code Administration
CGA	Compressed Gas Association
GPA	Gas Processors Association
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical, Electronic Engineers
ISA	Instrument Society of America
MSS	Manufacturers Standard Society of Valve & Fittings Industry
NACE	National Association of Corrosion Engineers
NEMA	National Engineers Mechanics Association
PFI	Pipe Fabrication Institute
SSPC	Steel Structures Painting Council
UL	Underwriters Laboratory Standards & Directories

In this context, the “community” includes not just the people who live close to a facility, but also academics, environmentalists, government, and unions.

Responsible Care programs have two components: the first is to strive to improve health, safety, and environmental performance; the second is to allay public fears and concerns regarding the process industries. The need for communication with the public is particularly important because most process companies and facilities do not produce products that are used directly by members of the public—hence these companies are perceived as being remote and irrelevant to peoples’ lives.

Table 2.3, which is derived from a presentation by the Australian Responsible Care industries, shows the “before and after” attitudes by industry toward health and safety issues.

Companies which commit to Responsible Care also agree to work with one another to improve safety. They do this by sharing best practices and developing benchmarks for performance, recognizing that, when it comes to safety, they are not in competition with one another. Indeed, a problem at one facility can sully the reputation of many other facilities and companies, regardless of whether they had anything to do with that problem.

Responsible Care programs are organized around the following six codes:

1. Manufacturing Process Safety
2. Storage and Transport
3. Employee Health and Safety

Table 2.3 Change in Approach Under Responsible Care

Old Ethic	Responsible Care Ethic
Do what the law required	Do the right thing (exceed the law if necessary)
Adopt a low profile	Be seen to do the right thing
Downplay public concerns	Seek out and address public concerns
Assume product innocence	Recognize that the public has a right to know about the products and processes being used
Defensive approach to new regulations	Lead the public policy process
Ignore or fight opponents	Work with opponents and seek their input

4. Environment Protection
5. Community Right to Know
6. Product Stewardship.

In the United States, those companies that have adopted Responsible Care are required to use approved third parties to conduct the certification audits at their headquarters and selected facilities. Companies have the option of being audited against ACC's Responsible Care Management System (RCMS®) Technical Specification or the RC14001 Technical Specification, which contains all of ISO 14001's requirements as well as additional Responsible Care elements.

American National Standards Institute

ANSI has an accredited Standards Developing Organization. This organization reviews procedures for writing standards in many of the standards bodies. For example, ANSI will review and accept the manner in which an organization resolves differences of opinion during the consensus phase of writing a new or revised standard.

American Petroleum Institute

Founded in 1919, the API is the U.S. petroleum industry's primary trade association. Its membership of more than 300 companies consists of a broad cross-section of petroleum and allied industries in exploration, production, transportation, refining, and marketing. The API provides public policy development, advocacy, research, and technical services to enhance the ability of the petroleum industry to fulfill its mission, which includes:

- Meeting the nation's energy needs, developing energy sources, and supplying high quality products and services
- Enhancing the environmental, health, and safety performance of the petroleum industry
- Conducting research to advance petroleum technology, and developing industry equipment and performance standards
- Advocating government decision making to encourage efficient and economic oil and natural gas development, refining, transportation, and use; promoting public understanding of the industry's value to society; and serving as a forum on issues affecting the petroleum industry.

The API has issued a large number of technical RPs, most of which are relevant to those managing PSM and OIM programs. The following are particularly pertinent to process safety:

- RP 75—Development of a Safety and Environmental Management Program for Offshore Operations and Facilities (SEMP)
- RP 76—Contractor Safety Management for Oil and Gas Drilling and Production Operations
- RP 752—Management of Hazards Associated with Location of Process Plant Buildings
- RP 2001—Fire Protection in Refineries
- Std 2217A—Guidelines for Work in Inert Confined Spaces in the Petroleum and Petrochemical Industries
- RP 14C—Analysis, Design, Installation, and Testing of Basic Surface Safety Systems on Offshore Production Platforms
- RP 14G—Fire Prevention and Control on Open Type Offshore Production Platforms
- RP 14J—Design and Hazards Analysis for Offshore Production Facilities.

American Society of Mechanical Engineers

Founded in 1880, the ASME develops standards and test codes through its extensive network of committees (ASME's first code was a boiler test code, published in the year 1884). The association has around 100,000 members. It is run through a Board of Governors that has delegated codes and standards work to a 22-member council. Roughly 4000 engineers, manufacturers, and other interested parties sit on the 120 main committees that work on standards and codes.

ASME allows products that manufactured in conformance with its standards to be stamped with an appropriate seal. A manufacturer first has to have his or her quality management program accepted by an ASME committee. The manufacturer can then certify products that he makes and can stamp them.

Section VIII of the ASME is of particular interest to the process industries because it covers design requirements for pressure vessels. The code consists of three divisions. Division I covers the general requirements for design, materials, and manufacturing of pressure vessels with an operating pressure from 15 to 3000 psig, as well as those operating below atmospheric pressure. Divisions II and III provide alternative rules to reduce the thickness and cost of vessels operating at very high pressure (15–10,000 psig and above 10,000 psig, respectively).

These codes require that a corrosion allowance be provided. The value for the allowance depends on the specific process and vessel.

International Organization for Standardization

The ISO has developed over 17,500 International Standards on a variety of subjects; some 1100 new ISO standards are published every year. Two of the standards—ISO 9000 and ISO 14000—are of particular interest to the process industries.

ISO 9000 is a family of standards for quality management systems. Some of the requirements in ISO 9001 (which is one of the standards in the ISO 9000 family) include the following:

- A set of procedures that cover all key processes in the business
- Monitoring processes to ensure they are effective
- Keeping adequate records
- Checking output for defects with appropriate and corrective action where necessary

- Regularly reviewing individual processes and the quality system itself for effectiveness
- Facilitating continual improvement.

A company or organization that has been independently audited and certified to be in conformance with ISO 9001 may publicly state that it is "ISO 9001 certified" or "ISO 9001 registered." Certification to an ISO 9000 standard does not guarantee the quality of end products and services; rather, it certifies that formalized business processes are being applied. In this regard, ISO 9000 is quite similar to PSM. There are no externally mandated standards; instead, each company has to develop standards that are appropriate for its circumstances. In essence, a company which is implementing ISO 9000 does four things:

- It writes down what it is going to do.
- It trains everybody in the standards that have been set.
- It implements an audit program.
- It suggests means for improving the present operation.

Registration is not a requirement. However, registration does increase an organization's credibility and official standing. This is particularly important for those organizations that deal directly with external customers, regulators, insurance companies, and other external groups. Moreover, there are indications that companies with a registered ISO 14001 system may see benefits if they are required to appear before a federal court for environmental violations.

Although not required, most organizations that choose to register will use third-party registration. Doing so makes it easier to demonstrate that the organization has objectively met the requirements of ISO 14001. If a company chooses self-declaration registration, it is harder to prove that the organization has met the standard's requirements.

ISO 14000 is a development of ISO 9000. It also consists of a set of voluntary standards—with a focus on environmental systems and management. Ultimately, ISO 14000 will incorporate 20 separate standards covering a wide range of topics, including environmental auditing, labeling, and product life cycles.

ISO 14000 does not establish environmental performance requirements or standards. The standard is written for all types of organization in diverse geographical, cultural, and economic settings. Multinational companies with large revenue streams will be able to set higher standards than smaller companies in less developed economies. However, even though the standard is nonprescriptive, its adoption by an organization should lead to an improvement in environmental performance for the following reasons:

- By ensuring that all the departments within an organization adhere to the agreed-upon standard, overall performance is likely to be enhanced.
- Environmental awareness within the organization will be increased.
- Programs must be put into place to address areas of environmental performance that may have been somewhat neglected.
- An organization must commit to continuous improvement in its environmental management system, thus improving environmental performance.

ISO 14001—environmental management systems—is the first in the ISO 14000 series. It covers implementation, monitoring, measurement, corrective action, procedures, standards, and management.

ISO 14001 provides an overall framework for environmental management and integrates that framework within the overall business activity. Features of an ISO 14001 management system include:

- Clear definition of responsibilities
- Documented systems
- Training, both initial and ongoing
- Records management and document control
- Control of critical processes
- Internal audits
- Corrective action
- Management reviews
- Continual improvement.

National Fire Protection Association

The NFPA publishes a wide range of codes and standards to do with the prevention and response to fires and explosions. Some of their codes that are particularly important to the process industries include the following:

- NFPA 54—National Fuel Gas Code
- NFPA 58—Liquefied Petroleum Gas Code
- NFPA 70—National Electrical Code
- NFPA 110—Standard for Emergency and Standby Power Systems
- NFPA 497—Recommended Practice for the Classification of Flammable Liquids, Gases, or Vapors and of Hazardous (Classified) Locations for Electrical Installations in Chemical Process Areas
- NFPA 921—Guide for Fire and Explosion Investigations
- NFPA 1600—Standard on Disaster/Emergency Management and Business Continuity Programs.

OTHER INDUSTRY SOURCES

In addition to the standards bodies described above, there are also various agencies and government bodies that provide information and guidance that can be used by the process risk professional. They include the Chemical Safety and Hazard Investigation Board and the Center for Offshore Safety (COS).

Center for Chemical Process Safety

The Center for Chemical Process Safety (CCPS) is a directorate of the American Institute of Chemical Engineers (AIChE). The CCPS, which is sponsored by approximately 80 companies in the process industries, was established in 1985 in response to a number of catastrophic incidents that had occurred prior to that time. The CCPS aims to improve process safety by publishing books, organizing conferences, conducting classes, and sponsoring research. The CCPS is probably best known through its very extensive list of books to do with process safety and the journal *Process Safety Progress*.

Center for Offshore Safety

The *Report to the President* concerning the Deepwater Horizon catastrophe discussed the creation of an industry-sponsored agency analogous to the nuclear industry's independent Institute of Nuclear Power Operations (INPO) that was created in the wake of the Three Mile Island event. The President's Commission to do with that event said the following.

> [T]he nuclear industry must dramatically change its attitudes toward safety and regulations. The Commission has recommended that the new regulatory agency prescribe strict standards. At the same time. . .the industry must also set and police its own standards of excellence to ensure the effective management and safe operation of nuclear power plants.

Given this background, the API created the COS following Deepwater Horizon. The intent is that the center will supplement and complement formal regulations, and would have a relationship to Bureau of Safety and Environmental Enforcement (BSEE) and the other agencies analogous to that between INPO and the Nuclear Regulatory Commission.

The COS started with a focus on Gulf of Mexico SEMS (Safety and Environmental Management System) audits. Longer-term goals are to add activities such as determining the leading causes of incidents.

Chemical Safety and Hazard Investigation Board

The Clean Air Act (1992) required that a five-member Chemical Safety and Hazard Investigation Board be established. Members would be appointed based on their technical knowledge of safety, engineering, and environmental issues. This Board was not created when the Act was passed, largely due to funding limitations, but it was revived in late 1997.

The board has legal authority to investigate incidents, but its remit is limited to finding out what happened, and to helping ensure that lessons learned are spread across the process industries.

COMPANY STANDARDS

In addition to the publicly available standards provided by professional bodies, many of the larger companies have their own internal standards. Generally, these internal standards are based on public standards but have additional requirements—often to do with specific aspects of their own processes or operations. For example, if a company manufactures a unique and proprietary chemical, management may need to create standards to do with the safe handling of that chemical, since little information is likely to be available in the public domain.

Sometimes, however, company standards can be more of a hindrance than a help. With some companies, every time there is an accident or near-miss associated with a piece of equipment, the company writes a standard to make sure that this particular problem cannot recur. Eventually, after many years, they find that they have painted themselves into a corner, and they have trouble buying equipment off the shelf—too many situations require custom-designed equipment. Consequently, costs rise, delivery times are extended, and it is not always clear that safety is actually improved. This phenomenon is sometimes referred to as "gold plating."

The use of unnecessarily rigorous standards can be a particular problem for those facilities which operate low hazard processes, but they are subsidiaries of larger companies which have developed corporate-wide standards intended to address much tougher situations.

INDUSTRY INFORMATION

Professional guidance, shown in Figure 2.1, is provided by regulators, industry experts, and by the manufacturers of specialized equipment. Facility management and PSM professionals are not required to follow such guidance, but doing so often helps them achieve high levels of performance within the budget and schedule constraints.

REGULATORY GUIDANCE

Guidance can come from the background material associated with regulations, from experts in the field, and from manufacturers and vendors. It is available in many forms such as books, papers, articles, web sites, and consulting services. Such guidance may not be as authoritative as codes and standards; nevertheless it can be very helpful, practical, and topical. Information from equipment manufacturers and vendors has an obvious commercial bias. However, this bias does not mean that the information is necessarily suspect, or that it should not be used. If a company that has been making a product such as relief valves issues a bulletin on the design and operation of relief valves, then the information provided will probably be useful and topical. Naturally, the manufacturing company will highlight the features and benefits of its own products, but that does not mean that the advice it provides is not useful.

OPEN LITERATURE

Much literature is published on all aspects of engineering design. Many of the articles, papers, and books that are published are of high quality and are authoritative. Frequently, the author has had many years of experience in an area and uses the publication to share his or her knowledge with his professional colleagues—particularly the younger ones who are entering the profession.

There are two types of professional publication. The first is written and published by people representing professional societies and organizations. Many of the professional societies publish books and booklets that fall into this category. These publications are typically very authoritative because the reputation and integrity of a professional society stands behind them. However, this authority does mean that the publications will tend to avoid controversial or difficult issues because this could put the organization on one side or another. This is particularly the case if the publication is being written by a committee of people from different companies. Since the people from each company may have different points of view, there is a danger that the final document could be bland and insufficiently specific to help people working in the field.

The second type of publication is one that is published by an individual author. Because such publications do not have to carry the responsibility of representing a professional organization, the authors are often more willing to state opinions and to put forward points of view that may be debatable, or even controversial. This does not mean that the authors are being irresponsible—it merely means that they are stating their opinion.

COMMERCIAL INFORMATION

A wealth of information to do with safety is available from companies that manufacture and sell chemicals and equipment. Naturally, this information tends to have a commercial bias; however, this bias does not mean that it is inaccurate or unprofessional. Indeed, companies who work in a particular area are often extremely knowledgeable about the issues involved. Furthermore, they are very interested in making sure that their products are used safely; an accident could seriously hurt their reputation and possibly expose them to legal action.

ANALYSIS

Sometimes analytical techniques can be used to show compliance. For example, ASME Section VIII Division 1 details the requirements for pressure vessel design. If a designer using a finite element program is able to demonstrate that a reduced wall thickness provides the same level of safety as is built into the code then his design may be acceptable. Another example may be the use of calculations showing that a safety instrumented system has such high integrity that it may be possible to operate a pressure vessel without a mechanically operated safety relief valve.

UNITED STATES FEDERAL REGULATIONS

A brief overview of how laws and regulations in the United States are written, interpreted, and enforced is provided here.

THE REGULATORY PROCESS

In the United States, the federal regulatory process starts when both Houses of Congress develop a law or statute. Generally, each House develops its own version. These are then sent to committee, where a compromise bill is agreed upon. This, in turn, goes to the President, who signs it (unless he chooses to use his power of veto).

With regard to process safety, the statute that provides the basis for both OSHA's PSM program and the EPA Risk Management Program (RMP) is the Amendments to the Clean Air Act, P.L. 101-549, signed into law by President Bush on November 15, 1990. This statute contains seven separate titles covering a wide range of regulatory programs. The risk management provisions are to be found under Title III (Hazardous Air Pollutants), part c (Accidental Chemical Releases). They are sometimes referred to as a Chemical Accident Release Prevention (CARP) programs. Statutes specify which agencies are to interpret and enforce their provisions. The Clean Air Act statute required OSHA to implement its requirements with regard to worker safety and the EPA for public safety.

Once a statute becomes law, the affected agencies must develop specific regulations from it. It is the regulation, not the law itself, that companies are expected to follow. (OSHA uses the word "regulation" whereas the EPA uses the word "rule." The two words are used synonymously in this chapter.)

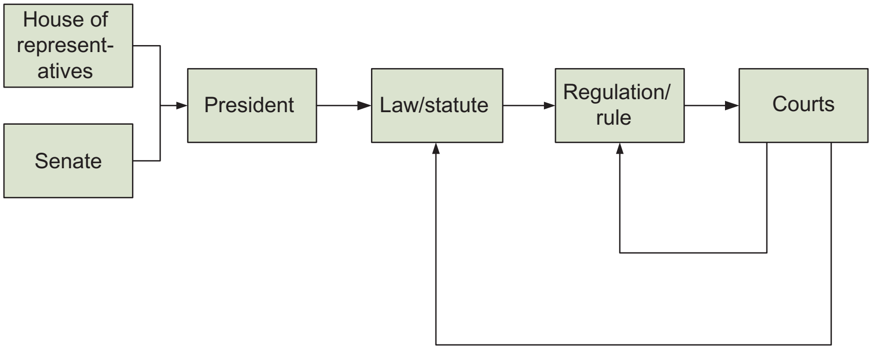


FIGURE 2.3

The regulatory process.

The agencies may also develop *standards*, which are more oriented toward technical issues. Regulations require less scientific and economic data than standards. A regulation is more difficult for a federal court to set aside.

When an agency has finished writing a regulation, it is listed in the Code of Federal Regulations (CFR) and indexed in the Federal Register (a daily publication of all federal government communications). The public and other interested parties are then invited to comment on this draft regulation. This is usually done by mail and at public hearings. The hearings are held in Washington, DC, and in other cities where the proposed regulation is likely to have a major impact.

At the conclusion of the hearings, all the comments are placed in a public docket. The reviewers consider these comments during the preparation of the final regulation, which is eventually published in the Federal Register. There is then a period of 3–6 months during which the first draft of the final regulation can be challenged in court. (This happened when OSHA introduced the PSM standard. The United Steelworkers of America and other labor unions challenged those parts of the regulation that covered contract workers. Also, some changes were made based on comments from organizations such as the CMA and the Dow Chemical Company.)

Following the implementation of a standard, the agency can modify it through Letters of Interpretation. However, there is a distinction between interpretation and making a new rule, and the agency must be careful not to indulge inadvertent rulemaking via the interpretation process.

If a person or organization disagrees with some part of the regulation, they can challenge it in court on the grounds that it does not meet the intent of the original Congressional statute. If the court agrees, the standard is implicitly changed.

The regulatory process is illustrated in Figure 2.3.

CODE OF FEDERAL REGULATIONS

Federal Regulations are listed in the CFR. The CFR is divided into numeric Titles; the pertinent Title in the case of PSM is 29, which covers Labor. Title 29 is further divided into Parts, numbered from 1900 to 1910; part 1910 covers PSM. The parts are subdivided and identified with suffix numbers. The number 119 covers the "PSM" standard. Therefore, the OSHA Standard is identified as CFR 29 1910.119. The sections of each Part are also grouped under letters. In this case, the letter "H" is the one that is used, signifying Hazardous Materials. These subpart letters are often not used; however, if they are, then the full title of this regulation is CFR 29 Subpart H 1910.119.

GENERAL DUTY CLAUSES

Both the OSHA and EPA statutes contain General Duty Clauses that can be used to cover situations not explicitly identified by the regulations, but which nevertheless, in the judgment of the agency, fall within its purview. The General Duty Clause can only be applied if the agency can demonstrate that the citation involved is a "recognized hazard" and that the hazard could cause death or serious physical harm.

One application of the General Duty clause with respect to process safety occurred following a serious accident in April 1995 at a plant in Lodi, NJ. None of the chemicals involved in the accident were on the OSHA list of highly hazardous materials. OSHA's citations, therefore, were based on the General Duty clause. (Since then, the chemicals involved in that accident have been incorporated into the standard.)

THE TENTH AMENDMENT TO THE UNITED STATES CONSTITUTION

When discussing regulations in the United States, it is important to consider the implications of the Tenth Amendment to the Constitution, which reads as follows:

> The powers not delegated to the United States by the Constitution, nor prohibited by it to the states, are reserved to the states respectively, or to the people.

This amendment is one of the foundations of the federal form of government. With respect to process safety, it means that any state has the right to promulgate its own standards as long as those standards are at least as stringent as the federal regulation. As long as this condition is met, the state regulation takes precedence over the federal regulation. This is explained in the OSHA Instruction CPL 2-2.45A CH-1, dated September 13, 1994, which reads:

> If the State adopts an alternative to Federal enforcement inspection procedures, the State's plan must identify and provide a rationale for all substantial differences from Federal procedures in order for OSHA to judge whether a different State procedure is as effective as the comparable procedure.

California is one state that chose to develop its own version of 29 CFR 1910.119. Their program, which is administered by CAL OSHA, was challenged by federal OSHA as being less rigorous than the federal standard. Implementation of the California standards was then blocked until they had been brought up to the level of the federal regulation.

States can also enact their own regulations. The various State PSM regulations are described later in this chapter.

THE EPA

The U.S. EPA is charged by Congress to protect the nation's land, air, and water systems. The EPA works in partnership with state, county, municipal, and tribal governments to carry out its mission. As with OSHA, State and local standards may implement their own rules as long as they exceed federal standards, but they cannot be less stringent.

The EPA administers 11 comprehensive environmental protection laws:

1. Clean Air Act
2. Clean Water Act
3. Safe Drinking Water Act
4. Comprehensive Environmental Response, Compensation, and Liability Act ("Superfund")
5. Resource Conservation and Recovery Act
6. Federal Insecticide, Fungicide, and Rodenticide Act
7. Toxic Substances Control Act
8. Uranium Mill Tailings Radiation Control Act
9. Lead Contamination Control Act
10. Ocean Dumping Ban Act
11. National Environmental Education Act.

The Clean Air Act is the one that covers process safety. The pertinent rule is referred to as the Risk Management Program and is administered by the Chemical Emergency Preparedness and Prevention Office (CEPPO), the EPA office that administers the Risk Management Plan (RMP).

THE OCCUPATIONAL SAFETY & HEALTH ADMINISTRATION

OSHA was formed in the year 1971 under the Nixon administration to provide and administer standards for safety and health in the workplace. Its jurisdiction covers the United States, Puerto Rico, and federally administered territories. OSHA's mandate is restricted to the workplace. Public safety and health is the responsibility of the EPA.

It is estimated that there are about 6000 injury deaths, 50,000 illness-related deaths, and 7 million nonfatal injuries each year in industries within the United States. OSHA's goal is to reduce the number of these accidents by taking the following actions:

- Encourage employers and employees to reduce workplace hazards and to implement new or improve existing safety and health programs
- Provide for research in occupational safety and health so as to develop innovative ways of dealing with occupational safety and health problems
- Establish "separate but dependent responsibilities and rights" for employers and employees for the achievement of better safety and health conditions
- Maintain a reporting and record keeping system to monitor job-related injuries and illnesses
- Establish training programs to increase the number and competence of occupational safety and health personnel

- Develop mandatory job safety and health standards and enforce them effectively
- Provide for the development, analysis, evaluation, and approval of state occupational safety and health programs.

The agency has approximately 800 federal and 1000 state compliance officers for all of the regulations that they administer—process safety is just a small part of the overall effort. These are not large numbers given the scope of their responsibilities. Therefore, with respect to the process safety standard, it is unlikely that a company will be inspected unless there has been an accident or unless someone complains of an unsafe condition.

One of the consequences of the Texas City explosion that occurred in 2005 is that OSHA came under criticism for not conducting inspections of refineries thoroughly enough or frequently enough. In response to this criticism, OSHA has implemented a National Emphasis Program (NEP) for refineries. The agency has since expanded this program to cover chemical plants.

OSHA INSPECTIONS

OSHA has its own protocol for inspections (Instruction CPL 2-2.45A). It is based on the Program-Quality-Verification (PQV) inspection method.

Each company should establish working guidelines as to how to work with regulators from agencies such as OSHA and the EPA during an inspection. These guidelines will involve issues such as:

1. How to react to an unexpected visit from an inspector
2. How to present the PSM documentation
3. How to respond to citations.

In all these cases, the guidance must be developed in conjunction with the company's own attorneys.

OSHA inspections or audits are typically divided into five parts:

1. Kick-Off Meeting
2. Plant Tour
3. Records Review
4. On-Site Inspection
5. Interviews.

At the kick-off meeting, the inspector will provide the employer with a copy of the standard and a letter notifying the employer that the facility is covered by the standard. The inspector, or Compliance Safety and Health Officer (CSHO), must have received the appropriate OSHA training. During the meeting, the CSHO must explain the purpose of the visit and which parts of the plant are to be inspected.

The inspection will usually start with a plant tour, during which the inspector will obtain a general overview of the facility and its operations. During this tour, a management representative may accompany the inspector (unless he or she wishes to speak to an employee privately). At the conclusion of the tour, the OSHA officer must inform the plant management of any violations found, along with a statement as to how much time is to be allowed for correction.

The inspector will ask to see documentation for each of the elements of the standard. He or she will probably also ask for copies of the OSHA 300 logs for the past 3 years. The inspector will want information from both the facility owner and from the management of any contractors that are on site.

During the visit, the OSHA inspector will take notes, collect information, and take pictures. It is perfectly in order for a representative of the company to take a matching set of notes and pictures in the event that there should be a dispute with OSHA's findings. Also, employees have a right to have one of their representatives present during an inspection tour. If there is a union, it will select the person; otherwise the employees will have to find some other way of finding a representative. This person cannot be appointed by management.

Variances

Should a company be unable to meet the requirements of an OSHA regulation, it can apply for a variance. The basis for this can be "shortage of materials, equipment or professional or technical personnel." A variance can also be applied for if the company's existing practices are "at least as effective as that required by OSHA."

With regard to the PSM standard, companies will sometimes apply for a temporary variance. This is similar to the full variance except that the company acknowledges that they fully intend to comply, but they need more time. In such cases, "Employers must demonstrate to OSHA that they are taking all available steps to safeguard employees in the meantime. . . ." This was particularly important for PSM because so many of the elements were in full force as soon as the standard was enacted in 1992; there was no grace period. Companies frequently found that they did in fact need time to get many of the elements up to speed. Variances allowed them to do so.

Temporary variances will not normally be given for a period of more than 1 year, and they cannot be renewed more than twice. Also, "the temporary variance will not be granted to an employer who simply cannot afford to pay for the necessary alterations, equipment, or personnel."

Enforcement

Associated with each citation is a proposed penalty. If the employer chooses to contest the alleged violations or proposed penalties, they first discuss it with the agency at a conference. If that does not lead to a solution, the case can be presented to an independent Occupational Safety and Health Review Commission (OSHRC).

Many environmental and safety regulations carry criminal liability provisions. This means that a person who breaks the law can be prosecuted under the criminal code. Furthermore, if anyone else approved of that act, or failed to stop it, knowing that a violation was taking place, then that person is also liable to criminal prosecution. In addition, a corporate officer can be held vicariously liable for the conduct of a subordinate employee. This also applies if that officer deliberately screens himself so as not to hear the facts. It is important that plant personnel know the seriousness of the regulations and the consequences of noncompliance.

Examination of the records of citations shows that, in many cases, the size of the fine is small as compared to the overall economics of the companies affected. However, the simple fact of being cited can be very detrimental to the reputations of those involved. In the broader context of law enforcement, people who are basically law abiding are deterred from doing something wrong not so much by the fear of punishment, but by the fear of getting caught. In the case of PSM, managers may be more concerned with the career implications of having their facility cited than they are with the magnitude of the fines themselves.

THE ENTRY PROCESS

The Fourth Amendment to the Constitution of the United States guarantees “the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures. . .and (that) no warrants shall issue, but upon probable cause. . ..” This protection applies to businesses also. The Supreme Court has stated that “The businessman, like the occupant of a residence, has a constitutional right to go about his business free from unreasonable official entries upon his private commercial property.” In spite of these fundamental protections, it has been noted that the laws and regulations to do with environmental and safety issues are now so strict that “. . .in some cases, legitimate businesses are being provided less constitutional protection than violent criminals.”

Strictly speaking, an OSHA inspector cannot enter a facility to conduct an inspection without having a warrant. In practice, common sense and common courtesy dictate that, should an inspector show up unannounced and without a warrant, it is appropriate to allow them into the facility (once they have presented their official identification, which should include a number to call so that the facility knows that the visit is authentic). It has been reported that those companies that deny entry receive nearly twice as many citations as those that do not. Furthermore, the average penalty is twice as large. A reason for this may simply be that those companies who deny entry initially may have more problems to hide than those which are more open. Nevertheless, it does suggest that cooperation with inspectors is effective.

Even when the inspector does have a warrant, it is possible to challenge the basis on which that warrant was obtained. These are decisions that should be handled by the company’s attorneys.

It is illegal for anyone to notify an employer that an OSHA audit is to be carried out.

The reasons for entry that OSHA uses include the following:

- A fatality or multiple serious injuries (discussed below).
- They are reasonably certain that a condition or situation exists that could cause death or serious injury before normal enforcement procedures would prevent it.
- If an employee believes that there is an imminent hazard, he or she may ask for an OSHA inspection. OSHA is not obliged to respond to such requests; it will use judgment as to which to follow up, thereby allowing them to avoid vindictive or trivial complaints.
- They may target specific industries which have been identified as having the potential for serious problems.
- Follow up to check on progress from a previous citation.

Fatality/Catastrophe

If a facility has a fatality or five or more people have been hospitalized, OSHA will conduct an investigation. Such investigations, often referred to as FAT/CAT, are performed when a very serious accident has occurred. The event must also be reported to the nearest OSHA office within 48 hours.

Programmed Inspections

Programmed inspections are planned at the beginning of the year by the OSHA regional offices. OSHA attempts to develop objective criteria for its choice of facilities to inspect so as to justify the warrant-application process.

Complaints

If a worker complains about unsafe conditions, the agency may follow up with an inspection. Although complaints are an important source of information about unsafe conditions, they can be used by workers merely to express general grievances against management. It is estimated that about 20% of all OSHA inspections are in response to a complaint, but that many of these—about 30%—do not result in a citation.

CITATIONS

If the OSHA inspector believes that a violation of the standard has taken place, he or she may choose to issue one or more citations. (Management then has to decide whether or not to challenge the citation.)

Associated with each citation is a proposed penalty. If the employer chooses to contest the alleged violations or proposed penalties, they first discuss it with the agency at a conference. If that does not lead to a solution, the case can be presented to an independent OSHRC, which is independent of both OSHA and the Department of Labor. It employs Administrative Law Judges (ALJs) to decide on disputed citations and penalties. There are also appeal levels above the individual ALJ.

Some companies choose to challenge citations even when the proposed fine is small. There are two reasons for this. First, there is a chance that the citation will be rejected. Up to 80% of citations have been rejected on the grounds that it contained an error that invalidated them. The second reason for challenging a citation is that it is important not to build up a record of incidents because each subsequent incident will lead to increasingly heavy fines. If, for example, a company is cited for a deficiency and a $5000 fine is proposed, they might decide to accept it on the grounds that it is not worth the cost of fighting. However, if there is a second citation and the first one is on the record, then the second citation might go to $50,000.

Not all managers agree with this approach to regulatory citations. Some feel that the time and effort spent battling the citations could be better spent on getting on with business and improving safety. Therefore, they choose to settle with the agency as quickly as possible so as to minimize the distraction caused by the dispute.

The categories of possible citation are described below.

Willful

Willful violations are defined by OSHA as follows:

> Willful violations are those committed with an intentional disregard of, or plain indifference to, the requirements of the Occupational Safety and Health Act and OSHA regulations.

OSHA must generally demonstrate that the employer knew about the facts of the cited condition and knew that the regulation required that action be taken. The essential point is that a willful violation is based not on what was done, but on being aware that a standard existed, and then choosing not to follow it. It is not considered a willful violation if the employer, in good faith, misinterprets the law or has a genuine dispute over the meaning of the law.

Since it can be difficult for OSHA to know whether an employer was deliberately ignoring a standard, or simply made an honest mistake, repeat violations of the same standard for which citations had already been issued is a strong indicator of a willful action (Vincoli, 1997).

Companies will usually go to considerable trouble to have willful violations downgraded to "serious" or less. Not only does a willful citation indicate a significant failure in management standards, it can also be used by plaintiffs in civil litigation to support their claims for high payment, and the employer may be criminally liable if someone dies.

The following are issues that could cause a citation to be willful.

1. Lack of effort

   A person did not follow the regulation simply because he or she could not be bothered to make the effort—particularly if they judged that the violation was only minor. What they fail to realize is that a willful citation depends not on the seriousness of the safety situation, but on knowledge of the regulation. Even if the violation itself is minor, if the employee knew of the regulation, it is still a willful act.
2. Paperwork

   Related to the above, an employee may take the correct steps to meet the requirements of a regulation, but fail to document the work properly. For example, an employee may develop a temporary operating procedure and discuss it with the operators. However, if it is not written down, it could generate a willful citation.
3. Time pressures

   If an employee is under pressure to complete a task in order to make a production target, he or she may be tempted to short circuit the regulatory process.
4. Concern over consequences

   Finally, an employee may choose to avoid addressing a regulatory requirement because he or she suspects that the regulation may not allow the desired action to be carried out. For example, an employee may decide to use a different model of gasket in a piping service without going through Management of Change (MOC) or a Mechanical Integrity review because he or she recognizes that the new gasket may not be allowed in this service.

In summary, if an employer or one of his employees chooses not to comply with an OSHA regulation, OSHA has grounds for a willful violation. Intent is not a factor.

Serious

A serious violation is one where there is a substantial probability that death or serious injury could result from the cited condition, and the employer either knew about, or should have known, about this condition. OSHA's definition is as follows:

> A serious violation is defined as one in which there is a substantial probability that death or serious physical harm could result, and the employer knew or should have known of the hazard.

Other-than-Serious

An Other-than-Serious violation is used when the hazard does not present a substantial probability of death or serious physical injury. This level of citation is not likely to be used with regard to PSM because according to OSHA, "Any violation of the PSM standard. . .is a condition which could result in death or serious physical harm to employees. Accordingly, violations of the PSM standard shall not normally be classified as 'other-than-serious'" (CPL 2-2.45A).

Repeat and Failure-to-Abate

A repeat violation is one that occurs more than once and that is noted on two separate inspections. OSHA's definition is as follows:

> Repeat violations are those in which an employer has previously been cited within the last three years for the same, or a substantially similar, violation and which has become a final order and not under contest.

Failure-to-Abate is similar to the Repeat citation, in that an employer has failed to correct a condition that was previously cited.

OSHA STANDARDS

Other regulations from other agencies are sometimes part of a process safety program. For example, with regard to docking facilities for ships and barges, OSHA normally covers the dock area and the dock employees. The Coast Guard normally covers the ship and the ship employees. Truck and rail safety is covered by various Department of Transportation (DOT) regulations. Sometimes, it is difficult to determine who has jurisdiction over what.

A brief overview of the way in which OSHA standards are structured is provided below. The PSM standard—29 CFR 1910.119—is used as an example. The system of headings and subheadings that OSHA uses within a standard is as follows:

Level 1—(a)
Level 2—(1)
Level 3—(i)
Level 4—(A)
Level 5—{1}.

Many parts of the PSM regulation refer to other OSHA standards. For example, the Emergency Planning & Response element basically requires that 29 CFR 1910.38—Emergency Plans and Fire Prevention—be properly implemented. Other related standards include 1910.147 (Lockout/Tagout) and 1910.165 (Employee Alarm Systems). Even when it is not necessary to follow them, these standards can still provide good general guidance.

Part 29

Regulations in the Federal Register are located in "Parts." Almost all OSHA regulations are in Part 29, hence they usually start with the term 29 CFR, meaning Part 29 of the CFR. Each part is then subdivided by number. Table 2.4 shows how Part 29 is divided. Process safety falls under 1910: Occupational Safety and Health Standards. Therefore, the regulations in this area have the prefix 29 CFR 1910.

Subparts of Part 29

Each part of the regulation is divided into Subparts, which are identified by letters. The Subparts for 29 CFR 1910 are shown in Table 2.5. Process safety is 29 CFR 1910 Subpart H—Hazardous Materials.

Table 2.4 Parts of 29 CFR

Part 70	Production or Disclosure of Information or Materials
Part 70a	Protection of Individual Privacy in Records
Part 1900	Reserved
Part 1901	Procedures for State Agreements
Part 1902	State Plans for the Development and Enforcement of State Standards
Part 1903	Inspections, Citations, and Proposed Penalties
Part 1904	Recording and Reporting Occupational Injuries and Illness
Part 1905	Rules of Practice
Part 1906	Administration Witness and Documentation in Private Litigation
Part 1908	Consultation Agreements
Part 1910	Occupational Safety and Health Standards
Part 1911	Rules of Procedure for Promulgating, Modifying, or Revoking OSHA Standards
Part 1912	Advisory Committees on Standards
Part 1912a	National Advisory Committee on OSHA
Part 1913	Rules Concerning OSHA Access to Employee Medical Records
Part 1915	Occupational Safety and Health Standards for Shipyard Employment
Part 1917	Marine Terminal
Part 1918	Safety and Health Regulations for Longshoring
Part 1919	Gear Certification
Part 1920	Procedure for Variations under Longshoremen's Act
Part 1921	Rules of Practice in Enforcement under Section 41 of Longshoremen's Act
Part 1922	Investigative Hearings under Section 41 of Longshoremen's Act
Part 1924	Safety Standards Applicable to Workshops and Rehab. Facilities
Part 1925	Safety and Health Standards for Federal Service Contracts
Part 1926	Safety and Health Regulations for Construction
Part 1927	Reserved
Part 1928	Occupational Safety and Health Standards for Agriculture
Part 1949	Office of Training and Education, OSHA
Part 1950	Development and Planning Grants for Occupational Safety and Health
Part 1951	Grants for Implementing Approved State Plans
Part 1952	Approved State Plans for Enforcement of State Standards
Part 1953	Changes to State Plans for Development and Enforcement
Part 1954	Procedures for the Evaluation and Monitoring of Approved State Plans
Part 1955	Procedures for Withdrawal of Approval of State Plans
Part 1956	Plans for State and Local Government Employees without Approved Plans
Part 1960	Basic Program Elements for Federal Employees OSHA
Part 1975	Coverage of Employees under the Williams-Steiger OSHA 1970
Part 1977	Discrimination against Employees under OSHA Act of 1970
Part 1978	Rules for Implementing Section 405 of the STAA of 1982
Part 1990	Identification, Classification, and Regulation of Carcinogens
Part 2200	Rules of Procedure

Table 2.5 Subparts of 29 CFR Part 1910

1910 Subpart A—General (1910.1–1910.8)
1910 Subpart B—Adoption and Extension of Established Federal Standards (1910.11–1910.19)
1910 Subpart C—General Safety and Health Provisions (1910.20–1910.20 App B)
1910 Subpart D—Walking–Working Surfaces (1910.21–1910.32)
1910 Subpart E—Means of Egress (1910.35–1910.40)
1910 Subpart F—Powered Platforms, Manlifts, and Vehicle-Mounted Work Platforms (1910.66–1910.70)
1910 Subpart G—Occupational Health and Environmental Control (1910.94–1910.100)
1910 Subpart H—Hazardous Materials (1910.101–1910.120 App E)
1910 Subpart I—Personal Protective Equipment (1910.132–1910.140)
1910 Subpart J—General Environmental Controls (1910.141–1910.150)
1910 Subpart K—Medical and First Aid (1910.151–1910.153)
1910 Subpart L—Fire Protection—Other Fire Protection Systems (1910.155–1910.165)
1910 Subpart M—Compressed Gas and Compressed Air Equipment (1910.166–1910.171)
1910 Subpart N—Materials Handling and Storage (1910.176–1910.190)
1910 Subpart O—Machinery and Machine Guarding (1910.211–1910.222)
1910 Subpart P—Hand and Portable Powered Tools and Other Handheld Equipment (1910.241–1910.247)
1910 Subpart Q—Welding, Cutting, and Brazing (1910.251–1910.257)
1910 Subpart R—Special Industries (1910.261–1910.275)
1910 Subpart S—Electrical—Definitions (1910.301–1910.399)
1910 Subpart T—Commercial Diving Operations—Recordkeeping (1910.401–1910.441)
1910 Subpart U—[Reserved] (1910 Subpart U)
1910 Subpart V—[Reserved] (1910 Subpart V)
1910 Subpart W—[Reserved] (1910 Subpart W)
1910 Subpart X—[Reserved] (1910 Subpart X)
1910 Subpart Y—[Reserved] (1910 Subpart Y)
1910 Subpart Z—Toxic and Hazardous Substances (1910.1000–1910.1500)

Sections of Subparts

Subparts are divided using numbers. Subpart H is divided into the range 101–120. The title for each of these is shown in Table 2.6. Process safety is 119. Therefore, the full title of the OSHA PSM standard is 29 CFR Subpart H 1910.119, often abbreviated to 29 CFR 1910.119, or even just 1910.119.

INTERPRETATIONS AND GUIDANCE

Once a regulation is in force, it is constantly being tested, interpreted, and challenged by specific cases that are borderline in some manner, and that were not anticipated when the regulation was written. Typically, there are two principal sources of information regarding updates: OSHA Letters of Interpretation and the findings of Courts who have jurisdiction over process safety.

In response to questions from the regulated community and from members of the public, Letters of Interpretation expand on, and amplify, the meaning and intent of the regulation.

Table 2.6 29 CFR Part 1910

1910 Subpart H—Authority for 1910 Subpart H
1910.101—Compressed gases (general requirements)
1910.102—Acetylene
1910.103—Hydrogen
1910.104—Oxygen
1910.105—Nitrous oxide
1910.106—Flammable and combustible liquids
1910.107—Spray finishing using flammable and combustible materials
1910.108—Dip tanks containing flammable or combustible liquids
1910.109—Explosives and blasting agents
1910.110—Storage and handling of liquefied petroleum gases
1910.111—Storage and handling of anhydrous ammonia
1910.112—[Reserved]
1910.113—[Reserved]
1910.114—Effective dates
1910.115—Sources of standards
1910.116—Standards organizations
1910.119—Process safety management of highly hazardous chemicals
1910.119 App A—List of highly hazardous chemicals, toxics and reactives (mandatory)
1910.119 App B—Block flow diagram and simplified process flow diagram (nonmandatory)
1910.119 App C—Compliance guidelines and recommendations for process safety management (nonmandatory)
1910.119 App D—Sources of further information (nonmandatory)
1910.120—Hazardous waste operations and emergency response
1910.120 App A—Personal protective equipment test methods
1910.120 App B—General description and discussion of the levels of protection and protective gear
1910.120 App C—Compliance guidelines
1910.120 App D—References
1910.120 App E—Training curriculum guidelines (nonmandatory)

However, since they have not been incorporated into the regulation itself through an Act of Congress, these letters do not have the force of law behind them. Nor does conforming to their suggestions necessarily create a defense in law. For this reason, OSHA puts the following preamble before the Letters of Interpretation that it issues.

> This Safety and Health Information Bulletin is not a standard or regulation, and it creates no new legal obligations. It is advisory in nature, informational in content, and is intended to assist employers in providing a safe and healthful workplace…

Whenever OSHA wishes to publicize an interpretation, it will often publish a letter at its web site, often written in response to a specific question from a company or individual.

THE OSHA PSM STANDARD

Information to do with the OSHA PSM standard (29 CFR 1910.119) is provided in this section.

COVERED PROCESSES

The rules for determining which facilities are covered by 29 CFR 1910.119 are shown in Table 2.7 (some of the nontechnical details have been omitted, and it should be noted that the list of covered chemicals can change).

OSHA has also prepared a list of covered chemicals (provided in Appendix A of the regulation). If a company has one or more of these chemicals on site in quantities greater than the amount specified, then it is required to develop a PSM program. Even if a chemical is not on the list, an accident involving it can still lead to a PSM citation under the General Duty clause, as discussed earlier.

It is not always clear when a process is covered and when it is not. Examples of potential ambiguity include the following.

- One section of a facility handles a hazardous chemical. Adjacent to it is another unit that does not handle hazardous chemicals, and that is not linked to the first unit by piping or any process equipment. However, the two are physically close. If there were to be an explosion on the noncovered unit, flying debris may puncture a tank in the neighboring plant, leading to the release of the hazardous chemical. This then raises the question as to whether process safety activities (such as hazards analyses) should be performed on the noncovered process.
- If a unit that does not handle hazardous chemicals is adjacent to one that does, then the employees on the noncovered process may need to be trained in emergency response techniques should their neighbor have a release.
- Sometimes a plant may have a total inventory of the hazardous chemical that exceeds the threshold level, but that inventory is distributed among small vessels, none of which is above the threshold individually.

Table 2.7 Covered Processes

1. A process which involves a chemical at or above the specified threshold quantities. . .
    i. A process which involves a flammable liquid or gas (as defined in 1910.1200I of this part) on site in one location, in a quantity of 10,000 pounds (4535.9 kg) or more except for:
        A. Hydrocarbon fuels used solely for workplace consumption as a fuel (e.g., propane used for comfort heating, gasoline for vehicle refueling), if such fuels are not a part of a process containing another highly hazardous chemical covered by this standard;
        B. Flammable liquids stored in atmospheric tanks or transferred which are kept below their normal boiling point without benefit of chilling or refrigeration.
2. This section does not apply to:
    i. Retail facilities
    ii. Oil or gas well drilling or servicing operations
    iii. Normally unoccupied remote facilities.

Each of these situations raises questions as to which processes are covered and which ones are not. These questions require legal clarification and/or advice from the appropriate regulatory agency. If a company wishes to establish that a process is not covered, even though there are other covered processes in the area, this decision should be backed up with a Process Hazards Analysis (PHA). If this analysis reasonably demonstrates that the noncovered process cannot be affected by the other plants, then this can be used in the event of a citation.

Another problem concerning the assignment of responsibility concerns the situation where a company owns equipment, but the equipment is located at another company's facility, and is operated and maintained by the people at the site. In this case, the owner has to initiate the PSM program, but it is run by the personnel from the operating company.

The OSHA web page provides details of some of the latest discussions concerning which facilities and chemicals are covered, and which are not.

The term "highly hazardous chemical" is also defined by the American Society of Mechanical Engineers in ASME B31.3—1990 Chemical Plant & Petroleum Piping. They define a "Category M Fluid Service" as that service in which the potential for personnel exposure is judged to be significant and in which a single exposure to a very small quantity of a toxic fluid can produce serious, irreversible harm to persons even when prompt restorative measures are taken.

OTHER STANDARDS

Many parts of the OSHA PSM regulation refer to other OSHA standards. For example, the Emergency Planning & Response element basically requires that 29 CFR 1910.38—Emergency Plans And Fire Prevention—be properly implemented. Other related standards include 1910.147 (Lockout/Tagout) and 1910.165 (Employee Alarm Systems). Even when it is not necessary to follow them, these standards can still provide good general guidance.

Other regulations from other agencies are sometimes part of a process safety program. For example, with regard to docking facilities for ships and barges, OSHA normally covers the dock area and the dock employees. The Coast Guard normally covers the ship and the ship employees. Truck and rail safety is covered by various DOT regulations. Sometimes, it can be difficult to determine who has jurisdiction over what.

AUDIT GUIDELINES

OSHA has prepared a set of publicly available audit guidelines and questionnaires for use by their own CSHOs. Generally, these audit guidelines mimic the wording of the standard very closely. Frequently, the wording of the standard is simply reversed in order to create the audit question. Table 2.8 provides an example of one of these guidelines (in this case, for the Employee Participation element).

NATIONAL EMPHASIS PROGRAMS

In 2007, OSHA initiated its Petroleum Refinery PSM NEP to reduce or eliminate the workplace hazards associated with the catastrophic release of highly hazardous chemicals in petroleum refineries. The program outlined a new approach for inspecting PSM-covered facilities that allowed for a greater number of inspections using better allocation of OSHA resources. In 2009, OSHA built

Table 2.8 Sample OSHA Audit Form

1910.119 (c) Employee Participation		
I. Program Summary		
The intent of this paragraph is to require employers to involve employees at an elemental level of the PSM program. Minimum requirements for an Employee Participation Program for PSM must include a written plan of action for implementing employee consultation on the development of PHAs and other elements of process hazard management contained within 1910.119. The employer must also provide ready access to all the information required to be developed under the standard.		
II. Quality Criteria References		
A. 1910.119(c): Employee Participation		
III. Verification of Program Elements	**Criteria Reference**	**Met Y/N**
A. Records Review		
1. Does a written program exist regarding Employee Participation?	.119(c)(1)	
2. Does the written program include consultation with employees and their representatives on the conduct and development of other elements in the PSM standard?	.119(c)(2)	
3. Does the written program provide employees (including contractor employees) and their representatives access to PHAs and all other information developed as required by the PSM standard?	.119(c)(3)	
B. On-site Conditions		
Not applicable		
C. Interviews		
1. Based on interviews with a representative number of employees and their representatives, have they been consulted on the conduct and development of the PHAs?	.119(c)(2)	
2. Based on interviews with a representative number of employees and their representatives, have they been consulted on the development of other elements of the PSM program?	.119(c)(2)	
3. Based on interviews with a representative number of employees (including contractor employees) and their representatives, have they been informed of their rights of access and provided access to PHAs and to all other information required to be developed by the PSM standard? (Ask about unreasonable delays in access to information and whether time is given during the working hours to access information required by the PSM standard.)	.119(c)(3)	

upon that inspection program by implementing a pilot PSM-covered Chemical Facilities NEP, which it later expanded into a full NEP. Under both of the PSM NEPs, OSHA was able to increase the number of PSM-covered facilities inspected and gained valuable inspection data.

PROPOSED UPDATE

The PSM standard was published in 1992 and has never been updated, even though the world of process safety has changed considerably since that date. OSHA has therefore proposed to reopen the standard. In response to Executive Order 13650, OSHA issued a Request for Information (RFI) on December 9, 2013 (OSHA, 2013), in which they ask for comments before March 10, 2014 (OSHA, 2013). The RFI contains 17 sections.

For a change to be accepted, OSHA has set the following general requirements.

- A safety standard must substantially reduce a significant risk or material harm
- Compliance must be technologically and economically feasible
- A standard must employ the most cost-effective means of achieving its goal
- A standard that deviates from an existing national consensus standard must better effectuate the purposes of the OSH Act than the national consensus standards
- The standard must be supported by the evidence in the rulemaking record and either must be consistent with prior agency practice or be supported by a justification for departing from that practice.

Some initial comments on the RFI are provided below.

- Much of the discussion and justification for changes refer to actual incidents. OSHA seems to be using more of a case-based approach to process safety. Incidents that they refer to include:
    - A fire at Formosa Plastics in Illiopolis, IL, in 2004 that killed five workers and severely injured three others.
    - On March 23, 2005, 15 workers died and more than 170 others were injured at the BP Refinery in Texas City, TX.
    - On April 2, 2010, an explosion and fire at the Tesoro refinery in Anacortes, WA, killed seven workers. The incident occurred when a heat exchanger suddenly ruptured during maintenance, releasing a highly hazardous chemical that subsequently exploded.
    - On April 17, 2013, an ammonium nitrate explosion at the West Fertilizer Company storage and distribution facility in West, Texas, killed at least 15 people—the majority of whom were firefighters responding to a fire at the facility—and injured over 160 others.
- There is considerable cross-referencing to other federal and state standards, including New Jersey's Toxic Catastrophe Prevention Act (TCPA), the EPA's RMP, and BSEE's SEMS.
- It is likely that the number of companies and facilities covered by the standard will increase substantially. Many of them will be small organizations that do not currently have process safety programs.
- The proposals to do with RAGAGEP reflect a healthy focus on engineering.

It will take years before the proposed changes (modified by comments) result in an updated standard. Indeed, the overall process could take more than 7 years before it is completed.

The proposed changes consist of 17 sections. They are briefly described and discussed below.

1. Atmospheric Storage Tanks

Currently flammable liquids stored in atmospheric tanks or transferred which are kept below their normal boiling point without benefit of chilling or refrigeration are excluded from the standard.

OSHA had not intended for this exemption to apply to tanks connected to a process. However, in the Meer Case (Secretary of Labor v. Meer Corporation) OSHA's interpretation was overturned. OSHA now proposes to include storage tanks that are connected to or that are within a process.

2. Oil and Gas Well Drilling and Servicing

The original intent was that oil and gas well drilling and servicing were to be covered by their own standard. This did not happen, so OSHA proposes to include them in this revised PSM standard. The preamble to the PSM final rule explained that OSHA excluded these operations because it had begun a separate rulemaking for oil and gas well drilling and servicing operations. However, the Agency subsequently removed the oil and gas well drilling and servicing operations rulemaking from its regulatory agenda and never promulgated a final rule for these operations.

3. Oil and Gas Production Facilities

OSHA states that oil and gas production facilities are those "...bringing well fluids to the surface, separating them, and then storing, gauging and otherwise preparing the product for the pipeline." This production phase occurs after a well has been drilled, completed, and placed into operation, or after it has been returned to operation following workover or servicing. A completed well includes a "Christmas tree" (control valves, pressure gauges, and choke assemblies to control the flow of oil and gas) which is attached at the top of the well where pressure is expected. It is at this point, the top of the well, where the covered PSM process begins.

OSHA's original intent was that these facilities should be covered, but they were excluded after a challenge by the API. OSHA now wants to cover these facilities under the PSM rule. Their test case was an incident leading to fatalities occurred at a Sonat facility in Pitkin, LA, in 1998. The incident involved deficiencies in two elements of PSM: Process Hazards Analysis and Operating Procedures.

The API challenge was based on the lack of an economic analysis. OSHA proposes to now conduct that analysis.

If the Oil and Gas Production facilities are to be included in the standard, a paper *Lessons Learned From Inspection of 25,000 Upstream Oil and Gas Wells and Associated Plants* (Schubert, 2011) provides useful background. Some of the conclusions of that report are as follows.

- Around 4% of the findings were Priority 1/Urgent, meaning that action was required within 24 hours.
- Nearly 80% of these Priority 1 findings were "Relief device is overdue for inspection and testing."
- Priority 4/Planning, an example of which is "Light corrosion or damage to support structure" made up just over 40% of the findings. Action on these can wait for the next turnaround.

It would appear that adding this element to the updated standard would greatly increase the number of covered facilities. But the work needed to be done at a typical facility would not be all that high. The main focus would be on the integrity of pressure relief systems.

4. Reactivity Hazards

The Chemical Safety Board has made recommendations that the scope of the standard be expanded with regard to reactive chemicals. OSHA's suggestion is to use the New Jersey TCPA as an example and also to follow the approach used by the Chemical Safety Board, which is performance based.

5. Highly Hazardous Chemicals

Currently, Appendix A of the standard lists 137 highly hazardous chemicals. OSHA is suggesting that the number of covered chemicals should be increased. The agency recognizes that the many hazards analyses conducted in the last 20 years have identified additional chemicals that should now be included in Appendix A.

6. Management System Elements

Since the standard was promulgated in 1992, best process safety practices have continued to evolve. OSHA refers to the 20 elements defined by the CCPS. Examples of additional elements include:

- Measurement and metrics
- Management review and continuous improvement
- Process safety competency.

They are also considering elements from SEMS used offshore. These elements include:

- Stop work authority
- Ultimate work authority
- Employee participation plan.

7. RAGAGEP

The acronym RAGAGEP stands for "Recognized and Generally Accepted Good Engineering Practices" (the concept is described in Chapter 9).

Currently, the OSHA standard requires employers to document that covered equipment complies with RAGAGEP, "For existing equipment designed and constructed in accordance with codes, standards, or practices that are no longer in general use." However, the PSM standard does not require employers to evaluate updates applicable to RAGAGEP or to examine new RAGAGEP after evaluating and documenting compliance with the standard. OSHA goes on to say that, since the practices constituting RAGAGEP under the PSM standard are constantly changing as a result of this process, evaluating updates to applicable RAGAGEP ensures that employers base a facility's PSM program on the most up-to-date and accurate safety information available.

OSHA is looking for suggestions that will update the standard's RAGAGEP requirements.

8. Definition of RAGAGEP

This section discusses ways in which RAGAGEP can be defined. They quote the CCPS definition.

> Recognized and Generally Accepted Good Engineering Practices (RAGAGEP) are the basis for engineering, operation, or maintenance activities and are themselves based on established codes, standards, published technical reports or recommended practices (RP) or similar documents.

> RAGAGEPs detail generally approved ways to perform specific engineering, inspection or mechanical integrity activities, such as fabricating a vessel, inspecting a storage tank, or servicing a relief valve.

It is worth noting that the above definition is all to do with mechanical systems; instrumentation is not mentioned.

OSHA suggests that a definition can be obtained by reviewing standards from organizations such as NFPA, ASTM, and ANSI. Many companies also have their own internal standards that are more stringent than public standards.

9. Safety Critical Equipment

Currently, the Mechanical Integrity element applies to a specific list of equipment items. OSHA is suggesting that any other equipment that is considered critical to safety be added to the list.

10. Organizational Changes

OSHA is proposing to include organizational changes in the MOC program. Examples are changes in management structure, budget cuts, or personnel changes.

The integration of such changes into the MOC program is something that many companies have elected to do in the years since the standard was promulgated. Now OSHA wishes to formalize such changes.

11. Emergency Planning

Currently, there is no requirement that emergency plans be coordinated with local emergency response authorities. OSHA is suggesting that this be changed.

12. Third-Party Compliance Audits

OSHA is looking at the use of third-party auditors (drawing from SEMS experience). They are also looking for comments on increasing the frequency of the audits and of the time required to address identified deficiencies.

13. Explosives, Blasting Agents, and Pyrotechnics

OSHA proposes to include explosives in the standard.

14. Flammable Liquids and Spray Finishing

These materials are covered by other standards that are considered to be outdated. Therefore, OSHA proposes to include them in the PSM standard.

15. Ammonium Nitrate

OSHA is looking for comments on how to regulate this widely used chemical, millions of tons of which are manufactured in the United States every year.

16. Retail Facilities

Currently, the retail facilities exemption from the PSM standard includes some activities that would not normally be considered as “retail.” An example is a company that sells anhydrous ammonia to farmers.

The agency is proposing to tighten the meaning of “retail” and to make the term consistent with definitions in other federal standards.

17. Concentrations of Highly Hazardous Chemicals

OSHA is proposing to resolve inconsistencies with regard to the concentrations of highly hazardous chemicals. They are suggesting that the EPA RMP system be used.

THE EPA

The U.S. EPA is charged by Congress to protect the Nation’s land, air, and water systems. The EPA works in partnership with state, county, municipal, and tribal governments to carry out its mission. As with OSHA, State and local standards may implement their own rules as long as they exceed federal standards, but they cannot be less stringent.

The EPA administers 11 comprehensive environmental protection laws:

1. Clean Air Act
2. Clean Water Act
3. Safe Drinking Water Act
4. Comprehensive Environmental Response, Compensation, and Liability Act (“Superfund”)
5. Resource Conservation and Recovery Act
6. Federal Insecticide, Fungicide, and Rodenticide Act
7. Toxic Substances Control Act
8. Uranium Mill Tailings Radiation Control Act
9. Lead Contamination Control Act
10. Ocean Dumping Ban Act
11. National Environmental Education Act.

The Clean Air Act is the one that covers process safety. The pertinent rule is referred to as the Risk Management Program, and is administered by the CEPPO, the EPA office that administers the Risk Management Plan (RMP).

THE EPA RISK MANAGEMENT PROGRAM—40 CFR 68

Although the OSHA and EPA standards are intentionally very similar to one another from a technical point of view, there are substantial administrative differences, particularly with regard to terminology. For example, EPA uses the phrase “Owner or Operator” rather than “Employer”—the term used by OSHA. Also, the RMP is referred to as a “rule,” whereas PSM is a “regulation” or “standard.” A Memorandum of Understanding (MOU) between the two agencies concerning joint inspection activities was agreed in 1990.

TIERING/PROGRAM LEVELS

EPA recognizes that many companies handle just small amounts of chemicals and that they do not have the resources to conduct full-scale risk analyses. Moreover, processes like these are often quite generic, and each plant is very similar to others of the same type. Therefore, EPA set up three Tiers or Program Levels.

Program Level 1 is the simplest; Level 2 is somewhat more complex. Level 3 is the most stringent and is the one that applies to major process facilities. It covers nine SIC codes (the meaning of these codes is given later in this chapter): 2611, 2812, 2819, 2821, 2869, 2873, 2879, and 2911. (OSHA does not use a tiering approach with regard to PSM; if a company is covered by the standard, it must develop a program that leads to a safe operation—whatever that takes.)

COVERED CHEMICALS

A list of the chemicals covered by the EPA RMP is provided in Attachments 1 and 2 (toxic chemicals and flammable substances, respectively). For each chemical, the following information is provided:

1. CAS Number
2. Threshold Quantity (TQ)
3. Toxic Endpoint (mg/l).

The RMP lists 77 toxic and 63 flammable substances. (The list is different from OSHA, as are some of the concentration limits.) Explosives and transportation are excluded.

FORMAL MANAGEMENT SYSTEM

One of the biggest differences between the RMP and PSM standards is that EPA requires that a formal, written program be prepared, and which is then placed in the public domain. OSHA does not require this. EPA needs a written plan because the RMP is very concerned with making sure that members of the public are fully informed as to what hazards are in their community, and what to do if there is an accident, and how the various emergency agencies can work together.

WORST CASE RELEASE

Another difference between the EPA and OSHA standards concerns offsite issues. EPA is more concerned about the long range impact of an accident, particularly what will happen if a cloud of toxic gas gets “over the fence.” With this in mind, one of the requirements of the first draft of the RMP rule was to prepare an absolute worst-case scenario, in which no credit is taken for any type of safety system (including passive systems such as earthen walls around a tank farm). It was defined as a release over a 10-minute period of the largest quantity of a regulated substance on the facility resulting from a piping or vessel failure. If a facility handled both flammable and toxic materials, a worst-case scenario needed to be prepared for each.

The worst-case requirement was controversial for three reasons. First, most worst-case scenarios are so very improbable that releasing information of that type would, it was claimed, cause unnecessary alarm among the general public. Second, there was a concern that highly sensitive information would be published on the Internet, and so become available to terrorists, and other hostile groups. Third, the likelihood of passive systems, such as earthen walls, totally failing is so low as to make the worst case to be almost incredible.

For these reasons, the worst-case requirement was reduced in scope, and a less serious scenario put in its place. However, the advantage to the use of worst-case scenarios—no matter how unlikely they were—was that they put all facilities on the same terms so that different industries and hazards could be compared on equivalent bases.

The modeling of vapor releases is complex and requires the resources of skilled analysts. Recognizing this, the EPA developed "look-up" tables where a facility would simply identify its particular situation and have a rough idea as to what the consequences of a release might be. These are particularly useful for Program (Tier) One and Two companies, which often have similar technologies and chemicals, and which do not have the resources to conduct a full-scale risk analysis. The look-up tables are generally considered to be conservative, i.e., their forecast as to vapor dispersions are likely to be worse than a forecast obtained from simulations.

EMERGENCY PLAN

The EPA requires that a formal emergency plan be prepared to include some of the offsite scenarios just touched on. By contrast, the OSHA PSM standard requires that an emergency response system be in place, but not necessarily a formal plan involving the public.

FIVE-YEAR ACCIDENT HISTORY

The rule requires that a 5-year accident history report be prepared for the facility. This report should include a description of injuries or fatalities on or off the site during the 5-year period. However, it does not have to include information about near-miss situations.

BSEE

The Bureau of Ocean Energy Management, Regulation and Enforcement (BOEMRE) was previously known as the **MMS**, a bureau in the **United States Department of the Interior**. It is the federal agency that manages the nation's natural gas, oil, and other mineral resources on the **outer continental shelf, beginning three miles off the coastal shoreline and extending 200** nautical miles out to sea. The safety of offshore oil and gas production operations in the United States is regulated primarily by the states to the limit of their jurisdiction (typically three miles from shore, with the exception of Texas and the west coast of Florida, which are nine miles from shore).

Most of the offshore activity of MMS is to do with operations in the Gulf of Mexico and the coasts of California and Alaska. At the end of 2003, oil production was about **1.7** million barrels per day, primarily from the Gulf of Mexico, where 56% of the leased acreage is located in deep water (more than 1,000 feet).

The Offshore Minerals Management program for MMS is the one that affects most professionals in the safety and environmental areas.

The MMS's Safety and Environmental Management Program (SEMP) was developed in response to the 1990 finding of the National Research Council's Marine Board that MMS's prescriptive approach to regulating offshore operations had forced industry into a compliance mentality. The Marine Board found further that this compliance mentality was not conducive to effectively identify all the potential operational risks or developing comprehensive accident mitigation. As a result, the Marine Board recommended and MMS concurred that a more systematic approach to managing offshore operations was needed.

SEMP combines a variety of offshore operating programs into a single, integrated, flexible, always-improving management scheme. It specifies how to:

- Operate and maintain facility equipment
- Identify and mitigate safety and environmental hazards
- Change operating equipment, processes, and personnel
- Respond to and investigate accidents, upsets, and "near misses"
- Purchase equipment and supplies
- Work with contractors
- Train personnel
- Review the SEMP to ensure it works and make it better.

The MMS has four principal SEMP objectives:

1. Focus attention on the influences that human error and poor organization have on accidents
2. Continuous improvement in the offshore industry's safety and environmental records
3. Encourage the use of performance-based operating practices
4. Collaborate with industry in efforts that promote the public interests of offshore worker safety and environmental protection.

API RP 75 was written in response to the need for a SEMP. The API also produced a companion document, RP 14J, for identifying safety hazards on offshore production facilities. In 1994, the MMS published a Notice in the *Federal Register* that recognized implementation of RP 75 as meeting the spirit and intent of SEMP. RP 75 was updated in July 1998 to focus more on contract operations, including operations on mobile offshore drilling units.

STATE REGULATIONS

Three States—New Jersey, Delaware, and Nevada—have their own risk management plans, and 25 have set up their own version of the OSHA standard. (The California Risk Management and Prevention Program (RMPP) was the first major regulation of its type in the United States but it has since been incorporated into CAL OSHA's process safety standard.)

NEW JERSEY TOXIC CATASTROPHE PREVENTION ACT

Companies in New Jersey must meet the requirements of the TCPA; it is administered by the New Jersey Department of Environmental Protection and Energy (DEPE).

One of the key features of the New Jersey standard is that it provides an empirical definition of an "Extremely Hazardous Substance" (EHS). Other regulations simply list the covered chemicals without providing much explanation as to what process was used for including chemicals in the list. Companies which handle, use, manufacture or store, or have the capability of generating an EHS within 1 hour are included in the standard. A list of EHSs is provided, along with the Registration Quantities (RQ) for each. The Registered Quantity does not all have to be in one location. The agency specifically states: "the RQ which triggers the requirements of the TCPA rule is "site" based, rather than "facility" based. Therefore, two or more facilities located on the same site, each with less than the RQ of an EHS will nonetheless be subject to the requirements of the Act and the rules if the total quantities of the EHS exceed the registered quantity."

Furthermore, all equipment that handles the EHS, even if some of that equipment is away from the site where the RQ of the EHS is located, is included in the rule. There is, however, some latitude if a hazard analysis shows that the concentration of the EHS does not exceed a certain level beyond the site boundary.

Another feature of the TCPA is that it is considerably more prescriptive than most PSM programs. The regulation is comparatively detailed.

DELAWARE/NEVADA

Delaware's Extremely Hazardous Substances Risk Management Act was passed in 1988. It covers 89 regulated substances. Nevada's Senate Bill No. 641 was passed in 1991.

THE SAFETY CASE REGIME

The Safety Case system for managing safety was introduced in the 1960s in the nuclear power industry. A safety case is *a documented body of evidence that provides a demonstrable and valid argument that a system is adequately safe for a given application and environment over its lifetime*.

Facility management develops a risk management program for ensuring adequate levels of safety. It then makes its "case" to the regulatory authorities that the facility is safe to operate. The authorities either accept or reject this "safety case." If they accept it then a "safety case regime" is implemented. At least three types of safety case are developed during a facility's lifetime: the case for design safety, the case for operational safety, and the case for eventual shutdown and termination of the operation.

The first safety cases prepared for the process industries were those developed for North Sea offshore oil and gas operations following the Piper Alpha disaster that occurred in the year 1988. The Cullen report (Cullen, 1990) that was written following that accident was highly critical of offshore operating practices and recommended that a safety case approach be implemented. The Seveso incident that occurred in Italy further prompted the increased use of safety cases. Since that time the use of safety cases has spread to other industries (such as mining and railway operations) and to other nations, primarily in Europe and Australasia. (It is notable that the safety case regime approach has *not* been taken up for offshore oil and gas operations in the Gulf of Mexico—instead a more prescriptive approach based on industry consensus standards is used.)

ELEMENTS OF A SAFETY CASE

Key elements of a safety case include:

- Duty-holder responsibility
- Auditor/assessor responsibility
- Risk management system
- Management systems
- Living document.

Duty-Holder Responsibility

At the heart of the safety case approach lies an understanding that is the operator of a facility—not the regulator—who decides how to ensure safe operations. This nonprescriptive approach to the management of safety is similar to the manner in which most PSM programs are prepared and administered. The operator of the facility, known as the duty holder, develops a safety system that is pertinent to that particular facility. The duty holder's performance is then assessed against his or her own standard.

Responsibility of the Auditor/Assessor

The auditor or assessor, who can represent either a government agency or a nongovernmental body, has three key roles:

1. Provide guidance to the owner as to what is required in the Safety Case.
2. Formally accept (or reject) the Safety Case after it has been prepared and presented by the operator. Not only must the Safety Case as written be accepted, the operator has to demonstrate that his organization has the ability, management commitment and resources to properly assess and effectively control risks to the health and safety of staff and the general public.
3. Ensure that the operator is actually doing what he said he would do in the Safety Case once operations commence.

The term "co-regulatory structure" is sometimes used to describe this method of managing safety.

Risk Management System

The Safety Case must incorporate include a formal risk analysis and a statement as to how risk will be managed. As a consequence of this requirement, safety cases are often large, very thorough and expensive to prepare and implement.

Management Systems

Systems for controlling risk should concentrate on management systems rather than just on hardware and instrumentation. Therefore, the safety case must show that the correct management systems for controlling safety are in place.

Living Document

A safety case is a living document that describes the safety of an operation from the initial concept design, all the way through normal operations, to the eventual termination and shut down of the facility. The Safety Case is modified and upgraded as needed in order to ensure that risk and safety are properly managed at all times.

STRUCTURE OF A SAFETY CASE

The nonprescriptive nature of the safety case means that the structure and organization of the documentation will vary according to the needs of the facility. The risks and management activities associated with a nuclear power plant, for example, are quite different from those for a freight railroad. Therefore, the respective safety cases are likely to be quite different. Nevertheless, it will usually be found that a Safety Case has three principal sections:

1. A description of the facility
2. A description of the safety management system (SMS)
3. A formal safety assessment (FSA).

1. Facility Description

The safety case should contain sufficient information about the facility to verify that the design and operating philosophy is consistent with the SMS and with the assumptions and outputs of the formal risk analysis. Using an offshore platform as an example, the safety case will generally contain the following minimum information.

- An overview of the facility, highlighting key assumptions and operation phases of development
- A summary of key design parameters with cross-references to key technical documents (covering storm/wave/current conditions, wind, seawater/air temperatures, earthquakes, cyclones, other extreme conditions, seabed stability)
- A description of the facility, including any unique features
- Equipment layout for all decks
- A description of the functions of the facility with reference to key processes, wellhead and utility systems, drilling, workover, wireline systems, and marine and helicopter operations
- A summary of hazardous substances that are used or stored at the facility, along with an estimate of the inventory of these substances
- A description of the design safety philosophy, features, and systems provided on the installation with emphasis on safety philosophy
- A description of key process equipment layout and process flow.

Not only should the safety case describe the facility itself, it should also discuss interactions with existing and planned facilities.

2. Safety Management System

The SMS is the central component of the safety case. It is the system by which hazards are identified and risks are continually and systematically assessed. These risks can then be either eliminated or controlled at the appropriate points in the facility's life, ranging from initial design through construction, commissioning, operation, and abandonment of the facility. In order to demonstrate that the operator has strategies, systems and procedures in place to comply with the various regulatory requirements that may be applicable, the SMS must be comprehensive, integrated and contain feedback loops that continually measure performance and drive change.

The activities undertaken by management to establish and operate an effective SMS are no different to those used to manage any other business. The same management features that underpin and distinguish organizations achieving business excellence form the basis of effective safety management. The SMS would be expected to cover as a minimum:

- Safety policies and the organizational and facility safety objectives
- Organization reporting structures—roles and responsibilities
- Risk assessment and risk management
- Methods of employee involvement in risk management
- Employee selection, competency, training, and induction
- Integration of contractor and support services in risk management
- Design, construction, and commissioning procedures
- Safe operational procedures for normal and abnormal circumstances
- Systems of maintenance, inspection, and modification
- Systems of managing change to ensure safety
- Methods, systems, and procedures for ensuring the occupational health of employees
- Emergency response including controls, personnel evacuation, escape, and rescue
- Incident investigation and reporting, corrective and follow-up action
- The method of performance review and audit including review in the light of external experience.

The SMS should ensure that all necessary linkages between system elements are identified and, where appropriate, should draw on the principles of quality management.

3. Formal Safety Assessment

The third element of a safety case is the FSA. The FSA requires the identification and evaluation of hazards over the life of the project from the initial feasibility study through the concept design stage, to construction and commissioning, then to operation, decommissioning, and abandonment of the facility. The FSA is a demonstration that, so far as is reasonably practicable, the risks to personnel have been minimized. It should:

- Provide reasoned arguments and judgments about the risk acceptance criteria including the rationale for their acceptance, references used, and details of the risk acceptance studies conducted into potential major accident events that may occur during the life of the facility.
- Demonstrate that the operator has identified the nature, likelihood, and consequence of potential major accident events that may occur at the facility.
- State the associated risks of fatality with respect to employees at the facility, and that the likelihood of these events and/or consequences have been minimized over the life of the facility.
- Demonstrate that all reasonably practicable steps have been taken to ensure the safety of employees in the event of an emergency and during transit to a place of safety. It should

demonstrate in particular that the integrity of the temporary refuge, escape, and evacuation routes is maintained in the case of a major accident event, and that all reasonably practicable steps have been taken to ensure the safety of employees in the event of an emergency and during transit to a place of safety (this requirement includes embarkation points and the use of escape craft for offshore facilities).

Both qualitative and quantitative methods of analysis can be applied to the assessment of risk.

PREPARATION AND IMPLEMENTATION

The preparation of a safety case should involve close interaction between the operator and the assessor, with regular meetings ensuring that the expectations of each party are reasonably in line as the development of the safety case proceeds. There should be no surprises when the safety case is formally submitted.

The safety case need not contain detailed procedures, calculations, drawings, or plans, but should contain sufficient information to allow the regulator to assess whether the systems and conclusions presented in the safety case are reasonable. General documentary evidence that supports the conclusions reached in the safety case should be referenced, and the regulator given access to the relevant documentation where necessary.

The use of external specialist resources to assist in the preparation of the safety case is commonplace. The duty holder should, however, be involved in all facets of the preparation of the safety case.

An essential part of the development of an appropriate culture is the involvement of employees through their representatives in the preparation of the safety case and the active participation of employees in the maintenance of a safe place of work. The safety case will need to clearly identify the methods used to involve employees in safety management of the facility.

- The safety case procedures must define the objections of the program and must identify which procedures and standards are in place.
- It must be clear who is responsible for implementing the procedures, the level of detail required, and the expected outcome.
- It is necessary to establish how the procedures are to be implemented, the resources that are to be made available, and the necessary skills and competencies of the persons involved.
- The procedures will describe how the system is monitored, reviewed, and audited, and the results are used to update and improve the systems ability to produce the desired outcome.
- Safety cases generally include a quantitative risk analysis (QRA), particularly when analyzing the risk associated with fires, explosions, and toxic gas releases.

ASSESSMENT

Inspectors are engaged both in onsite appraisal of the delivery of improvements and assessing the complex technical arguments put forward for alternative approaches. They must be able to review and evaluate the quality and effectiveness of the Safety Case without duplicating the work.

Risk analysis, while it can employ scientific methodologies, is very much based in the experiences of those involved in undertaking the analysis, and, where qualitative analysis is undertaken, by the data used in the assumptions made about likelihood and consequences of events. Therefore, as discussed in Chapter 1, the high degree of uncertainty inherent in most risk analyses means that the results are most useful for comparing alternate strategies—not for coming up with an unequivocal measure of risk.

Demonstrating that the level of residual risk is acceptable will always be based on a degree of subjectivity. The safety case assessment procedures recognize the limitations of the risk analysis process and the problems associated with determination that risk has been reduced to as low as is reasonably practicable. This is achieved by focusing on the analysis of the operator's methodology in undertaking the risk analysis process.

Factors that will be considered in the assessor's reviews include:

- The operator's incident/accident experience and causal factors, complaints, legislative compliance reviews, and the operator's internal audit results
- The combined national experience of operators
- National and international trends and experience
- General industry experience and developing standards
- The effectiveness with which the commitments in the safety case are being implemented
- Monitoring the effectiveness of SMS and operator audits of them
- The degree to which the work force is involved in implementing the Safety Case Regime.

Overall, the assessor's job is to ensure that management systems are in place, that they are effective, and they are being followed. Rather than checking on the details of the safety program, the assessor will evaluate management systems and their effectiveness.

PERFORMANCE MEASUREMENT

Performance standards are the key to an effective safety system. They specify what has to be done, when, by whom, and to what extent and ensure that the system is operating as planned in the achievement of objectives through linking roles and responsibilities to actions in a measurable way.

Measurement of performance has traditionally been focused on "lag" indicators such as Lost Time Injury Frequency Rates. Current thinking recognizes that there are severe limitations in relying on such historical data, and instead is examining the use of "lead" indicators. Lead indicators (such as the number and quality of safety audits conducted, the measurement of management commitment to safety through employee perception studies, and the quality of the facility safety plan) will hopefully provide a real-time measure of the effectiveness of the safety management arrangements. They measure proactivity, represent management's commitment to identify potential loss events, and signal the presence of management systems, which can uncover weaknesses before they develop into full-fledged problems.

INTERNATIONAL AGENCIES

Increasingly, international laws are defining how industrial facilities organize and manage their HSE programs. For example, the World Bank's Reduced Flaring Initiative calls on oil and gas-producing nations to reduce continuous flaring in order to reduce the emissions of greenhouse gases and to conform to the requirements of the Kyoto protocol.

International bodies such as the World Bank cannot usually exert direct control over managers in the way that national bodies can. However, these international bodies often control the financing of large projects, particularly in poorer countries, and so can affect action through their decisions as to whether or not to release funds for these projects.

ELEMENTS OF PSM

This section discusses each of the elements of PSM in terms of OSHA compliance. The elements, which were listed in Table 1.1, are repeated below in Table 2.9. Each of the elements (with the exception of Trade Secrets) is discussed in depth in the remaining chapters of this book. Specific guidance for each of the elements with respect to the OSHA standard is provided below. Each section provides the OSHA standard, along with the nonbinding guidance that accompanies the standard. In some cases, details that are immaterial to technical compliance are omitted.

1. EMPLOYEE PARTICIPATION

Discussion to do with this important topic is provided in Chapter 3. The OSHA standard and guidance to do with Employee Participation are shown below.

Table 2.9 OSHA Elements of PSM

1. Employee participation
2. Process safety information
3. Process hazards analysis
4. Operating procedures
5. Training
6. Contractors
7. Prestartup safety review
8. Mechanical integrity
9. Hot work
10. Management of change
11. Incident investigation
12. Emergency planning and response
13. Compliance audits
14. Trade secrets

Standard

1. Employers shall develop a written plan of action regarding the implementation of the Employee Participation required by this paragraph.
2. Employers shall consult with employees and their representatives on the conduct and development of PHAs and on the development of the other elements of PSM in this standard.
3. Employers shall provide to employees and their representatives access to PHAs and to all other information required to be developed under this standard.

Guidance

Employers are to consult with their employees and their representatives regarding the employers efforts in the development and implementation of the PSM program elements and hazard assessments. [Employers must] train and educate their employees and to inform affected employees of the findings from incident investigations required by the PSM program. Many employers, under their safety and health programs, have already established means and methods to keep employees and their representatives informed about relevant safety and health issues and employers may be able to adapt these practices and procedures to meet their obligations under this standard. Employers who have not implemented an occupational safety and health program may wish to form a safety and health committee of employees and management representatives to help the employer meet the obligations specified by this standard. These committees can become a significant ally in helping the employer to implement and maintain an effective PSM program for all employees.

Written Plan of Action

OSHA requires that the Employee Participation program be written down. This can be difficult to do well because Employee Participation is involved in so many areas of process safety and because participation represents a state of mind rather than a specific program.

The plan of action should identify who is responsible for the management of the PSM program, how employees can learn about it, and how suggestions for improvement can be implemented.

Consultation

As already discussed, employees must be involved in all aspects of PSM, not merely informed about decisions that have been made by other people. Their opinions matter and should always be acted on. Even when an idea is rejected, management should always communicate with the employee as to why that decision was made.

On union plants, the employee representatives will be appointed by the union. On nonunion plants, the employees may choose someone to represent their interests. The appointment must be made by the employees, not management.

Access to Information

In addition to consulting with employees, it is important that management makes sure that employees know that they have a right to access to information to do with process safety. The fact that PHAs are specifically identified within this element has prompted many companies to make sure that operators participate in the PHAs, often on a rotating basis.

2. PROCESS SAFETY INFORMATION

The topic of Process Safety Information (PSI) is covered in Chapter 4. The OSHA standard and guidance on the topic are shown below.

Standard

. . .The employer shall complete a compilation of written PSI before conducting any PHA required by the standard. The compilation of written PSI is to enable the employer and the employees involved in operating the process to identify and understand the hazards posed by those processes involving highly hazardous chemicals. This PSI shall include information pertaining to the hazards of the highly hazardous chemicals used or produced by the process, information pertaining to the technology of the process, and information pertaining to the equipment in the process.

1. Information pertaining to the hazards of the highly hazardous chemicals in the process. This information shall consist of at least the following:

- **i.** Toxicity information
- **ii.** Permissible exposure limits
- **iii.** Physical data
- **iv.** Reactivity data
- **v.** Corrosivity data
- **vi.** Thermal and chemical stability data
- **vii.** Hazardous effects of inadvertent mixing of different materials that could foreseeably occur.

Note: Material Safety Data Sheets (MSDSs) meeting the requirements of 29 CFR 1910.1200(g) may be used to comply with this requirement to the extent they contain the information required by this subparagraph.

2. Information pertaining to the technology of the process.

- **i.** Information concerning the technology of the process shall include at least the following:
    - **A.** A block flow diagram or simplified process flow diagram
    - **B.** Process chemistry
    - **C.** Maximum intended inventory
    - **D.** Safe upper and lower limits for such items as temperatures, pressures, flows, or compositions
    - **E.** An evaluation of the consequences of deviations, including those affecting the safety and health of employees.
- **ii.** Where the original technical information no longer exists, such information may be developed in conjunction with the PHA in sufficient detail to support the analysis.

3. Information pertaining to the equipment in the process.

- **i.** Information pertaining to the equipment in the process shall include:
    - **A.** Materials of construction
    - **B.** Piping and instrument diagrams (P&IDs)
    - **C.** Electrical classification
    - **D.** Relief system design and design basis
    - **E.** Ventilation system design
    - **F.** Design codes and standards employed
    - **G.** Material and energy balances for processes built after May 24,1992
    - **H.** Safety systems (e.g., interlocks, detection, or suppression systems).
- **ii.** The employer shall document that equipment complies with recognized and generally accepted good engineering practices.
- **iii.** For existing equipment designed and constructed in accordance with codes, standards, or practices that are no longer in general use, the employer shall determine and document that the equipment is designed, maintained, inspected, tested, and operating in a safe manner.

Guidance

Complete and accurate written information concerning process chemicals, process technology, and process equipment is essential to an effective PSM program and to a PHA. The compiled information will be a necessary resource to a variety of users including the team that will perform the PHA as required under paragraph (e); those developing the training programs and the operating procedures; contractors whose employees will be working with the process; up reviews; local emergency preparedness planners; and insurance and enforcement officials.

The information to be compiled about the chemicals, including process intermediates, needs to be comprehensive enough for an accurate assessment of the fire and explosion characteristics, reactivity hazards, the safety and health hazards to workers, and the corrosion and erosion effects on the process equipment and monitoring tools. Current MSDS information can be used to help meet this requirement which must be supplemented with process chemistry information including runaway reaction and over pressure hazards if applicable.

Process technology information will be a part of the PSI package and it is expected that it will include diagrams of the type shown in Appendix B of this section as well as employer established criteria for maximum inventory levels for process chemicals; limits beyond which would be considered upset conditions; and a qualitative estimate of the consequences or results of deviation that could occur if operating beyond the established process limits. Employers are encouraged to use diagrams which will help users understand the process.

A block flow diagram is used to show the major process equipment and interconnecting process flow lines and show flow rates, stream composition, temperatures, and pressures when necessary for clarity. The block flow diagram is a simplified diagram.

Process flow diagrams are more complex and will show all main flow streams including valves to enhance the understanding of the process, as well as pressures and temperatures on all feed and product lines within all major vessels, in and out of headers and heat exchangers, and points of pressure and temperature control. Also, materials of construction information, pump capacities and pressure heads, compressor horsepower and vessel design pressures and temperatures are shown when necessary for clarity. In addition, major components of control loops are usually shown along with key utilities on process flow diagrams.

P&IDs may be the more appropriate type of diagrams to show some of the above details and to display the information for the piping designer and engineering staff. The P&IDs are to be used to describe the relationships between equipment and instrumentation as well as other relevant information that will enhance clarity. Computer software programs which do P&IDs or other diagrams useful to the information package may be used to help meet this requirement.

The information pertaining to process equipment design must be documented. In other words, what were the codes and standards relied on to establish good engineering practice. These codes and standards are published by such organizations as the ASME, API, ANSI, NFPA, American Society for Testing and Materials, National Board of Boiler and Pressure Vessel Inspectors, National Association of Corrosion Engineers, American Society of Exchange Manufacturers Association, and model building code groups.

In addition, various engineering societies issue technical reports which impact process design. For example, the AIChE has published technical reports on topics such as two phase flow for venting devices. This type of technically recognized report would constitute good engineering practice.

For existing equipment designed and constructed many years ago in accordance with the codes and standards available at that time and no longer in general use today, the employer must document which codes and standards were used and that the design and construction along with the testing, inspection, and operation are still suitable for the intended use. Where the process technology requires a design which departs from the applicable codes and standards, the employer must document that the design and construction is suitable for the intended purpose.

OSHA stresses the fact that the PSI should be written down. Not only does this mean that safety information is needed as required, it also will help identify any hazards that may be present. The specific elements of the standard are discussed in the following sections of this chapter.

3. PROCESS HAZARDS ANALYSIS

The OSHA standard and guidance are shown below (some administrative detail has been removed).

Standard

1. The employer shall perform an initial PHA (hazard evaluation) on processes covered by this standard. The PHA shall be appropriate to the complexity of the process and shall identify, evaluate, and control the hazards involved in the process. Employers shall determine and document the priority order for conducting PHAs based on a rationale which includes such considerations as extent of the process hazards, number of potentially affected employees, age of the process, and operating history of the process.

[Schedule details follow. . .]

2. The employer shall use one or more of the following methodologies that are appropriate to determine and evaluate the hazards of the process being analyzed.

- **i.** What-If
- **ii.** Checklist
- **iii.** What-If/Checklist
- **iv.** Hazard and Operability Study (HAZOP)
- **v.** Failure Mode and Effects Analysis (FMEA)
- **vi.** Fault Tree Analysis
- **vii.** An appropriate equivalent methodology.

3. The PHA shall address:

- **i.** The hazards of the process
- **ii.** The identification of any previous incident which had a likely potential for catastrophic consequences in the workplace
- **iii.** Engineering and administrative controls applicable to the hazards and their interrelationships such as appropriate application of detection methodologies to provide early warning of releases. (Acceptable detection methods might include process monitoring and control instrumentation with alarms, and detection hardware such as hydrocarbon sensors.)
- **iv.** Consequences of failure of engineering and administrative controls
- **v.** Facility siting
- **vi.** Human factors
- **vii.** A qualitative evaluation of a range of the possible safety and health effects of failure of controls on employees in the workplace.

4. The PHA shall be performed by a team with expertise in engineering and process operations, and the team shall include at least one employee who has experience and knowledge specific to the process being evaluated. Also, one member of the team must be knowledgeable in the specific PHA methodology being used.

5. The employer shall establish a system to promptly address the team's findings and recommendations; assure that the recommendations are resolved in a timely manner and that the resolution is documented; document what actions are to be taken; complete actions as soon as possible; develop a written schedule of when these actions are to be completed; communicate the actions to operating, maintenance and other employees whose work assignments are in the process and who may be affected by the recommendations or actions.

6. At least every 5 years after the completion of the initial PHA, the PHA shall be updated and revalidated by a team meeting the requirements in paragraph (e)(4) of this section, to assure that the PHA is consistent with the current process.

Guidance

A PHA, sometimes called a process hazard evaluation, is one of the most important elements of the PSM program. A PHA is an organized and systematic effort to identify and analyze the significance of potential hazards associated with the processing or handling of highly hazardous chemicals. A PHA provides information which will assist employers and employees in making decisions for improving safety and reducing the consequences of unwanted or unplanned releases of hazardous chemicals. A PHA is directed toward analyzing potential causes and consequences of fires, explosions, releases of toxic or flammable chemicals and major spills of hazardous chemicals. The PHA focuses on equipment, instrumentation, utilities, human actions (routine and nonroutine), and external factors that might impact the process. These considerations assist in determining the hazards and potential failure points or failure modes in a process.

The selection of a PHA methodology or technique will be influenced by many factors including the amount of existing knowledge about the process. Is it a process that has been operated for a long period of time with little or no innovation and extensive experience has been generated with its use? Or, is it a new process or one which has been changed frequently by the inclusion of innovative features? Also, the size and complexity of the process will influence the decision as to the appropriate PHA methodology to use. All PHA methodologies are subject to certain limitations. For example, the checklist methodology works well when the process is very stable and no changes are made, but it is not as effective when the process has undergone extensive change. The checklist may miss the most recent changes and consequently the changes would not be evaluated. Another limitation to be considered concerns the assumptions made by the team or analyst. The PHA is dependent on good judgment and the assumptions made during the study need to be documented and understood by the team and reviewer and kept for a future PHA.

The team conducting the PHA need to understand the methodology that is going to be used. A PHA team can vary in size from two people to a number of people with varied operational and technical backgrounds. Some team members may only be a part of the team for a limited time. The team leader needs to be fully knowledgeable in the proper implementation of the PHA methodology that is to be used and should be impartial in the evaluation. The other full- or part-time team members need to provide the team with expertise in areas such as process technology, process design, operating procedures and practices, including how the work is actually performed, alarms, emergency procedures, instrumentation, maintenance procedures, both routine and nonroutine tasks, including how the tasks are authorized, procurement of parts and supplies, safety and health, and any other relevant subject as the need dictates. At least one team member must be familiar with the process.

The ideal team will have an intimate knowledge of the standards, codes, specifications, and regulations applicable to the process being studied. The selected team members need to be compatible and the team leader needs to be able to manage the team and the PHA study. The team needs to be able to work together while benefiting from the expertise of others on the team or outside the team, to resolve issues, and to forge a consensus on the findings of the study and the recommendations.

The application of a PHA to a process may involve the use of different methodologies for various parts of the process. For example, a process involving a series of unit operations of varying sizes, complexities, and ages may use different methodologies and team members for each operation. Then the conclusions can be integrated into one final study and evaluation. A more specific example is the use of a checklist PHA for a standard boiler or heat exchanger and the use of a Hazard and Operability PHA for the overall process. Also, for batch type processes like custom batch operations, a generic PHA of a representative batch may be used where there are only small changes of monomer or other ingredient ratios and the chemistry is documented for the full range and ratio of batch ingredients. Another process that might consider using a generic type of PHA is a gas plant. Often these plants are simply moved from site to site and therefore, a generic PHA may be used for these movable plants. Also, when an employer has several similar size gas plants and no sour gas is being processed at the site, then a generic PHA is feasible as long as the variations of the individual sites are accounted for in the PHA. Finally, when an employer has a large continuous process which has several control rooms for different portions of the process such as for a distillation tower and a blending operation, the employer may wish to do each segment separately and then integrate the final results.

Additionally, small businesses which are covered by this rule will often have processes that have less storage volume, less capacity, and less complicated than processes at a large facility. Therefore, OSHA would anticipate that the less complex methodologies would be used to meet the PHA criteria in the standard. These PHAs can be done in less time and with a few people being involved. A less complex process generally means that less data, P&IDs, and process information are needed to perform a PHA.

Many small businesses have processes that are not unique, such as cold storage lockers or water treatment facilities. Where employer associations have a number of members with such facilities, a generic PHA, evolved from a checklist or what—if questions, could be developed and used by each employer effectively to reflect his/her particular process; this would simplify compliance for them.

When the employer has a number of processes which require a PHA, the employer must set up a priority system of which PHAs to conduct first. A preliminary or gross hazard analysis may be useful in prioritizing the processes that the employer has determined are subject to coverage by the PSM standard. Consideration should first be given to those processes with the potential of adversely affecting the largest number of employees. This prioritizing should consider the potential severity of a chemical release, the number of potentially affected employees, the operating history of the process such as the frequency of chemical releases, the age of the process and any other relevant factors. These factors would suggest a ranking order and would suggest either using a weighing factor system or a systematic ranking method. The use of a preliminary hazard analysis would assist an employer in determining which process should be of the highest priority and thereby the employer would obtain the greatest improvement in safety at the facility.

Initial Hazard Analysis

Before starting a hazards analysis program, management should determine if their process is covered by the regulation. A list of covered chemicals along with the legal threshold quantities is provided in an attachment to the standard. Generally, small quantities of hydrocarbons used as fuel are excluded. However, legal advice as to which chemicals are included should always be sought. The list of covered chemicals can change as OSHA issues letters of interpretation and when courts adjudicate on the scope of the standard.

The order in which hazards analyses are carried out is usually determined by a preliminary consequence ranking; i.e., those processes which have the potential for creating the most serious consequences are analyzed first. This can be done through the use of a Major Hazards Screening. In practice, the order in which hazards analyses are carried out is also affected by logistical issues such as the availability of up-to-date P&IDs or of key personnel to serve as hazards analysis team members.

Methodology

The standard lists six different methods for conducting a hazards analysis. It also provides for the use of other methods that are not listed in the regulation. The key point is that the regulation permits a great deal of flexibility regarding the choice of method. In particular, there is no requirement that the HAZOP method always be used. The *onus* is on the facility's management to choose the techniques that most effectively reduce risk.

Issues to Address

The hazards identification process must include a review of previous incidents and those near misses which had the potential to create a serious accident. The OSHA standard also identifies administrative issues (such as operating procedures and training) as being an important part of a hazards analysis. In addition, the standard calls for an analysis of siting and human factors.

Team

OSHA stresses the importance of a team-based approach to all types of hazards analysis, but such an approach is fundamental for those techniques that fall into the first category, i.e., those that are primarily creative or imaginative. (Other techniques such as fault tree analysis are less suitable for team participation. However, even in such cases, a team is needed to identify the base events, and to discuss the cause and effect relationships that exist within the system being analyzed.)

Team members should represent the various operations, technical disciplines, and contractor groups present in the facility or on the design team. The use of such team encourages the development of cross-discipline thinking and also helps address the Employee Participation requirements of the standard.

Revalidation

OSHA requires that the hazards analysis be updated and revalidated at least every 5 years. The regulation does not require that a full hazards analysis be conducted for the revalidation—although it may make sense to do so if many changes have been made to the facility since the first hazards analysis was carried out, and/or the MOC process was not always followed.

If it is decided that a full hazards analysis is not required for the revalidation, then what can be called a “hazards analysis-by-exception” is required. Such an approach evaluates the full hazards analysis that was performed originally, then checks out the impact of changes that have been made since that time.

If the other elements of the PSM program have been properly implemented, particularly the MOC and Prestartup Safety Review (PSSR) elements, then the hazards analysis validation should be quite straightforward. If the first hazards analysis was a HAZOP, it is often appropriate for the subsequent analyses to use either the What−If or the Checklist methods. Doing so will save time, and will probably provide for a superior analysis because the team members will be using a fresh way of thinking and will be less likely to be bored.

4. OPERATING PROCEDURES

In this book, Operating Procedures is covered in Chapter 6. The OSHA standard and guidance are shown below (some administrative detail has been removed).

Standard

1. The employer shall develop and implement written operating procedures that provide clear instructions for safely conducting activities involved in each covered process consistent with the PSI and shall address at least the following elements.

  i. Steps for each operating phase:

    A. Initial startup

    B. Normal operations

    C. Temporary operations

    D. Emergency shutdown including the conditions under which emergency shutdown is required, and the assignment of shutdown responsibility to qualified technicians to ensure that emergency shutdown is executed in a safe and timely manner

    E. Emergency operations

F. Normal shutdown
G. Startup following a turnaround or after an emergency shutdown.

ii. Operating limits:
A. Consequences of deviation
B. Steps required to correct or avoid deviation.

iii. Safety and health considerations:
A. Properties of, and hazards presented by, the chemicals used in the process
B. Precautions necessary to prevent exposure, including engineering controls, administrative controls, and personal protective equipment
C. Control measures to be taken if physical contact or airborne exposure occurs
D. Quality control for raw materials and control of hazardous chemical inventory levels
E. Any special or unique hazards.

iv. Safety systems and their functions.

2. Operating procedures shall be readily accessible to employees who work in or maintain a process.

3. The operating procedures shall be reviewed as often as necessary to assure that they reflect current operating practice, including changes that result from changes in process chemicals, technology, and equipment, and changes to facilities. The employer shall certify annually that these operating procedures are current and accurate.

4. The employer shall develop and implement safe work practices to provide for the control of hazards during operations such as lockout/tagout; confined space entry; opening process equipment or piping; and control over entrance into a facility by maintenance, contractor, laboratory, or other support personnel. These safe work practices shall apply to employees and contractor employees.

Guidance

Operating procedures describe tasks to be performed, data to be recorded, operating conditions to be maintained, samples to be collected, and safety and health precautions to be taken. The procedures need to be technically accurate, understandable to employees, and revised periodically to ensure that they reflect current operations. The PSI package is to be used as a resource to better assure that the operating procedures and practices are consistent with the known hazards of the chemicals in the process and that the operating parameters are accurate. Operating procedures should be reviewed by engineering staff and operating personnel to ensure that they are accurate and provide practical instructions on how to actually carry out job duties safely.

Operating procedures will include specific instructions or details on what steps are to be taken or followed in carrying out the stated procedures. These operating instructions for each procedure should include the applicable safety precautions and should contain appropriate information on safety implications. For example, the operating procedures addressing operating parameters will contain operating instructions about pressure limits, temperature ranges, flow rates, what to do when an upset condition occurs, what alarms and instruments are pertinent if an upset condition occurs, and other subjects. Another example of using operating instructions to properly implement operating procedures is in starting up or shutting down the process. In these cases, different parameters will be required from those of normal operation. These operating instructions need to clearly indicate the distinctions between startup and normal operations such as the appropriate allowances for heating up a unit to reach the normal operating parameters. Also the operating instructions need to describe the proper method for increasing the temperature of the unit until the normal operating temperature parameters are achieved.

Computerized process control systems add complexity to operating instructions. These operating instructions need to describe the logic of the software as well as the relationship between the equipment and the control system; otherwise, it may not be apparent to the operator.

Operating procedures and instructions are important for training operating personnel. The operating procedures are often viewed as the standard operating practices (SOPs) for operations. Control room personnel and operating staff, in general, need to have a full understanding of operating procedures. If workers are not fluent in English then procedures and instructions need to be prepared in a second language understood by the workers. In addition, operating procedures need to be changed when there is a change in the process as a result of the MOC procedures. The consequences of operating procedure changes need to be fully evaluated and the information conveyed to the personnel. For example, mechanical changes to the process made by the maintenance department (like changing a valve from steel to brass or other subtle changes) need to be evaluated to determine if operating procedures and practices also need to be changed. All MOC actions must be coordinated and integrated with current operating procedures and operating personnel must be oriented to the changes in procedures before the change is made. When the process is shutdown in order to make a change, then the operating procedures must be updated before startup of the process.

Training in how to handle upset conditions must be accomplished as well as what operating personnel are to do in emergencies such as when a pump seal fails or a pipeline ruptures. Communication between operating personnel and workers performing work within the process area, such as nonroutine tasks, also must be maintained. The hazards of the tasks are to be conveyed to operating personnel in accordance with established procedures and to those performing the actual tasks. When the work is completed, operating personnel should be informed to provide closure on the job.

Written Down

In many facilities, the tasks that the operators have to perform are well understood, with much of the information as to how to run the facility being passed on verbally. OSHA, and all other regulators, makes it clear that such informal practices are not acceptable. All procedures and instructions must be written down—either on paper or on a computer screen.

Initial Startup

By “initial” startup, it is assumed that OSHA is referring to the startup of a facility that has just been commissioned. The term is used in this chapter more broadly to describe the startup of a unit after a total shutdown when equipment has been cleared for entry so that major maintenance work can be performed.

Temporary and Emergency Operations

It is tempting not to bother with procedures for temporary operations because of the transitory nature of such operations. Yet the need for procedures in such situations may actually be greater than it is for normal operations because the facility is *prime facie* operating outside its normal operating range (and possibly outside its safe range). Moreover, the operators may be operating outside their experience envelope and so are more likely to need procedures than they would for the normal operations with which they are already very familiar.

Procedures are also needed to handle emergencies and sudden shutdowns.

Certification

OSHA requires that operating procedures be certified annually. This requirement does not mean that the procedures have to be revised every year—revisions are needed only when there has been a change in the operation. However, this requirement does mean that each procedure has to be checked as to its current validity at least once a year.

OSHA does not define the word “certification.” In general, it is probably a good idea for the operations manager of a covered facility to put a letter in the file each year stating the following:

- A complete set of operating procedures for the facility is in place.
- Someone on the manager’s support staff reviews the complete list of procedures annually and checks for gaps or inconsistencies.

- The MOC process captures those changes that require modifications to procedures, and the procedures are updated accordingly.
- There is a system for the operators and other personnel to suggest changes and improvements to the procedures.
- A process is in place such that operators and technical specialists can report gaps or deficiencies in the procedures and that those problems are addressed in a timely manner.
- The procedures are subject to a formal audit on a regular basis.

Therefore, when a manager signs an operating procedure, he or she is not saying that the content is technically correct; it is very unlikely that he or she will have sufficient detailed operating knowledge to make such a statement. The manager's signature is simply stating that a system for writing and checking procedures exists (based on the bullet points above) and that the system was followed.

5. TRAINING

In this book, Training is covered in Chapter 7. The OSHA standard and guidance are shown below (some administrative detail has been removed).

Standard

1. Initial training.

  i. Each employee presently involved in operating a process, and each employee before being involved in operating a newly assigned process, shall be trained in an overview of the process and in the operating procedures as specified in paragraph (f) of this section. The training shall include emphasis on the specific safety and health hazards, emergency operations including shutdown, and safe work practices applicable to the employee's job tasks.

  ii. In lieu of initial training for those employees already involved in operating a process on May 26, 1992, an employer may certify in writing that the employee has the required knowledge, skills, and abilities to safely carry out the duties and responsibilities as specified in the operating procedures.

2. Refresher training. Refresher training shall be provided at least every 3 years, and more often if necessary, to each employee involved in operating a process to assure that the employee understands and adheres to the current operating procedures of the process. The employer, in consultation with the employees involved in operating the process, shall determine the appropriate frequency of refresher training.

3. Training documentation. The employer shall ascertain that each employee involved in operating a process has received and understood the training required by this paragraph. The employer shall prepare a record which contains the identity of the employee, the date of training, and the means used to verify that the employee understood the training.

Guidance

All employees, including maintenance and contractor employees, involved with highly hazardous chemicals need to fully understand the safety and health hazards of the chemicals and processes they work with for the protection of themselves, their fellow employees and the citizens of nearby communities. Training conducted in compliance with 1910.1200, the Hazard Communication standard, will help employees to be more knowledgeable about the chemicals they work with as well as familiarize them with reading and understanding MSDS. However, additional training in subjects such as operating procedures and safety work practices, emergency evacuation and response, safety procedures, routine and nonroutine work authorization activities, and other areas pertinent to process safety and health will need to be covered by an employer's training program.

In establishing their training programs, employers must clearly define the employees to be trained and what subjects are to be covered in their training. Employers in setting up their training program will need to clearly establish the goals and objectives they wish to achieve with the training that they provide to their employees. The learning goals or objectives should be written in clear measurable terms before the training begins. These goals and objectives need to be tailored to each of the specific training modules or segments. Employers should describe the important actions and conditions under which the employee will demonstrate competence or knowledge as well as what is acceptable performance.

Hands-on-training where employees are able to use their senses beyond listening will enhance learning. For example, operating personnel, who will work in a control room or at control panels, would benefit by being trained at a simulated control panel or panels. Upset conditions of various types could be displayed on the simulator, and then the employee could go through the proper operating procedures to bring the simulator panel back to the normal operating parameters. A training environment could be created to help the trainee feel the full reality of the situation but, of course, under controlled conditions. This realistic type of training can be very effective in teaching employees correct procedures while allowing them to also see the consequences of what might happen if they do not follow established operating procedures. Other training techniques using videos or on-the-job training can also be very effective for teaching other job tasks, duties, or other important information. An effective training program will allow the employee to fully participate in the training process and to practice their skill or knowledge.

Employers need to periodically evaluate their training programs to see if the necessary skills, knowledge, and routines are being properly understood and implemented by their trained employees. The means or methods for evaluating the training should be developed along with the training program goals and objectives. Training program evaluation will help employers to determine the amount of training their employees understood, and whether the desired results were obtained. If, after the evaluation, it appears that the trained employees are not at the level of knowledge and skill that was expected, the employer will need to revise the training program, provide retraining, or provide more frequent refresher training sessions until the deficiency is resolved. Those who conducted the training and those who received the training should also be consulted as to how best to improve the training process. If there is a language barrier, the language known to the trainees should be used to reinforce the training messages and information.

Careful consideration must be given to assure that employees including maintenance and contract employees receive current and updated training. For example, if changes are made to a process, impacted employees must be trained in the changes and understand the effects of the changes on their job tasks (e.g., any new operating procedures pertinent to their tasks). Additionally, as already discussed the evaluation of the employee's absorption of training will certainly influence the need for training.

OSHA places great emphasis on the documentation of training; unless the training is properly documented, it will not be recognized as satisfactory by an auditor.

The OSHA regulation with regard to training is quite straightforward. Basically, operators must be trained in the operating procedures for the unit in which they are working, and their training must be updated as needed, but always within 3 years. The "grandfather" clause for those operators who were working on the facility before the standard was issued is becoming less relevant as new operators come on board and as experienced operators go through the 3-year refresher programs. This topic of "grandfathering" can be sensitive. Management may suspect that some of the experienced operators do not fully understand the tasks for which they are responsible and which they are currently performing. Therefore, they can use the training program to (i) test everyone to determine if their suspicions are correct and (ii) bring everyone up to the same standard. However, the operators may resent this; they may feel that they are being "put down" by being tested on actions that they feel they know very well indeed.

The OSHA Guidance refers to the 1910.1200 (HAZCOM) standard as a source of training, particularly with regard to hazardous chemicals.

In terms of meeting the OSHA standard, documentation of training is often a major problem. Companies may sponsor training programs of all types, but, unless the training is properly documented, it will not be recognized as satisfactory by an auditor.

6. CONTRACTORS

The OSHA standard and guidance to do with contractors are shown below (some administrative detail has been removed).

Standard

1. Application. This paragraph applies to contractors performing maintenance or repair, turnaround, major renovation, or specialty work on or adjacent to a covered process. It does not apply to contractors providing incidental services which do not influence process safety, such as janitorial work, food and drink services, laundry, delivery or other supply services.

2. Employer responsibilities.

- **i.** The employer, when selecting a contractor, shall obtain and evaluate information regarding the contract employer's safety performance and programs.
- **ii.** The employer shall inform contract employers of the known potential fire, explosion, or toxic release hazards related to the contractor's work and the process.
- **iii.** The employer shall explain to contract employers the applicable provisions of the emergency action plan required by paragraph (n) of this section.
- **iv.** The employer shall develop and implement safe work practices consistent with paragraph (f)(4) of this section, to control the entrance, presence and exit of contract employers and contract employees in covered process areas.
- **v.** The employer shall periodically evaluate the performance of contract employers in fulfilling their obligations as specified in paragraph (h)(3) of this section.
- **vi.** The employer shall maintain a contract employee injury and illness log related to the contractor's work in process areas.

3. Contract employer responsibilities.

- **i.** The contract employer shall assure that each contract employee is trained in the work practices necessary to safely perform his/her job.
- **ii.** The contract employer shall assure that each contract employee is instructed in the known potential fire, explosion, or toxic release hazards related to his/her job and the process, and the applicable provisions of the emergency action plan.
- **iii.** The contract employer shall document that each contract employee has received and understood the training required by this paragraph. The contract employer shall prepare a record which contains the identity of the contract employee, the date of training, and the means used to verify that the employee understood the training.
- **iv.** The contract employer shall assure that each contract employee follows the safety rules of the facility including the safe work practices required by paragraph (f)(4) of this section.
- **v.** The contract employer shall advise the employee of any unique hazards presented by the contract employer's work or of any hazards found by the contract employer's work.

Guidance

Employers who use contractors to perform work in and around processes that involve highly hazardous chemicals will need to establish a screening process so that they hire and use contractors who accomplish the desired job tasks without compromising the safety and health of employees at a facility. For contractors, whose safety performance on the job is not known to the hiring employer, the employer will need to obtain information on injury and illness rates and experience and should obtain contractor references.

Additionally, the employer must assure that the contractor has the appropriate job skills, knowledge, and certifications (such as for pressure vessel welders). Contractor work methods and experiences should be evaluated. For example, does the contractor conducting demolition work swing loads over operating processes or does the contractor avoid such hazards?

Maintaining a site injury and illness log for contractors is another method employers must use to track and maintain current knowledge of work activities involving contract employees working on or adjacent to covered processes. Injury and illness logs of both the employer's employees and contract employees allow an employer to have full knowledge of process injury and illness experience. This log will also contain information which will be of use to those auditing PSM compliance and those involved in incident investigations.

Contract employees must perform their work safely. Considering that contractors often perform very specialized and potentially hazardous tasks such as confined space entry activities and nonroutine repair activities, it is quite important that their activities be controlled while they are working on or near a covered process. A permit system or work authorization system for these activities would also be helpful to all affected employers. The use of a work authorization system keeps an employer informed of contract employee activities, and as a benefit the employer will have better coordination and more management control over the work being performed in the process area.

A well run and well maintained process where employee safety is fully recognized will benefit all of those who work in the facility whether they be contract employees or employees of the owner.

Application

This paragraph provides guidance as to what constitutes a contract worker. Subcontractors and their employees are included.

Although OSHA separates contract workers who are providing "incidental" services from those who are working with hazardous chemicals, it is important to ensure that their work is indeed incidental to the process and that they do not become inadvertently involved with the process in some manner. For example, if a contract worker is supplying snacks and soft drinks for the lunch room inside a plant, he or she will probably need to know about the use of basic safety clothing and what to do in the event of an emergency.

Employer Responsibilities

This paragraph highlights what the employer is expected to do when hiring and training contractors. Note that all of these requirements explicitly require the employers to be involved in the management of contractors. Companies cannot distance themselves from safety responsibilities by handing off the work to an outside contractor and then leaving them to it.

The standard makes it clear that a contract company's safety record is to be reviewed before they are hired and that safety record should be evaluated as part of the overall contractor selection process. Generally, the contractor's OSHA 300 logs will be used for this evaluation.

7. PRESTARTUP SAFETY REVIEW

The topic of PSSRs is covered in Chapter 8. The OSHA standard and guidance to do with PSSRs is to be found in paragraph (i) of the regulation. They read as follows:

Standard

The employer shall perform a prestartup safety review for new facilities and for modified facilities when the modification is significant enough to require a change in the PSI.

The prestartup safety review shall confirm that prior to the introduction of highly hazardous chemicals to a process:

i. Construction and equipment is in accordance with design specifications
ii. Safety, operating, maintenance, and emergency procedures are in place and are adequate
iii. For new facilities, a PHA has been performed and recommendations have been resolved or implemented before startup; and modified facilities meet the requirements contained in MOC, paragraph (l) [of this regulation].

Guidance

For new processes, the employer will find a PHA helpful in improving the design and construction of the process from a reliability and quality point of view. The safe operation of the new process will be enhanced by making use of the PHA recommendations before final installations are completed. P&IDs are to be completed along with having the operating procedures in place and the operating staff trained to run the process before startup. The initial startup procedures and normal operating procedures need to be fully evaluated as part of the prestartup review to assure a safe transfer into the normal operating mode for meeting the process parameters.

For existing processes that have been shutdown for turnaround, or modification, etc., the employer must assure that any changes other than “replacement in kind” made to the process during shutdown go through the MOC procedures. P&IDs will need to be updated as necessary, as well as operating procedures and instructions. If the changes made to the process during shutdown are significant and impact the training program, then operating personnel as well as employees engaged in routine and nonroutine work in the process area may need some refresher or additional training in light of the changes. Any incident investigation recommendations, compliance audits or PHA recommendations need to be reviewed as well to see what impacts they may have on the process before beginning the startup.

Process Safety Information

The first paragraph of the regulation states that a PSSR is needed whenever PSI is changed. In effect, this states that any modification significant enough to go through MOC will have to be evaluated with a PSSR because virtually all changes at this level trigger a change in PSI.

In reality, many companies elect not to perform a PSSR on small changes since the change itself occurs almost as soon as the MOC approval has been obtained, so the PSSR appears to be redundant. Also, it is less likely that a small project will suffer from some of the cost-cutting/schedule-meeting difficulties alluded at the beginning of this chapter. Nevertheless, a strict interpretation of the standard would seem to indicate that a PSSR should be carried out on any change that is significant enough to lead to a change in the PSI, which means virtually all changes: large and small.

In all cases, the PSSR should include a field walk down of the changed system before that system is started.

Construction and Equipment

Many of the potential short-cutting activities discussed at the start of this chapter will involve construction and equipment installation. The first part of the OSHA regulation discusses this issue explicitly.

There are two ways in which the correct implementation of design specifications can be checked. The PSSR team members can carry out spot checks of the installed piping and equipment, and compare it with the piping lists and equipment data sheets. The second way is to make sure that a system of turnover packages (which are discussed below) has been implemented and followed.

Procedures

The Readiness Review should check that safety, operating, and emergency procedures for any new operation have been written down. The standard also mentions maintenance procedures here, even though they are not identified elsewhere in the regulation.

New/Modified Facilities

The regulation requires that new facilities conduct a PHA. Therefore, the PSSR should check that the PHA was in fact carried out and that its recommendations were either resolved or implemented. During the pressure of construction, there is sometimes a tendency to postpone some of the PHA recommendations for "further study" as a convenient way of putting them off because there is insufficient time and/or money to implement them. The PSSR team members should carefully check any recommendations that were postponed, and satisfy themselves that such postponements are justified, and do not jeopardize the safety of the plant.

8. MECHANICAL INTEGRITY

The title "Mechanical Integrity" is too limiting in scope because the standard covers instrumentation items such as controls and emergency shutdown systems. In this book, the topic of Mechanical Integrity is covered in Chapter 9. The OSHA standard and guidance to do with Mechanical Integrity is to be found in paragraph (j) of the regulation.

Standard

1. Application. Paragraphs (j)(2)–(j)(6) of this section apply to the following process equipment:
   i. Pressure vessels and storage tanks
   ii. Piping systems (including piping components such as valves)
   iii. Relief and vent systems and devices
   iv. Emergency shutdown systems
   v. Controls (including monitoring devices and sensors, alarms, and interlocks)
   vi. Pumps.
2. Written procedures. The employer shall establish and implement written procedures to maintain the ongoing integrity of process equipment.
3. Training for process maintenance activities. The employer shall train each employee involved in maintaining the ongoing integrity of process equipment in an overview of that process and its hazards and in the procedures applicable to the employee's job tasks to assure that the employee can perform the job tasks in a safe manner.
4. Inspection and testing.

  - **i.** Inspections and tests shall be performed on process equipment.
  - **ii.** Inspection and testing procedures shall follow recognized and generally accepted good engineering practices.
  - **iii.** The frequency of inspections and tests of process equipment shall be consistent with applicable manufacturers' recommendations and good engineering practices, and more frequently if determined to be necessary by prior operating experience.
  - **iv.** The employer shall document each inspection and test that has been performed on process equipment. The documentation shall identify the date of the inspection or test, the name of the person who performed the inspection or test, the serial number or other identifier of the equipment on which the inspection or test was performed, a description of the inspection or test performed, and the results of the inspection or test.

5. Equipment deficiencies. The employer shall correct deficiencies in equipment that are outside acceptable limits (defined by the PSI in paragraph (d)) before further use or in a safe and timely manner when necessary means are taken to assure safe operation.

6. Quality assurance.

  - **i.** In the construction of new plants and equipment, the employer shall assure that equipment as it is fabricated is suitable for the process application for which they will be used.
  - **ii.** Appropriate checks and inspections shall be performed to assure that equipment is installed properly and consistent with design specifications and the manufacturer's instructions.
  - **iii.** The employer shall assure that maintenance materials, spare parts, and equipment are suitable for the process application for which they will be used.

Guidance

Employers will need to review their maintenance programs and schedules to see if there are areas where "breakdown" maintenance is used rather than an ongoing mechanical integrity program. Equipment used to process, store, or handle highly hazardous chemicals needs to be designed, constructed, installed, and maintained to minimize the risk of releases of such chemicals. This requires that a mechanical integrity program be in place to assure the continued integrity of process equipment. Elements of a mechanical integrity program include the identification and categorization of equipment and instrumentation, inspections and tests, testing and inspection frequencies, development of maintenance procedures, training of maintenance personnel, the establishment of criteria for acceptable test results, documentation of test and inspection results, and documentation of manufacturer recommendations as to meantime to failure for equipment and instrumentation.

The first line of defense an employer has available is to operate and maintain the process as designed, and to keep the chemicals contained. This line of defense is backed up by the next line of defense which is the controlled release of chemicals through venting to scrubbers or flares, or to surge or overflow tanks which are designed to receive such chemicals, etc. These lines of defense are the primary lines of defense or means to prevent unwanted releases. The secondary lines of defense would include fixed fire protection systems like sprinklers, water spray, or deluge systems, monitor guns, etc., dikes, designed drainage systems, and other systems which would control or mitigate hazardous chemicals once an unwanted release occurs. These primary and secondary lines of defense are what the mechanical integrity program needs to protect and strengthen these primary and secondary lines of defenses where appropriate.

The first step of an effective mechanical integrity program is to compile and categorize a list of process equipment and instrumentation for inclusion in the program. This list would include pressure vessels, storage tanks, process piping, relief and vent systems, fire protection system components, emergency shutdown systems and alarms and interlocks and pumps. For the categorization of instrumentation and the listed equipment, the employer would prioritize which pieces of equipment require closer scrutiny than others. Meantime to failure of various instrumentation and equipment parts would be known from the manufacturers data or the employer's experience with the parts, which would then influence the inspection and testing frequency and associated procedures. Also, applicable codes and standards such as the National Board Inspection Code, or those from the American Society for Testing and Material, API, NFPA, ANSI, ASME, and other groups provide information to help establish an effective testing and inspection frequency, as well as appropriate methodologies.

The applicable codes and standards provide criteria for external inspections for items such as foundation and supports, anchor bolts, concrete or steel supports, guy wires, nozzles and sprinklers, pipe hangers, grounding connections, protective coatings and insulation, and external metal surfaces of piping and vessels. These codes and standards also provide information on methodologies for internal inspection, and a frequency formula based on the corrosion rate of the materials of construction. Also, erosion both internal and external needs to be considered along with corrosion effects for piping and valves. Where the corrosion rate is not known, a maximum inspection frequency is recommended, and methods of developing the corrosion rate are available in the codes. Internal inspections need to cover items such as vessel shell, bottom and head; metallic linings; nonmetallic linings; thickness measurements for vessels and piping; inspection for erosion, corrosion, cracking, and bulges; internal equipment like trays, baffles, sensors and screens for erosion, corrosion, or cracking and other deficiencies. Some of these inspections may be performed by state or local government inspectors under state and local statutes. However, each employer needs to develop procedures to ensure that tests and inspections are conducted properly and that consistency is maintained even where different employees may be involved. Appropriate training is to be provided to maintenance personnel to ensure that they understand the preventive maintenance program procedures, safe practices, and the proper use and application of special equipment or unique tools that may be required. This training is part of the overall training program called for in the standard.

A quality assurance system is needed to help ensure that the proper materials of construction are used, that fabrication and inspection procedures are proper, and that installation procedures recognize field installation concerns. The quality assurance program is an essential part of the mechanical integrity program and will help to maintain the primary and secondary lines of defense that have been designed into the process to prevent unwanted chemical releases or those which control or mitigate a release. "As built" drawings, together with certifications of coded vessels and other equipment, and materials of construction need to be verified and retained in the quality assurance documentation. Equipment installation jobs need to be properly inspected in the field for use of proper materials and procedures and to assure that qualified craftsmen are used to do the job. The use of appropriate gaskets, packing, bolts, valves, lubricants, and welding rods need to be verified in the field. Also, procedures for installation of safety devices need to be verified such as the torque on the bolts on ruptured disc installations, uniform torque on flange bolts, and proper installation of pump seals. If the quality of parts is a problem, it may be appropriate to conduct audits of the equipment supplier's facilities to better assure proper purchases of required equipment which is suitable for its intended service. Any changes in equipment that may become necessary will need to go through the MOC procedures.

Application

This section describes the equipment to which the standard applies. The list covers not just equipment and piping but also instrumentation (hence the term *mechanical* integrity seems to be too limiting). It is assumed here that the word "Pumps" in paragraph (vi) includes all types of rotating equipment.

Written Procedures

The development of Mechanical Integrity procedures can be based on the principles used for writing operating and maintenance procedures.

Training

This covers more than just maintenance training. All employees need to be aware of mechanical integrity issues. For example, Chapter 11 describes an accident that was caused by the installation of an incorrect gasket. This incident involved both an operator and a warehouse worker, both of whom needed training in mechanical integrity as it applied to their work.

Inspection and Testing

Inspection and testing are at the heart of a mechanical integrity program. Guidance as to how and when inspection and testing should be done is based on manufacturer recommendations, engineering practice, and operating experience. As with all other elements of PSM, thorough documentation is needed.

One issue to watch for with regard to inspection is that the inspection activity may itself introduce an uncontrolled change into the system which in turn could lead to the occurrence of an accident.

Deficiencies

Any identified deficiencies must be addressed. This means that a budget should be prepared to take care of those items that will require attention following the Mechanical Integrity inspections.

Quality Assurance

In the context of process safety, quality assurance is more concerned with problems that lead to accidents rather than product quality in the customer satisfaction sense. However, there is generally a close relationship between the two.

9. HOT WORK

In this book, the topic of Hot Work is covered in Chapter 8. The OSHA standard and guidance to do with Hot Work is to be found in paragraph (j) of the regulation.

Standard

1. The employer shall issue a hot work permit for hot work operations conducted on or near a covered process.
2. The permit shall document that the fire prevention and protection requirements in 29 CFR 1910.252(a) have been implemented prior to beginning the hot work operations; it shall indicate the dates authorized for hot work and identify the object on which hot work is to be performed. The permit shall be kept on file until completion of the hot work operation.

Guidance

Nonroutine work which is conducted in process areas needs to be controlled by the employer in a consistent manner. The hazards identified involving the work that is to be accomplished must be communicated to those doing the work, but also to those operating personnel whose work could affect the safety of the process. A work authorization notice or permit must have a procedure that describes the steps the maintenance supervisor, contractor representative, or other person needs to follow to obtain the necessary clearance to get the job started. The work authorization procedures need to reference and coordinate, as applicable, lockout/tagout procedures, line breaking procedures, confined space entry procedures, and hot work authorizations. This procedure also needs to provide clear steps to follow once the job is completed in order to provide closure for those that need to know the job is now completed and equipment can be returned to normal.

The PSM standard cross-references 29 CFR 1910.252(a), which is the provision of the Welding, Cutting, and Brazing Standards dealing with fire prevention and protection.

The OSHA PSM standard also refers to the NFPA Standard for Fire Prevention in Use of Cutting and Welding Processes (51B, 1962). One of NFPA's principle concerns is to do with the isolation of hot work from flammable materials. The following steps must be followed:

1. Remove the object to be welded or cut to a safe place, i.e., away from the flammable materials.
2. If (1) cannot be done, remove the flammable materials to a safe place.
3. If (2) cannot be done, place guards around the work to prevent heat, sparks, and slag from reaching the fire hazard.
4. If (3) cannot be done, the work shall not be performed.

While the work is being performed, fire extinguishers must be in place, and a fire watch shall be maintained.

10. MANAGEMENT OF CHANGE

MOC is discussed in Chapter 10. The OSHA standard and guidance is to be found in paragraph (k) of the regulation.

Standard

1. The employer shall establish and implement written procedures to manage changes (except for "replacements in kind") to process chemicals, technology, equipment, and procedures, and changes to facilities that affect a covered process.
2. The procedures shall assure that the following considerations are addressed prior to any change:
   - i. The technical basis for the proposed change
   - ii. Impact of change on safety and health
   - iii. Modifications to operating procedures
   - iv. Necessary time period for the change
   - v. Authorization requirements for the proposed change.
3. Employees involved in operating a process and maintenance and contract employees whose job tasks will be affected by a change in the process shall be informed of, and trained in, the change prior to start-up of the process or affected part of the process.
4. If a change covered by this paragraph results in a change in the PSI required by paragraph (d), such information shall be updated accordingly.
5. If a change covered by this paragraph results in a change in the operating procedures or practices required by paragraph (f), such procedures or practices shall be updated accordingly.

Guidance

To properly manage changes to process chemicals, technology, equipment, and facilities, one must define what is meant by change. In this PSM standard, change includes all modifications to equipment, procedures, raw materials, and processing conditions other than "replacement in kind." These changes need to be properly managed by identifying and reviewing them prior to implementation of the change. For example, the operating procedures contain the operating parameters (pressure limits, temperature ranges, flow rates, etc.) and the importance of operating within these limits.

While the operator must have the flexibility to maintain safe operation within the established parameters, any operation outside of these parameters requires review and approval by a written MOC procedure.

MOC covers issues such as changes in process technology and changes to equipment and instrumentation. Changes in process technology can result from changes in production rates, raw materials, experimentation, equipment unavailability, new equipment, new product development, change in catalyst, and changes in operating conditions to improve yield or quality. Equipment changes include among others change in materials of construction, equipment specifications, piping prearrangements, experimental equipment, computer program revisions, and changes in alarms and interlocks. Employers need to establish means and methods to detect both technical changes and mechanical changes.

Temporary changes have caused a number of catastrophes over the years, and employers need to establish ways to detect temporary changes as well as those that are permanent. It is important that a time limit for temporary changes be established and monitored since, without control, these changes may tend to become permanent. Temporary changes are subject to the MOC provisions. In addition, the MOC procedures are used to insure that the equipment and procedures are returned to their original or designed conditions at the end of the temporary change. Proper documentation and review of these changes is invaluable in assuring that the safety and health considerations are being incorporated into the operating procedures and the process.

Employers may wish to develop a form or clearance sheet to facilitate the processing of changes through the MOC procedures. A typical change form may include a description and the purpose of the change, the technical basis for the change, safety and health considerations, documentation of changes for the operating procedures, maintenance procedures, inspection and testing, P&IDs, electrical classification, training and communications, prestartup inspection, duration if a temporary change, approvals and authorization. Where the impact of the change is minor and well understood, a checklist reviewed by an authorized person with proper communication to others who are affected may be sufficient. However, for a more complex or significant design change, a hazard evaluation procedure with approvals by operations, maintenance, and safety departments may be appropriate. Changes in documents, such as P&IDs, raw materials, operating procedures, mechanical integrity programs, and electrical classifications, need to be noted so that these revisions can be made permanent when the drawings and procedure manuals are updated. Copies of process changes need to be kept in an accessible location to ensure that design changes are available to operating personnel as well as to PHA team members when a PHA is being done or one is being updated.

Employer Responsibility

The first paragraph makes it clear that it is the employer who is responsible for the development and implementation of the MOC program. In this context, the employer is the organization responsible for line management at the plant or facility. Other people and organizations may be involved in the design, implementation, and organization of the MOC program, but ultimately the responsibility for its success lies with the employer at the site. (If a contract company works at the facility, then management of that company also has PSM responsibilities.)

Written Down

Like all the elements of process safety, MOC procedures must be written down. This ensures consistency, and it means that they can be audited. This section of the standard introduces the phrase “replacement in kind.” The basic idea is that if an item is being replaced by something that is absolutely identical to it, then a change has not occurred, so the MOC process does not need to be implemented.

There are two aspects to this requirement. First, management must prepare a formal, written program as to how they intend to manage change in their facility. Second, all changes made through the MOC process must be fully documented, along with an explanation as to why the change was needed and what support work (such as a hazards analysis) was carried out.

On some small facilities, particularly those where the same people have been working together for many years, there is a temptation to skip the documentation of process safety activities on the grounds that "everyone knows what's going on anyway." In these situations, it is sometimes felt that verbal and informal communications are all that are needed. Even if this assumption is true (which is unlikely), the regulation still requires that all changes be properly documented. This requirement makes sense because, without written records, there can be no assurance that information was transmitted to all affected parties, or that what was transmitted was accurate. Furthermore, the changes have to be written down so that they can be audited and reviewed by outsiders.

Replacement In-Kind

The first paragraph of the OSHA MOC standard uses the phrase "Replacements In-Kind" and lists those aspects of the operation to which it can apply.

This first paragraph requires that the MOC program be written down. There are two aspects to this requirement. First, management must prepare a formal, written program as to how they intend to manage change in their facility. Second, all changes made through the MOC process must be fully documented, along with an explanation as to why the change was needed and what support work (such as a hazards analysis) was carried out.

Factors that Affect Change

The second paragraph of the regulation discusses some of the factors that must be considered when managing change. The impact of the change on safety and health and the need to update operating procedures are mentioned, along with the need to make sure that temporary changes contain a termination date and time. This paragraph also requires that the facility management determine who is authorized to approve the change.

Training and Participation/Accountability

The third paragraph covers the issues of training and employee Participation/Accountability. All affected personnel must know about the change before it is implemented. They must know how to operate the facility in the new way, recognize when problems are occurring, and respond to those problems.

Information Base

The fourth paragraph requires that PSI be updated as needed. This means that all aspects of the change must be documented, either on paper or within a computer system. The updated documentation must be complete, accurate, and provided in a timely manner.

Operating Procedures

The fifth paragraph of the regulation makes it clear that operating procedures must be brought up to date when the change is made. Maintenance procedures are not actually mentioned, but good practice would suggest that these be included in this effort. OSHA recognizes that almost all changes to the process will result in changes to the operating procedures.

Making the Change

If the change is not “in kind,” it should be properly analyzed for its impact on safety and health. For a large change, one that requires a full AFE (Authorization for Expenditure) and PHA studies, this type of analysis will usually be performed anyway. However, small, quick changes are more likely to be made with little or no analysis.

Training/PSI/Operating Procedures

Many changes will result in a different way of operating the plant. Therefore, it is important, as part of the MOC program, that all affected individuals are informed as to the change and trained in the new mode of operation. Also, PSI and the Operating Procedures must be updated.

11. INCIDENT INVESTIGATION

Incident Investigation and Root Cause Analysis is discussed in Chapter 11. The OSHA standard and guidance is to be found in paragraph (l) of the regulation.

Standard

1. The employer shall investigate each incident which resulted in, or could reasonably have resulted in a catastrophic release of a highly hazardous chemical in the workplace.
2. An incident investigation shall be initiated as promptly as possible, but not later than 48 hours following the incident.
3. An incident investigation team shall be established and consist of at least one person knowledgeable in the process involved, including a contract employee if the incident involved work of the contractor, and other persons with appropriate knowledge and experience to thoroughly investigate and analyze the incident.
4. A report shall be prepared at the conclusion of the investigation which includes as a minimum:
   - **i.** Date of incident
   - **ii.** Date investigation began
   - **iii.** A description of the incident
   - **iv.** The factors that contributed to the incident
   - **v.** Any recommendations resulting from the investigation.
5. The employer shall establish a system to promptly address and resolve the incident report findings and recommendations. Resolutions and corrective actions shall be documented.
6. The report shall be reviewed with all affected personnel whose job tasks are relevant to the incident findings including contract employees where applicable.

Guidance

Incident investigation is the process of identifying the underlying causes of incidents and implementing steps to prevent similar events from occurring. The intent of an incident investigation is for employers to learn from past experiences and thus avoid repeating past mistakes. The incidents for which OSHA expects employers to become aware and to investigate are the types of events which result in or could reasonably have resulted in a catastrophic release. Some of the events are sometimes referred to as “near misses,” meaning that a serious consequence did not occur, but could have.

Employers need to develop in-house capability to investigate incidents that occur in their facilities. A team needs to be assembled by the employer and trained in the techniques of investigation including how to conduct interviews of witnesses, needed documentation, and report writing. A multidisciplinary team is better able to gather the facts of the event and to analyze them and develop plausible scenarios as to what happened, and why. Team members should be

> selected on the basis of their training, knowledge, and ability to contribute to a team effort to fully investigate the incident. Employees in the process area where the incident occurred should be consulted, interviewed, or made a member of the team. Their knowledge of the events form a significant set of facts about the incident which occurred. The report, its findings and recommendations are to be shared with those who can benefit from the information. The cooperation of employees is essential to an effective incident investigation. The focus of the investigation should be to obtain facts, and not to place blame. The team and the investigation process should clearly deal with all involved individuals in a fair, open and consistent manner.

Investigation

The first paragraph identifies two important issues. First, it is the duty of the employer to conduct the investigation—he cannot rely on the agency or any other organization to do it for him. Second, the employer must investigate not only actual events but also near misses that could have led to a catastrophic release.

Timing

The second paragraph states the time within the investigation must start (in this case 48 hours is the maximum time allowed). No allowance is provided for holidays or other scheduled breaks. In practice, the Go Team will probably be on site much sooner than this—often within an hour or two.

Team

The regulation makes it clear that the investigation is a team effort and that the team members must be properly qualified to participate. The team must include someone who understands the process and someone who is trained in incident investigation and analysis. Contract workers must be involved where appropriate.

Report

A written report is required. This particular regulation does not call for a root cause analysis *per se*, but such an analysis will generally be carried out for an incident that is serious enough to require regulatory involvement.

Follow up

There must be prompt follow up to the investigation. Action to prevent similar events from occurring again is required.

Participation

This paragraph of the regulation also requires that people affected by the incident should be properly informed as to what corrective actions were taken, and how they themselves should be involved.

12. EMERGENCY PLANNING AND RESPONSE

The process safety regulation to do with emergency planning and response provides very little detail. Instead it refers companies to other OSHA standards which already cover this topic in detail, particularly §1910.38(a) (Employee Emergency Plans and Fire Prevention Plans) and §1910.165 (Alarm Systems). Other OSHA documents that can be of assistance with regard to emergency planning and response include:

- 29 CFR 1910.36 (b)—Building and Structure Egress
- 29 CFR 1910.38 (a)—Employee Emergency Plan
- 29 CFR 1910.120 (a)(g)(p)—HAZWOPER
- 29 CFR 1910.156—Fire Brigades
- 29 CFR 1910.165—Employee Alarm Systems.

In most areas of process safety, there is very little difference between the OSHA PSM standard and the EPA RMP rule. However, emergency response is an exception to this—there are significant differences between the two, largely due to the fact that the EPA is concerned with the impact of a release on members of the general public, whereas OSHA is more interested in worker safety.

Standard

The employer shall establish and implement an emergency action plan for the entire plant in accordance with the provisions of 29 CFR 1910.38(a). In addition, the emergency action plan shall include procedures for handling small releases. Employers covered under this standard may also be subject to the hazardous waste and emergency response provisions contained in 29 CFR 1910.120(a), (p), and (q).

Guidance

Each employer must address what actions employees are to take when there is an unwanted release of highly hazardous chemicals. Emergency preparedness or the employer's tertiary (third) lines of defense are those that will be relied on along with the secondary lines of defense when the primary lines of defense which are used to prevent an unwanted release fail to stop the release. Employers will need to decide if they want employees to handle and stop small or minor incidental releases. Whether they wish to mobilize the available resources at the plant and have them brought to bear on a more significant release. Or whether employers want their employees to evacuate the danger area and promptly escape to a preplanned safe zone area, and allow the local community emergency response organizations to handle the release. Or whether the employer wants to use some combination of these actions. Employers will need to select how many different emergency preparedness or tertiary lines of defense they plan to have and then develop the necessary plans and procedures, and appropriately train employees in their emergency duties and responsibilities and then implement these lines of defense.

Employers at a minimum must have an emergency action plan which will facilitate the prompt evacuation of employees when there is an unwanted release of highly hazardous chemical. This means that the employer will have a plan that will be activated by an alarm system to alert employees when to evacuate and, that employees who are physically impaired, will have the necessary support and assistance to get them to the safe zone as well. The intent of these requirements is to alert and move employees to a safe zone quickly. Delaying alarms or confusing alarms are to be avoided. The use of process control centers or similar process buildings in the process area as safe areas is discouraged. Recent catastrophes have shown that a large life loss has occurred in these structures because of where they have been sited and because they are not necessarily designed to withstand overpressures from shockwaves resulting from explosions in the process area.

Unwanted incidental releases of highly hazardous chemicals in the process area must be addressed by the employer as to what actions employees are to take. If the employer wants employees to evacuate the area, then the emergency action plan will be activated. For outdoor processes where wind direction is important for selecting the safe route to a refuge area, the employer should place a wind direction indicator such as a wind sock or pennant at the highest point that can be seen throughout the process area. Employees can move in the direction of crosswind to upwind to gain safe access to the refuge area by knowing the wind direction.

If the employer wants specific employees in the release area to control or stop the minor emergency or incidental release, these actions must be planned for in advance and procedures developed and implemented. Preplanning for handling incidental releases for minor emergencies in the process area needs to be done, appropriate equipment for the hazards must be provided, and training conducted for those employees who will perform the emergency work before they respond to handle an actual release. The employer's training program, including the Hazard Communication standard training is to address the training needs for employees who are expected to handle incidental or minor releases.

Preplanning for releases that are more serious than incidental releases is another important line of defense to be used by the employer. When a serious release of a highly hazardous chemical occurs, the employer through preplanning will have determined in advance what actions employees are to take. The evacuation of the immediate release area and other areas as necessary would be accomplished under the emergency action plan. If the employer wishes to use plant personnel such as a fire brigade, spill control team, a hazardous materials team, or use employees to render aid to those in the immediate release area and control or mitigate the incident, these actions are covered by §1910.120, the Hazardous Waste Operations and Emergency Response (HAZWOPER) standard. If outside assistance is necessary, such as through mutual aid agreements between employers or local government emergency response organizations, these emergency responders are also covered by HAZWOPER. The safety and health protections required for emergency responders are the responsibility of their employers and of the on-scene incident commander

Responders may be working under very hazardous conditions and therefore the objective is to have them competently led by an on-scene incident commander and the commander's staff, properly equipped to do their assigned work safely, and fully trained to carry out their duties safely before they respond to an emergency. Drills, training exercises, or simulations with the local community emergency response planners and responder organizations is one means to obtain better preparedness. This close cooperation and coordination between plant and local community emergency preparedness managers will also aid the employer in complying with the EPA's Risk Management Plan criteria.

One effective way for medium to large facilities to enhance coordination and communication during emergencies for on plant operations and with local community organizations is for employers to establish and equip an emergency control center. The emergency control center would be sited in a safe zone area so that it could be occupied throughout the duration of an emergency. The center would serve as the major communication link between the on-scene incident commander and plant or corporate management as well as with the local community officials. The communication equipment in the emergency control center should include a network to receive and transmit information by telephone, radio, or other means. It is important to have a backup communication network in case of power failure or one communication means fails. The center should also be equipped with the plant layout and community maps, utility drawings including fire water, emergency lighting, appropriate reference materials such as a government agency notification list, company personnel phone list, SARA Title III reports and MSDSs, emergency plans and procedures manual, a listing with the location of emergency response equipment, mutual aid information, and access to meteorological or weather condition data and any dispersion modeling data.

Although the regulation itself is largely limited to references to other standards, the OSHA Guidance does provide some useful information for setting up an Emergency Plan. Some of the key points are as follows:

1. Employers need to decide what type of release their own employees can reasonably be expected to handle. For small releases, the best action to take is often to find the isolation valves on either side of the release and to close them. For a major incident, operators need to close the unit Emergency Isolation Valves (EIVs). There is a balance here; on the one hand, having a person move into a situation to close the valves puts him at risk. On the other hand, if he does not take prompt action, the small release may become bigger and could lead to many more

people being affected. Some companies implement a rule that a person will always move away from a situation, not toward it, unless he is part of the emergency response team and is dressed in the appropriate protective clothing.

2. For each type of release and fire, employers must ensure that emergency evacuation routes are in place.
3. There must be an alarm system. OSHA §1910.165 provides information on how to set up such a system.
4. The Guidance discourages the use of control rooms as safe areas on the assumption that such buildings are not blast proof. If they are, then they would be an excellent place to assemble, depending on their proximity to the accident. If the danger is from the release of a toxic gas, it is important to make sure that the air conditioning for these buildings can be isolated so that the gas is not pulled into the control room. Some companies provide air packs inside the control room.
5. Guidance on the emergency release of hazardous chemicals is provided in §29 CFR 1910.120 (the HAZWOPER) standard.

13. COMPLIANCE AUDITS

The OSHA standard and guidance to do with auditing is to be found in paragraph (o) of the regulation.

Standard

1. Employers shall certify that they have evaluated compliance with the provisions of this section at least every 3 years to verify that the procedures and practices developed under the standard are adequate and are being followed.
2. The compliance audit shall be conducted by at least one person knowledgeable in the process.
3. A report of the findings of the audit shall be developed.
4. The employer shall promptly determine and document an appropriate response to each of the findings of the compliance audit, and document that deficiencies have been corrected.
5. Employers shall retain the two (2) most recent compliance audit reports.

Guidance

Employers need to select a trained individual or assemble a trained team of people to audit the process safety management system and program. A small process or plant may need only one knowledgeable person to conduct an audit. The audit is to include an evaluation of the design and effectiveness of the process safety management system and a field inspection of the safety and health conditions and practices to verify that the employer's systems are effectively implemented. The audit should be conducted or lead by a person knowledgeable in audit techniques and who is impartial towards the facility or area being audited. The essential elements of an audit program include planning, staffing, conducting the audit, evaluation and corrective action, follow-up and documentation.

Planning in advance is essential to the success of the auditing process. Each employer needs to establish the format, staffing, scheduling, and verification methods prior to conducting the audit. The format should be designed to provide the lead auditor with a procedure or checklist which details the requirements of each section of the standard. The names of the audit team members should be listed as part of the format as well. The checklist, if properly designed, could serve as the verification sheet which provides the auditor with the necessary information to expedite the review and assure that no requirements of the standard are omitted. This verification sheet format could also identify those elements that will require evaluation or a response to correct deficiencies. This sheet could also be used for developing the follow-up and documentation requirements.

The selection of effective audit team members is critical to the success of the program. Team members should be chosen for their experience, knowledge, and training and should be familiar with the processes and with auditing techniques, practices, and procedures. The size of the team will vary depending on the size and complexity of the process under consideration. For a large, complex, highly instrumented plant, it may be desirable to have team members with expertise in process engineering and design, process chemistry, instrumentation and computer controls, electrical hazards and classifications, safety and health disciplines, maintenance, emergency preparedness, warehousing or shipping, and process safety auditing. The team may use part-time members to provide for the depth of expertise required as well as for what is actually done or followed, compared to what is written.

An effective audit includes a review of the relevant documentation and PSI, inspection of the physical facilities, and interviews with all levels of plant personnel. Utilizing the audit procedure and checklist developed in the preplanning stage, the audit team can systematically analyze compliance with the provisions of the standard and any other corporate policies that are relevant. For example, the audit team will review all aspects of the training program as part of the overall audit. The team will review the written training program for adequacy of content, frequency of training, effectiveness of training in terms of its goals and objectives as well as to how it fits into meeting the standard's requirements, documentation, etc. Through interviews, the team can determine the employee's knowledge and awareness of the safety procedures, duties, rules, emergency response assignments, etc. During the inspection, the team can observe actual practices such as safety and health policies, procedures, and work authorization practices. This approach enables the team to identify deficiencies and determine where corrective actions or improvements are necessary.

An audit is a technique used to gather sufficient facts and information, including statistical information, to verify compliance with standards. Auditors should select as part of their preplanning a sample size sufficient to give a degree of confidence that the audit reflects the level of compliance with the standard. The audit team, through this systematic analysis, should document areas which require corrective action as well as those areas where the process safety management system is effective and working in an effective manner. This provides a record of the audit procedures and findings, and serves as a baseline of operation data for future audits. It will assist future auditors in determining changes or trends from previous audits.

Corrective action is one of the most important parts of the audit. It includes not only addressing the identified deficiencies but also planning, follow up, and documentation. The corrective action process normally begins with a management review of the audit findings. The purpose of this review is to determine what actions are appropriate, and to establish priorities, timetables, resource allocations and requirements and responsibilities. In some cases, corrective action may involve a simple change in procedure or minor maintenance effort to remedy the concern. MOC procedures need to be used, as appropriate, even for what may seem to be a minor change. Many of the deficiencies can be acted on promptly, while some may require engineering studies or in-depth review of actual procedures and practices. There may be instances where no action is necessary and this is a valid response to an audit finding. All actions taken, including an explanation where no action is taken on a finding, needs to be documented as to what was done and why.

It is important to assure that each deficiency identified is addressed, the corrective action to be taken noted, and the audit person or team responsible be properly documented by the employer. To control the corrective action process, the employer should consider the use of a tracking system. This tracking system might include periodic status reports shared with affected levels of management, specific reports such as completion of an engineering study, and a final implementation report to provide closure for audit findings that have been through MOC, if appropriate, and then shared with affected employees and management. This type of tracking system provides the employer with the status of the corrective action. It also provides the documentation required to verify that appropriate corrective actions were taken on deficiencies identified in the audit.

Certification

The OSHA standard requires that an audit be carried out at least every 3 years. Failure to do will likely lead to a willful citation from OSHA. Some elements of the PSM program may need to be audited more frequently depending on the degree of risk that they represent.

In an interpretation letter, OSHA states

> Government safety inspectors will not routinely request that employers who voluntarily evaluate work sites for potential safety and health problems provide the findings to the government during safety and health inspections, the Occupational Safety and Health Administration announced today.

Technical Qualifications

The standard requires that at least one of the investigators should be knowledgeable in the process. Usually, this expertise will be provided by a process or operations expert who works on the unit being audited. If the audit is large and/or complex, specialists can be called in to review specific areas, such as electrical or instrumentation systems.

The OSHA guidance does not require that the audit team include someone from outside the organization or facility being audited. Nevertheless, it is often a good idea to use such a person. He or she will not be affected by internal personality issues, and, if a major problem is identified, will be able to report it without fear of retribution. Also, an outsider will be able to bring his or her experience from other companies to provide a reference against which to evaluate the present facility. Another reason for bringing in an outsider is that it is unusual for an operating facility to have someone on its payroll who is an expert in the audit process.

Report

The end product of all audits is a report. The layout of a typical report is discussed in Chapter 20.

Response

The standard requires that any findings from the audit are properly addressed. It is important to make sure that, once a problem has been resolved, the resolution is properly documented.

Retention of Reports

The audit reports must be retained as specified. They become part of the facility's PSI.

CHAPTER

CULTURE AND PARTICIPATION

3

CHAPTER OUTLINE

INTRODUCTION

The discussion in Chapter 1 showed how safety and risk management programs developed over the last 200 years. Typically new programs and approaches were introduced once existing systems had become mature and well established. The discussion also showed that current risk management initiatives are largely to do with the topic of culture and employee participation. Hence much of the recent literature to do with Process Safety Management (PSM) speaks to the topic of company culture. For example, the Baker Commission report to do with the 2005 accident at Texas City

Process Risk and Reliability Management. DOI: http://dx.doi.org/10.1016/B978-0-12-801653-4.00003-5

(Baker, 2007) uses the word culture many times; the following is a representative quotation from that report:

> BP has not instilled a common, unifying process safety culture among its U.S. refineries. Each refinery has its own separate and distinct process safety culture.

This chapter discusses the nature of culture as it applies to the safety and general risk management of process facilities. Also discussed here are related issues such as Key Performance Indicators (KPIs), Employee Participation, Behavior-Based Safety (BBS) and Inherent Safety.

Although the topic of culture is now receiving a good deal of attention from companies in the process and energy businesses, the word itself is very difficult to define in the context of process risk management systems. A dictionary definition is:

> The predominating attitudes and behavior that characterize the functioning of a group or organization.

The key word in the above definition is "functioning"—culture is about what people actually *do*—not what they say, think, or plan to do.

Other definitions of culture, such as "Culture is the way we do things around here," may be true, but they are basically circular and self-referential. Such definitions offer little practical help at eight o'clock on Monday morning.

It can be argued that there really is no such thing as an organizational culture. Any organization is made up of individuals, each of whom has knowledge, attitudes, and beliefs. It is the sum of these traits that makes up an organization's culture. As people join and leave the organization so its culture changes. In the words of Trevor Kletz, "Organizations don't have memory—only people do." Nevertheless organizations with a strong culture (either positive or negative) can, to some degree, cause people to change their behaviors and attitudes, and the culture will remain stable, even as people enter and leave the organization. Moreover, a strong culture adapts to new circumstances without its basic values being affected by issues such as economic downturns or the introduction of new technologies.

An organization's culture is determined not only by the people who work for and with the company, but also the larger environment in which it works, including the industry, the physical environment (such as offshore vs. onshore), national characteristics, and laws.

REGULATIONS AND STANDARDS

Because of its abstract nature it is difficult to write regulations to do with culture. Nevertheless some agencies have developed guidance on the topic.

BSEE STANDARD FOR CULTURE

In December 2012, the Bureau of Safety and Environmental Enforcement published a Draft Safety Culture Policy Statement (BSEE, 2012) with a request for public comments. This proposed policy is based on a Culture Policy Statement from the Nuclear Regulatory Commission.

Because the BSEE policy statement represents one of the first attempts to develop a regulation to do with culture in the process and energy industries it is analyzed in Table 3.1, which has three columns. The first column shows the page number of the Statement, the second column provides an extract from the Statement, and the third column provides some analysis and discussion.

An important issue that is not discussed in the draft Policy Statement is how to measure an organization's culture. A topic such as culture is inherently abstract and it is difficult to develop a means of measuring progress. Discussion of this topic with regards to KPIs is provided below.

Table 3.1 Analysis of BSEE Draft Statement on Culture

Page	Policy Statement	Analysis/Discussion
1	The BSEE defines safety culture as the core values and behaviors resulting from a collective commitment by leaders and individuals to emphasize safety, over competing goals, to ensure protection of people and the environment.	This definition looks is concerned only with the organization in question. It does not explicitly discuss the fact that an organization's culture is affected by the broader environment in which it works, including industry norms, regulations and national characteristics.
3	A major component of each report that has followed the *Deepwater Horizon* explosion and resulting oil spill is the recommendation to improve the safety culture upon the Outer Continental Shelf.	An analysis of these reports is provided in an upcoming OTC paper.
3	The National Commission recommended looking at the nuclear industry for an example of drastic improvement in safety culture.	No reference document is cited.
3	The BSEE has reviewed the NRC's safety culture policy and believes it provides a strong foundation for a similar approach for oil and gas operations on the OCS. . .	A draft NRC document is located at www.stb07.com/downloads/NRC-Culture-Draft.pdf.
4	. . . BSEE will include appropriate means to monitor safety culture in its oversight programs and internal management processes.	It is not clear if the topic of culture will become part of a regulation, such as an extension to SEMS.
4	. . . an appreciation for the importance of safety, emphasizing the need for its integration and balance with competing performance objectives to achieve optimal protection without compromising production goals.	The Statement is circling the issue of acceptable risk, but there are no definitions of terms such as "balance" and "optimal performance." In the limit, the only way of achieving optimal safety performance is not to work offshore. BSEE does not attempt to address, even peripherally, ALARP ("As Low as Reasonably Practical Risk").
4	(1) Leadership Leaders demonstrate a commitment to safety in their decisions and behaviors.	This statement is true, but the true test of leadership from senior managers is their willingness to spend money or to take production delays in order to ensure safe operations.
5	(2) Problem Identification and Resolution . . . issues are promptly. . . addressed and corrected commensurate with their significance.	The Statement does not provide any guidance as to how the "significance" is to be determined or evaluated (this comment relates to the issue of ALARP, discussed above).

Table 3.1 Analysis of BSEE Draft Statement on Culture *Continued*

Page	Policy Statement	Analysis/Discussion
5	(3) Personal Accountability All individuals take personal responsibility for safety.	One of the concepts of BBS is that, if a person sees an unsafe situation, then he or she must take action, regardless of who has the formal responsibility.
5	(4) Work Processes The process of planning and controlling work activities is implemented so that safety is maintained.	
5	(5) Continuous Learning Opportunities to learn about ways to ensure safety are sought out and implemented.	
5	(6) Environment for Raising Concerns	
5	(7) Effective Safety Communication	
5	(8) Respectful Working Environment	
5	(9) Inquiring Attitude	

HSE AND CULTURE

This brochure was published by the Petroleum Safety Authority of Norway. The Table of Contents is:

1. Introduction
2. HSE and culture
3. Characteristics of a sound HSE culture
4. Factors with can affect the HSE culture
5. Management and culture.

The basis for this brochure is that, when no recommendations are provided as to how high standards of safety are to be reached then each enterprise must set its own standards—including the creation of a culture.

NATIONAL ENERGY BOARD

The Canadian National Energy Board has published a draft standard to do with culture (NEB, 2013). The following are the key elements of the document:

- Cultural Threat #1: Production Pressure
- Cultural Threat #2: Complacency
- Cultural Threat #3: Normalization of Deviance
- Cultural Threat #4: Tolerance of Inadequate Systems and Resources
- Cultural Defense #1: Committed Safety Leadership
- Cultural Defense #2: Vigilance
- Cultural Defense #3: Empowerment and Accountability
- Cultural Defense #4: Resiliency.

SURVEY

The DuPont Company has developed a 24-question survey to do with culture. They report the following perception gaps based on many years of results (Soczek, 2011):

- 88% of managers say they themselves give safety top priority while 51% of workers think managers give safety top priority.
- 94% of supervisors say they themselves give safety top priority while 62% of hourly workers think supervisors give safety top priority.
- 87% of workers say they themselves give safety top priority while only 74% of workers say that other workers give safety top priority.

WARNING FLAGS OVER YOUR ORGANIZATION

One way of understanding culture and determining means of improving it is to examine actual incidents in order to determine what lessons can be learned from them.

One event is discussed here to show how lessons can be learned from such catastrophes. In the late 1990s, a processing plant in the southern United States suffered a severe explosion. Although no one died, some workers were seriously injured and the economic loss was calamitous. Following the disaster the plant manager wrote an unpublished paper called *Warning Flags over Your Organization*. In this paper, which he presented to his management team, he attempted to explain how this facility, whose normal safety metrics (such as lost time accidents and recordables) were quite good, could have reached a point where it quite literally blew up. The subtitle of the paper was *How Lucky Are You Feeling Today?* The author recognized that most facility managers elect to take risks, and, that most of the time, there are no serious consequences resulting from such decisions. Moreover, their tenure in their current job is likely to be relatively short, so they can hope to run out the clock—any problems can be addressed by the next manager. However, in the case of this manager the good luck ran out on his watch. His paper spoke to those issues that "everyone knows about, but that no one is willing to address."

The manager started his paper by noting that virtually all process facilities in the United States fly three flags at the front gate: the flag of the United States, the flag of the State in which the facility is located, and the company flag. He suggested that if a facility has crossed a safety threshold then a fourth flag—analogous to a storm warning flag—should be flown. Of course the idea of flying a warning flag in this manner was suggested tongue-in-cheek, but the idea of recognizing that an unsafe zone has been entered and that a storm threatens is a vital component of any company's culture.

The basic idea behind warning flag concept is that, as an organization is stretched further and further sudden and catastrophic failure is more likely to occur. An analogy is with a rubber band, which, as it is stretched further and further, will eventually reach a point where it suddenly snaps; it fails not gradually, but suddenly and totally. In other words, health, safety, and environmental (HSE) problems do not necessarily provide early indications of potentially serious problems; the first signs of trouble could be a sudden and massive failure.

The following six indicators or warning flags can help management determine if they have crossed a safety threshold.

1. Unrealistic stretch goals
2. Excessive cost reduction
3. Belief that “It Cannot Happen Here”
4. Overconfidence based on rule compliance
5. Departmentalized information flow
6. Ineffective audit processes.

Discussion to do with each of the flags is provided below. In some cases, guidance is provided as to what corrective actions can be taken to help lower that particular flag.

FLAG ONE—UNREALISTIC STRETCH GOALS

Managers are under constant pressure to increase production, improve efficiencies, enhance quality, and beat safety and environmental records. All this generally has to be done without employing more people, equipment or investment capital. Therefore, these managers must “stretch” the organization. But, if the organization is stretched too far a major failure will occur—the rubber band snaps.

Stretch goals often illustrate the Law of Unintended Consequences: attempting to achieve increased production leads to a major failure such that the losses are greater than the hoped-for benefits—many times over.

Stretch goals include the following:

- Production creep
- Production records
- Initiative overload.

Production Creep

Production creep occurs when production goals are gradually increased without a corresponding increase in resources (equipment or personnel) to help management achieve those goals. Nor is capital provided to upgrade the capacity of the facility.

For example, if a facility makes say 1000 tons of product (or 100,000 barrels or whatever) per month, production creep occurs if the managers are asked to increase rates to say 1100 tons per month using just current resources. If this production increase is successful then the managers may then be encouraged to try for say 1200 tons—once more without additional resources being made available.

Eventually, this stretching leads to the occurrence of a major failure, the rubber band snaps, and all the incremental revenue that has been generated in previous years from the stretching of the production resources is more than canceled out by the losses associated with that single catastrophic failure.

Production Records

Everyone wants to be on a winning team. Production records are one mark of such a team. Such records are achieved either by making ever increasing quantities of product in a short period of time, or by running the facility for longer and longer periods of time without shutting down for routine maintenance and inspection.

The risk associated with attempts at production records is that management may be tempted to let equipment run in a potentially unsafe mode in order to avoid a shutdown to conduct maintenance. For example, a pump rotor may become imbalanced, leading to mild vibration of the pump itself. Rather than shutting down the affected section of the facility to repair the pump, management may decide to keep the pump running, thus creating the possibility of a seal leak and a release of large amounts of toxic or flammable materials.

Operating personnel may also be expected to work longer hours without sufficient breaks. (This was a factor in the 2005 Texas City explosion.)

Initiative Overload

Operating and maintenance personnel are frequently asked to implement a wide range of performance-improvement initiatives—often simultaneously. Examples of such initiatives include ISO 14001, Six Sigma, asbestos abatement, statistical process control, and the installation of sophisticated computer-control systems. Taken in isolation, each initiative is usually a good investment of time and resources, and may even be required by regulation or in response to litigation. The difficulty is that, if too many initiatives are being implemented at one time, managers and workers become overloaded. Consequently, the initiatives may not be implemented properly, and/or they take up so much of the time of key employees such that not enough attention is paid to maintaining safe normal operations. Such employees will tend to respond to the introduction of yet more new initiatives with the response, “When will I find time to do my real work?”

One means of ensuring that production creep and other stretch goals do not lead to unsafe conditions is to be sure that new targets and goals are reviewed as part of the Management of Change (MOC) program, as discussed in Chapter 10. If the safe upper limit for production is defined as being say 1000 tons per month, then any instruction to go above that rate should be treated as a “not-in-kind” change, and be subject to scrutiny through hazards analyses, audits, prestartup safety reviews, and other PSM tools.

FLAG TWO—EXCESSIVE COST REDUCTION

The discussion in the previous section to do with production creep stated that managers are often asked to achieve greater production using just existing resources. In fact, the situation is often worse than this; managers are often also asked to cut expenses at the same time as they are increasing production rates. The mantra for this philosophy is, “Do More with Less.” If the cost cutting becomes excessive, then a warning flag should be raised.

The book *Lessons from Longford* (Hopkins, 2000) states, “when we extend the causal network <for an accident> far enough, market forces and cost-cutting pressures are almost invariably implicated.”

The paper *The Titanic Disaster*: *An Enduring Example of Money Management vs. Risk Management* (Brander, 1995) that was referenced in Chapter 1 discusses cost-cutting pressures. The following is a quotation from that paper.

> Most of the discussion of the accident revolves around specific problems. There was the lack of sufficient lifeboats (enough for at most 1200 on a ship carrying 2200). There was the steaming ahead at full-speed despite various warnings about the ice-field. There was the lack of binoculars

> for the lookout. There were the poor procedures with the new invention, the wireless (not all warnings sent to the ship reached the bridge, and a nearby ship, the operator abed, missed Titanic's SOS). Very recently, from recovered wreckage, "Popular Science" claimed the hull was particularly brittle even for the metallurgy of the time. (A claim now debunked.) Each has at one time or another been put forward as "THE reason the Titanic sank."
>
> What gets far less comment is that most of the problems all came from a larger, systemic problem: the owners and operators of steamships had for five decades taken larger and larger risks to save money—risks to which they had methodically blinded themselves. The Titanic disaster suddenly ripped away the blindfolds and changed dozens of attitudes, practices, and standards almost literally overnight.

Of course, managers have always been under pressure to cut costs. However, for the last 20 years or so this pressure has become ever more relentless—largely due to global competition. In such an environment a manager may think on the following lines:

> Three years ago, under pressure from head office, we downsized our engineering department from 20 to 15 professionals. The savings helped the plant meet its financial goals (and also improved my bonus). Head office was so pleased with the result that a year later we cut another five engineering professionals. Some of the nagging reliability problems we have had since then can probably be attributed to these cuts, but we did improve profitability once again, and I have to accept that our operation is hanging in there.
>
> Maybe it was because of this success in cutting costs, senior management decided to relocate four of the remaining ten professionals to head office (200 kilometers away) so as to reduce travel costs and office expenses. So now we are down to six on-site engineers from the 20 we had just 3 years ago.
>
> I'm worried that we may be heading for a major accident because we have cut our technical support so drastically. Maybe I should raise a warning flag. However, I can't be sure, so I'll just have to trust to luck. After all, serious accidents happen only rarely, and I expect to be assigned to a new position within a year or two. Then these worries become someone else's problem.

Another quotation of the same type as Brander's comments to do with the Titanic is shown below. It is taken from an unattributed slideshow presentation prepared following the sinking of a 33,000 tonne offshore platform (P36 in Brazil)—what was then the world's largest floating production platform—in the year 2001. The quotation purports to be taken from a memo written by a manager on the project during the design and construction phases of the project.

> <Our company> has established new global benchmarks for the generation of exceptional shareholder wealth through an aggressive and innovative program of cost cutting on its new facility. Conventional constraints have been successfully challenged and replaced with new paradigms appropriate to the globalized corporate market place. Through an integrated network of facilitated workshops, the project successfully rejected the established constricting and negative influences of prescriptive engineering, onerous quality requirements, and outdated concepts of inspection and client control. Elimination of these unnecessary straitjackets has empowered the project's suppliers and contractors to propose highly economical solutions, with the win-win bonus of enhanced profitability margins for themselves. The platform shows the shape of things to come.

Examples of cost-cutting measures that can lead to problems include the following:

- Reduction of “nonessentials”
- Reductions in the size of the workforce
- The “Big Crew Change”
- Flattened organizations
- Aging infrastructure
- Outsourcing
- Not enough time for detailed work
- Project cutbacks
- Organizational spread.

Reduction of “Nonessentials”

When managers want to cut costs they first look for supposedly “nonessential” activities or resources, such as training or excessive inventory of spare parts in the warehouse. Reducing expenditures on such activities and resources certainly leads to short-term cost reductions. However, over a longer period of time these cuts can create unsafe conditions. In *Lessons from Longford* Hopkins notes that cuts in the maintenance budget played a major role in that disaster.

A careful analysis of the findings from a facility’s incident investigations can help determine if cost-cutting measures may have gone too far. For example, if many incidents result from people not having sufficient training, then maybe the Training Department was “slimmed down” too far. Alternatively, if those incidents result from failed equipment items then the Maintenance Department needs to be provided with more resources.

Reductions in Workforce

In recent decades, companies have been relentless in their drive to reduce headcount. The pressures to do so have often resulted from mergers and acquisitions where the justification for the merger was that overlapping and duplicated functions could be eliminated, thus resulting in the elimination of “unnecessary” jobs. However, such cuts may represent a false economy; indeed merging two organizations may actually require a temporary *increase* in the number of service personnel so that the two different systems and cultures can be integrated successfully.

One particularly troublesome issue to do with workforce reductions is that, when cuts are made, it is often the personnel with more experience who leave. Such people, being older, are more likely to be qualified for early retirement or “the package.” Also, their departure leads to a greater reduction in costs because they are paid more than the younger employees. Unfortunately, this means that the newer people have fewer gray-haired mentors to monitor their actions and decisions. This loss of experience problem is not new—indeed it is the theme of Trevor Kletz’s book, *Lessons from Disaster—How Organizations Have No Memory and Accidents Recur* (Kletz, 1993).

Staff reductions have been particularly noticeable in corporate and engineering departments because many of the people who work in those departments are not perceived as being critical to the attainment of short-term production goals. Therefore, it is often felt that they can be released (or not replaced when they retire). If their expertise is required, it is argued, then experts from outside companies can be brought in on a contract basis. In fact, managers may choose not to bring in anyone at all. They may simply ask their remaining personnel to carry out a larger number of tasks. Such a strategy creates three difficulties:

1. The engineers who remain have more work to do in the same amount of time than they had in the past. Therefore, no matter how dedicated they may be, it is likely that their work will not be as thorough as it would have been in the past when more time was allowed to study specific technical issues.
2. There will be fewer subject matter experts to help identify and correct problems. If the company expert to do with pressure relief valves, say, retires and is not replaced, then problems with the design and operation of relief valves may not even be identified.
3. Even if outside experts or retirees are brought in, they will not be *au courant* with what is going on at the facility, so it is less likely that they will be able to offer immediate help.
   There is some company knowledge that cannot be brought in off the street. If a person has worked at a company for many years, particularly in a specialist department, and he leaves without having trained a replacement, there is almost certain to be a loss of "corporate memory." People brought in from the outside may be very knowledgeable, but they cannot possibly know all of the history and background as to why things are the way they are at this particular location.

The "Big Crew Change"

A phrase sometimes used in the petroleum industry to describe the loss of experienced personnel is "Big Crew Change" (Gell, 2008). The phrase is mainly used with regard to the large number of baby-boomer generation engineers and technical experts who will be retiring after the year 2010. These experienced personnel are not being replaced by sufficient younger people with comparable technical skills and experience. For example, it has been reported that

> Between 1983 and 2002, the number of U.S. petroleum engineers declined from 33,000 to 18,000...

In other areas of plant operations, the loss of personnel is compensated for by using increasingly powerful computer systems. For example, a Distributed Control System (DCS) can carry out many of the functions previously performed by several operators. Similarly, sophisticated design software lets one engineer carry out calculations that previously had to be done by a team. Yet there remain certain actions that have to be carried out by people; the loss of skilled personnel in these situations represents a true loss.

Flattened Organizations

Gaps between the layers of management have grown as a result of programs that "flatten the organization." Consequently, the gaps between the layers of supervision and management have increased. Relatively junior and inexperienced employees are called on to make decisions without being able to tap into the guidance and assistance of more experienced personnel. Moreover, newer employees will have fewer opportunities to learn from their more experienced predecessors during the normal course of their work.

Another concern is that the number of experienced people in many organizations has been reduced. Hence, many process changes that were previously handled quickly and effectively on a semiformal basis by experienced personnel who knew each other very well, and who also had an intimate knowledge of the processes for which they were responsible now must be handled in a more formal manner.

Aging Infrastructure

Not only is the workforce aging, so is the equipment itself. The manager of a large U.S. oil refinery dating from the 1920s recently said of his facility that, “The steel is tired.” He was concerned that an accident could occur because so much of the equipment was old and worn out and that it was not being replaced or upgraded quickly enough. Another manager, this time at an old petrochemical plant, said, “My plant is old but the engineers are young.” He did not intend his phrase as a compliment. He was worried about the problems caused by old equipment and the fact that his technical staff lacked the knowledge and experience to address those problems.

Outsourcing

One way in which staff reductions can be made, while keeping the organization functioning, is to outsource work to outside companies and personnel. If the work is truly one-off, such as the engineering and installation of a new piece of equipment, then the use of an outside company will usually be the best choice. However, if the work being outsourced is a core function then this strategy can create difficulties. No outsider, no matter how experienced and talented, can know all aspects of an operation in the way that a long-term employee can.

For example, on one plant a particular compressor started to vibrate slightly. The long-term employees knew that this vibration was the precursor to a more serious problem, and that immediate corrective action was needed. However, these employees had been replaced with outside contract workers. The new workers did not recognize the seriousness of the vibration, hence they did not take corrective action quickly enough, and a serious leak of process fluids occurred.

The loss of experienced personnel also reduces the chance of developing long-term solutions to operational or maintenance issues. A contract worker is less likely to care about such long-term issues, and so is less likely to make suggestions and contributions. Yet the involvement of all employees is crucial to the success of a process safety program.

Not Enough Time for Detailed Work

One consequence of the relentless reductions in the workforce is that people become so busy that they do not have enough time for detailed work. In particular, they do not have time to check their work, or the work of their colleagues. Hence a greater chance that errors will slip through exists.

In engineering and design companies, the lack of resources can lead to calculations not being properly checked. In the case of operating facilities, the lack of time for detailed work may lead to operating instructions being written without being checked or work permits being issued in haste.

Project Cutbacks

It is an unusual project that does not run into scheduling and/or budget problems. Such problems inevitably create pressure to take shortcuts or to eliminate some equipment items so as to get the project back on schedule thereby increasing the chance of a PSM shortcut. The MOC and Operational Readiness programs should help ensure that such actions do not create an unacceptable safety problem.

Organizational Spread

One feature of the increased globalization of commerce is that an increasing amount of project work is spread around the world. This is done to reduce costs and to exploit the availability of skilled personnel.

Spreading work around the world means that companies have to rely heavily on their formal decision-making processes; there is less opportunity for person-to-person interaction. Yet it is just such interactions that are invaluable in risk management work, particularly with regard to the identification and assessment of hazards. The more the organization is spread, the greater the belief that process is all and that no special, subjective skills are required.

FLAG THREE—BELIEF THAT “IT CANNOT HAPPEN HERE”

Behind much of the thinking associated with the “Do More with Less” approach is a feeling that, “it cannot happen here.” After all, catastrophic events happen so rarely that it is unlikely that a particular manager will actually experience such an event on his or her watch.

The following factors contribute toward the “I’ll chance it” syndrome.

- Lack of direct experience
- Good occupational safety performance
- Lack of imaginative thinking
- Failure to learn from near misses
- Failure to draw on experience elsewhere.

Lack of Direct Experience

Catastrophic accidents occur only rarely. This means that most employees will not have actually experienced such an event. Ironically, this lack of direct experience can be a particular problem for those conducting hazards analyses at those facilities that have excellent safety and environmental records. Managers and workers in such organizations do not necessarily become complacent but they may become a little too comfortable and satisfied with what they have achieved. They have trouble “thinking the unthinkable.” Conversely, on those plants that have witnessed a serious accident within the last few years there can be no denial that such events happen. For example, Process Hazards Analysis (PHA) leaders will often hear remarks from highly experienced team members such as “I’ve been here 14 years, and I’ve never seen that happen. . .” with the unspoken implication, “. . . therefore it cannot happen.” It is the job of the PHA leader to crack that shell of unjustified self-satisfaction.

Following the incident at the “Warning Flags” facility discussed at the beginning of this chapter, management at that facility decided to conduct a series of Hazard and Operability Studies (HAZOPs). During those HAZOPs, whenever any team member took the, “It can’t happen here” approach, all that the leader had to do was point out of the window. There, lying on the ground behind police evidence barrier tape, was the wreckage of the destroyed equipment. No words were needed.

Good Occupational Safety Performance

One root of the “It Cannot Happen Here” attitude is that, managers and employees fail to distinguish between occupational safety and system safety. Yet, as discussed in the previous chapter, the actions needed to improve occupational safety, as measured by the number of lost time accidents, say, are different from those needed to prevent catastrophic, low frequency, process-safety-related events. Companies that have routinely reported excellent day-to-day and month-to-month safety figures have been shocked to find that one of their plants has had a major fire or a large chemical release that came "out of the blue."

Failure to Learn from Near Misses

The investigation of a serious event frequently shows that a similar accident had occurred before, but that one item in the chain of events was not in place. For example, at one facility, certain critical safety valves were known not be reliable. If they did not close properly, large quantities of flammable gas would vent to the atmosphere. This event had occurred a number of times over a period of years with no serious consequence. However, one particular release occurred during a lightning storm. The lightning lit off the gas; the subsequent fire initiated a train of events that resulted in a serious explosion.

The use of Incident Analysis to understand cultural issues is discussed by Sutton (2008).

Failure to Draw on Experience Elsewhere

All organizations can learn from the experience of others. In spite of the litigious atmosphere in which the process industries work, information on accidents is available. Organizations such as the Center for Chemical Process Safety (CCPS) and the Chemical Safety Board (CSB) publish information, as do industry trade groups and specialist groups at professional meetings.

FLAG FOUR—OVERCONFIDENCE IN RULE COMPLIANCE

The process safety business is permeated with regulations, rules, codes, and standards. And these rules are important—one large oil company estimated that 80% of its incidents in the year 2006 could have been avoided had workers simply followed the rules. Yet, although compliance with the rules helps ensure a high level of safety performance, it can also induce a false sense of confidence when it comes to safety—particularly catastrophic accidents. Such false confidence is based on an assumption that the occurrence of all possible incident scenarios has been anticipated by the writers of the rules and regulations. Such an assumption is, of course, highly unlikely to be correct, not least because most serious accidents are unusual, even weird.

Therefore, almost by definition, the rules cannot anticipate those combinations of events that could lead to serious incidents. Indeed, the nonprescriptive basis of many regulations, such as the PSM standard from Occupational Safety and Health Administration (OSHA) and the Safety Case regime in the North Sea, recognizes that rules and regulations can provide no more than a framework for successful operational integrity work. Detailed analyses must be carried out by the managers and workers at the facility itself to decide how the safety and risk management program is to be structured.

FLAG FIVE—DEPARTMENTALIZED INFORMATION FLOW

The fifth flag has to do with information that could help a facility manager determine if he or she has serious safety problems, but where that information is not provided to the manager such that corrective actions can be taken in a timely manner.

The topics included in this category are:

- Critical safety information is buried, lost, or diluted
- Team player culture
- Fear of litigation
- Mergers and acquisitions.

Critical Safety Information Is Buried, Lost, or Diluted

Referring once more to *Lessons from Longford*, Hopkins states,

> . . . one of the recurrent findings in disaster research is that information that something was wrong was available somewhere within the organization but was not communicated to the relevant decision-makers. For a variety of reasons the bad news never landed on the desk of someone who had the authority and inclination to do something about it.

To illustrate this point, incident investigators often find that the incident they are examining has already been described in a design or process hazards carried out before the event. Yet the insight had not led to the needed changes being made.

In the words of the facility manager who wrote the original "Warning Flags" paper, "If you want to know the cause of an incident, look in the filing cabinet; chances are that someone described it before the event actually took place."

One reason for the lack of response to such findings is the common human concern about passing along bad news. No one wants to be the bearer of bad tidings. Therefore, even if the information is passed on, it may get softened in the process, as illustrated in the following fictional (and somewhat tongue-in-cheek) example of diluted information flow.

Maintenance Mechanic:
"That safety valve is totally unreliable. One day its failure is going to lead to a major explosion. We need to fix it now!"
Maintenance Supervisor:
"The safety valve is unreliable and it is in a critical service—we must repair it as soon as possible."
Maintenance Manager:
"The valve is important, and we will make sure it is repaired at or before the next turnaround."
Plant Manager:
"All valves requiring maintenance work have been identified, and will be repaired on schedule."
Operations Vice President:
"I am proud to report that we have an effective and proactive maintenance program—all opportunities for improvement have been identified."

Of course, the above vignette is a parody, but many managers could probably report a similar sequence of communication events having occurred at some point in their own career.

Team Player Culture

Companies rightly encourage a team culture in which everyone works together for the common good. However, there is a potential downside to such a culture—it can create an atmosphere of not highlighting problems because doing so may “make waves” or get another team player into trouble. The willingness to tackle problems head on and to let the chips fall where they may is one of the attributes of BBS programs.

Fear of Litigation

If someone does report a problem they have created potential legal exposure for the company if there were to an accident. Plaintiffs will point out that management knew of the situation, and the chance of a “willful” citation from an agency goes up.

However, management has no choice but to encourage the reporting of bad news, although they should want to train their employees on the use of nonemotive language, and protocols as to who receives which communications. In particular, employees should be trained in what to say to outsiders such as reporters, regulators, and attorneys immediately following a serious event.

Mergers, Acquisitions, and Divestitures

Companies in the process industries frequently merge with other companies, or are broken up and sold piecemeal. The upshot of all these changes is that many of the new companies that are created from the heritage organizations inherit safety and process systems that are profoundly different from one another. Many of the assumptions as to how process safety issues are to be managed that were good for the old organization no longer apply to the new establishment, and an accident may occur simply because people from different backgrounds did not fully understand one another. Also, lines of responsibility may take some time to clarify.

Einolf and Menghini (2007) note that environmental liabilities and costs are carefully considered during most acquisitions. However, the same degree of care and thoroughness is rarely applied to process safety issues. They refer to PSM “choke points,” i.e., those elements that have been most often cited in litigation and regulatory findings and that could therefore create difficulty during a due diligence process. (The choke points are listed in Chapter 1.)

FLAG SIX—INEFFECTIVE AUDIT PROCESS

Related to the above topic of impaired information flow is the failure to respond promptly to audit findings. Audits (which are discussed in Chapter 13) are an essential part of any management system. There is always bad news to do with safety, and managers must be made aware of such news so that they can take corrective action. Failure to provide management with effective audit results can be a factor in an eventual incident.

The topics discussed under this flag are:

- “Softened” news to senior managers
- Failure to identify root causes
- Inadequate follow-up.

Softened News to Senior Managers

It has already been pointed out that employees tend to soften bad news—they are worried about the “shoot the messenger” syndrome. But they are not the only ones facing this problem; auditors and other outside reviewers face the same temptation to play down bad news. They do not want to hurt anyone's feelings, and, if the auditor is being paid by the host company, he or she may feel a temptation to remain "in" with facility management so as not to lose the opportunity for further work.

Following the "Warning Flags" event the plant manager insisted that all future safety audit reports to land directly on this desk; he insisted on seeing the findings before any "smoothing" took place.

Failure to Identify Root Causes

If an audit report is to be fully effective, either the auditor or a team at the facility must try to identify root causes behind the findings in the report. For example, if the auditor finds that operating procedures have not been written for a certain section of the facility, it is not enough to respond by getting the procedures written. Management must attempt to find out why procedures were not written, why the operating personnel were willing to work without good procedures and why previous analyses and reviews had failed to identify this problem or why no corrective actions had been taken.

Inadequate Follow-Up

An audit is of no value if the facility management does not follow up on its findings. Ideally, senior management will review the audit, the audit process and the audit follow-up very carefully—all the time asking what improvements can be made to the management systems.

THINKING BACKWARD

As already discussed, risk is generally divided into three main elements: hazard, consequences, and likelihood, as shown in Eq. (1.1). The risk is also ameliorated through the presence of safeguards.

Many people, particularly safety professionals, tend to approach safety improvement from the right-hand side of the equation, i.e., first they seek to improve the safeguards, then they look to reduce the likelihood. If the risk level is still too high they try to reduce the consequences of the event. Finally, they consider removing or changing the hazard.

For example, a facility may have a pump handling a flammable, toxic chemical. The seal on the pump fails quite frequently. Potential consequences of a seal leak include workers in the area being sprayed with the chemical, a fire at the pump, and health problems for the maintenance workers who have to replace the seal. Management determines that these seal problems are unacceptable and that the risk should be reduced to an acceptable level.

1. Safeguards can be improved. For example, the maintenance workers can be provided with better Personal Protective Equipment (PPE). Or maybe additional emergency procedures can be put in place so that someone can be quickly rescued if he or she is overcome by the chemical.
2. Of course, there is nothing wrong with these measures, and they may be needed in the short term. But a better long-term approach is to work backward along the risk equation and to ask if the frequency of pump seal failures can be reduced. Actions that can be taken to reduce likelihood include installing a more reliable seal, improving the training of the maintenance workers, and filtering the liquid being pumped so that solids do not damage the seal.

3. Even better is to continue to move to the left along the risk equation and to reduce the consequence of the hazard, should it occur. In the case of the pump means of doing this could include replacing the liquid with one that is less toxic or flammable, or reducing the inventory of liquid in the pumping system so as to reduce the worst-case scenario.
4. However, the best approach of all is to continue moving left along the equation and remove the hazard itself. One of Trevor Kletz's mottos was, "If a tank's not there, it can't leak." So, in the case of the leaking pump seal the smart safety professional asks questions such as, "Can we use a canned/seal-less pump?" or "Can we replace the pump with a gravity feed system?" (These new concepts introduce a new set of risks that also must be analyzed and deemed to be acceptable before they are implemented.)

IMAGINATION

With regard to the elimination of hazards, however, not only is there a need for thinking, there is a particular need for *imaginative* thinking. And this type of thinking is hard work. To think imaginatively and creatively puts one in mind of the Monty Python quotation, "My brain hurts."

CULTURE MATRICES

Many ways of understanding and organizing the topic of culture have been proposed. What is shown in Figure 3.1 is an example. It looks at two features of culture: personalities and systems.

In the bottom left corner is "chaotic" culture. Both the systems and the people in a company are weak. The "tribal" square (top left) represents those facilities, often small ones, that are run by strong and knowledgeable people, but where managerial systems are inadequate. The bottom right square—"bureaucratic"—typifies many larger or older organizations: the systems are strong but the

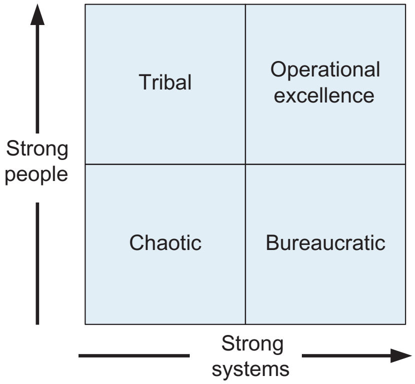


FIGURE 3.1

Culture matrix.

people running the company are weak, or else their strengths are smothered by the bureaucracy. The ideal culture is shown in the top right square—"operational excellence"—where both people and systems are strong.

Another view of culture is shown in Figure 3.2 (Transportation Research Board, 2012), which is also a 2 × 2 matrix.

One of the difficulties to do with managing risk is that, when there is a problem, companies and regulators tend to look at the top left-hand square: the Management System. For example, they may note that an incident was grounded in a problem to do with the manner in which a change was managed. Therefore, the inclination is to improve the MOC system. Failing that the next step is to improve the competence of the individuals working in the organization, i.e., the bottom left-hand square.

Yet it is more than likely that the MOC system is quite mature and that the people who use it have been well trained. The real improvements are more likely to be found in the improvement of company culture and individual motivation. But such improvements are difficult to implement so management will tend to focus on the MOC system and the people who use it.

ELEMENTS OF CULTURE

Although it is difficult to formally define and understand culture, the following attributes are good indicators of a positive culture:

- Ongoing and consistent
- Actions and words
- External evaluation
- Learning from incidents
- Attention to basics/housekeeping.

Ongoing and Consistent

Culture is an ongoing trait—not a one-time event. A facility in which everyone is continuously striving to identify and correct problems and to improve safety has a strong positive culture,

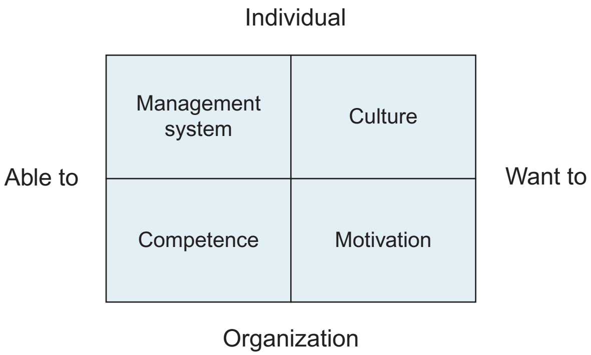


FIGURE 3.2

Culture matrix.

whereas a facility which makes only spasmodic and irregular efforts to improve such conditions does not. The ongoing nature of a strong culture is expressed through an avoidance of a “fad of the month mentality” in which new concepts and systems are constantly being introduced, while earlier initiatives, which were probably just as good, are left to wither. With regard to HSE issues, the organization does not place excessive emphasis on just one of the elements, to the detriment of the other two.

Actions and Words

Organizations with a strong, positive culture exhibit a minimal disconnect between words and actions. All managers and workers “walk the talk”; their words and deeds match. Senior leaders, in particular, act on their stated principles.

The thrust of most process safety and operational integrity programs is to establish control and to make sure that employees do not deviate from acceptable practice. Yet there are times when relatively low-level personnel do have to make big decisions, such as shutting down a plant during an emergency. A strong culture allows such people to take the initiative and make such decisions as necessary without there being a concern about retribution or blame to do with crossing departmental lines.

Any disconnect between words and actions will usually show up if a serious accident occurs. It is crucial to a positive culture that employees believe that they will be treated fairly and that no one will be blamed or reprimanded (except for fair cause), or selected as a fall guy, when things go wrong, particularly when such events can be attributed to management failings.

External Evaluation

It is difficult for any organization to truly assess the quality of its own culture (“Does a fish know that it’s wet”?). Everyone learns to live with situations that really need attention. It generally takes an outsider to truly evaluate the quality of a company’s culture, particularly the negative aspects. Therefore, an organization with a strong culture will make frequent use of outside auditors, inspectors, and reviewers to identify areas of weakness and to suggest corrective actions. (In large companies, the “outsiders” may come from corporate headquarters or from another division.)

Learning from Incidents

One of the most effective means of understanding and improving culture is to learn lessons from incidents and near misses such as the Warning Flags event just described. Such events show unequivocally that the facility culture did not operate effectively and that improvements need to be made. Evidence of a strong culture is the ratio of the number of reported near misses to the number of actual incidents in which someone is hurt, or the environment is impacted. A high ratio is evidence of a positive culture.

When a strong and positive culture exists employees believe that management looks upon the incidents as a means of improving its systems, not as a way of finding fault with employees or contract workers. In such an environment, employees (and contract workers) will report incidents and near misses rather than trying to hide them. On the other hand, if employees believe that the end result of an investigation is simply the chastisement of line-level workers then they will shut up like clams. The reality is that everyone makes mistakes: operators turn the wrong valves, managers take shortcuts and engineers make flawed calculations. Management must show that they generally regard such mistakes as symptomatic of bigger issues.

One way of building a strong culture is to ensure that the employee who first reports an incident or near miss is kept fully informed as to the status of the follow-up actions, as should anyone who was injured in the event. Also, it is important not to make incident reporting too much of a hassle or too bureaucratic, otherwise people will not bother to use the system.

Attention to Basics/Housekeeping

A company with a strong culture pays a good deal of attention to its basic operations in the same way that Vince Lombardi created a winning team through the effective execution of football basics such as blocking and tackling.

Some of these basics include:

- The proper use of PPE at all times
- The availability of complete, accurate, and readable operating and maintenance procedures
- Adherence to all rules
- The absence of temporary repairs and fixes such as clamps and hoses.

The word "housekeeping" is a catchall that is difficult to define, but which is easily recognized. A facility with a good culture will be clean; all pipes will be horizontal or vertical and be wrapped in fresh insulation; the workers will be smartly dressed; and there will be no alarm signals frozen in place.

MERGERS AND ACQUISITIONS

When two companies merge, or when one company acquires another, there will also be a merger of two different cultures. This can lead to many problems. For example, if the two companies have different engineering standards it has to be decided which one "wins," and whether retrofit work is required.

During the merger process companies have learned to pay close attention to environmental issues and remedial liability. They do this not only because environmental liabilities can be enormous but also because relevant information is available in publicly reported documents. However, less attention is usually paid to safety and health, particularly process safety.

If the team conducting the evaluation does find any problems or deficiencies in the process safety program the acquiring company should create a contingency fund so that upgrades and modifications can be made once the purchase is complete.

Probably the most important issue to evaluate is the closure of items on the risk register. These items can come from hazards analyses, incident investigations and audits. If an item is not closed then it represents a liability—after all the issue was known about but not responded to in a timely manner. But failure to close out findings and recommendations is symptomatic of a deeper problem—it shows that the overall PSM systems is not being operated properly.

The company acquiring the facility should recruit process safety experts to evaluate the quality of the PSM program. This evaluation goes beyond a simple compliance-style audit—it aims to determine if the management system is working properly.

It is also important for the acquiring company to make sure that the engineering standards used in the design and ongoing technical work at the facility are at least equal to those that the company itself uses.

GENERATIONAL DIFFERENCES

An important factor in understanding culture is that of generational differences. Workers can be divided into the following groups:

- *Matures* are people born prior to 1946. Their numbers and influence is declining as they retire and leave the workforce. They are driven by a need for security, they accept a hierarchical organization and are good at following rules.
- *Baby Boomers* consists of people born in the period 1946–1965. Like Matures they tend to define themselves by what they do and by the nature of their job. They expect to put in time learning the skills that are needed by the company; in return they expect the company to advance them and their careers. They tend to trust the company that they work for and they are willing to make work hard and make sacrifices of personal and family time for the company. Current leadership in the process industries often comes from the ranks of Boomers. However, they are leaving the workforce as part of the Big Crew Change discussed above, so their influence is waning.
- *Generation X* consists of people born between 1965 and 1977. They are at the heart of the current workforce. Along with the late Boomers they have much less respect for political leadership than their predecessors and tend to distrust authority in general. They are somewhat cynical and are distrustful of company promises. Hence they rely mostly on themselves to advance their career.
- *Millennials:* made up of people born after 1977. They are well educated, optimistic, and ambitious. They share some of the individualistic traits of Generation X, but are more group-oriented. Work is important, but it does not define their lives in the way that it does for earlier generations. Many of the Millennials are from minority groups. They are typically at the entry level of companies but are rapidly moving into positions of greater responsibility.

The above divisions are very approximate, of course, and many individuals will not conform to their group stereotype. However, when developing an organization's management strategies it is useful to keep these distinctions in mind.

Senior managers who are trying to improve a company's culture need to recognize these generational differences. In particular those managers must recognize that the young people that they are hiring cannot be expected to have the same commitment or loyalty to the company that was frequently taken for granted by earlier generations.

Managers also need to recognize that the younger generations are motivated by more than salary, benefits, and interesting projects. For example, Millennials will be attracted to organization and projects that allow them to connect to others. The Generation X workers will quickly look for work elsewhere if they are not satisfied with where they are.

MEASUREMENT

Two commonly used quotations are, "What gets measured gets done" and, "You become what you measure." The philosophy embedded in those two statements applies to the management of safety culture in process facilities. If the topic cannot be measured quantitatively and objectively then companies are just guessing as to the progress that is being made.

With occupational safety measurement is fairly simple: recordables and other statistics provide a reliable indication of how a company is doing and how it compares to others. The measurement of results with regard to Process Safety is much more tricky. But the measurement problem is even more severe when it comes to the topic of culture. In particular it is very difficult to assess "people are people" issues. For example, one of the reports that was written following the *Deepwater Horizon* catastrophe (BOEMRE, 2011) records in some detail the tension that existed between two of the managers and publishes some of the emails that were sent prior to the event. These clashes illustrate the difficulties of implementing a positive culture, particularly when personalities clash or department managers are squabbling with one another.

Or, to take a more mundane example, if a set of operating procedures is messy—crumpled, coffee-stained, and scribbled on—then the factors indicate a poor culture. But possibly not: it could be that the condition of the procedures shows that the technicians are using them a lot and so the culture is good. Once more, the measurement of culture in a context such as this is problematic.

KEY PERFORMANCE INDICATORS

One way of measuring the PSM program and the culture of a facility or company is through the use of KPIs. The organization will select a few parameters that, it is believed, will give a clear picture of the overall culture. These KPIs should be quantified and have as little subjectivity as possible (having said which, it is very difficult to quantify items such as Employee Participation or MOC).

The number of KPIs in use should be small but they should provide a credible measurement as to trends. Generally they will be normalized. For example, rather than simply reporting the number of process safety incidents (PSIs), it is more useful to report the number of incidents per employee. Doing so facilitates comparisons between different sites and organizations.

In order to establish reliable quantification measures, a consistent set of terms and reporting standards is required. In the area of occupational safety, considerable standardization has already been achieved through the use of measures such as the number of first-aid cases or recordable injuries. Although different organizations will apply these terms slightly differently from one another there is sufficient consensus to allow for their use across broad swathes of industry. For process safety it is much more difficult to come up with comparable yardsticks. Hence comparisons between different facilities may lack validity and credible trend lines are difficult to develop.

LAGGING AND LEADING INDICATORS

KPIs can be either lagging or leading. A lagging indicator is like a rearview mirror; an event has occurred. A leading indicator is one that suggests that an event may occur sometime in the future.

Many events are both lagging and leading. For example, a control valve may have a small leak through its packing. This is a lagging indicator, and it has minor consequences, such as the need to complete an environmental report. But it is also a leading indicator. The small leak could ignite and lead to a large explosion and fire.

These two terms are discussed below.

LAGGING INDICATORS

The lagging or trailing indicators as used in the process industries for safety and reliability have been defined as,

> Retrospective metrics based on incidents that meet a threshold of severity...
>
> **Overton (2008)**

These indicators include well-established parameters such as lost time accidents, first-aid cases and recordable injuries. Figure 3.3 illustrates how the indicators are tracked over time. Lagging indicators are widely used because, assuming that there are enough events to ensure statistical significance; they allow management to establish baselines, measure trends, and to compare results with other facilities and companies.

Lagging indicators are used to generate KPIs. One oil company, for example, has set the following KPIs for itself (some are monthly, others quarterly, and the remainder annual).

- Fatalities
- Days away from work
- Recordable injuries (as a function of exposure hours)
- Recordable illnesses
- Spills from primary containment (even if secondary containment was effective)
- Spills affecting the environment (failure of all containment barriers)
- Volume of oil spilled that is not recovered

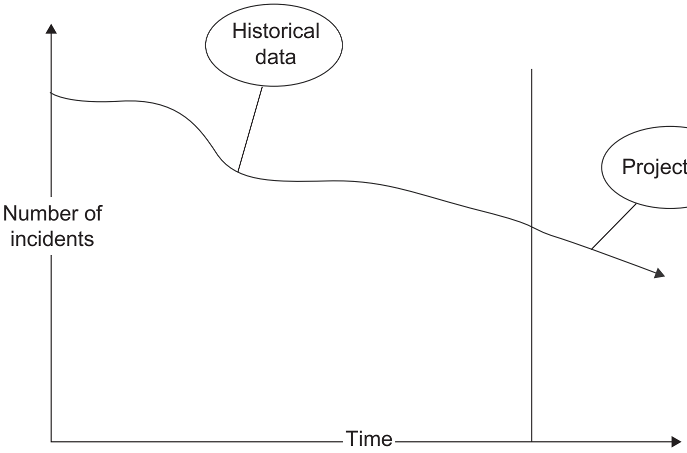


FIGURE 3.3

Lagging indicators.

- Greenhouse gas emission equivalents
- Total hydrocarbon emissions
- Total SO_x and NO_x emissions
- Total discharges to water
- Total hazardous waste energy use.

Lagging indicators by themselves do not provide much explicit guidance to management as to what needs to be done to keep improving safety. The events themselves have to be analyzed using some type of root cause analysis. Also, lagging indicators tend to react quite slowly to system changes.

OSHA Recordable Rate

Companies in the United States pay particular attention to the OSHA recordable rate. Onshore facilities are required to report this number anyway, so it provides a reliable means of comparing different organizations with one another.

An OSHA recordable injury is an occupational injury or illness that meets one of the following criteria:

- Death
- Loss of consciousness
- Days away from work
- Restricted work activity or job transfer
- Medical treatment beyond first aid.

It is calculated for the previous 3 years and is defined as:

$$\frac{\text{Number of Recordable Cases} \times 200{,}000}{\text{Total Hours Worked}}$$

The OSHA Lost Workday Incident Rate is similar:

$$\frac{\text{Number of Lost Workday Cases} \times 200{,}000}{\text{Total Hours Worked}}$$

A lost workday—equivalent to a lost time injury—is one where an individual misses more than one day of work due to an injury sustained while at work. It is another widely used criterion for measuring occupational safety.

Process Safety

It is difficult to identify effective lagging indicators for use with process safety. The most obvious problem is that major PSIs do not occur frequently enough to develop a statistically significant trend such as that shown in Figure 2.3. If many facilities and companies pool their data it may be possible to that some trending results can be developed. However, such results are always open to doubt, not least because different organizations define terms differently. For example, the Baker report (Baker, 2007) provides a list of events that fall under the term “fire.” That list includes “a fault in a motor control center.” It is questionable as to how many organizations would call such an event a “fire” unless it resulted in actual flames.

An additional difficulty is that many process safety events (PSEs)—particularly those that are near misses—may simply not be recognized for what they are. For example, an operator and a mechanic may fix a leaking pump seal, not realizing how close they were to having a major accident.

LEADING INDICATORS

Leading indicators are forward-looking. They provide management with an assessment of their process safety program. Most leading indicators measure some type of activity or work process that prevent incidents.

The first round of so-called “leading indicators” was little more than a measurement of safety-related activities: hours of safety training, attendance at safety meetings, participation in safety programs, etc. OSHA’s crackdown on incentives that could potentially suppress reporting of accidents drove many organizations to base their incentives on these activity metrics rather than simply not having an accident.

When BBS became the rage, the measurement of behaviors from observations came to be thought of as a leading indicator. As safety culture became a buzz phrase, perception surveys gained in popularity and came to be considered another potential leading indicator. The search for meaningful leading indicators goes on because no one of these has proven adequate in predicting and preventing injuries.

Where none of these alone succeed, all of them together potentially can. A balanced-scorecard approach in which the metrics not only complement, but predict each other has proven quite effective in proactively predicting how to prevent accidents. When you measure how much activity it takes to change perceptions, how much of a change in perceptions it takes to change behaviors, and how much behavior change it takes to change the lagging indicators, you begin to truly measure the effectiveness of safety efforts.

Leading indicators can be either positive or negative. The following are examples of positive leading indicators:

- Number of field visits and inspections
- Thoroughness of inspection programs
- Number of safety audits
- Number of safety communications and safety meetings
- Percentage of incidents investigated
- Number of near miss responses
- Number of positive rewards and recognition given
- Number of safe behaviors observed.

Negative indicators include the number of equipment items overdue for inspection and claims reports.

Although topics such as these provide useful guidance as to how much progress is being made, there are serious limitations. In particular, it is difficult to make a quantitative link between these topics and the risk associated with PSEs. For example, a manager cannot know what impact say doubling the number of field visits will have compared with doubling the number of positive awards ceremonies.

Near Misses

A near miss (which is more properly called a near hit) is typically a low severity incident that nevertheless had the potential to be much more severe, and, in many cases, triggered a layer of protection or safeguard. Also, a failure in the PSM system could be regarded as a near miss. For example, if someone has to carry out a task without being provided with procedures or being trained then a near miss situation has occurred.

Near misses are often both lagging and leading indicators. For example a leak of hydrocarbon from a pump seal is a lagging indicator. An event occurred, and it had consequences, such as the need to fill out an environmental report form. But this event is also leading; if a source of ignition had been present it could have caused a major fire.

Unplanned Maintenance

Some organizations classify unplanned maintenance jobs as near misses because such events will generally put the system in a less safe condition and they indicate deficiencies in the management systems, i.e., the problem should have been anticipated and included in the preventive maintenance program. Some organizations choose to classify unplanned maintenance as a near miss only when it affects safety critical equipment (Vancauwenberghe, 2011).

The chart shows a remarkable drop in the incident rate as the number of unplanned jobs goes down. (It could also be that those companies that are well organized have both better maintenance planning and good safety programs—they both share the same cause.)

Process Safety Incident

A PSI provides a strong indication as to the quality of a company's culture. It should meet all of the following criteria:

- Involves a chemical or chemical process
- Is above the minimum reporting threshold
- Occurs in a production, storage, distribution, utility, or pilot plant location
- Is an acute release.

Overton and Berger Overton (2008) provide detail regarding each of the above criteria, including the reporting thresholds.

A formula similar to the OSHA recordable rate described above can be used to measure PSIs. Known as the Process Safety Total Incident Rate (PSTIR), it is calculated as follows:

$$\frac{\text{Total Number of PSIs} \times 200,000}{\text{Total Employee and Contractor Work Hours}}$$

The PSTIR can be further modified to take into account the severity of the incidents. Each incident is given a severity level as follows:

- Level 4—1 point
- Level 3—3 points
- Level 2—9 points
- Level 1—27 points

Then the Process Safety Incident Severity Rate (PSISR) can be calculated using the following formula:

$$\frac{\text{Severity Score for all PSIs} \times 200,000}{\text{Total Employee and Contractor Work Hours}}$$

The severity score is determined by assigning points in the areas of Safety/Health, Fire or Explosion (including overpressure), Potential Chemical Impact, and Community/Environmental Impact.

In the standard example, if one of the pump seals leaks but does not catch fire then the severity would be calculated as follows:

- Safety/Health: No one is injured, so the score is 0.
- Fire/Explosion: No ignition, so the score is 0.
- Potential Chemical Impact: Chemical released within the unit. Level 4, Score 1.
- Community/Environmental Impact: Short-term remediation required. Level 4, Score 1.

So the total score for this event is 2.

KPI LIMITATIONS

Some of the limitations to do with leading and lagging indicators have already been discussed. Further issues to consider are listed below.

Activity and Quality

It is important to distinguish between *activity* and *quality* when analyzing process safety data (Hopkins, 2000) and not to confuse activities with results. For example, managers may be encouraged to close out findings from hazards analyses and incident investigations more quickly than they did in the past in order achieve a good KPI score. However, if those managers achieve the improvement by not implementing the findings as thoroughly as before, the net effect may be a reduction in performance. They score an “A” for effort, but a “B” for results.

Quality of Reporting

The effectiveness of both lagging and leading indicators depends heavily on the quality of incident reporting. For lagging indicators this is not a major problem. As already noted, indices such as OSHA recordables are widely understood and are consistent across industries. However, minor incidents are often not reported for the following reasons:

- Fear of looking bad
- Desire to “tough it out” or to appear manly
- Not realizing how serious the injury might be (for example, a small scratch may have allowed toxic chemicals to enter a person’s blood stream)
- Desire to keep the numbers “looking good.”

With regard to leading indicators, the quality of the reported data is likely to be worse than it is for lagging results because it relies on the reporting of unsafe conditions and near misses—not on actual events. Hence the value of the reported results is likely to be patchy and inconsistent. Some people are very diligent about reporting such events; others are not. Therefore, it is difficult to establish a consistent estimating system—particularly between different companies.

A related difficulty is that leading indicators may be subject to mere formal compliance and pencil whipping. For example, training may be identified as a KPI so the workforce receives more training in PSM-related topics. However, management cannot be sure that the additional training will actually result in changed performance on the job.

Management Elements

The reporting of leading and lagging indicators provides no guidance as to which of the elements of process safety contributed to the system failure. In Chapter 14—Incident Investigation and Root Cause Analysis—it is noted that different incident investigators can come up with widely disparate perceptions as to the root causes of events. Similarly with leading and lagging indicators—different people will have different perceptions as to the causes of events.

Using the example of the leading control valve once more, the leak through the packing could be attributed to problems in any of the following areas:

- *Asset Integrity.* The valve was not properly maintained.
- *Hazards Analysis.* The team failed to identify that the wrong packing material was being used.
- *Training.* The maintenance technicians had not been properly trained in the installation of the packing.
- *Technical Information.* It may be that information to do with the control valve had either not been provided by the vendor or was not accessible to the facility personnel.
- *Operating Procedures.* It is possible that the operators had not been given update procedures for operating the section of the facility containing the control valve.

API RP 754

Following the fire and explosion at BP's Texas City refinery in Texas City, Texas, in the year 2005, the CSB conducted an investigation. One of the recommendations from that investigation called for the American Petroleum Institute (API) and the United Steel Workers (USW) to work together to develop an ANSI standard for leading and lagging indicators. The recommendation reads:

> Work together to develop two new consensus American National Standards Institute (ANSI) standards. In the first standard, create performance indicators for process safety in the refinery and petrochemical industries. Ensure that the standard identifies leading and lagging indicators for nationwide public reporting as well as indicators for use at individual facilities. Include methods for the development and use of the performance indicators.

Although the USW later withdrew from the program the API continued with the development of a standard which became Recommended Practice 754, *Process Safety Indicators for the Refining and Petrochemical Industries.* It was published in April 2010 (API, 2010). RP 754 is based on the same concepts are as found in the OGP Report No. 456 (OGP, 2011).

RP 754 was written for the refining and petrochemical industries but it can be used in any hydrocarbon processing industry such as offshore oil and gas. However, the following are not considered to be within the scope of the standard:

a. Releases from pipeline transfer operations occurring outside the process or storage facility fence line
b. Marine transport operations, except when the vessel is connected to the process for the purposes of feedstock or product transfer
c. Truck or rail operations, except when the truck or rail car is connected to the process for the purposes of feedstock or product transfer, or if the truck or rail car is being used for on-site storage
d. Vacuum truck operations, except on-site truck loading or discharging operations, or use of the vacuum truck transfer pump
e. Routine emissions that are allowable under permit or regulation
f. Office, shop, and warehouse building events (e.g., office fires, spills, and personnel injury or illness)
g. Personal safety events (e.g., slips, trips, and falls) that are not directly associated with on-site response to a loss of primary containment (LOPC) event
h. LOPC events from ancillary equipment not connected to the process (e.g., small sample containers)
i. Quality assurance (QA), quality control (QC), and research and development (R&D) laboratories (pilot plants are included)
j. Retail service stations
k. On-site fueling operations of mobile and stationary equipment (e.g., pick-up trucks, diesel generators, and heavy equipment).

The performance indicators identified by RP 754 should meet the following principles:

- Indicators should drive process safety performance improvement and learning.
- Indicators should be relatively easy to implement and easily understood by all.
- Indicators should be statistically valid at one or more of the following levels: industry, company, and site.
- Indicators should be appropriate for industry, company, or site level benchmarking.

TIERS

RP 754 suggests that process safety performance can be measured through the use of four tiers of indicators. These tiers represent a transition from leading to lagging indicators. Tier 1 is the most lagging, Tier 4 is the most leading. They are shown in Figure 3.4.

Figure 3.4 is a performance triangle similar to that shown in Chapter 1. Events in the bottom section occur more frequently than in the top section and generally have a lower consequence.

It is assumed that there is a direct correlation between the tiers, i.e., that a shift in performance at one level will have a corresponding change at the level above. However, as discussed in Chapter 1, it is important to watch for false assumptions. For example, a newly invigorated incident reporting program may lead to more Tier 4 incidents being recorded, even if there has been no actual performance change.

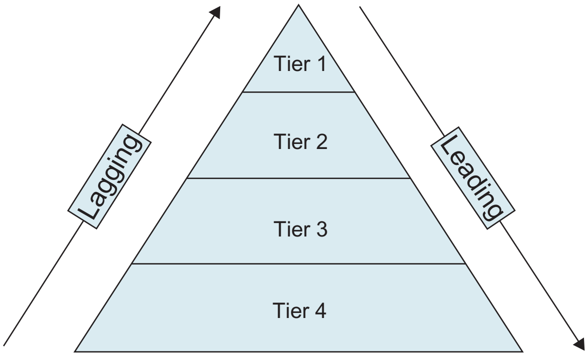


FIGURE 3.4

Performance triangle.

Tiers 1 and 2 are suitable for nationwide public reporting, and thus have a tightly defined scope. Any Tier 1 or Tier 2 PSE begins with an unplanned or uncontrolled release of any material, including nontoxic and nonflammable materials resulting in one or more consequences described in the RP. These events are referred to as an LOPC, which is defined as follows.

> An unplanned or uncontrolled release of any material from primary containment, including nontoxic and nonflammable materials (e.g., steam, hot condensate, nitrogen, compressed CO_2, or compressed air).

Tiers 3 and 4 are intended for internal use at individual sites.

Quantification is measured through use of the PSE rate, which is calculated as follows:

$$\text{PSE Rate} = \frac{\text{Total PSE Count} \times 200,000}{\text{Total Workforce Hours}}$$

Each tier has its own PSE rate.

The tiers are defined as follows.

Tier 1—Process Safety Event

A Tier 1 event is one that includes loss of containment (LOPC) with the greatest consequence, as defined by RP 754. These include:

- An employee, contractor, or subcontractor “days away from work” injury and/or fatality or
- A hospital admission and/or fatality of a third party or
- An officially declared community evacuation or community shelter in place or
- A fire or explosion resulting in greater than or equal to $25,000 of direct cost to the Company
- A pressure relief device discharges to the atmosphere (directly or *via* an downstream destructive device such as a flare) that results in one or more the of the following consequences:
  - Liquid carryover
  - Discharge to a potentially unsafe location

- An on-site shelter in place
- Public protective measures such as a road closure
- Release of materials greater than the threshold quantities.

Tier 2—Process Safety Event

Tier 2 events are similar to Tier 1 but have a lower consequence. They include:

- An employee, contractor, or subcontractor recordable injury or
- A fire or explosion resulting in greater than or equal to $2500 of direct cost to the Company
- Pressure relief discharges but with different threshold quantities.

Tier 3—Challenge to Safety Systems

Tier 3 events typically represent challenges to the barriers that prevent near misses from turning into actual events. They are events that stop short of Tiers 1 or 2. Examples include:

- Safe operating limits excursions
- Demands on safety systems such as pressure safety relief valves
- Primary containment inspection or testing results outside acceptable limits
- Other LOPC events that are less than what is required for Tier 2.

Tier 3 indicators are intended for internal use; the results will not normally be shared with other organizations.

Tier 4—Operating Discipline and Management System Performance

Tier 4 indicators provide measurements of operating discipline and the management system performance. Like Tier 3 they are site-specific and will not generally be used to compare the performance of different companies.

Examples of Tier 4 items are:

- A process safety action item is closed on schedule
- Training is completed on schedule
- Safety critical equipment items are inspected
- Emergency response drills are completed.

DATA SUBMISSION

In order to encourage consistent reporting, the API has published a *Guide to Reporting Process Safety Events* along with a matching spreadsheet. The Guide provides information for the reporting of Tier 1 and Tier 2 events. It also provides a glossary defining the terms used in RP 754. It also provides guidance on the selection of categories (such as types of refining process) to be used in reporting.

SELECTION OF KPIs

The performance indicators provided above for Tiers 1 and 2 are useful for comparing facilities with one another. However, events at this level occur only rarely and do not provide an adequate statistical basis whereby a company can improve its own performance and implement a continuous improvement program.

Table 2 in the OGP document provides many examples of Tier 3 and 4 KPIs. They are divided into the following categories:

- Management and workforce engagement
- Hazard identification and risk assessment
- Competence of personnel
- Operational procedures
- Inspection and maintenance
- Plant design
- Safety instrumentation and alarms
- Start-ups and shutdowns
- Management of change
- Permit to work
- Contractor management
- Emergency management
- Compliance with standards.

Further detail is provided in each category. For example, under Emergency Management, the Tier 3 indicator is:

- Number of emergency response elements that are not fully functional when activated in
  - **a.** A real emergency
  - **b.** An emergency exercise.

The corresponding Tier 4 indicators are:

1. Number of emergency exercises on schedule and total staff time involved
2. % of staff who have participated in an emergency exercise
3. Number of emergency equipment and shutdown devices tested versus schedule.

SURVEYS

Another way of measuring safety culture is simply to ask people through the use of structured surveys. Such surveys typically ask participants to answer a series of questions on a 5-point Likert scale:

1. Strongly agree
2. Agree
3. Neutral
4. Disagree
5. Strongly disagree.

The following is a list of questions that can be asked (it is derived from O'Toole (2005)):

1. Senior Management Commitment to Safety and Safety Communication
2. Line Management Commitment to Safety

3. First Line Supervisor Commitment to Safety
4. Self-Perception of Safety
5. Influence of Peer Groups on Safety
6. Safety Competence
7. Risk Taking Behaviors by Self and Others
8. Roadblocks to Safe Behavior
9. Accident Investigations and Near Miss Reporting.

It should go without saying that, once a survey is complete and the results are in, management must act on those results. To ignore the opinions of those surveyed with throwaway phrases such as, "Our employees don't understand the big picture" destroys management's credibility.

CREATING A STRONG CULTURE

A company that aims to create a strong culture must first understand that there is no single quality—it varies over time and from place to place. Culture has been defined as having three elements:

1. It is not something we own or have constructed once and for all. It finds expression through the things that we do together, and is in constant development.
2. Culture is seldom a unified and collective quality. It is usually fragmented, diversified, and split into different subculture.
3. Culture is not an individual quality. It develops through the interaction between people and specified frame conditions.

The following three actions can help create a strong and positive operational integrity culture:

1. Prepare and publish a Mission Statement that spells out the organization's stated commitment to quality, safety, environmental, and operational integrity management principles.
2. Develop guiding tenets that show how these principles are to be implemented.
3. Develop a detailed program showing how the guiding tenets are to be achieved.

These three steps are discussed below.

MISSION STATEMENT

Many companies, particularly large corporations, will publish a Mission Statement that includes an explicit commitment to operational integrity values and programs. Mission statements are a high-level expression of the culture that management wishes to foster. Table 3.2 is an example of such a statement for an operational excellence.

It is relatively easy to write and publish a mission statement—it is much more difficult to maintain a commitment to the mission statement's values, week after week, month after month, year after year. As already stressed, culture is expressed in actions, not in thoughts, words or good intentions. If a company publishes an ambitious mission statement, but fails to make a serious effort to meet its goals, then it would have been better not to have published the mission statement in the first place.

Table 3.2 Representative Mission Statement

Our mission is to be a leader in our industry for operational integrity performance. In order to achieve this we will:

- Create a culture throughout our organization where the importance of personal health, safety and environmental ethics, and decision making is clearly understood at all levels, both among employees and contract workers.
- Create a business environment in which our emphasis is on the prevention of incidents and releases that could endanger our employees, our contract workers, the public, the environment, or our facilities.
- Develop cost-effective solutions to HSE challenges.
- Include the HSE performance of contractors in our contractor selection process, and require all contractors to conduct their work in a healthy, safe, and environmentally sound manner.
- Maintain the highest ethical standards in our relations with host governments, communities, regulators, and the media by promoting open and honest communications, integrity and accountability.
- Retain highly qualified professionals at all levels in the organization (both employees and contractors).

GUIDING TENETS

Related to the mission statement concept is the idea of Guiding Tenets that provide a practical framework in which all managers and workers can operate. The following is an example of a set of Guiding Tenets:

- Do it safely, or not at all.
- There is always time to do it right.
- Always operate within design limits—otherwise use MOC.
- When a situation is not understood, always move toward a safe, controlled condition.
- Ask for assistance when a situation is not understood.
- Never bypass or deliberately disconnect safety devices.
- Correct unsafe conditions and practices.
- Never sell off-specification product.
- Always report safety and environmental problems in a timely manner.
- Always follow written procedures.

Tenets such as those written in Table 3.2 are more pithy and practical than the statements in the Mission Statement. They are short enough that they can be turned into posters and documents of exhortation.

DETAILED PROGRAM

The final step is to develop a detailed program for operational integrity and other management systems.

One view of process safety culture is to divide the topic into 12 elements (Arendt, 2009) as shown below:

1. Establish safety as a core value.
2. Provide strong leadership.
3. Establish and enforce high standards of performance.
4. Formalize the safety culture emphasis/approach.
5. Maintain a sense of vulnerability.

6. Empower individual to successfully fulfill their safety responsibilities.
7. Defer to expertise.
8. Ensure open and effective communications.
9. Establish a questioning/learning environment.
10. Foster mutual trust.
11. Provide timely response to safety issues and concerns.
12. Provide continuous monitoring of performance.

BEHAVIOR-BASED SAFETY

A BBS plan aims to make permanent changes in the manner in which people work. Much of the change is brought about by observing how people work, and identifying and correcting at-risk behaviors, as well as identifying those actions that merit positive feedback. If an unsafe behavior is observed, a nonthreatening discussion should follow. Problems are seen as opportunities to improve safety performance and to share concern, coach, and learn. All persons, including company workers and contractors, create a mind-set of "doing everything right."

Figure 3.5 illustrates the concept behind BBS.

The basic idea is that a person thinks about the correct actions to take. If he or she does this often enough then the right actions follow, and so on. Eventually that person has developed a set of positive habits that contribute toward his or her overall character.

Workers on the frontline are often in a position to identify problems that indicate process safety problems. Issues to look for include:

- Be alert to things that are different, including noises, smells, drips, leaks and vibration.
- Fill out inspection sheets accurately.
- Promptly report safety concerns.

One company is building its safety culture and behavior-based actions through the use of the following three BBS "golden rules":

1. You and I comply with the law, standards, and procedures.
2. Intervene in unsafe or noncompliant situations.
3. Respect our neighbors.

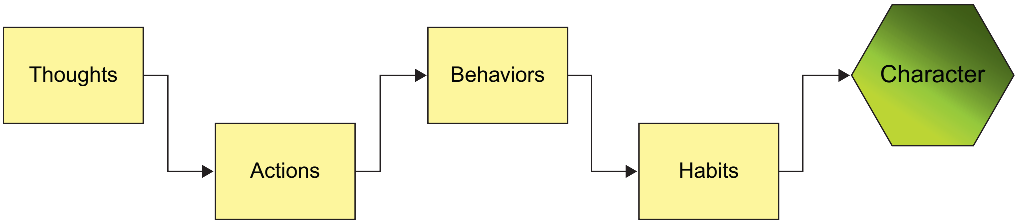


FIGURE 3.5

Development of BBS.

All programs such as the above are based on the philosophy of, "If you see a problem then *you* have a problem."

OBSERVED HAZARD CARD

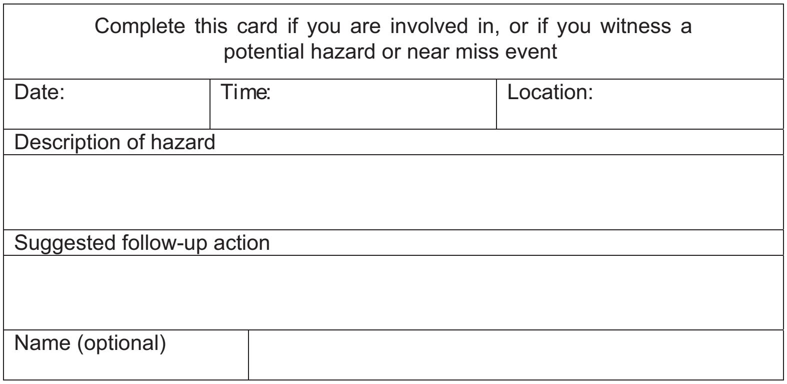
As part of their BBS program, many companies use an Observed Hazard card (also called a NEAR Event or "STOP" card). An example is shown in Figure 3.6. The card is used to record observations of hazardous situations. If the employee considers the observed situation to present an immediate danger he or she has the authority to stop the work until a review has been carried out.

Figure 3.6 is very simple. However, it does possess two features worthy of note. First, the person who completes the form is asked to suggest follow-up action. This is a request, not a requirement. Second, the card can be filled out anonymously. Nevertheless, employees should be encouraged to provide their names—the intent of the BBS program is to encourage open communication, not secret reporting.

FIVE BY FIVE POLICY

Another policy to do with behavior improvement is the "Five by Five" approach to maintenance. Before a person takes an action, he or she is encouraged to take five steps back and to take 5 minutes to mentally walk through the job before actually starting work. He or she will think through issues such as the following:

- Tools needed for the work
- PPE requirements
- Other people in the area
- Competence to do the work
- Escape routes.



Complete this card if you are involved in, or if you witness a
potential hazard or near miss event

Date:	Time:	Location:

Description of hazard

Suggested follow-up action

Name (optional)

FIGURE 3.6

Example of an observed "observed hazard" card.

OFF-THE-JOB SAFETY

A core feature of BBS is that a person's behavior does not change as soon as he or she leaves work. Therefore, employees are encouraged to practice the principles discussed above when they are at home. This is why many Safety Moments are to do with activities such as driving, the use of ladders and hanging decorations on a house.

POINTLESS ACTIVITIES

In order for a BBS program to retain its effectiveness it is important not to apply safety measures that are not needed—a point made by Olesky (2012). He notes that the intent of reflective safety vests is to protect workers from vehicular traffic. Yet these vests are often worn by workers who have no exposure at all to vehicles, electricians working on the upper stories of a building, for example. Doing so reduces the perceived usefulness of the safety program and reflects adversely on the judgment of the safety managers.

EMPLOYEE PARTICIPATION

Employee participation lies at the heart of any PSM program. It is probably for this reason that OSHA placed the topic of Employee Participation, also known as Workforce Involvement, as the first of its 14 PSM elements.

All employees (including contract workers) must be involved in the program. Although PSM programs are often conceived of primarily in technical topics such as hazards analysis, risk quantification, and fire and explosion modeling, the involvement of all employees at every level is fundamental to the success of such programs. When employees feel involved they are much more likely to make suggestions for improvement, participate in new initiatives and "walk the extra mile." Moreover, the effective involvement of the workforce provides a sanity check for new ideas, projects, and analyses. Anything new or unusual should be reviewed by the employees; they will immediately identify any common sense problems because they are the ones who know the facility best.

It is important to note that this element is called Employee *Participation*, not Employee *Communication*. The intent is that employees fully engage in the spirit of the process safety program. For example, a PHA offers an opportunity for participation in two ways.

First, all employees should be encouraged to participate in the PHA meetings themselves. They should have a chance to contribute their knowledge, experience, and ideas. Second, and maybe more important, carrying out PHAs creates state of mind for all employees; they will start to look at everything they do in terms of its risk impact. The insights generated will then suggest ideas for reducing that risk. In other words, the purpose of a PHA is not just to identify hazards, but also to encourage a particular way of thinking among all employees. So, an operator working by himself at one o'clock in the morning may be about to open a valve on a line that connects two tanks. If, before doing so, he spends a few moments going through some of the PHA guidewords such as "reverse flow" or "contamination" he may identify a possible accident situation, and decide not to open the valve until he has talked over the proposed action with his supervisor or colleagues.

When the operator acts in this manner both the participation and the PHA elements of the process safety program are working perfectly. Employee participation is not a stand-alone activity; instead, it should be woven into the fabric of all the elements of a risk management program.

Additional examples of workforce involvement occur when a pipefitter learns that a new chemical is about to be used in the process. He may question whether the current gaskets are safe in the new service. Or an outside contractor may feel that he or she has not been given sufficient instructions as to what to do and where to go in an emergency, and makes that concern known to the host company.

Although there are many benefits to do with participation, management has to recognize that, by asking employees to get involved in decision making they are also asking those employees to take more risk with regards to their career and reputation. It is much easier for an employee merely to follow orders—even if he or she knows that those orders are not sensible—than to take initiative. Moreover, increased employee participation may run into roadblocks with unions and other organizations that represent those employees. Consequently, employees must feel that they are sufficiently rewarded for participating in management programs. One way of achieving this is to provide employees with long-term rewards if the company does well, for example, by giving them stock rather than cash bonuses.

DEVELOPING EMPLOYEE PARTICIPATION

Management and the employees should develop a written plan showing how they plan to implement Workforce Involvement. An example of one of these is shown below:

- The PSM program will involve all employees and contract workers, as appropriate to their job function and experience level.
- The program will involve the full participation of "employee representatives"—where such duly elected representatives exist.
- "Employees" includes not only full-time workers, but also temporary, part-time, and contract workers.
- Decisions as to which kinds or classes of employees should be consulted regarding specific PSM matters will take into account factors such as job functions, experience, and their degree of involvement with PSM and the company's general background.

Safety Committees

Safety committees provide a formal channel through which management and the employees can communicate with regard to process safety issues and overall company culture. There are many references to the involvement of employee representatives in the OSHA standard. These would usually be on the safety committee. If the facility is nonunion, it is essential that the employees' representative is selected by the employees, not appointed by management. But it is important to ensure that the committee is not isolated; the effective implementation of this element requires that *everyone* participate in the process safety program.

Involvement in PSM elements

Employees can participate in the PSM program by taking leadership of some of the elements of process safety. This type of involvement does not have to be universal; employees will be selected based on their understanding and knowledge of the topic in question. Nevertheless, it is a good idea to involve employees with lower levels of experience wherever possible in order to train them in the details of the process safety program.

DIFFICULTIES WITH WORKFORCE INVOLVEMENT

Although effective workforce involvement and employee participation bring many benefits, there are costs and drawbacks, as discussed below.

Inefficiencies

Increased participation of employees in the PSM program can lead to short-term inefficiencies brought about by spreading work among a large number of people, rather than assigning it to a small number of full-time specialists. For example, rotating operators through a HAZOP means that the analysis will be slowed down because the newcomers will have to get up to speed on what has already been covered by the previous team members.

Another example of this type of problem (and opportunity) occurs when the operators are each asked to check the P&IDs for a small section of the plant. It would be much quicker to have one designer go out and do the whole job—but doing so would lose the important benefits that would be gained when the operators check their own unit line by line and valve by valve. Furthermore, the operators may be able to identify problems with the P&IDs because they know how “things really are.” Ultimately, the short-term inefficiencies consequent on using all the operators to perform such tasks will be more than compensated for by the gains in the overall knowledge and understanding of the operational integrity system.

Unwillingness to Accept Change

Implementation of workforce involvement can create anxiety—particularly among managers—because they are likely to hear facts about their organization that are critical of their efforts. Moreover, many workers prefer to work in a “command and control” management system because they can thereby avoid the responsibility for mistakes that are made and because thinking is such a hard work.

Labor/Management Relations

It has to be recognized that the ideal workforce involvement situation depends heavily on good labor/management relations. If there is a good deal of strife and disagreement between the two parties, then, realistically, progress in this area is likely to be difficult. For this reason, it is important to set realistic goals, and not to overcommit as to how much progress can be made in this area.

STAKEHOLDER OUTREACH

The discussion to do with workforce involvement can be taken further; a truly effective operational integrity management program will also involve a wider range of stakeholders including people living near the facility, stock holders, and local businesses. They all want to be associated with a facility that operates safely, cleanly, and profitably.

In some communities, the process industries have a bad reputation in spite of the fact that their actual safety record is good when compared to other industries. Process plants are often seen as places of mystery, where strange and dangerous substances are manufactured. This perception that industry does not care can be exacerbated following an actual incident. For example, a report on a fire at a California refinery contained the following quotations (CPSF, 1996):

> [the] plant manager at the... refinery, did not return phone calls
>
> [the spokesperson] did not return phone calls seeking further comment
>
> the three employees that [the refinery] considers to be responsible for the accident have been identified and the company has responded by suspending one employee for a week and firing the other two

To an outside observer, it appears as if neither the official spokesperson nor the manager considered the community's reaction as important. Furthermore, by disciplining the workers involved in the accident, there appears to be an attitude of blaming the operator rather than looking for root causes of the accident. In fact, it is likely that these managers did indeed care very much about safety, but this is not the perception that was created with these actions.

Trust is not automatically granted to experts (Hadden, 1990). Generally, people will trust those that they know well. Hence the neighbor across the street—who may know nothing about the process industries—will be trusted more than a plant manager when it comes to discussing the risks associated with chemical releases. If the plant manager is to gain the trust of the public, then he and his staff must not only talk frequently to members of the local community—they must listen and respond to what people say. Moreover, many of the subjective factors to do with risk that were discussed in Chapter 1 are particularly relevant when discussing the public reaction to risk. To reemphasize what was said in Chapter 1: risk is fundamentally a subjective topic; it is perceived not measured.

Sooner or later some unexpected crisis will hit. This means that it is important to have a Crisis Communication Plan in place—the basic philosophy of that plan should be that the company has to communicate with public openly and quickly.

In the United States, the legislation known as SARA Title III (Superfund Amendments and Reauthorization Act) has led to the creation on Local Emergency Planning Committees (LEPCs). These committees can be used as a forum for community communication and for the creation of emergency response plans.

CHAPTER

TECHNICAL INFORMATION

4

CHAPTER OUTLINE

Some of the technical information that makes up a process risk management system has been transferred from this book to *Design and Operation of Process Facilities*. This includes details to do with specific chemicals such as hydrogen sulfide and hydrogen fluoride.

INTRODUCTION

All operational integrity and process safety programs are built on a foundation of complete, accurate, and timely technical information. For example, a process hazards analysis requires that up-to-date and accurate piping and instrument diagrams (P&IDs) be provided to the team, operating procedures require information about process limits, and the asset integrity program requires information about equipment and piping. Moreover, regulations and standards require that good written records be maintained so that outside auditors can evaluate the status of the integrity management systems.

Process Risk and Reliability Management. DOI: http://dx.doi.org/10.1016/B978-0-12-801653-4.00004-7

The development and management of high quality technical information, particularly the safe upper and lower limit values, can be difficult and time-consuming but it is a vital activity. Without a sound information base, the quality of all of the other elements of the process safety program will always be in doubt. Therefore, it is critical that high priority be given to the development and maintenance of a high quality technical database.

The original term used for this topic by the Occupational Safety and Health Administration (OSHA) was "Process Safety Information." The more recent term, used by the Center for Chemical Process Safety (CCPS), is *Knowledge Management*. The change in terminology indicates that it is important not only to have sound and complete technical information, but that the information must be accessible to those who need it in a practical and timely manner.

The speed with which information needs to be available varies. Some information, such as safe information limits and Material Safety Data Sheets (MSDSs), must be accessible with no delay. Other information, such as employee training records, generally need not be available so quickly because such information is not likely to be needed for minute-to-minute decisions. It is, however, essential that the all employees know that the information exists, where it is located and how it can be accessed.

Some of the basic questions to be asked before implementing a knowledge management program include the following:

- Which documents are included?
- Where are the documents located?
- Who has access to them?
- Who has the authority to change them?
- How are revisions and changes noted?
- Who has authority to make copies?
- What is the retention/purge schedule?

In this context, the word "document" covers not only written information, such as is to be found in books or manuals, but also electronic images, video clips, and voice recordings.

TABLE OF CONTENTS

Table 4.1 summarizes the technical information that should be available to operations, maintenance, and technical staff. It is organized in the form of a Table of Contents for an Information Manual (this structure can also be used as an indexing system for an electronic database). The Table is structured for the facility shown in the first standard example in Chapter 1; it has five major operating units (100−500) and a Utilities section.

Table 4.1 Representative Table of Contents for Information Manual

- **Process Description**
  - **Process Overview**
    - Unit 100
    - Unit 200
    - Unit 300
    - Unit 400
    - Unit 500
    - Utilities
  - **Geographical Location**
  - **Environmental Concerns**
  - **Major Equipment Items and Layout**
  - **Process Chemistry**
  - **Engineering Information**
    - Block Flow Diagrams
    - Process Flow Diagrams
    - Piping & Instrument Diagrams
    - Utility Flow Diagrams
    - One Line Drawings
  - Area Classification
  - Electrical Information
  - **Instrumentation**
    - Instrument List
    - Control Strategy
    - Safety Systems
    - Alarm Settings
    - Cause and Effect Charts
    - SAFE Charts
    - Emergency Isolation Valves
- **Safety Systems**
  - Normal Operating Limits
  - Safe Operating Limits
    - Maximum Intended Inventory
    - Maximum Allowable Working Pressure
    - Unsafe Mixing Scenarios
    - Materials of Construction Table
    - Procedure for Changing Safe Limits
- **Asset Integrity**
  - Corrosion
  - Cathodic Protection
  - Relief Valve Settings
- **Duties and Responsibilities**
  - Emergency Response
  - DCS Technician
    - Outside Technician
    - Coordination with the DCS Technician
    - Shift Change
  - Visual Checks
  - Maintenance
- **Safety, Health, and Environmental**
  - Hazardous Chemicals
  - Health Information
  - Safety Diamond
  - Material Safety Data Sheets
  - Personal Protective Equipment
  - Housekeeping
    - General Rules
    - Inspection Teams
    - Disposal of Trash and Refuse
  - Safe Work Practices
    - Lock out/tag-out
    - Confined Space Entry
    - Opening Equipment or Piping
  - Safety Lists
    - Bleed and Vent Points
    - Blind List
    - Car Seal and Lock Lists
- **Quality Control**
  - Raw Materials
  - Product
  - Statistical Process Control
  - Environmental Information and Regulations
- **Security**
  - Protection
  - Facility Entrance Control
  - Threatening Calls
- **Contacts**
  - Emergency Services
  - Management
  - Environmental
  - Vendors

PROCESS DESCRIPTION

The first part of the Information Manual provides an overview description of the process facility, what its primary functions and products are, and what those products are used for. The process overview can include information to do with the facility's location, its impact on the environment, and general public relations issues to do with the local community. An overview of meteorology data can be included in this section also. The overview will also provide a summary of the major equipment items such as distillation columns, fired heaters, compressors, pumps, and heat exchangers. A layout sketch for each level of the facility (or each deck of a platform) should be provided.

Knowledge of the process chemistry must be made available to those who need such information in order to carry out their work safely. It is important to make sure that the information is presented in a usable form. Most operators, for example, are not trained to understand complex chemical equations, so the process chemistry must be explained in terms appropriate to their background and training.

If the process chemistry is a trade secret then management is still responsible for conveying sufficient information about the process such that the operators can do their work safely.

Chemicals are usually classified and labeled through the use of MSDSs or the Global Harmonization System (GHS).

FLOWSHEETS

Flowsheets/flow diagrams are fundamental engineering documents used by everyone on a facility. The terminology used by different companies and industries varies somewhat, but the general hierarchy is from block flow diagrams (BFDs) to process flow diagrams (PFDs) to P&IDs.

BLOCK FLOW DIAGRAMS

BFDs provide an overall view of the process, generally on a single sheet of paper, with each major operating step represented by a block. BFDs are used primarily for training people who are not familiar with the unit. They are also useful for conceptual safety studies because they provide a good overview of the process.

Major process streams are shown connecting the blocks. The flow of process streams is generally from left to right, with a gravity bias, where possible, which means that liquids will leave from the bottom of a block, gases from the top. A BFD may also show a few of the more important operating parameters, such as flow rates and temperature. Excluded from BFDs are single pieces of equipment and package numbers.

Figure 4.1 is an example of a very simple block diagram. Two feed streams enter the unit. Each is purified; they are then mixed with one another and sent to the reaction section. The material

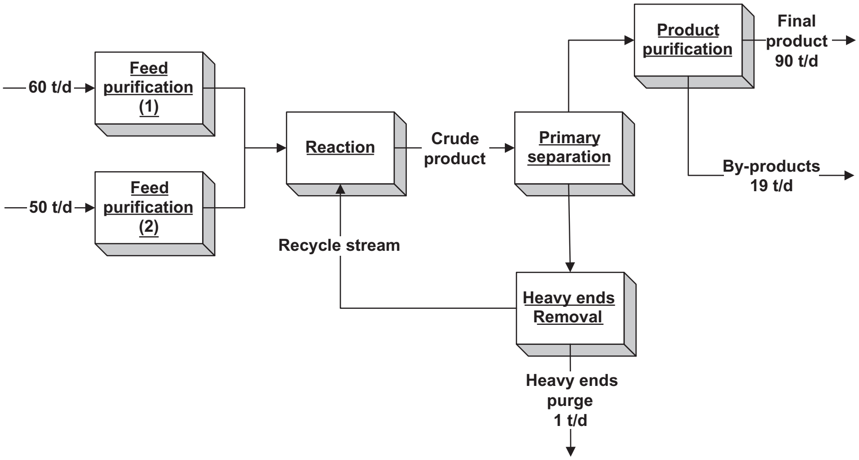


FIGURE 4.1

Block flow diagram.

leaving the reaction section—a mixture of product and unreacted feed materials—goes to a separation unit. Product is sent to purification; unreacted feed returns to the reaction section.

PROCESS FLOW DIAGRAMS

Material and energy balances are normally shown on the PFDs, which are a development of the block diagrams discussed above. A PFD contains process information for all significant streams. This information typically includes flow rates, chemical compositions, phases, temperatures, pressures, viscosities, thermal conductivities, and specific heats. A PFD will often show the major control systems, but will not provide instrument detail. In general, the following information is provided on a PFD:

- Process piping above a certain size, such as 2 inches
- Process flow directions
- Major equipment
- Bypass and circulation lines
- Control valves and process-critical block valves
- Connections between systems located on other PFDs.

The general layout guidance provided for BFDs, such as flows going from left to right, applies to PFDs also.

PFDs are not usually used much once a facility is built. They are too complex to provide a simple overview, such as is obtained from the BFDs. Nor do they contain mechanical information, so they have limited value to those working in operations or maintenance. Furthermore, once a facility is built, operating conditions are usually changed soon after start-up, often to obtain either higher production rates or improved yields. It is unusual for a facility to keep the PFDs up to date to reflect such changes.

PIPING & INSTRUMENT DIAGRAMS

P&IDs show all the process lines in a unit, including valves, material specs, and insulation detail. The P&ID may or may not include minor piping such as vent and drain lines and tubing. They provide a pictorial representation of all equipment, instrumentation, and piping in a facility. They are crucial documents in almost all types of safety study and analysis.

Information that is typically to be found on a P&ID includes the following:

- Equipment (with principal dimensions and a unique name and number)
- Piping (with sizes and specifications)
- Valves (including sizes)
- Vents and drains
- Interfaces to vendor packages
- Instruments (with unique names and numbers)
- Emergency shutdown systems
- Control loops
- Types of process connections
- Insulation
- Materials of construction
- Strainers and traps.

The following information is not usually entered on the P&ID:

- Process information (flows, temperatures, and pressures)
- Distances (P&IDs are not to scale)
- Small fittings such as vents and drains.

Because P&IDs are the foundation for all other engineering documents and for virtually all safety analyses, they should always be kept up to date (this is often a legal requirement). For a facility that is starting a new process safety program, updating the P&IDs should be one of the first tasks to be carried out. Otherwise, all other elements of PSM will be built on insecure foundations.

When checking or validating P&IDs, good practices to follow include the following:

- They should not be too crowded, otherwise they are difficult to follow. It is also hard to make further additions.
- They should be neat and clearly laid out.
- They should be consistent. Generally, consistency is achieved by using the first P&ID in a series—the Legend Sheet—to define the symbols and conventions used on this particular process (such as line labeling conventions).
- They must be accurate. This is really the most important item of all. If they contain many errors, users will lose confidence in them, and they will not be used. Moreover, incorrect engineering decisions may be made as a result of those errors.

Further information to do with P&IDs is provided by Toghraei (2014).

Design Phases

During the design of a process facility, P&IDs are issued at different stages such as the following:

- *FCA—For Client Approval*

  If the P&ID has been drawn or modified by an outside company, they will issue it to their client for approval. The client will make comments, those comments will be addressed, and the client will sign off the drawing.
- *AFD—Authorized for Design*

  Once all approvals have been obtained, the drawing is issued for design; it can be used as the basis for equipment detail, the purchase of equipment and pipe, and for detailed material takeoffs.
- *AFC—Authorized for Construction*

  During the detailed design and procurement phases, some changes to the P&IDs may be required. Also, reviews such as Process Hazards Analyses may lead to changes being made. All these changes and modifications are assembled, entered into the P&IDs, which are then issued to the construction teams. At this point in a project, every attempt must be made to prevent any more changes being made.
- *As-Built*

  This version of the P&ID shows what is actually installed in the field.

Equipment and Line Designations

Each equipment item on a P&ID will have a unique number, generally of the form X-00000. The letter designates the equipment type. Examples are:

- V—Vessel
- E—Heat Exchanger
- P—Pump
- T—Tank.

Different companies will use other symbols. For example, a distillation column may be designated with either a “C” or a “‘D.”

The first two numbers in the five digit identifier can identify a type of system or a section of the process. The final three numbers identify the specific piece of equipment.

Line numbers are often of the form 00″-XX-00000-X0X-X0″. The first two numbers are the nominal line diameter. The next two letters show the type of process stream, such as PG for process gas. The next five digits identify the process type or area and the number of the line. The next three digits (X0X) indicate the pipe specification, and the last two digits provide information about the type of insulation. Hence the line number 12″-PG-30012-A1A-P1″ tells the reader that the line has nominal diameter of 12 inches, it carries process gas, it is located in Section 30 of the facility, the line number is 012, the specification is A1A, and the line is provided with 1 inch of personnel protection insulation.

Instrument Designations

The nomenclature used for instrumentation is more complex than for equipment and process lines. Walker (2009) provides a list of commonly used instrument symbols. Typically an instrument balloon on a P&ID contains two or three letters followed by five digits. So PI-30012, for example, identifies a pressure indicator number 12 in Section 30.

Updating P&IDs

When P&IDs are updated, there should be some method of quickly identifying which items have changed. There is no single way of doing this. The conventions used when adding a lot of new equipment, for example, can be quite different from those when only a few minor changes to an existing drawing are being made. Some of the methods used for highlighting changes include the following:

- Changed areas are "clouded." A freehand line in the shape of a cloud is placed around those items that have changed.
- If the P&ID contains mostly new items, then they can be in solid, and the existing lines and equipment shown with dashed lines. The opposite applies just a few changes are being made; in these cases, the new items can be shown with dashed lines.
- Sometimes, it is sufficient simply to place a legend at the bottom of the drawing to describe what has changed.

Whatever method is used, it is essential that the title box be updated, and that it clearly identifies what has been changed. The title box should also clearly indicate why a change has been made, and why the P&ID is being issued at this time.

In order to indicate their status, P&IDs will often have a code letter in front of their number. For example, the letter "W" may means working, i.e., the P&ID is still being checked or developed. The letter "I" may mean that the drawing has been issued for construction and that it has received all the necessary engineering checks, and can be used for turnover packages. The letter "A" can be used to indicate "as-built."

EDITING ENGINEERING INFORMATION

Engineering documents can be edited through use of a system of colored highlighter pens. One system that is quite widely used is as follows:

- *Yellow* means that an item has been checked, and that it is satisfactory. This includes all cross-references to other sections of the book, every line of the Table of Contents and the Index, and links between the text and the titles of Tables and Figures. Citations can also be "yellowed out" (by checking them against the source).
- *Blue or Green* is used for deletions. Often the blue marks will be associated with red inserts.
- *Red* is used for new material. The new text is written in the margins, with an arrow pointing to the section of the manuscript that is to be replaced or added to.

When the document is completely "yellowed out," and contains no blue or red markings, it is ready to be issued.

Table 4.2 Materials of Construction Matrix

	Carbon Steel	Stainless Steel 304	Stainless Steel 316	Gasket Material A	Gasket Material B
A	√	√	√	√	√
B	‡	√	√	X	X
C	‡	N/A	N/A	N/A	N/A
D	X	X	‡	√	√
E	N/A	√	√	√	N/A

MATERIALS OF CONSTRUCTION TABLE

Many accidents result from the use of incorrect materials of construction, particularly when corrosive chemicals are being used. A Materials of Construction table such as that shown in Table 4.2 provides how various materials of construction can be used for containing chemicals A—E.

The symbols in Table 4.2 have the following meanings:

√ No known problems
‡ Potential problems, further information may be needed
X Not allowed
N/A Information not available.

MSDS OR SAFETY DATA SHEET

The safety data sheet (the word “material” has been dropped in recent terminology) or SDS is specifically aimed at use in the workplace. It should provide comprehensive information about the chemical product that allows employers and workers to obtain concise, relevant, and accurate information that can be put in perspective with regard to the hazards, uses, and risk management of the chemical product in the workplace. The SDS should contain 16 sections. While there were some differences in existing industry recommendations, and requirements of countries, there was widespread agreement on a 16 section SDS that includes the following headings in the order specified:

- Identification
- Hazard(s) identification
- Composition/information on ingredients
- First aid measures
- Fire-fighting measures
- Accidental release measures
- Handling and storage
- Exposure control/personal protection
- Physical and chemical properties
- Stability and reactivity

- Toxicological information
- Ecological information
- Disposal considerations
- Transport information
- Regulatory information
- Other information.

Suppliers and generators of hazardous materials used in the workplace are required to document the specific hazards and related safety precautions and procedures. To do this, they generally create MSDSs. An MSDS contains information about chemical properties, health and physical hazards, first aid and medical treatment, emergency response, and the handling and disposal of chemicals. The MSDS should be concise, and immediately accessible and usable. MSDSs are available for chemical products from all U.S. and most European suppliers or manufacturers.

Chemicals that require an MSDS include the following:

- Treating chemicals
- Laboratory chemicals/solvents
- Industrial cleaning agents
- Bulk solvents/thinners/paints
- Crude oil, natural gas, and other process streams
- Fuels such as jet, gasoline, and diesel.

MSDS should be made available to all affected employees and contractors at work locations, field offices, or control rooms. MSDSs have to be provided not only for the principal products and materials used in a process but also for any chemical that may be present on site, even if the quantities are small. Therefore, a large facility may possess a library of thousands of MSDS.

For companies operating in the United States, the design, content, and application of an MSDS are explained in detail in OSHA's 1910.1200 (g) Hazard Communication Standard (HCS). Some of the key points with regard to this four page standard are as follows

- The manufacturer and/or distributor of a chemical is responsible for writing and distributing the MSDS.
- The MSDS must contain information describing the hazardous properties of the chemical.
- The MSDS must also describe flammability and explosively properties of the chemical.
- First aid and other treatment measures should be described.
- A name and address of where more information can be obtained, if needed.

The MSDS should provide the following information on the hazardous chemicals:

- The chemical's physical status—for example, whether the phase is solid, liquid, or gas.
- The chemical reactivity of the hazardous chemical, both when isolated and when mixed with other chemicals in the process, or with air that might enter the system.
- Information regarding the corrosivity of the various streams should be supplied. If an operator is provided with a new type of sample container, for example, there should be information which tells him whether the material is safe.

OSHA provides the following guidance with respect to MSDS:

> Chemical manufacturers and importers are required to obtain or develop a material safety data sheet for each hazardous chemical they produce or import. Distributors are responsible for ensuring that their customers are provided a copy of these MSDSs. Employers must have an MSDS for each hazardous chemical which they use. Employers may rely on the information received from their suppliers. The specific requirements for material safety data sheets are in paragraph (g) of the standard...
>
> The role of MSDSs under the rule is to provide detailed information on each hazardous chemical, including its potential hazardous effects, its physical and chemical characteristics, and recommendations for appropriate protective measures. This information should be useful to you as the employer responsible for designing protective programs, as well as to the workers. If you are not familiar with material safety data sheets and with chemical terminology, you may need to learn to use them yourself. A glossary of MSDS terms may be helpful in this regard. Generally speaking, most employers using hazardous chemicals will primarily be concerned with MSDS information regarding hazardous effects and recommended protective measures. Focus on the sections of the MSDS that are applicable to your situation.
>
> MSDSs must be readily accessible to employees when they are in their work areas during their workshifts. This may be accomplished in many different ways. You must decide what is appropriate for your particular workplace. Some employers keep the MSDSs in a binder in a central location (e.g., in the pickup truck on a construction site). Others, particularly in workplaces with large numbers of chemicals, computerize the information and provide access through terminals. As long as employees can get the information when they need it, any approach may be used. The employees must have access to the MSDSs themselves—simply having a system where the information can be read to them over the phone is only permitted under the mobile worksite provision, paragraph (g)(9), when employees must travel between workplaces during the shift. In this situation, they have access to the MSDSs prior to leaving the primary worksite, and when they return, so the telephone system is simply an emergency arrangement.

When conducting an inspection, OSHA looks for the following information to do with MSDS.

- Designation of person(s) responsible for obtaining and maintaining the MSDSs
- How the sheets are to be accessed and kept up to date in the workplace
- Procedures to follow when the MSDS is not received at the time of the first shipment
- For producers, procedures to update the MSDS when new and significant health information is found
- Description of alternatives to actual data sheets in the workplace, if used.

For employers using hazardous chemicals, the most important aspect of the written program in terms of MSDSs is to ensure that someone is responsible for obtaining and maintaining the MSDSs for every hazardous chemical in the workplace. The list of hazardous chemicals required to be maintained as part of the written program will serve as an inventory. As new chemicals are purchased, the list should be updated. Many companies have found it convenient to include on their purchase orders the name and address of the person designated in their company to receive MSDS.

Within the United States, there is no regulation as to how often MSDSs should be updated or revalidated. Canadian law requires that this be done at least every 3 years; this update frequency is often used as a good practice, even when it is not the law.

OSHA states the following regarding storing MSDS in electronic format only.

> If the employee's work area includes the area where the MSDSs can be obtained, then maintaining MSDSs on a computer would be in compliance. If the MSDSs can only be accessed out of the employee's work area(s), then the employer would not be in compliance with 1910.1200(g) (8) or (9) and 1926.59 (h)(1)(i–v).

GLOBAL HARMONIZATION SYSTEM

Currently, many different countries have their own standards for chemical hazard classification and communication. The Globally Harmonized System of Classification and Labeling of Chemicals (GHS) is intended to replace these multiple systems with one uniform system.

GHS is an internationally agreed upon system set to replace the various different classification and labeling standards used in different countries. The system, whose development started in the year 1992, supersedes the pertinent European and United States standards. Its goals are to:

- Provide an internationally comprehensible system for hazard communication, hazard classification, and labeling
- Provide a framework for those countries without an existing system
- Facilitate international trade in chemicals whose hazards have been properly assessed and identified on an international basis
- Reduce the need for animal testing and evaluation of chemicals.

GHS uses a common and consistent approach to defining and classifying hazards, and to communicating hazard information on labels and SDSs. It covers all hazardous chemicals and products, including mixtures, and classifies them according to their physical, health, and environmental hazards.

The GHS is not a regulation. Therefore, compliance with the GHS is voluntary for each country but companies in countries that do not adopt the GHS will be at a disadvantage when doing business internationally. The GHS guidance, also known as "The Purple Book," establishes criteria and methods for hazard classification and communication. It provides countries with the regulatory framework to develop or modify existing programs. The data used for classification may be obtained from tests, literature, and practical experience. The main elements of the hazard classification criteria are summarized below.

There is no international implementation schedule for the GHS.

In the United States, the OSHA has revised its HCS so as to be in alignment with the GHS system. The HCS will be fully implemented in 2016.

THE SAFETY DIAMOND

NFPA 704 (NFPA 2012) defines the "fire or safety diamond" used by emergency personnel to quickly and easily identify the risks posed by nearby hazardous materials. It is also used within process facilities, particularly in storage areas and tank farms.

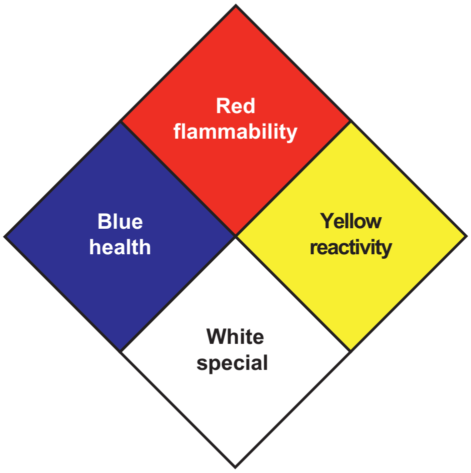


FIGURE 4.2

Safety diamond.

Table 4.3 Safety Diamond Numbering System

	Flammability (Red)	Reactivity (Yellow)	Health (Blue)
4	Will rapidly or completely vaporize at normal atmospheric pressure and temperature, or is readily dispersed in air and will burn readily	Readily capable of detonation or explosive decomposition at normal temperatures and pressures	Very short exposure could cause death or major residual injury
3	Liquids and solids that can be ignited under almost all ambient temperature conditions. Flash point below 38°C (100°F) but above 23°C (73°F)	Capable of detonation or explosive decomposition but requires a strong initiating source, must be heated under confinement before initiation, reacts explosively with water, or will detonate if severely shocked	Short exposure could cause serious temporary or moderate residual injury
2	Must be moderately heated or exposed to relatively high ambient temperature before ignition can occur. Flash point between 38°C (100°F) and 93°C (200°F)	Undergoes violent chemical change at elevated temperatures and pressures, reacts violently with water, or may form explosive mixtures with water	Intense or continued but not chronic exposure could cause temporary incapacitation or possible residual injury
1	Must be preheated before ignition can occur. Flash point over 93°C (200°F)	Normally stable, but can become unstable at elevated temperatures and pressures	Exposure would cause irritation with only minor residual injury
0	Will not burn	Normally stable, even under fire exposure conditions, and is not reactive with water	No health hazard

The fire diamond has four color-coded sections, as illustrated in Figure 4.2. The blue, red, and yellow fields correspond to chemical's effect on health, flammability, and reactivity, respectively. They all use a numbering scale ranging from 0 to 4. A value of 0 means that the material poses essentially no hazard; a rating of 4 indicates extreme danger. Table 4.3 provides further description of the numbering system for the first three fields.

The fourth field is white; its use tends to be more variable than the other three, both in meaning and in what letters or numbers are written there. It can contain symbols such as:

- **~~W~~**: reacts with water in an unusual or dangerous manner
- **OX** or **OXY**: oxidizer
- **COR**: corrosive
- **ACID** and **ALK** strong acid or base
- **BIO**: biological hazard
- **POI**: poisonous
- ☢: radioactive
- **CRY** or **CRYO**: cryogenic.

CHAPTER

HAZARD IDENTIFICATION

5

CHAPTER OUTLINE

INTRODUCTION

In Chapter 1, it was shown that a risk analysis has four elements:

1. A hazard
2. The consequences of that hazard (safety, environmental, and economic)
3. The likelihood of occurrence of that hazard
4. Safeguards that reduce consequences or likelihood

Process Risk and Reliability Management. DOI: http://dx.doi.org/10.1016/B978-0-12-801653-4.00005-9

The relationship between the first of the above three terms is shown in Eq. (1.1), which is repeated below as Eq. (5.1).

$$\text{Risk}_{\text{Hazard}} = \text{consequence} \times \text{predicted frequency} \tag{5.1}$$

The first and most important step in any risk management program is to identify the hazards. Hazards analysis is the most important step in risk analysis because, unless hazards are identified, consequence and likelihood reduction cannot be implemented. In the context of process safety and operational integrity programs, this usually means that a Process Hazards Analysis (PHA) must be conducted.

Not only is hazard identification (HAZID) the most important part of any risk analysis, removal of hazards is almost always the best way of reducing risk, and it is the only way in which risk can be reduced to zero. As noted in Chapter 1, reductions in the consequence and frequency terms—the second and third elements of Eq. (5.1)—can only reduce risk; they cannot eliminate the risk entirely.

Companies in the process industries habitually handle large quantities of toxic, flammable, and explosive materials—often at high temperature and pressure. Such processes are inherently hazardous and have the potential to cause loss of life, serious injuries, and severe pollution. Since these processes are often quite complex and sophisticated and have many recycle streams, it means that the identification of hazards is not an easy process. Therefore, a wide range of PHA techniques has been developed and used over the years. The key to almost all of these techniques is that a team of experts analyzes the process in question to determine how major failures—often involving a very unlikely sequence of events—could occur. A PHA is not concerned with occupational hazards such as trips, falls, and the use of lock-out/tag-out rules. Instead it focuses on process-related issues such as overpressuring a vessel or damage caused by corrosion.

Effective hazards analyses go beyond the mere identification of hazards, however—they help create a frame of mind in which everyone is looking for hazards all the time, and then taking corrective action. For example, an operator working by himself at two o'clock in the morning may be about to open a valve, but before doing so he pauses for a moment, and says to himself:

> You know, opening this valve could lead to reverse flow, which could lead to wrong chemicals mixing with each other, and... you know what—before opening the valve, maybe I should take a break, make a cup of tea, and talk over what I'm planning to do with my colleagues and supervisor.

When an employee thinks and acts in this manner, the hazards analysis program is working very well indeed because it has become a part of the broader topics of culture and workforce involvement.

Although companies in the process industries have always worked on the identification and control of hazards, the formal discipline of PHA, specifically the HAZOP (Hazard and Operability) method, was not developed until the 1960s by process plant professionals in the United Kingdom, many of whom worked for the company ICI (Lawley, 1976; Knowlton, 1992; Kletz, 1997). More recent guidance is provided in ISO 17776 (2000).

The introduction of process safety regulations—particularly in the United States—in the late 1980s and early 1990s gave an additional impetus to the use of PHAs. Indeed, the high level of awareness of PHAs—particularly the HAZOP method—led to statements such as that made by a plant manager in the early 1990s, "I know what process safety management is—it's HAZOPs!"

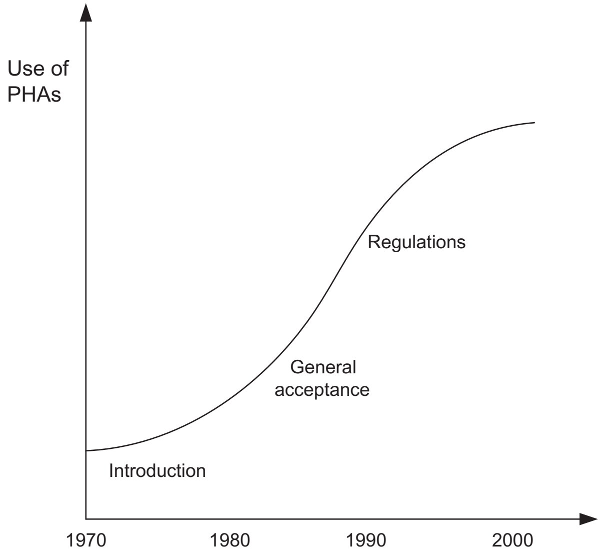


FIGURE 5.1

Growth in the use of PHAs.

His statement was technically incorrect, but it did reflect the rightful importance that was attributed to PHAs in the early days of process safety compliance. For reasons such as these, the use of PHAs grew rapidly in the 1970s and 1980s, as illustrated in Figure 5.1.

Figure 5.1 shows that the growth in the use of PHAs is leveling off. From one point of view this leveling is commendable; it shows that PHAs are now "part of the furniture," and are being carried out as a routine means of ensuring process safety. However, some practitioners feel that the existing approaches to hazards analyses offer diminishing returns and that new ideas are needed in order to generate fresh insights into hazards identification and risk reduction. The flattening in usage may be occurring because management does not feel to be gaining as many insights from their PHAs as they did in the past.

HAZARDS MANAGEMENT PROCESS

Figure 5.2 outlines the process for conducting a PHA. The basic idea behind Figure 5.2 is that, once a hazard has been identified, its associated risk is evaluated as to whether that level of risk is acceptable or not. If it is, the analysis moves on to the next hazard. If, however, it is determined that the risk is too high a series of corrective measures are carried out in the order shown. At each step, the risk is reevaluated until it reaches a very low level.

The steps shown in Figure 5.2 are described below.

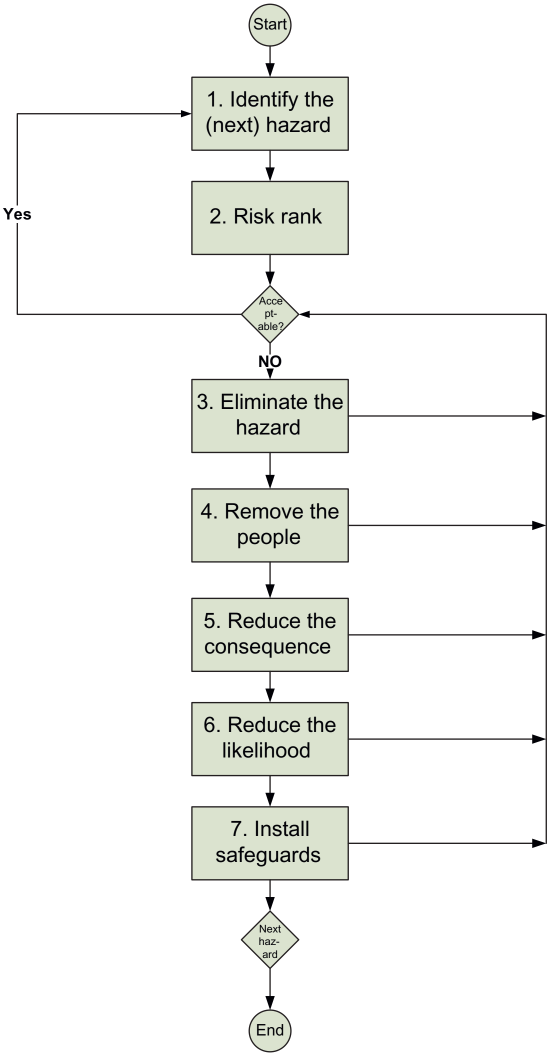


FIGURE 5.2

Hazards analysis process.

STEP 1. IDENTIFY THE HAZARDS

PHAs are generally conducted by a team [although some of the more specialized techniques, such as Fault Tree Analysis (FTA), may be conducted by a specialist working alone or with just one other person]. The team members should represent a cross section of disciplines and functions at the facility or on the project—at a minimum including operations, engineering, maintenance, and process design. Having all the disciplines present in the meeting helps ensure that all types of hazard scenarios are discussed. Furthermore, the interaction between team members helps uncover those hazards that may be caused by communication difficulties or misunderstandings between departments.

Hazards usually have multiple causes. For example, high level in T-100 could be caused by instrument malfunction, operating error, or equipment malfunction. As many as possible of these causes need to be listed.

Broadly speaking, hazards analyses can be divided into one of three categories:

- Creative/imaginative
- Experience based
- Logical/rational

Each approach is appropriate at its own time and place—none of them is inherently better than any of the others. Indeed, they are often used in combination with one another. Moreover, the different approaches have much in common; it is important not to overemphasize the differences between them. Experienced hazards analysis leaders tend to find that they shift from one method to another rather as persons who are multilingual will switch from one language to another, almost without realizing that they are doing so.

For example, the FTA approach is logical and rational. The persons building the tree assume that the base events, and the manner in which they interact with one another, have been defined before the analysis starts. However, fault tree analysts will often identify new incident scenarios and find new types of hazard. In other words, this "logical/rational" approach to hazards analysis can also be "creative and imaginative."

The choice of PHA method will depend on many factors, including the following:

- Whether the analysis is of a facility that is already in operation or of one that is still being designed
- The history of events at the facility
- The level of analytical detail required
- The sophistication of process technology being used
- The regulatory environment

A list of the more commonly used hazard identification techniques is provided below. They are discussed in greater detail in later sections of this chapter and also in Chapter 5.

- HAZOP Analysis
- Checklists
- What-If Analysis
- Failure Modes and Effects Analysis (FMEA)
- FTA
- Major Hazards Screening (MHS)
- Monte Carlo Simulation and Markov Analysis

Creative/Imaginative Techniques

The first group of hazards analysis techniques covers those that are creative and that encourage "out of the box" or "off the wall" thinking. The What-If and HAZOP methods fall into the "creative/imaginative" category.

Imaginary gardens with real toads in them

The poet Marianne Moore wrote the phrase quoted above—a phrase that captures the essence of a creative hazards analysis. The scenarios that the team members discuss are imaginary, but the "toads"—the injuries and losses—are very real. When using techniques in this group, team members are encouraged to "think the unthinkable," i.e., to visualize low probability accident scenarios that have never occurred before, but which are still plausible.

> . . .there are known knowns; . . .We also know there are known unknowns; . . .But there are also unknown unknowns—the ones we don't know we don't know.
>
> **Donald Rumsfeld (1932–)**

In the year 2002, the then Defense Secretary Donald Rumsfeld conveyed the same concept of "imaginary gardens" in the quotation provided above. He received much derisive criticism from his political opponents for what he had said. Yet Rumsfeld's words can be useful for a hazards analysis team to consider.

The "known knowns" are those issues that pose a hazard, but that have been identified, and that have probably been addressed effectively. For example, the reaction step in the manufacture of ethylene oxide can involve the mixing of pure ethylene with pure oxygen. Not only are these two chemicals hazards in and of themselves; at some point in the mixing process they *must* go through the flammable range. Although this mixing operation has high risk, it is well understood and is effectively handled through the use of sophisticated instrument systems. Because it is a "known known," the hazards analysis team does not need to spend much creative time discussing the mixing of ethylene and oxygen.

The "known unknowns" are the focus of most hazards analyses. For example, a process may involve the transfer of chemical from a high-pressure vessel to another vessel that operates at lower pressure. The designers of the system may not have considered the possibility that the pressure gradient could reverse, i.e., that the pressure in the first vessel could drop to a value less than that in the second vessel, thus creating the possibility of reverse flow. Such a scenario is a valid topic for the hazards analysis team to discuss. This scenario is a "known unknown"—it may not have been considered, but it is part and parcel of a normal hazards analysis.

It is the "unknown unknowns" that the team—and particularly the team leader—needs to give special consideration to. These situations require creative and imaginative thinking. In this context, another Rumsfeld quotation—*absence of evidence is not the evidence of absence*—should be considered. Getting team members to "think the unthinkable" is one of a team leader's biggest challenges. First, he or she has to overcome the "I've never seen it happen, therefore it can't happen" syndrome. Second, these low probability scenarios usually involve the simultaneous occurrence of contingent events (which is why they occur so rarely). Once more, team members typically have trouble accepting and understanding unlikely combinations of events. To help overcome this block, the leader may choose to describe a number of real accidents that occurred elsewhere to show how "weird" they were—yet they happened.

Experience Based

The second style of hazards analysis is based on the experience of experts and of engineering standards. Their knowledge is used to build up a set of checklist questions that can be specific to a company or facility, or that can be published by bodies such as American Petroleum Institute (API) and American Society for Mechanical Engineers. The hazards can also be evaluated against *Recognized and Generally Accepted Good Engineering Practice* (RAGAGEP), as discussed in Chapter 9.

The Checklist and the FMEA methods both fall into the experience-based category of hazards analysis.

Logical/Rational

The third style of hazards analysis consists of those methods that make use of logical analytical techniques—generally based on the principles of Boolean algebra. This approach attempts to provide an understanding of hazards and risk in a strictly logical and rational manner. The techniques of FTA and Monte Carlo simulation fall into the logical/rational category.

This type of hazards analysis can be either deductive or inductive. A deductive (top-down) analysis is one that first defines an undesirable event, and then considers what events and chains of circumstances are needed to occur before the overall undesirable event occurs. A deductive approach is used by detectives to solve crimes. A widely used type of deductive analysis in process risk analysis is the fault tree method, described in the next chapter.

An inductive analysis works bottom upwards. A failure event is postulated. The analysis team then determines what effect this failure could have on the overall system. The HAZOP and Event Tree Analysis methods are both inductive.

STEP 2. RISK RANK

The next step in the hazard management process, as shown in Figure 5.2, is to determine the level or risk associated with the hazard once it has been identified. The hazards analysis team must decide if their discussions are to focus on high-*risk* or high-*consequence* events. Either approach is valid, but the team members must be clear as to which goal they are pursuing. It is commonly observed, e.g., that teams will state that their goal is to identify *high-risk* situations, yet, in practice, such hazards analysis teams frequently concentrate more on the identification of high-*consequence* hazards because it is such hazards that are the ones that tend to get the most publicity, that are the most emotionally wrenching, that generate law suits, and that have the potential of destroying a business (and the careers of those associated with that business).

STEP 3. ELIMINATE OR SUBSTITUTE THE HAZARD

The next step is to eliminate the hazard or substitute a hazardous chemical with one that is less hazardous. These concepts fall under the topic of Inherent Safety, which is discussed in detail in Chapter 8.

STEP 4. REMOVE THE PEOPLE

> If a man’s not there he can’t be killed
>
> **Ian Sutton**

If the hazard cannot be removed, the next best option, at least with regard to safety, is to remove people from the site of the potential incident. The increased use of sophisticated control and safety instrument systems makes this option increasingly plausible. People are not needed to bring the system to a safe condition.

This topic is also discussed in Chapter 8 under the section to do with Inherent Safety.

STEP 5. REDUCE THE CONSEQUENCE

If the hazard cannot be removed and the workers must stay in the area then the next option generally is to mitigate the consequences associated with a hazard. Mitigation can also be achieved by relocating hazardous facilities to a relatively remote location.

STEP 6. REDUCE THE LIKELIHOOD

Reducing the likelihood of occurrence of a hazard is often the first option selected in a risk reduction program, yet it is generally less effective than eliminating the hazard or minimizing the consequences. In the standard example, the likelihood of an incident to do with tank overflow can be reduced through the use of more reliable instrumentation and by upgrading the operator training programs.

Further discussion to do with consequence and likelihood analysis is provided in the next chapter.

STEP 7. INSTALL SAFEGUARDS

If it is not possible to remove the hazard or to reduce the consequences or likelihood then safeguards must be installed, ideally in the following order: passive, active, and procedural. A passive safeguard is one that is always there and that cannot fail; the tank berm shown in Figure 5.3 is an excellent example of a passive safeguard. An active safeguard takes action to control a hazard. Instrument alarms and pressure safety relief valves are examples of active safeguards. The least attractive type of safeguard, because of its low reliability, is procedural—typically achieved through the use of procedures and training.

ORGANIZATION OF A HAZARDS ANALYSIS

Details as to how the hazards analysis itself is to be organized will vary depending on the goals of the analysis, the method used, and the facility being studied. However, an overall organization such as that shown in Figure 5.3 is representative.

At the top of Figure 5.3 is the senior manager or client who has requested and who is paying for the analysis. The team must understand this person's needs. For example, some clients just want to be sure that they are in regulatory compliance, others want to identify major events only, and others want a detailed equipment analysis. The PHA must be structured appropriately.

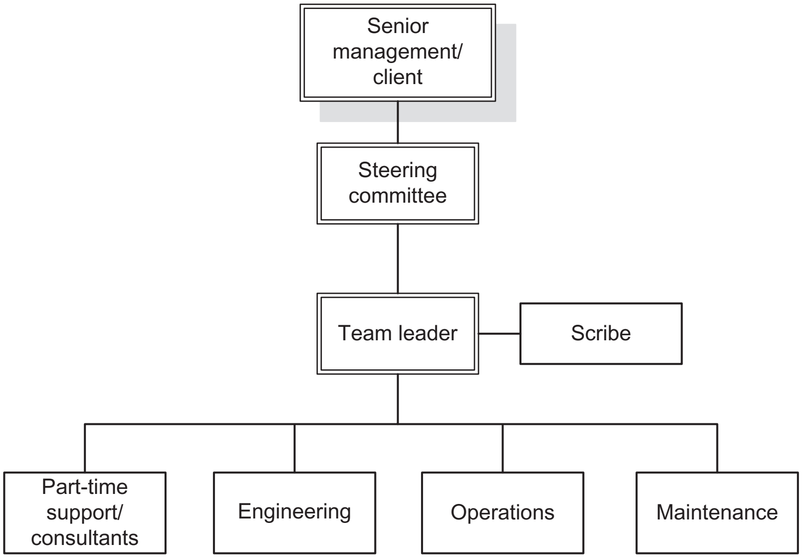


FIGURE 5.3

Team structure.

The hazards analysis process will often be managed by a steering committee. The committee will typically include representatives from operations, maintenance, and the risk management group. The committee usually has the following responsibilities:

- Provide the analysis team with a charge or scope letter, as discussed below.
- Ensure that links with other hazards analyses are established. On a large facility, a single analysis usually covers only a relatively small fraction of the total process. Therefore, it is important to make sure that the connections between the different processes are properly analyzed, particularly with regard to plant utilities. [The important and difficult topic of Interface Hazards Analysis (IHA) is discussed later in this chapter.]
- Ensure that the team members, particularly the leader, are fully qualified and trained.
- Ensure that the manner in which the analysis was conducted conforms to company standards and government regulations, recognizing that, in the worst case situation, the PHA report may wind up as a pivotal document in a court case.
- Approve policy changes and variances. For example, one team was reviewing the hazards associated with an ethylene/oxygen mix station. In the mixing process, ethylene and oxygen pass through the explosive range, thus creating a well-known and well-understood high-risk scenario, which had already been analyzed in depth many times using a variety of techniques. Consequently, the steering committee agreed that the hazards analysis team could exclude this mix station from its scope of work. (An additional reason for this decision was that the instrumentation associated with the mixing station was so complex that it would have been difficult for a team of nonspecialists to have analyzed it properly.)
- Ensure that a detailed, accurate, and readable report is issued on time.

- Establish links between the analysis and the other elements of the process safety management (PSM) program.
- Audit the follow-up to the analysis in order to ensure that all findings are closed out in a professional and timely manner.

Many hazards analyses—particularly those generated by the Management of Change (MOC) program—can be quite short. If say a gate valve is being replaced with a ball valve, only one node is to be discussed, and probably only three guideword combinations ("High Flow," "Low/No Flow," and "Reverse Flow") will be pertinent.

For such analyses, the leader must still make sure that the formal analysis process is followed, that a fully qualified team was assembled, and that a proper report is issued.

CHARGE/SCOPE LETTER

Management should issue a charge letter before the hazards analysis starts. The letter should list the basic parameters of the upcoming hazards analysis including items such as given below.

Objective

The objective and purpose of the analysis must be explained clearly. For example, a team may be charged with identifying only major safety problems or just with ensuring compliance with regulatory standards.

Physical Scope

The area to be analyzed must be clearly defined; it is usually a discrete process unit, such as "The Secondary Reaction Section" or "Boilers #1 and #2." Such units usually have multiple connections with other areas and often with other companies (via pipelines and truck deliveries, for example). It is essential to define these boundaries and to decide how the hazards associated with these interfaces are to be analyzed.

Method(s) To Be Used

The charge letter will describe which techniques are to be used for the analysis. It may, e.g., specify that HAZOP is to be used for all process units, a checklist for batch operations, and FMEA for the analysis of machinery such as turbines and motors.

Assigned Personnel

The charge letter will specify who is to be on the team. Generally, specific individuals will be named. However, it may be enough simply to specify a job function such as "Operations Specialist."

Risk Management Guidance

If the team is expected to determine the risk associated with each hazard then a description of the methods to be used (e.g., risk matrices) should be provided.

Schedule and Reporting

The charge letter should provide an estimate as to how long the analysis is expected to take, when the report is to be delivered and what form of risk register is to be used.

ABANDONED EQUIPMENT

The steering committee should provide guidance as to how unused or abandoned equipment is to be analyzed. An unused storage tank, e.g., may have been declared as abandoned. Yet, if that tank can be filled with process liquids merely by opening valves, then it is not really abandoned, and so it has to be included in the analysis. True abandonment of equipment only occurs when the equipment (including all associated instrumentation and electrical equipment) is positively isolated and/or disconnected.

PREPARATIONS

One of the keys to a successful hazards analysis is that all the team members, particularly the leader and scribe, are thoroughly prepared. The importance of this step cannot be overstated. When a hazards analysis goes awry the reason, more often than not, is inadequate preparation. Hence, the meeting gets off to a bad start from which it never recovers. As a working number, it is good to budget half a day of preparation time for each meeting day, and maybe another day per meeting week for writing the report.

A few days prior to the start of the team meeting, the scribe should provide the team members with all pertinent information, such as the charge letter, the relevant drawings, and other background material such as the facility's operating procedures. The team members should study this material before showing up to the meeting.

LOGISTICS

The scribe should make sure that logistical issues such as the following have been addressed.

- Has a room been reserved?
- Is it big enough?
- Does it have walls to which drawings can be attached?
- Are drinks, snacks, and lunch to be provided?
- If so, have they been ordered, and is there a charge number for them?
- Is a computer available?
- Is a projector available?
- Does the scribe have the right software?
- Does the software work? (Key disks can be a problem.)
- Have the participants been provided with a "package" containing the charge letter, shot-down Piping and Instrument Diagrams (P&IDs), copies of key Material Safety Data Sheet (MSDS) and other pertinent materials?
- Is there an ample supply of pens and paper (including highlighters to mark the drawings)?
- Are name place cards provided?

PHAs can take a considerable amount of time. A general rule of thumb is that the meetings should not go on for more than 6 hours a day, otherwise the participants will lose their concentration. But not all PHAs take a long time. If a team is analyzing a small MOC problem, e.g., the PHA itself may take just a few minutes. For these PHAs, the biggest problem can be making sure that the team's findings are properly documented.

MEETING PROTOCOL

PHAs often take a long time and they require the involvement of key personnel. Hence, there is often considerable pressure for these people to skip a session or two so that they can get back to do their "real work." It should be made clear that a PHA is real work. This means that team members should not take telephone calls or answer beepers and radios during the meetings.

All conversation and comments should be directed through the team leader. Side conversations are distracting to the other team members.

LOCATION OF THE MEETING

Generally, hazards analyses are held at the location where most of the team members work. If the facility being reviewed is still at the design stage the hazards analysis will probably be held in the design engineering office. If the facility is already in operation, then the hazards analysis will typically be held at or near the plant site.

Sometimes the analysis may be held off-site, say in the conference room of a local hotel. Although more expensive than using the company's own offices, taking the team off site does have the advantage of making sure that they focus on the hazards analysis. If someone such as an operations supervisor is on the team, and the hazards analysis is held at the site, there is every chance that he or she will be pulled away from the team to address day-to-day operating problems.

In many larger facilities, hazards analyses are taking place almost all the time. In such situations, management may choose to create a dedicated hazards analysis room which will contain built-in facilities such as an overhead projector, a library of risk management materials, and a large coffee pot (with coffee in it).

PROJECTION OF NOTES

Many teams choose to have the scribe's notes displayed live on a screen so that they can be reviewed as they are being written. If this technique is used, and if the scribe is a bad typist, it is crucial that he or she have a thick skin.

Another way of sharing the notes among the team members is for the scribe to turn off the projector while actually recording the notes. At the conclusion of the discussions to do with that node, the scribe and leader then spend a few minutes cleaning up the notes. The projector is then turned on, and the updated notes for that node are reviewed with the team. Once the team has agreed that the notes are correct there is no need for further review, thus getting around the problems associated with sending draft reports in the days following the analysis.

Some teams may choose to have two projectors: the first projects the scribe's notes and the second shows the P&ID that is being discussed. Having an electronic copy of the P&ID displayed helps ensure that all team members are focused on the same issue. It also eliminates the need for each team member to have his or her own copy of the P&IDs.

DOCUMENTATION REQUIREMENTS

The documentation needed for a hazards analysis will vary according to the scope of the work. However, the following are usually required, depending on the level of detail that is required:

- Process Chemistry
- Block Flow Diagrams (BFDs)
- Process Flow Diagrams (PFDs)
- P&IDs
- Cause and Effect Charts
- Plot Plans
- Operating Procedures
- Safe Upper and Lower limits (particularly pressure and temperature limits for the equipment items)
- MSDS
- Piping Specifications
- Electrical Area Classification Plot Plans

A description of each of the above items is provided in Chapter 5.

One set of P&IDs should be designated as being the official record for the analysis meetings. This set contains all the comments and marks representing the team discussions. It is also the one that is kept on file in the event that there is an incident investigation or an audit following the completion of the study. Once the meetings start, the official set of P&IDs is often maintained by the process or facilities engineer on the team. Neither the scribe nor the team leader should have this responsibility. The scribe is already very busy just making sure that the notes are accurate and representative of the discussion. The team leader needs the freedom to concentrate on stimulating the discussion and encouraging thinking. This does not leave sufficient time to mark up the P&IDs.

SECURITY OF THE INFORMATION

Some hazards analyses review confidential processes or other information that must be kept secure. In such situations, the scribe should collect all drawings and notes made at the end of each day. Then, once the analysis is complete, he or she can destroy all documents except those that constitute the official record of the meeting.

TIME REQUIRED

A simple and convenient method of estimating the time needed for an analysis, and then measuring the progress of that analysis, particularly a HAZOP, is simply to count the number of P&IDs to be analyzed, and then to determine how many actually have been fully analyzed. Naturally, not all P&IDs are equal in terms of size of complexity, and similar P&IDs may require substantially different discussion times. Nevertheless, this metric does provide a useful starting point for measuring progress.

For example, a company may have four operating areas:

- Section A—10 P&IDs
- Section B—21 P&IDs
- Section C—11 P&IDs
- Section D—Plot Plan only

Experience in this company indicates they can analyze three P&IDs per day. Therefore, the full HAZOP analysis will take around 14 working days.

Some P&IDs are virtually duplicates of others, particularly when parallel operating trains are in use. After the first P&ID has been analyzed thoroughly, the other P&IDs can be reviewed much more quickly by analyzing only those sections that differ from the first drawing.

As the analysis progresses, the team should check its progress against the goals set down in the charge letter. In particular, the team should check that it is moving at the right pace. If the analysis is moving more quickly or slowly than expected, management must be informed as soon as possible.

KICK-OFF AND CLOSE-OUT MEETINGS

Before the analysis commences, it is a good idea for a senior manager to lead a brief kick-off meeting. He or she will explain the company's commitment to the hazards analysis process and describe some of the details of the charge letter. The team leader can then explain the detailed plans for the work that is to be done during the course of the analysis.

Once the hazards analysis is finished, the team should present its findings to the Steering Committee. Also, it is useful to have a close-out meeting at which all parties will evaluate the work that was done; in particular, they will discuss the extent to which the original goals were met. Questions that the team members can pose include the following:

- Was the team composition correct?
- Was the most appropriate hazards analysis method used?
- Was the preparatory work complete and thorough enough?
- Were there any problems with the information provided to the team, particularly the P&IDs?
- Did the analysis move at the right speed?
- Did the team members feel that they had time to think about issues before the leader moved on?
- Were the team members bored?
- Does the report fairly and accurately summarize what was said? (This question applies only if the report has been written before the close-out meeting.)
- Was the report comprehensive and readable?

The results of this critique, which will be reported to the Steering Committee, can be used to modify the way in which future hazards analyses are conducted and to help develop more templates for the analysis of similar processes.

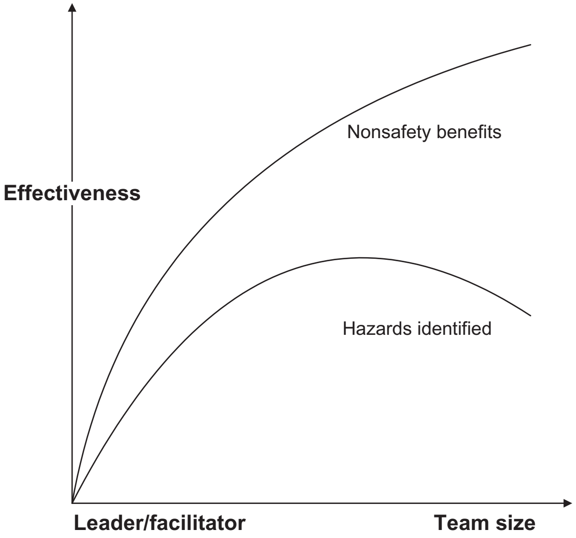


FIGURE 5.4

Effect of increased team size.

THE TEAM

The success of any hazards analysis depends almost entirely on the quality of the team, which is why it is so critical to have the facility's most experienced and knowledgeable people on the team, in spite of the fact that they are needed in so many other areas. Therefore, one of the most important of the leader's jobs is to ensure that he or she has the best possible team.

As with any team effort, the quality of the leadership is critical. The leader must somehow allow people to dream up potentially bizarre situations in anticipation that one or two of these situations will actually turn out to be plausible. At the same time, he or she has to keep the hazards analysis on track in terms of schedule and budget. Also, some team members enjoy the brainstorming process so much that they become counterproductive in terms of overall team effort. The leader needs to keep them focused.

The team size will vary according to the nature of the process, the analysis technique, and the degree of experience of the individual team members. Figure 5.5 shows that the number of hazards identified will increase as the team size increases up to a certain point. Beyond that point, it is likely that adding more people will degrade the quality of the analysis because the discussion is more likely to be difficult to follow and control.

Figure 5.4 also shows, however, that the nonsafety benefits of a hazards analysis, such as the general training of the team members in the process that they are analyzing, will continue to increase as more people join the team.

LEADER/FACILITATOR

The team leader is responsible for the overall conduct of the hazards analysis, the quality of the final report, and for ensuring that the project is completed on time and within budget. Some organizations describe the person filling this role as a facilitator. But use of this word can give a misleading impression. (In fact, the scribe will frequently act as the facilitator.) An effective leader actually *leads* the team. He or she sets the pace, manages different personalities, reads the body language of the team members, and adds his or her own thoughts and insights. This means that the leader's job consists of much more than reeling off a set of guidewords in sequence. For example, if the team is discussing the handling of a highly hazardous chemical, the leader may decide to let the discussion run on for a long period of time during which some previously unthought-of hazard may be identified. However, if the team is analyzing a low hazard situation, the leader should move the discussion along promptly. Team leaders have to work with the constraints of budget, schedule, and the availability of key people, while meeting their personal and corporate obligations to conduct a professional and responsible analysis.

The leader should be from outside the immediate organization of the facility being analyzed and, ideally, will be from a completely independent company for the following reasons:

- An outsider is truly independent. He or she should have no hesitation in speaking out about hazards, regardless of day-to-day economic "realities" or internal personal relationships. The loss of a client should not be a concern.
- An outsider can sometimes see obvious hazards and risks right away, whereas people who work at a facility may have become oblivious to those problems.
- An experienced outsider will bring a wealth of experience and knowledge from all the other analyses and evaluations in which he or she has participated. This fund of experience provides an invaluable basis for challenging the status quo and coming up with fresh insights. External hazards analysis leaders move from project to project, in the same way that medieval masons moved from cathedral to cathedral, taking their experience and skills with them.
- The outside leader is likely to have experience with a variety of industries. Such diversity can help create fresh insights.

Larger companies often have a corporate group that leads hazards analyses (and that also conducts safety audits). Personnel from these groups will provide more of an outside perspective than plant people. They will also have a good knowledge of internal standards and policies. However, their knowledge of "the realities" of internal company issues and reporting structures may unconsciously affect their independence.

In spite of the benefits of using an outsider to lead hazards analyses, most companies use their own personnel as leaders. They do this because there is usually no direct cost (the leader's salary is being paid anyway) and because there is no need to negotiate a contract (with its associated liability issues). Also, because internal employees know the processes and organizational systems that are being reviewed, they do not need much time to get up to speed.

Some of the attributes of a good leader are discussed below.

Process Knowledge

The leader should have in-depth knowledge of process technology. However, he or she will not know the unit being examined in detail. Nor need the leader be expert on the specific technology being discussed. (He must, however, be able to read the P&IDs fluently.) Indeed, the leader's background in other industries can help generate some very useful cross-fertilization during the team discussions.

Stimulate Thinking

Often one of the leader's biggest challenges is to get the team members to accept that serious accidents can happen. This acceptance can be a particular problem in those facilities which have a good safety record. Indeed, the most difficult analyses for a leader can be those where standards are high and the team members consistently exhibit a high level of professionalism. In such cases, the leader can have a hard time persuading the team members that risk never is zero, and serious accidents can happen anywhere and in any place. These team members can have trouble "thinking the unthinkable." They will make statements such as "I've been here 14 years, and never seen that"—with the unspoken follow-on, "therefore it can't happen."

However, at a facility that has just experienced a serious accident, all personnel readily accept that "it" can happen. Indeed, one of the most effective actions that a corporation can take following a large accident is to have as many employees as possible come from other sites to look at the destruction in order to make them realize that bad events really can occur.

Creative Thinking

One of the leader's most important roles is to generate creative discussions and to stimulate what is sometimes referred to as "helicoptic" thinking, i.e., the ability to rise up above a problem and to see the forest as well as the trees. One way of doing this is by asking "stupid" questions, knowing that these questions will, at times, make him or her look a little foolish. Nevertheless, some of these "stupid" questions may generate a useful discussion, which in turn will encourage other people to think more broadly.

If a leader is having trouble generating a discussion, he or she may challenge the team members and deliberately try to put them on the defensive. Their emotional response may help trigger a useful discussion. Such a conversation may go something as follows:

- Leader: "Could high temperature create a fire?"
- Team Member: "No, there is nothing to worry about."
- Leader: "Really?"—followed by dead silence.
- Team Member: "No, the last time we had high temperature we managed to avoid a fire."
- Leader: "Oh. Could it be that you were just lucky?"

At this point the team members may start to talk about this and other incidents, if only to prove that there is no problem and that the leader is completely wrong. But the leader has, in fact, achieved his goal, which was to start an honest and candid discussion; even he did have to stir up some emotions.

Casual Remarks

The leader should be sensitive to throw-away comments because these can lead to the identification of a hazard. For example, if the team member says that a certain valve "works OK now," the team leader might pick on the word "now" and find out what the source of the original problem was, and whether it could occur again. Sometimes a leader will observe that one of the team members looks uncomfortable, indicating that they may be aware of a problem, but they are not sure. The leader should be sensitive to body language and follow up with the person concerned.

Jokes and laughter can also open up new lines of inquiry because they are often indicative of a deep-seated or endemic problem; it is the truth that lies behind a joke that makes it funny. If a team member makes a laughing comment such as "Management would never pay for this" the leader may want to probe more deeply. He may find, e.g., that previous suggestions have been turned down because they were not properly documented or justified; in which case the issue is not lack of money, but lack of communication.

"If We had Unlimited Money"

The leader can sometimes generate good ideas by asking the team, "What would you do to improve safety if you have unlimited money (and time and skilled people)?" Most team members have trouble accepting such a business environment, but, when they do, they can often come up with some very useful insights.

Generalizations

Effective team leaders develop generalizations from the hazards analysis discussion. For example, the leader may note that many of the identified hazards could be mitigated with better operating procedures. This finding indicates that a general recommendation concerning upgrading procedures may be in order.

When presenting the final report to management, the leader should provide a few succinct generalizations to do with the findings of the analysis. For example, after one lengthy hazards analysis the leader made a 30-minute presentation to management that summarized many of the 46 recommendations (some of which addressed high-risk hazards) under the word "instrumentation." He noted that a large percentage of the identified hazards were attributable to outdated or inadequate instrumentation systems, and suggested that management consider development of a high-level strategy for improving the quality of the plant's instrumentation.

Team Management

The ability to manage and lead a team discussion is a critical ability for a hazards analysis leader. In addition to general meeting management issues such as the use of mobile phones for texting, he or she needs to consider the following:

- Team members who dominate the discussion and also team members who hardly participate.
  It is important to make sure that everyone contributes their thoughts and experience and insights without restricting the input of others. The leader encourages quiet people to talk and talkative people to shut up.
- Some participants can become quite defensive to the point of treating the findings of the analysis as challenges to their professional competence. An effective leader makes it clear to all that the purpose of the hazards analysis is to ensure process safety and operational integrity, not to challenge the proficiency, competence, or professionalism of any person or group of persons.

- The leader should not answer his or her own questions or lead the "witnesses" too strongly. An experienced leader will often identify the major hazards as soon as a P&ID is put on the wall and will quickly foresee what findings will probably be generated. However, it is his or her responsibility to lead the team through the thinking process, and not to pre-empt the discussion by coming up with instant answers. Also the leader must recognize that other team members have their own insights, and must be given time to think, particularly if they are unfamiliar with the hazards analysis process.
- The leader must be particularly sensitive to the rather hesitant comments made by those who are not used to being in meetings, and/or who fear retribution from their bosses for "whistle blowing." The fact that they are speaking at all shows that they have a pressing concern that they wish to share with others. The leader should make every effort to give that person an opportunity to speak. The question "Have we overlooked anything obvious?" may encourage the more reticent team members to be more forthcoming. On one HAZOP, e.g., the leader quickly noted to himself that a certain valve needed to be locked open. Instead of just saying this, however, he had the team work through the thinking process in order to reach the same conclusion. As the team did so, a highly experienced operator, but one who was not used to public speaking, hesitatingly raised an interesting issue: in his facility the term "locked valve" always meant "locked *closed* valve." He was puzzled as to why the team wanted to *close* the valve when it should be *open*. If the leader had jumped straight to the finding, this minor but interesting insight would have been missed. As it was, a second recommendation was generated calling for the standard operating procedures to clearly define what was meant by the phrase "locked valve" and for the Training Department to put everyone through a refresher course on this topic.
- Develop the discussion unhurriedly in order to make sure that the leader has not missed anything or has made unjustified assumptions.

Knowledge of Actual Incidents

In the book *Study in Scarlet* (1887), Dr. Watson enumerates some of Sherlock Holmes' unique characteristics one of which is Knowledge of Sensational Literature—Immense. He appears to know every detail of every horror perpetrated in the century. By studying earlier crimes, Holmes is able to apply the lessons learned to current crimes.

Like Holmes, an effective hazards analysis leader should possess extensive knowledge of actual incidents that are relevant to the process being analyzed, thus allowing him to develop meaningful analogies. Experienced leaders may even use the names of major incidents to summarize the state of a facility. For example, one leader once described a certain facility to another leader as containing "many little Flixboroughs." Those three words told the second leader that MOC was a problem at the location in question. Knowledge of actual incidents can also help the leader illustrate potential problems to team members who are suffering from the "but it couldn't happen here" syndrome.

One danger associated with having a lot of knowledge and experience to do with actual events is that discussions can degenerate into an almost endless sequence of rather boring war stories. Anyone calling on experience of actual events must be sure that they are not just trying to make themselves look good; appropriate lessons and generalizations must be derived from the anecdotes.

Lawyer-like Behavior

In many ways, a good hazards analysis team leader has the characteristics of a trial attorney. He or she asks probing questions, and always works to throw the "witness" (the team member who is speaking) a little off balance thus generating fresh insights and new ways of thought. This behavior means that the team leader is not always a "nice guy." (However, unlike the attorney, the team leader is seeking to find positive insights, not to merely affix blame.)

Occasionally, a leader may choose to explicitly cross-examine one of the members of the team, particularly if there has been an incident, the follow-up to which may not have been adequate. However, the leader must be careful not to be too tough on those who are unused to having their thought processes challenged; the purpose of a hazards analysis is to identify hazards, not to put down people.

Persona

The leader does far more than merely call out the guidewords and organize the team logistics. He or she must set the tone of the hazards analysis through behavior and style. Indeed, the leader should think through the approach that to be selected before the hazards analysis starts.

For example, if the hazards analysis is on the critical path of a project or is part of an urgent MOC review, the hazards analysis team may be under pressure to move quickly, and not to make any substantial changes to the scope of work. In such cases, the leader may have to play the "heavy," making it clear to management that the hazards analysis is going to be conducted professionally, that no corners will be cut, and that the creation of findings will not be influenced by budgetary or scheduling issues.

In general, the leader will often find it to be most effective to be sympathetic with working people who are unused to the hazards analysis process, while at the same time being much more assertive with senior managers.

Personal Preparation

The team leader should spend as much time as needed getting ready for the PHA. Before the team meetings actually start, he or she must have learned the process technology, studied the P&IDs, read recent incident reports, and made sure that the software is ready to go.

If the leader comes from an outside organization, the preparation time may not be billable. Even so, he or she must prepare in order to be fully up to speed on the first day of the analysis meeting.

Engineering Standards

A PHA team contains people who are expert in the process for which they are responsible, but it is unlikely that they will possess specialist knowledge to cover each and every topic that may be raised. Even if a team member does have expertise in one or two areas such as vessel design, he or she will not know about other topics such as fire protection, secondary containment, and burner management systems. Therefore, one of the roles that the leader can play is in listing standards that can provide expert guidance to specialist problems.

THE SCRIBE

The scribe records the team discussion, usually using special software on a laptop computer. Generally the scribe is a full member of the team and is expected to participate in the discussions. In many cases, the scribe is fully qualified to lead; hence he and the leader may switch roles every so often. On other occasions, the leader may be forced to accept someone such as a secretary who has lesser technical qualifications.

For short analyses, it may not be necessary to utilize the services of a scribe. For a study lasting less than say half a day, it may make sense for the leader to record the discussion. However, it may not.

OPERATIONS/MAINTENANCE EXPERT

The operations expert is a very important team member. He will know the unit in great detail and will be able to explain "how things really work around here." He will also have knowledge of past incidents, including those that were not necessarily serious enough to be reported within the Incident Investigation process, but which nevertheless can provide useful pointers to the hazards analysis team.

The only drawback to the experience of the operations expert is that they may have trouble thinking broadly. They know the unit so well that they cannot visualize any other type of operation other than what they have seen.

Hazards analysis teams will often include a maintenance expert. The leader must be sensitive to the fact that many of the comments made during a hazards analysis can be interpreted as being a criticism of the ability of the maintenance group to keep the plant running. The people making these comments may not realize that they are causing offense—but whenever they make offhand remarks, such as "Nothing around here works as it used to," the maintenance personnel could take such remarks personally. Yet they are the ones who have probably done a valiant job in keeping the facility running during times of budget cuts and management turmoil.

PROCESS AND INSTRUMENT EXPERTS

The process expert supplies knowledge about the process itself. He or she will often be a chemical engineer. Generally, he is expected to explain how the process works, what the basic chemistry is, and what would be the process impact of identified hazards. Sometimes, the process expert is also the team leader. If this is the case, he or she must make it clear which role they are filling as the discussion progresses.

The instrument expert provides expertise on the instruments, the cause and effect charts, the control systems, and the safety shutdown systems. He or she should be a full-time member of the team.

SPECIALISTS

At times, it is appropriate to call in specialists for limited periods of time. For example, if the team is struggling with some specialized issues to do with corrosion, it may choose to call in a corrosion expert for that part of the hazards analysis. Sometimes, a team will save up its questions to do with a specialized area—say the shipping of samples to the lab—and deal with them all at once when that particular subject matter expert is present.

USE OF SOPHISTICATED LANGUAGE

Hazards analyses often use complex language constructs. A statement such as "If the valve *could* leak, a vapor cloud *would* form, and so we *should* reduce the pressure" is far from easy to understand, especially for those whose first language is not English. Doubtless, all languages could come up with similar examples of complexity and potential ambiguity. If the team members are not fluent in the language being used for the analysis then the quality of the analysis will be degraded if sophisticated wording is used. Yet many hazards analysis teams are international consisting of members from many nations. One HAZOP team, e.g., was made up of participants whose respective native tongues were German, Spanish, and English. It was agreed that English would be the language of record since all the team members spoke English to varying degrees of fluency. However, the leader, recognizing that people need to think and speak in their own languages, established the following rules:

- Any person on the team could declare a "language time-out" like a quarterback in a game of American Football. The leader then declared an official timeout using the official's signal.
- During the course of the timeout (which usually lasted for around 5 minutes), the team members broke into language groups and chatted in their own language about the hazard in question.
- At the end of the timeout, each team reported to the scribe who recorded the insights and concerns of that particular group in English in the HAZOP software.

Ironically, far from detracting from the quality of the analysis, this "language time-out" method actually enhanced the quality of the analysis because it forced everyone to slow down and to think things through. It effectively short circuited the "Oh, come on! That's no big deal—let's get on with it!" attitude sometimes observed in experienced (and bored) analysis teams.

THE ONE-MINUTE ENGINEERING DEPARTMENT

Typically, hazards analysis teams consist primarily of engineers and others with a technical background. By training and instinct, these people have a tendency to want to solve problems, yet they must understand that the purpose of the analysis is to identify hazards, not to come up with solutions; a hazards analysis team is not a one-minute engineering department.

In point of fact, once the meetings are concluded these same people are likely to be the ones who are assigned the task of follow-up. Yet everyone must clearly understand that the role of team member and that of engineering support are different.

Another reason for not having the hazards analysis team develop recommendations is that the mental process for finding hazards is quite different from that for solving problems. When finding hazards, the team is looking for problems and hazards. When generating recommendations, the team is in a constructive, problem-solving mode. The two thought processes can be difficult to integrate in a single meeting.

If the leader can keep a grip on the tendency of the team to want to solve problems, he or she will find that the meeting proceeds quite quickly—which will please everyone, particularly upper management.

RESULTS OF THE ANALYSIS

A hazards analysis generates findings, which are turned into recommendations. Also, during the course of the analysis, the team will generate action items. These terms are discussed below.

FINDINGS

A hazards analysis team generates findings or causes for concern. The team does *not* generate recommendations, as discussed in the previous section to do with the "One-Minute Engineering Department." A finding is what it says it is: the team has found a hazard whose risk level is such that action is required. Someone else, outside the team meeting, will turn the finding into a recommendation.

Sometimes, the steering committee or management may choose to reject a finding. Further research after the team meetings may show that the team did not have all the salient facts in front of them. Or management may simply disagree with the team's judgment. If management does reject a finding, they must fully document why they did so.

Most of those who read a hazards analysis report are interested only in the findings and recommendations. Therefore, it makes sense to ensure that the report associated with each recommendation is as complete and discursive as possible. Once someone has read the recommendations report, he or she will have a complete picture of the issues faced by the team. In practice, it is hard to make a recommendation too detailed.

RECOMMENDATIONS

The findings from the analysis will be assigned by the steering committee to those experts and specialists who are best qualified to handle them. The committee will have to use judgment as to which department should is most appropriate for each finding. For example, a hazard to do with high pressure in a vessel could be handled by operations (new operating procedures), instrument engineering (additional interlocks), or process engineering (eliminate the source of high pressure).

When selecting a recommendation from a variety of solutions, it is important to show how it was chosen, especially if it happened to be the cheapest option. There should never be any indication that safety was traded off against cost, nor that a safety recommendation was not implemented because it was too expensive.

Some recommendations are best handled by outside experts. For example, if the team has found that a certain compressor represents a hazard, the recommendation as to what needs to be done may need to come from the compressor manufacturer. For this reason, care should be taken about giving the hazards analysis team the responsibility for fully resolving recommendations. If it does have that responsibility, then the leader should understand the importance of reaching outside the team for specialist help. Hazards analysis teams are made up of people who are expert on the unit being analyzed, but who are not specialists in specific areas of technology. The team members may simply not have the knowledge to be able to find the right solution, and they will be less efficient than the experts.

It is often found that as many as 10% of the team's findings are hard to defend in the cold light of day in the follow-up to the analysis. Some of the findings may turn out to be based on inaccurate data, others may have been made irrelevant due to subsequent changes in the process conditions, others may be duplicates of previous findings, and yet others may simply not make sense when scrutinized more closely. Management has every right to refuse to act on such findings; however, they must document their decision very clearly, and they must give the team an opportunity to defend the original work.

In spite of the above comments, the hazards analysis team will usually be asked to provide guidance on follow-up and the implementation of solutions. Proposed solutions must reduce the identified risk to an acceptable level, and they should be within the control of the persons involved. Solutions should also be cost effective.

It is important to avoid jumping to "obvious solutions"—all possible recommendations should be considered. For example, the obvious recommendation to do with a reverse flow problem could be to install a check valve. However, it may be possible to change the process to prevent the possibility of reverse flow from taking place. It is also important to side step some of the more common objections to proposed solutions. These include the following:

- That will never work here/that idea is not practical
- We do not have time to do that
- We already tried that, and it didn't work
- It is not our policy
- It is not in our budget
- Use common sense
- Our management would never accept that idea
- That is OK for other industries, but not for ours

ACTION ITEMS

Action Items are generated when the team found that it needed more information before a defensible finding could be issued. Usually action items are assigned to team members during the course of the analysis; they can often be completed quite quickly—say at the next break in the hazards analysis meetings. Action items may be written in the form of a nascent recommendation, i.e., they are a recommendation with a qualifying statement saying that more information is needed before the recommendation is firm.

Action Items may be written in the form of a nascent finding, i.e., they are a finding with a qualifying statement saying that more information is needed before the recommendation is firm.

Table 5.1 shows a representative action item.

Table 5.1 Representative Action Item

#	Action	Node	Assigned To	Discussion	Results
1	Confirm the code requirements for relief valves in V-101 service	2.4	Manuel Harrera	No documentation on this topic was available at the start of the hazards analysis	
2	. . .				

RISK REGISTER

Hazards are generally recorded in the facility's risk register, an example of which is provided in Table 5.2. Handwritten notes should be scanned, and pictures should be digitized.

The development of some of the risk information shown in Table 5.2, such as consequences and likelihood, is discussed in the next chapter. The table also has a Follow-Up section—the management of which is often under the control of the PSM coordinator or someone who is charged with managing the facility's overall risk program.

The rows to do with hazard identification are discussed below.

Finding Number and Date

Each identified risk item is given its own number—often corresponding to a finding from a hazards analysis or from a MOC review.

Hazard

The identified hazard is described in this row. A perennial complaint to do with hazards analysis reports is that they are too cryptic, and that insufficient background material is provided. Therefore, it is important to provide as much detail at this point—people who read and use the register months or even years later will not have any knowledge of the discussion that led up to the creation of the finding.

Table 5.2 Sample Risk Register

Finding	**Notes**
Finding number	
Date of finding	
Hazard	
Source	
Consequences	
Safety	
Environmental	
Health	
Economic	
Likelihood	
Risk Rank	
Follow-up	
Assigned to	
Company	
Department	
Recommendation	
Status	
Resolution	
Date approved	
Approved by	

Source

The register should contain information as to how and where the hazard was identified. Typically this will be a hazards analysis, but the information may come from other sources such as incident investigations or employee observations.

Consequence(s)/Likelihood/Risk

The hazards analysis team spells out the hazard, consequence, and likelihood for each finding. A perennial complaint to do with hazards analysis reports is that they are too cryptic, and that insufficient background material is provided. Therefore, it is important to provide as much detail at this point—people who read and use the risk register months or even years later will not have any knowledge of the discussion that led up to the creation of the finding.

Follow-up

The follow-up section of the risk register describes how the identified hazard was handled, and when the associated recommendation was completed. On a large project, it is necessary to have one person who is assigned the task of making sure that all findings are closed out properly before the new facility is started up. In addition to managing the Risk Register itself, the person in charge of follow-up generally is assigned the broader responsibility of filing all of the hazards analysis reports. Questions that have to be answered in this context include the following:

- How are the hazards analysis records to be managed?
- How are the recommendations and action items to be managed?
- How are the recommendations to be communicated?
- What media are to be used for storing the hazards analysis records?
- How and when are they to be purged?
- Who has access to the hazards analysis records?
- Who can modify the hazards analysis records?

THE HAZARDS ANALYSIS REPORT

All hazards analyses result in a written report.

Probably, the biggest single complaint that clients and management have regarding hazards analyses is that the reports are delivered late (or sometimes not at all). One reason for the delay is that the leader and/or scribe are pulled off on to other urgent projects which are perceived as being more important than getting the report finished, particularly if the analysis did not uncover any major problems. Nevertheless, the client can reasonably expect to have a report on their desk within a day or two of the conclusion of the team meetings. If the team members review the notes and findings during the course of the analysis itself, then the writing of the report itself should not take long. The initial report may be called a draft report, but it should be technically complete; all that is left is editing and checking of the notes.

Unless the analysis is particularly mundane, there will always be a sense of occasion regarding what the team is finding; the hazards analysis will be on center stage. If the final report is issued quickly, it will be reviewed and assessed quickly, and there is a good chance that its findings will receive a high level of attention. However, if the issuance of the report is delayed by more than a few days, the whole subject will go “off the boil,” and people will transfer their attention to other issues.

General guidance to do with report writing is provided in Chapter 20. Some specific issues with regard to a hazards analysis report are discussed below.

COMPLETENESS OF THE NOTES

Every node discussion box should have material entered into it. Blanks are not allowed. If the team did not have anything to say about a certain topic, then words such as “No issues identified” should be inserted into the notes. By doing so, the leader and scribe have stated that all scenarios were considered and that nothing was skipped. The team may have failed to have identified a hazard, but it was not slipshod or remiss in its discussions.

During the notes cleanup stage, the leader and scribe should expand and clarify cryptic sentences so that they become clear when reviewed later. Table 5.3 uses the standard example to provide examples regarding the expansion of cryptic notes.

Some scribes use short-hand terms to help speed up their note taking. The following are examples:

- *NBD*—No big deal
- *OP*—Operational problem only
- *Good*—No issue identified

Table 5.3 Expansion of Notes

Original Note	Expanded Note
Hi inlet press due to block in at S/U	High pressure in the vessel V-101 could be created if V-101 is blocked in when Pumps P-101 A/B are being started up. The dead-head pressure of either pump is greater than V-101’s MAWP (Maximum Allowable Working Pressure) This scenario was considered most likely to occur following a maintenance turnaround because an operator may forget to open the valves from V-101 before turning on the pump Protection is provided by high-pressure interlocks and by the V-101 pressure safety relief valve
Low-level OK but prodctn problem	Both “Low” and “No” level in Vessel V-101 can occur. Although no safety issues were identified, a flow of gas down the liquid line could cause a serious production upset
Hi flow: op err, instr	Causes of high flow from T-100 to V-101 include operating error and/or instrument failure (FCV-101 fails in the closed position on loss of power or of instrument air)
PSV-101 co. stds OK?	The team was concerned that PSV-101, the relief valve on V-101 has been designed to company standards that may not be in compliance with the latest API standards

It goes without saying that such terms should be expanded and explained in the published set of notes.

The team members should check all information for accuracy, particularly documentation supporting the recommendations and findings. It is particularly important to check for silly errors that anyone can spot, and to make sure the written English is spell-checked, and is grammatically and syntactically correct. As one engineer put it "Vice presidents can add up, but they can't multiply."

CROSS-REFERENCE

Even at this early stage in the report writing process, the leader and scribe should be cross-referencing information and findings in order to identify common cause events. For example, if the cause of "high pressure" in two or more vessels is the same, the leader can note this as being a generic issue.

ANONYMITY

While taking the notes, the scribe may link comments and remarks to the names of specific individuals in order to expedite the review process. However, with few exceptions, names should be removed before the notes are published. A hazards analysis is a team effort, one in which participants should be free to say what they think.

Findings Terminology

The leader needs to take particular care regarding his choice of words when a problem of significant risk is identified. In particular, it is important not to place the client management in a position where he or she *must* follow a particular path of action when, in reality, various options are open. Therefore, any statement of the type "Recommend that the following change be made..." should be modified through use of words such as "consider" or "review options for." After all, others may be able to find better ways of addressing a hazard. To reiterate what has been stated already, the purpose of a PHA is to find hazards, not to fix them.

For example, a statement such as "A check valve should be installed in the 6-inch line connecting V-100 to V-101" should be written as "Consider options for preventing reverse flow in the 6-inch line from V-101 to V-100. The PHA team determined the use of a check valve to be a viable option."

Another reason for the team not to develop recommendations is that the mental process for detecting hazards is quite different from the process for solving problems. When finding hazards, the team is creatively looking for trouble. However, when generating recommendations, the team is in a constructive, problem-solving mode. The two thought processes are difficult to integrate in a single meeting.

Given that risk management work is concerned largely with low probability accident scenarios, it can be perceived as being very abstract. The great majority of the recommendations only show their benefit by preventing something from happening that has never happened anyway and probably never will happen. This is not a weakness of the hazards analysis concept, but it can constitute a major communication problem. The writer of the report must try to make low probability events as real as possible.

Completeness

No matter how good a job the scribe may have done in taking notes, the leader and scribe will need to spend some time after the team meetings fleshing out the notes, and adding further information and interpretation to what was written down. They need to do this because what may appear to be obvious and self-explanatory at the time of the meeting may be far from being so when someone who was not on the team reviews the work 2 or 3 years later. It is almost impossible to provide too much information, particularly when explicating findings and recommendations.

The analysis notes themselves can remain in note format, but they should be intelligible.

Nonfindings

Sometimes, teams will not generate findings in situations where findings are expected. In these cases, it is useful if the report can discuss the reasons for the "nonfinding." The report should make it clear that the team did not just ignore or skip the issue; the team did conduct a thorough discussion but was unable to come up with a finding. Similarly, the final report should explain why risk ranking values that appear to be too high or too low are the way they are.

When writing such "nonfindings" down, it is better to say "no problem identified" rather than "no problem" because the second phrase suggests that there are no hazards, whereas the first recognizes that hazards may exist, but this particular team was unable to find them.

Appearance

In the words of the proverb, *You don't get a second chance to make a first impression*. With modern desktop publishing systems, there is little excuse for not turning out a report that is well formatted, clean, and easy to use. Clients expect reports not only to be good but also to look good.

Pictures

The advent of inexpensive, high quality digital cameras has had a dramatic impact on the process safety business. With regard to hazards analysis reports, pictures can help illustrate the findings and issues discussed. If the team was concerned with the high failure rate of a pump seal, e.g., a picture of that seal will help everyone understand what is being described.

Unfortunately, the very clarity of a picture makes some managers nervous. For example, it is one thing to have a written statement "External leaks at valve due to corrosion." It is quite another to print a high quality, color picture of a dirty, corroded, leaking valve. Once more, the report has to balance considerations of accuracy with sensitivity and usefulness.

REPORT DISTRIBUTION

A hazards analysis report is a sensitive document over which management must exert careful control. If the report is being written by an outside consultant, he or she must be particularly careful regarding distribution; otherwise, he is likely to step on a political landmine by sending it to the wrong people or by not sending it to the right people. For this reason, it is suggested that, at the start of the project, the consultant establish a one-point contact with his or her client. This one-point contact will handle all internal document distribution issues.

COMMUNICATION WITH THE PUBLIC

The writer of the report must understand that what is often obvious to the team members and client professionals may be neither obvious nor acceptable to readers or reviewers not familiar with process facilities. For example, a team member may state “We looked at the possibility of a fire and determined that the low probability of the event means that the associated risk does not require further action.” A member of the public may interpret this statement to mean “Fires can happen, and they’re doing nothing about it!”

TABLE OF CONTENTS

An example of a Table of Contents for a representative hazards analysis report is provided in Table 5.4.

1. Disclaimer

The report should start with a disclaimer that outlines the objectives of the hazards analysis and clearly defines the scope of the analysis. The disclaimer should include language to cover the following contingencies:

> No hazards analysis can identify all the hazards; therefore, if an accident occurs as a consequence of a hazard that had not been identified this does not mean that the hazards analysis was a failure or that the analysis had been improperly managed.

Table 5.4 Representative Table of Contents for a Hazards Analysis Report

- Disclaimer
- Executive Summary
  - Major Findings
  - General Conclusions
- Objectives of the Analysis
- Summary of Findings
- Method Used
- Risk Ranking
- The Team
- Regulations and Standards
  - Regulations
  - Standards
  - The Operational Integrity Management Program
- Attachments
  - Attendance Records
  - Drawings
  - Equipment and Instrument Data Sheets
  - References
- Meeting Notes

The focus of the analysis was on the identification of high risk, process-related issues rather than occupational safety concerns.

The quality of the analysis is partially dependent on the quality of data from external sources such as vendors, equipment suppliers, and consultants.

2. Executive Summary

The Executive Summary provides an overview of why the hazards analysis was carried out, how it was performed and what the major findings of the analysis were. Unless there is a serious incident that requires a close reading of the report, the only section that most people will read is the Executive Summary, therefore, it should be written well.

Managers generally want to cut to the chase; specifically they want to know:

- What major issues were identified during the analysis?
- Which of the findings are likely to lead to a costly follow-up?
- Which of the findings could materially delay the project schedule?

Any “show stopper” findings that could result in significant changes to budgets or schedules should be highlighted.

The Executive Summary will also briefly cover the following points to do with the analysis itself.

- The objectives and purpose of the analysis
- The choice of methodology
- The disciplines represented on the hazards analysis team

The final section of the Executive Summary will identify any general conclusions that can be drawn from the study. For example, the report may note that many of the findings were to do with the possibility of spills leading to contaminated groundwater. Therefore, a general finding may be that an overall improvement to the facility’s secondary containment system should be made.

3. Objectives of the Analysis

The reader must be provided with a statement as to why the hazards analysis is being conducted at this particular time. Topics that might be included are the following:

- Regulations
- Corporate standards and programs
- Follow-up to actual incidents
- Follow-up to significant near misses

4. Summary of Findings

This section should list all of the findings that were generated, along with their risk ranking and as much background detail as possible. The need for detail is one reason it is important to write the report quickly. No matter how good the scribe’s notes may be, a lot of information is in peoples’ heads, and this information should be captured as soon as possible. For the same reason, the team members must review the report immediately.

Table 5.5 shows a typical part of a typical findings report; it is cross-referenced to the hazards analysis notes through the node number.

Table 5.5 Example Findings Report

#	Finding	Risk Rank	Node	Discussion
1	Dead-head operation of the Pumps P-101 A/B could lead to a high pressure in V-101, if the relief valve, RV-101, fails to operate	C	2.4	The MAWP for V-101 is 200 psig, and the dead-head pressure of the pump is 280 psig; therefore, while this scenario is not acceptable, it is not likely to cause vessel rupture. Moreover, no evidence exists suggesting that the relief valve is unreliable The team discussed the following possible recommendations: 1. Install a high-pressure interlock on V-101 to shut down Pumps P-101 A/B 2. Develop upgraded procedures and training so that the operators can respond to high pressure in V-101 3. Evaluate the feasibility of upgrading the MAWP of V-101 to 280 psig

The analysis notes should ensure that nonissues are labeled as such. If the team could not find a hazard during a particular discussion, a phrase such as “none identified” should be used, thus showing that consideration was given to this item—it was not just ignored.

5. Method Used

The report should explain which method(s) were used and why. It should make clear that the alternative methods were carefully considered and that the one selected was the most appropriate for the system being analyzed.

6. Risk Ranking

Generally findings will be assigned a risk ranking using a system such as that described in Chapter 1.

7. The Team

The report should highlight the composition of the hazards analysis team and show that the members were properly qualified to participate in the study.

When describing the composition of the team, the leader—particularly if he or she is an outside consultant—should take care when listing job titles in the report. It is all too easy to inadvertently demote or promote someone, thereby creating all kinds of unnecessary ructions. Generally, it is enough just to identify the person’s department, e.g., “Operations” or “Process Engineering,” rather than their actual title. (If a person’s title indicates a specific expertise—Pressure Vessel Engineer, e.g.—it may be worth using it to convey the professional authority of that person.)

Table 5.6 Example of Response to Regulatory Requirements

Regulation	Response
(2) The employer shall use one or more of the following methodologies that are appropriate to determine and evaluate the hazards of the process being analyzed (i) What-If (ii) Checklist (iii) What-If/Checklist (iv) HAZOP Study (v) Failure Mode and Effects Analysis (vi) Fault Tree Analysis (vii) An appropriate equivalent methodology	The hazards analysis team elected to use the HAZOP process for this analysis. Reasons for choosing this method include the following: This was the first hazards analysis conducted on this part of the process, and the HAZOP method is generally regarded as the most thorough of the named techniques, thus making its selection appropriate for this project The process being analyzed involves flows of gases and liquids, thus lending itself well to a HAZOP style of analysis Other sections of the plant have successfully used the HAZOP method, so the technique is well understood by employees and managers and has high credibility

8. Regulations and Standards

If the hazards analysis is being carried out in response to a regulation or corporate standard, it is useful to parse the regulation or standard through use of a two-column table such as Table 5.6. The first column simply quotes the regulation or standard verbatim (in this example, the OSHA PSM hazards analysis regulation is used); the second column shows how those sections were addressed by this particular study.

9. Attachments

Attachments to the report include items such as

- Attendance records
- Drawings
- Cause and effect charts
- Equipment and instrument data sheets
- Documents such as MSDS and operating procedures
- References to previous relevant hazards studies
- Pertinent regulations and industrial standards

10. Meeting Notes

The original hazards analysis notes can be included as an Attachment (most reports do not bother doing this; the notes are simply filed away).

DEVELOPMENT OF THE REPORT

The writing and publishing of the report can be divided into the following six steps:

- Notes cleanup
- Team review

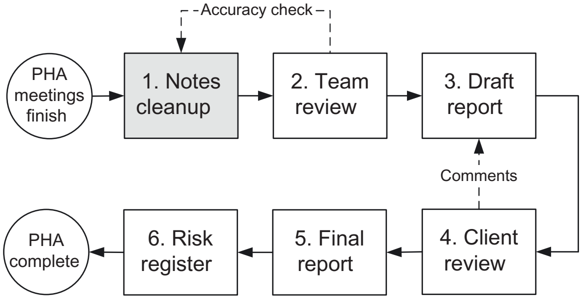


FIGURE 5.5

Reporting process—Step 1.

- Draft report
- Client review
- Final report
- Enter results into the risk register

Step 1. Notes Cleanup

The first step in the development of the report is shown in Figure 5.5.

During the course of the hazards analysis, the scribe will be transcribing the team's discussions on the fly. Only in the rarest of circumstances with the notes be of publishable quality. Therefore, the first step in the report preparation is for the leader and scribe to clarify and expand the notes while their memories are still fresh. This can be done every day or two, rather than waiting for the conclusion of the analysis meetings. The cleaned up notes can be included as an Attachment to the final report.

The leader and scribe should check for the following as a minimum.

Completeness and clarity of the raw notes
Cross-referencing of information
Anonymity of comments

Step 2. Team Review

The next step in the reporting process (Figure 5.6) is for the team members to review the notes and to agree that the notes accurately represent what was said during the analysis. The team members should also review the risk rank levels that were assigned to hazards and that assigned action items are all properly closed out.

It is suggested that the notes be reviewed by the team once a day. A good time for the review is the start of the following day. In other words, after the day's analysis is complete, the leader and scribe will cleanup the notes, and then present them to the team first thing the next day. In order to minimize the amount of paper that is generated (and also to minimize potential legal problems), it is suggested that the notes be projected on a screen using a computer projector and that printed copies will only be issued on an as-needed basis.

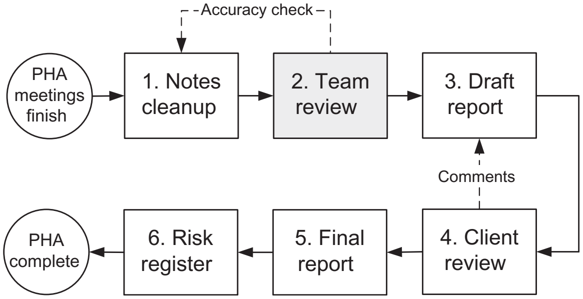


FIGURE 5.6

Reporting process—Step 2.

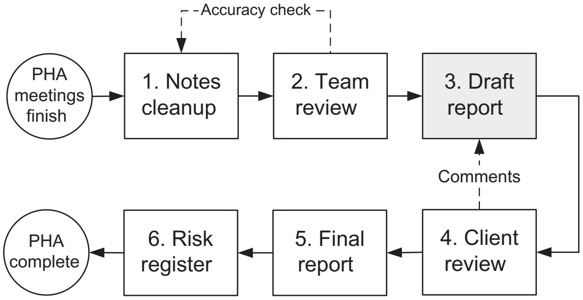


FIGURE 5.7

Reporting process—Step 3.

It is normal for the number of findings to go down by say 10% during the team review process. Some of the issues that seemed so important during the heat of the discussion sometimes turn out to be something of a *non sequitur* or simply incomprehensible when reviewed some time later. Also, findings can sometimes be merged with one another.

Occasionally, the team members may not reach a consensus among themselves. Although this rarely happens, the team leader must be prepared to publish a minority report that provides dissenting opinions. This is the one situation where it is necessary to associate sections of the report with specific names.

Step 3. Draft Report

The third step in the reporting process (Figure 5.7) is to prepare a draft report. As already discussed, it is suggested that the report be issued within 24 hours of the completion of the analysis itself. The draft report should be complete in all essentials; in particular, it must provide an executive summary identifying the major findings and their risk rankings. The draft report must be as complete, accurate, and good looking as possible. Even though the writer makes it clear that the

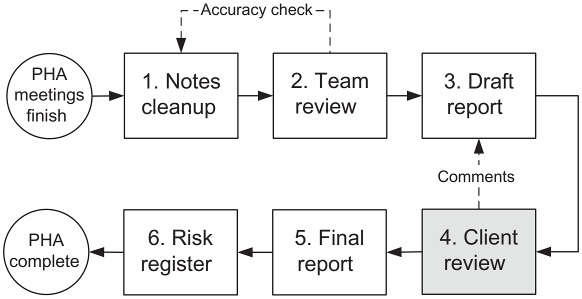


FIGURE 5.8

Reporting process—Step 4.

report is still in the draft phase, most readers will fixate on the first version that they see, and that is all they will remember.

One of the leader's most important tasks is to draw general conclusions from the discussion notes. These conclusions will be included in the draft report as part of the Executive Summary. The following are examples of such conclusions.

- Many of the findings indicated difficulties with operating procedures. A program to write a second generation of procedures would be beneficial.
- The team spent too much time discussing issues that are addressed by pertinent codes and standards. It is suggested that the engineering department provides a summary of these codes and standards to the hazards analysis team at the start of each analysis.
- It was noted that many hazards resulted in a spill to the ground. A program for upgrading all secondary containment in the facility is appropriate.
- Many findings suggested installation of redundant instrumentation. Consideration should be given to the use of Safety Instrumented Systems across the facility.

Step 4. Client Review

The draft report will then be issued to the following groups for comment and review, as shown in Figure 5.8.

- The steering committee or management oversight team.
- Line management of the facility for which the hazards analysis was conducted, or the project manager if the analysis was for a facility in the design stage.
- Technical specialists, who will be expected to validate the findings and to challenge any conclusions that are based on faulty information.
- The legal department.

Figure 5.9 shows a dashed line from the "Client Review" back to the "Draft Report." This indicates that some iteration will be going on at this phase of the report writing process. The client will be asked to ensure that the hazards analysis meets his or her needs, and that the findings and risk rankings are clearly understood.

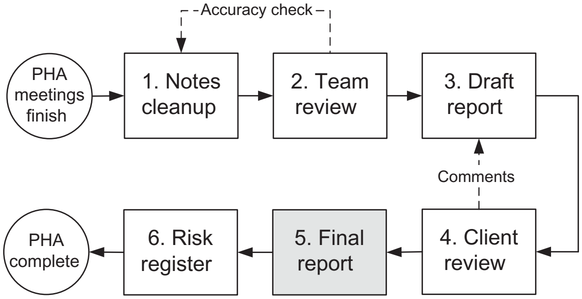


FIGURE 5.9

Reporting process—Step 5.

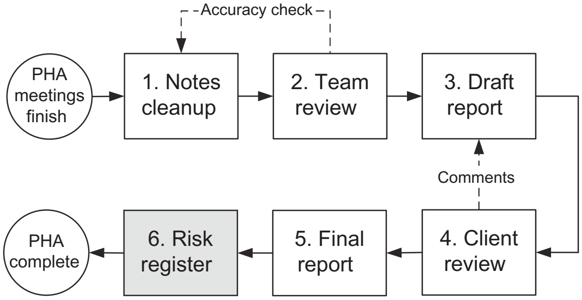


FIGURE 5.10

Reporting process—Step 6.

If the analysis is lengthy—say more than 5 days—the client should be given interim reports, particularly if any of the findings are costly, controversial, or sensitive. The client must never be surprised by the contents of the final report.

Step 5. Final Report

The fifth step in the six-step process is to issue and distribute the final report as shown in Figure 5.9.

Step 6. Risk Register

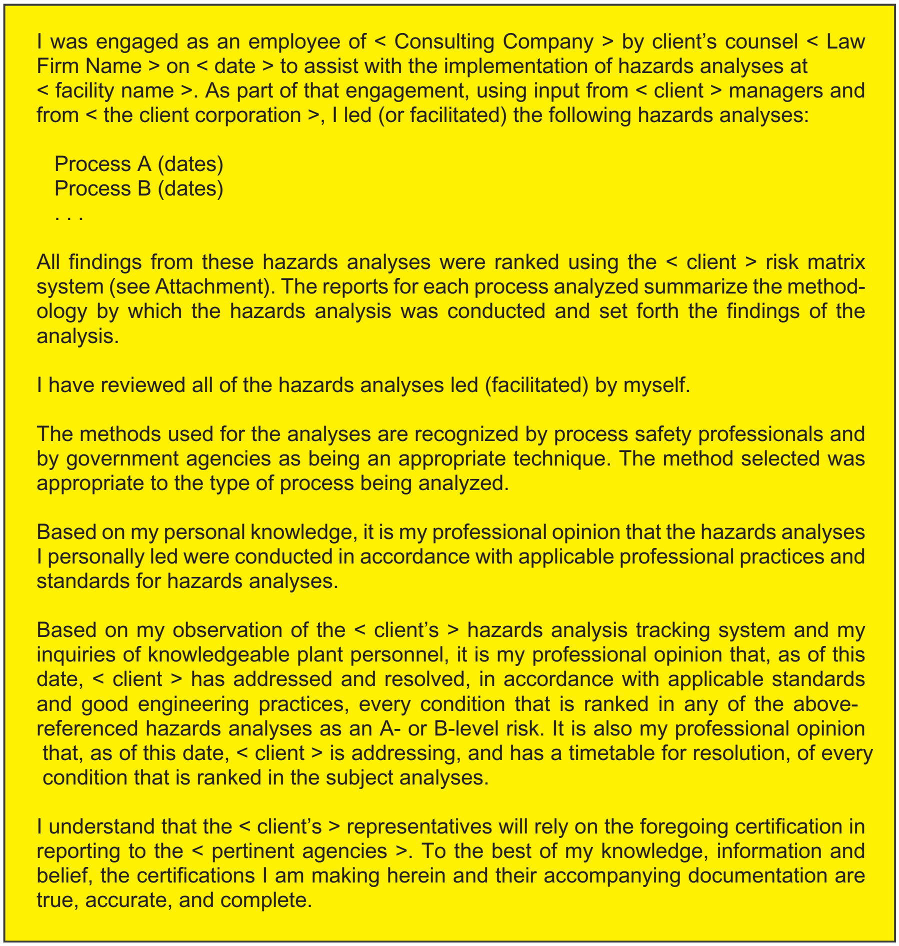
Finally, as shown in Figure 5.10, the findings and associated information will be recorded in the risk register. (The consequences and likelihood sections of the register will be completed once a risk analysis has been carried out, as discussed in the next chapter.)

LEGAL ISSUES

The hazards analysis team, and particularly the leader, must be sensitive to the legal implications of their work. By its very nature, such an analysis creates “smoking guns” and potential liability for the facility management. If a facility does have an accident, the hazards analysis report will most surely be presented as evidence in the follow-up investigations. For this reason, the hazard team leader may be asked to sign a Letter of Certification such as that shown in Figure 5.11. Such a letter creates legal liability on the leader and/or his employer, so it has to be written very carefully, and all statements in it must be verifiable.

In rough order of importance, the three situations most likely to lead to such legal challenges are the following:

> A serious accident involving fatalities, serious injuries, or major economic loss occurring in an area that has been analyzed by a hazards analysis, but in which the hazards analysis failed to identify the accident scenario.



I was engaged as an employee of < Consulting Company > by client's counsel < Law Firm Name > on < date > to assist with the implementation of hazards analyses at < facility name >. As part of that engagement, using input from < client > managers and from < the client corporation >, I led (or facilitated) the following hazards analyses:

Process A (dates)
Process B (dates)
. . .

All findings from these hazards analyses were ranked using the < client > risk matrix system (see Attachment). The reports for each process analyzed summarize the methodology by which the hazards analysis was conducted and set forth the findings of the analysis.

I have reviewed all of the hazards analyses led (facilitated) by myself.

The methods used for the analyses are recognized by process safety professionals and by government agencies as being an appropriate technique. The method selected was appropriate to the type of process being analyzed.

Based on my personal knowledge, it is my professional opinion that the hazards analyses I personally led were conducted in accordance with applicable professional practices and standards for hazards analyses.

Based on my observation of the < client's > hazards analysis tracking system and my inquiries of knowledgeable plant personnel, it is my professional opinion that, as of this date, < client > has addressed and resolved, in accordance with applicable standards and good engineering practices, every condition that is ranked in any of the above-referenced hazards analyses as an A- or B-level risk. It is also my professional opinion that, as of this date, < client > is addressing, and has a timetable for resolution, of every condition that is ranked in the subject analyses.

I understand that the < client's > representatives will rely on the foregoing certification in reporting to the < pertinent agencies >. To the best of my knowledge, information and belief, the certifications I am making herein and their accompanying documentation are true, accurate, and complete.

FIGURE 5.11

Representative letter of certification.

An accident occurring in an area that has been subject to a hazards analysis and for which the analysis generated a finding, but the follow-up was inadequate or tardy. This situation could generate a willful finding from an agency.

The area that has been analyzed is audited by a third party (such as a government agency) who finds major deficiencies in the quality of the analysis or the effectiveness of the follow-up.

The following parties could be involved in the legal follow-up to a hazards analysis:

- The operating company running the plant, including the managers of that company
- The engineering company that designed and built the plant
- The service or consulting company that provided the team leader, if he or she came from outside the client organization
- The team members themselves

Particular attention should be paid to the following issues when conducting a hazards analysis within a legal framework.

Need to Act on Findings

Management must show that they are acting on findings in an orderly and expeditious manner, usually through use of a risk register. It is bad to have an accident, but it is much worse to have an accident caused by a situation that had been identified by a hazards team, but not acted upon.

Informal Notes

During the course of an analysis, it is normal for the team members to make their own informal notes and to mark up their own copies of drawings. These notes could contain comments that are in conflict with the formal report. Therefore it is suggested that, at the time that the final report is being distributed, the scribe should contact each team member to ensure that all informal and personal notes have been discarded. Any conflict between what the notes and the final report say should be resolved. In particular, if a team member expressed a concern that was not adequately addressed, this cleanup phase is a time to take care of such concerns.

Internal Communication

Related to the issue of informal notes are the potential problems associated with internal correspondence that took place during the course of the hazards analysis itself. Informal communications, particularly e-mails, should be written in anticipation that they may one day be used in an inquiry. Even if an e-mail is erased some copy of it is likely to remain in an electronic archive for a long time, and such copies are legally discoverable. Moreover, e-mails can be easily copied and then inadvertently sent to people not on the original distribution list.

If a hazards analysis is ever brought into court, some communications between an attorney and his client can be protected and thus cannot be presented as evidence. Privilege allows clients and attorneys to talk freely with one another. Many nonlawyers believe that simply putting “Privileged and Protected Client/Attorney Communication” on the cover of a letter, e-mail, or report is all that is needed to gain that privilege. Such is not the case. In fact, if the material is communicated with others at any time, the privilege will probably be lost. In general, it is best to assume that all written material is discoverable. As with all legal matters, professional advice should be sought.

	Failure to identify	Inadequate followup	Audit
Preparation		▨	
Conducting the PHA		▨	
Writing the report			
Following up on the findings	▨		

FIGURE 5.12

Defining elements of liability control.

PHA Leadership

The leader of a PHA is charged by his client or employer with conducting a team-based study to identify hazards—particularly those hazards that could lead to a loss of life, serious injury, or major economic loss. This means, therefore, that, should there be a serious incident in an area for which a PHA was conducted, the leader (and possibly the other team members) may be involved in litigation. During the litigation, the PHA leader may find that his professional abilities and judgment are critically challenged. In order of importance, the following three situations are the most likely to lead to such a legal challenge:

- An accident occurs in an area that has been analyzed by a PHA, but the PHA failed to identify the accident scenario.
- An accident occurs in an area that has been subject to a PHA, and the PHA generated a finding, but the follow-up was inadequate or tardy.
- The area that has been analyzed is audited by a third party (such as a government agency), and the auditor finds major deficiencies in the quality of the analysis or the effectiveness of the follow-up.

In order to clarify responsibilities, it is suggested that the PHA leader first clearly define the phases of the PHA, and then spells out what his or her role is in each of these. Typically, there are four major phases:

- PHA preparation
- Conducting the PHA
- Writing the report
- Following up on the findings

In order to properly minimize legal liability, it is useful to cross-reference the two lists shown above, and to identify what needs at each point. This approach is illustrated in Figure 5.12.

SPECIAL TYPES OF HAZARDS ANALYSIS

The previous discussions have been written for a team that is analyzing a full facility. Some analyses are for special circumstances. These include:

- Temporary operations
- Nonprocess applications
- Decommissioning and demolition

Table 5.7 Transportation Hazards Analysis (THA) Guidewords

Traditional Guidewords	THA
High flow	High speed of vehicle
Low/no flow	Vehicle accidentally stops
	Ship hits dock
	Train locomotive loses power
Reverse flow	Truck reverses into a loading dock
	Inadvertent reversing of train
High temperature	Locomotive fire
	Engine room fire
	Truck fire
	Freight car fire
Loss of containment	Derailment of a tank car
	Ship runs aground
	Truck overturns

TEMPORARY AND TRANSIENT OPERATIONS

Many accidents involved some type of temporary operation—usually as part of a maintenance activity or an engineering upgrade. By definition, it is not impossible for the designers of the facility to know what types of temporary operation are likely to be carried out, nor can operational integrity experts anticipate such events ahead of time. Hence, it is vital that each facility have a program for identifying temporary events during the planning stage of an activity, and checking that the temporary operation is safe.

Ostrowski and Keim (2008) discuss the issues to do with conducting HAZOPs during transient operations.

NONPROCESS APPLICATIONS

The discussions to do with hazards analyses that have been provided up to this point in this chapter have been predicated on an assumption that the unit being analyzed is a processing operation—typically a section of a refinery, chemical plant, or oil/gas production facility. However, the techniques that have been discussed can be used, when adapted appropriately, to other types of industrial operation. For example, the deviation guidewords of a HAZOP study (the technique is discussed in the next chapter) can be modified to address transportation issues, as illustrated in Table 5.7. “Reverse Flow,” e.g., becomes “Vehicle, Train, or Ship Reverses.”

DECOMMISSIONING/DEMOLITION

When a plant is decommissioned, it faces two possible destinies. The first is that it will be mothballed so that it can be renovated and restarted when economic conditions improve. The second possibility is that the plant will be torn down and the site and equipment used for something else.

In either case, a hazards analysis should be performed with the What-If technique probably being the preferred method. In the case of the plant that is being mothballed, the analysis will include items such as the following:

- Ensure that rotating equipment is turned on a regular basis
- Check for leaks into and around equipment
- Check electrical and instrument systems for integrity

If the plant is to be demolished, the checklist will focus on items such as the following:

- Hidden pockets of hazardous chemical in the equipment and piping
- Contaminated soil
- Hazardous construction materials such as asbestos insulation

One particular problem regarding the demolition hazards analyses concerns underground piping—particularly out-of-service underground piping. These pipes may not have been considered during normal hazards analyses and other process safety work, but they can be extremely hazardous to the crew charged with removing them, particularly if preliminary investigation indicates that they are filled with a "mystery chemical."

REVALIDATION HAZARDS ANALYSES

The material provided up to this point has been written on the assumption that the hazards analysis is the first to be conducted on the facility being reviewed. However, given that most companies in the process industries started their hazards analysis program in the late 1980s or early 1990s, the majority of facilities have been analyzed at least once.

In principle, once the first hazards analysis has been completed and its findings resolved, all subsequent changes to the process should be handled through the facility's MOC and Prestartup Review programs. If these programs are managed properly, the revalidation hazards analysis should be just a formality because all issues should have been identified at the time a change was made. However it is likely that some hazards will not have been correctly identified or controlled. This being the case, a revalidation hazards analysis is a useful and important activity. Furthermore, the revalidation hazards analysis may uncover issues and hazards that the first team missed, particularly if a different hazards analysis technique is used the second time around.

The leader of the revalidation effort should start by carefully reviewing the original hazards analysis report and notes. An experienced leader will be able to judge the quality of the hazards analysis largely by assessing completeness and insights. The leader should check to make sure that all the guidewords were considered, and that the notes were complete, and that the P&IDs were properly marked up. The leader should then check that the findings and recommendation from the first hazards analysis have been completed and closed out in a professional manner.

Crumpler and Whittle (1996) suggest the following approaches to a revalidation hazards analysis:

- Redo the hazards analysis as if it were the initial one
- Identify limitations or deficiencies in the original hazards analysis, and correct them
- Update the original hazards analysis for process changes only

It is suggested here that a revalidation analysis can follow one of two routes. The first route is for those cases where all changes to the process that have been made since the first analysis have been fully documented, and where those changes have been properly processed through the MOC system. In these cases, the revalidation team can focus on generating fresh insights, possibly through the use of a different technique. For example, if the first analysis was conducted using the HAZOP method, then a subsequent analysis that use say FTA may be more effective than carrying out a second HAZOP. Also in these cases, the team may look at topics that were not considered at all in the original analyses. For example, the original analysis may not have considered human factors in depth; the revalidation provides an opportunity to do so.

The second route for the revalidation analysis covers those cases where the MOC process was not effectively followed, or where the information base has not been kept up to date. In such cases, the team will have to conduct a full hazards analysis in order to ensure that no changes or modifications are overlooked.

In some situations, a middle ground approach may be followed. The original analysis may be thorough but not well documented. In particular, some of the findings and/or risk ranking values may be hard to understand from the original report. In such cases, the revalidation team may choose to revisit those findings, particularly if they are deemed to be critical, in order to provide better documentation, and to establish if they are as important as thought by the original hazards analysis team.

In all cases, the team should consider the effect of changes in other facilities that are linked to the one under analysis. A change in the utility systems, e.g., could create a widespread change in the facility being analyzed. (The interaction between systems is discussed under the topic of IHA.) The team should also be sure that any major incidents that may have occurred since the first analysis are identified, and that the follow-up to those incidents was satisfactory.

BENEFITS AND LIMITATIONS OF HAZARD ANALYSES

The material in this chapter up to this point has assumed that hazards analysis is inherently worthwhile; yet it is useful to examine some of the benefits and limitations of such analyses, if only to provide a sense of proportion as to what might be achieved by them.

STRENGTHS

The strengths of a typical hazards analysis include the following:

- Providing time to think
- Challenging conventional thinking
- Cross-discipline communication
- Education
- Development of technical information
- Economic payoff

Providing Time to Think

One of the greatest benefits of a hazards analysis is that it gives the team members time to break away from their daily assignments and to think through the safety and operability issues to do with the facility that they are operating or designing in a systematic and thorough manner. Providing "mental space" for the team members is why the team leader should make sure that there are no distractions in the form of telephone calls or radio messages. He or she must ensure that the commitment to the hazards analysis is not violated by the demands of "real work." The team members generally are experts in the unit being discussed, hence there is constant pressure to take them off the hazards analysis so that they can work on other urgent tasks. Resisting this pressure is one of the most important tasks of the team leader.

Challenging Conventional Thinking

An effective hazards analysis will place the team members in a mental space that they are not used to occupying. The team discussions will create incident scenarios that had not been considered before, and that will challenge the comfort, and even complacency, that is so often felt by people with a lot of experience.

Cross-discipline Communication

One of the most valuable features of hazards analysis is that it brings together people with different skills and backgrounds; this can lead to very fruitful brainstorming. It can also help flush out potentially hazardous assumptions, particularly at departmental interfaces. ("I thought that your department handled that. Oh really, I thought your people were taking care of it.")

Education

A hazards analysis often provides a thorough education in the process itself for the team members. They obtain an excellent overall picture of the process; and they see how different aspects of the operation—instrumentation, operating strategy, and equipment performance—all fit together.

Even people with years of experience on the facility being analyzed are often surprised to find that they learn a considerable amount about their process, particularly with regard to the original design decisions and the roles of other departments. In particular, maintenance workers often get to understand the process as a process—often for the first time.

Development of Technical Information

Another important side benefit of the hazards analysis process is that it puts management's feet to the fire with respect to developing up-to-date technical and process information. In particular, it ensures that the time and effort is spent on making sure that the P&IDs and other drawings do indeed reflect the "as-built" condition of the unit.

During the course of the hazards analysis, the team may generate empirical information that can be fed back to the technical department, particularly with respect to safe upper and lower limits.

Economic Payoff

Although the normal reason for carrying out a hazards analysis is to improve safety, many companies feel that these analyses provide an economic payback. Unfortunately, such feelings are hard to verify. The problems to do with trying to determine economic payoff are those associated with all kinds of risk–benefit analysis. If a team identifies a high-consequence hazard that has never actually occurred, and then recommends spending money to make its probability much lower, there is no direct financial benefit to the company. It is difficult to justify spending funds on protecting against what has never actually happened. Other benefits such as the improved understanding of the process that the analysis provides the operators and maintenance workers are even harder to quantify.

LIMITATIONS AND CONCERNS

The hazards analysis and risk management techniques that have been described to this point are well established and have been widely used for 20 years or more. Some of the techniques, such as FTA, may not be widely used in the process industries, nevertheless they are well understood and their use presents few difficulties to experienced practitioners. The maturity of these systems and their widespread acceptance means that risk analysis work can be carried out efficiently and effectively. But there is a downside to this maturity: as facilities are repeatedly analyzed fewer and fewer significant findings are generated; the hazards analysis teams find that they are increasingly working over plowed ground. Moreover, it does not appear as if the number of incidents, particularly the number of major incidents, is declining significantly. These two factors—the diminishing returns to do with hazards analyses and the continuing occurrence of major events—suggest that fresh approaches to risk management in the process industries are needed.

The benefits associated with hazards analyses have been described in the previous pages. Some of the limitations and concerns to do with such analyses, and with risk analysis in general, are listed below.

- Imprecision in defining terms
- Multiple contingencies
- Complexities and subtle interactions
- Dynamic conditions
- Common cause events
- Knowledge of safe operating limits
- Lack of quantification
- Team quality
- Personal experience
- Boredom
- Confusion with design reviews
- False confidence
- Equipment orientation
- Interfaces
- Human error

The intent of such a list is *not* to suggest that conventional risk analysis work is of little value or that such programs are no longer worth carrying out. However, a review of some of the difficulties may suggest ideas as to how improvements can be made.

The topics listed above are discussed in greater detail below.

Imprecision in Defining Terms

Throughout this book, the importance of defining risk terms correctly is emphasized. Words such as "probability," "risk," and "consequence" have specific meanings. Yet even when risk terms are defined correctly, the words tend to have different meanings to different people and in different contexts. As discussed, the hazard of "Spill from T-101" may mean that just a few drops of RM-12 flowed into a closed drain system, or it may mean that large quantities of the liquid entered an environmentally sensitive wetland area. Nonetheless, many hazards analysis teams will not thoroughly define the term "Spill from T-101" in detail.

Multiple Contingencies

Most hazards analysis teams work on just one hazard at once. Indeed, they will sometimes prohibit discussion to do with multiple contingencies through use of phrases such as "Double contingency doesn't count." Yet the occurrence of multiple events at the same time is a factor in many accidents, particular large events. Most single incident events have already been considered in the design; indeed they are often addressed by codes or standards. For example, the design of a pressure vessel such as V-101 in the worked example will always incorporate standard safeguards such as high-pressure interlocks and pressure relief valves. Such safeguards will have been introduced at the design stage, and the possibility of them being overlooked is negligible. Therefore, the single hazard—"high pressure in the vessel"—is not likely to generate any new insights or findings.

Some hazards analysis methods, particularly FTA, lend themselves to an understanding of multiple contingencies. However, the more commonly used methods, particularly the HAZOP technique, do not do so because it is hard to discuss complex logic in a team environment.

Complexities and Subtle Interactions

Related to the difficulties associated with multiple contingencies are those to do with complexities and subtle interactions.

Hazards analyses are usually team exercises. Interactions between the team members and the different sets of knowledge that each person brings to the meetings are crucial to the success of the outcome. However, teams typically have trouble discussing scenarios that involve issues such as the following:

- Common cause events
- Contingent events, in which one failure triggers a second failure, and so on
- Failures of utility systems

When hazards analysis teams have trouble analyzing the complex systems, the leader should consider opting for a technique such as FTA that uses rigorous logic and that can deal with intricate interactions of systems.

It is a platitude to say that major incidents are not the fault of a single individual. Modern complex systems fail in complex ways, usually requiring multiple simultaneous failures. Single failures are almost always understood, and safeguards will be in place. However, many real accidents actually involved multiple failures, occurring either at the same time or in sequence. These complex systems are likely to contain connections and subtle interactions that are not always apparent, at least until after an incident has occurred. Such undetected interactions are, in effect, common cause events that have either not been identified or for which no precautions have been taken.

In addition, most industrial facilities operate within a larger system of industrial plants—some of which are operated by the same company, and others of which are owned and operated by other companies. Increasingly companies are developing a better and better understanding of the hazards and risks that exist within their own processes, and are taking the appropriate corrective actions. However, these facilities may not fully understand the nature of the hazards that exist at the interfaces with other facilities and organizations.

Dynamic Conditions

Just as it is difficult for a team to discuss complex interactions, so it is tricky for the team to handle dynamic conditions, i.e., conditions that change over time.

Knowledge of Safe Operating Limits

The topic of safe operating limits is discussed in Chapter 4. In spite of their importance, these limits are often not known, particularly those limits that affect critical safety parameters because the act of finding out the safe limit would itself create a hazard. For example, it would be irresponsible for management to authorize a test on a commercial facility to find out at what temperature an exothermic chemical reaction starts to run away, with the possibility of a ruined catalyst bed, and even an explosion.

Lack of knowledge to do with safe operating limits leads to the problem of circularity in which hazards are defined self-referentially. For example, a team may be discussing the guide phrase, "High Pressure." Implicit in the discussion is often the following train of thought:

- Could "High Pressure" cause an accident?
- What is "High Pressure?"
- "High Pressure" is that pressure that could cause an accident.

The only way to break this circle is to define the word "High" quantitatively. Then the phrase "High Pressure" is replaced by a specific number such as 21 barg. This is the reason why it is so important to define safe upper and lower limit values for key variables before the discussion starts.

Lack of Quantification

Quantification, particularly the use of the Pareto Principle (see Chapter 15), helps get around many of the "I think/you think" discussions that can arise during a hazards analysis. Yet most analyses are not quantified beyond use of a simple risk matrix such as that shown in Chapter 1.

Team Quality

The quality of any hazards analysis depends entirely on the composition of the team and on the capabilities of the team members. The downsizing trends that have become so prevalent have had a double impact on hazards analyses.

First, the need for hazards analyses has increased as fewer people in the organization possess "corporate memory" as to what can go wrong. But, second, because experienced people are fewer in number, the demands on their time from all quarters have dramatically increased, so it is increasingly difficult to get them to schedule blocks of time to participate in the analysis.

Personal Experience

The findings of any hazards analysis depend heavily on the personal experiences of the team members. In particular, people will tend to emphasize those events that they have actually witnessed. However, they tend to downplay events that they have not experienced.

Boredom

All too often hazards analysis meetings are lengthy, tedious, and boring. Boredom is particularly serious for experienced team members, many of whom feel that they have seen it all before, and that they really do not need to go through a full guideword discussion of every point. To a large extent, they are correct in this opinion. The catch is that they may overlook an unusual situation that falls outside their previous experience.

Boredom also induces a pressure to "just get on with it." If one of the purposes of a hazards analysis is to make sure that everyone—including those with a high level of experience—is forced to think the unthinkable, then boredom obviates that intent.

One response to the problem of boredom is to switch from one of the more rigorous methods, such as HAZOP, to a checklist approach. This is probably where the judgment of an experienced hazards analysis facilitator can be very valuable. He or she can decide when the team has enough experience to use one of the quicker methods without losing thoroughness or creativity.

The above comments on the potentially boring nature of a hazards analysis are not merely aesthetic. Only if the discussions are lively and interesting will the team members participate to the fullest extent. No one can maintain enthusiasm over a long period of time unless he or she feels that meaningful results are being obtained.

TRIZ

One means of livening up the analysis is to use the TRIZ approach in which the team considers *how* to cause a problem rather than *what* might go wrong. How this can be done is summarized by Hipple (2008).

1. State the Ideal Final Result (e.g., We want the chemical process to operate safely at all times without injury to personnel or release of chemicals to the environment)
2. Invert this ideal result (e.g., We want the chemical process to operate unsafely at times and occasionally cause injuries and release of hazardous substances)
3. Now comes the key step—exaggerating this inverted ideality statement. (e.g., We don't want this process to *ever* run safely. We want *constant* release of hazardous materials resulting in *mass* injury within the external community, *large* environmental damage, etc.) We want the plant manager to be thrown in jail and the corporation sued for millions of dollars, threatening the survival of the corporation. This extreme exaggeration is the key to forcing participants to think about the absolute worst case and how to cause it. This is not only a key step, but the most difficult. It is analogous to the difficulty of defining an Ideal Final Result in normal TRIZ problem solving. It is important that a strong adjective ("always," "never," "make sure,"

"completely") be part of this statement. If it does not contain such a strong word, it is unlikely that the statement is sufficient.

4. Now we ask, "How would we accomplish this?" "What resources do we need?" "How could we convert existing resources into a negative resource?" In this step, we utilize the comprehensive list of resources developed for TRIZ problem solving: time, space, fields, field conversion, materials, and information.

Confusion with Design Reviews

A problem that faces many hazards analysis teams is that the discussion often slips into being a design review, as distinct for a search for hazards. This problem becomes particularly evident if some of the documentation, especially the P&IDs, are not up to date, or if the team members are seeing the documents for the first time.

Questions that people will typically ask during a design review are:

- Will it work?
- Is it safe?
- Is it operable?
- What is the purpose of this instrument or equipment item?
- Are equipment, piping, and valve sizes correct?

During a hazards analysis, the predominant questions are:

- Could a deviation from design conditions create a hazard?
- What are the safe limits?
- What happens if the equipment or instruments fail?

On one project, a team was asked to attend a 1-day meeting. In the morning, the team conducted a P&ID review; in the afternoon the same team, meeting in the same room, carried out a HAZOP on the same P&IDs (with some marks from the morning's work). Yet the two meetings—the review and the HAZOP—were totally different in style and substance.

False Confidence

Given the investment that management makes in the hazards analysis process, they tend to expect that the hazards analysis team will uncover all hazards. Management sometimes has trouble understanding that the team—no matter how well qualified and no matter how serious their commitment to the hazards analysis—will miss potential hazards. If there is an accident in a unit after the hazards analysis has been performed, and the team did not identify that particular scenario, some people will use this to "prove" that hazards analyses "don't work." The defense that risk management by its very nature deals only in probabilities is seen as being evasive.

A better response to this line of argument is that the number of potential accident scenarios on a facility is very large indeed—so large that no hazards analysis team can spot them all. However, the hazards analysis will identify many of the potential accidents. Furthermore, everyone should understand that the purpose of a hazards analysis is not just to find hazards, but also to create a way of thinking among all employees.

The response that hazards analyses are not intended primarily to find hazards but to create awareness among all employees and contract workers on how to look for hazards all the time is generally too abstract, even if it is true.

Safeguards present another source of false confidence. It is very unlikely that a highly hazardous situation has never been considered at all, hence safeguards will be present. This can lead to a problem because those safeguards may not actually be working as expected. However, because they are not normally used, this type of covert failure may remain in place for many years unless there is a good testing and inspection system. Hence, overall system safety may not be as good as anticipated.

Some safeguard devices are routinely tested. For example, most plants will bench test the set pressures of their relief valves every 2 years, at least. However, even this program has two potential weaknesses. First, the performance of a relief valve depends not only on its set pressure but also on its capacity, i.e., how quickly it can remove vapors once it is open. It is uncommon for relief valve capacity to be checked, in spite of its importance. Second, if the relief valve fails between tests, there is no way of knowing this. (Some safeguards, particularly electronic shutdown systems can test themselves, but mechanical equipment cannot.)

Equipment Orientation

Most hazards analysis teams are composed of persons who have a technical background. As such, they tend to view the plant in terms of equipment rather than people. There is nothing wrong with this, but it is limiting.

For example, an equipment-oriented team might say “The tank overflowed because the level controller failed.” A people-oriented team may say “The tank overflowed because the instrument technician did not service the level controller.” A management-oriented team would say “The tank overflowed because we did not have a good enough training program for our instrument technicians.”

Interfaces

Many hazards exist at the interfaces between interconnected systems. Each system, representing a section of the overall facility, may have been thoroughly analyzed, but no single hazards analysis team is charged with integrating the separate studies into a holistic picture. Interface problems can be particularly troublesome with regard to utilities such as steam, cooling water, and instrument air because such systems run throughout the whole facility. They thus provide a means of transporting upsets and problems from one section to another.

Human Error

Most accidents involve some sort of human error. By its very nature, human error appears to be intractable: it is difficult to predict and will vary from person to person. Nevertheless, a hazards analysis team needs to understand the unpredictable nature of human error, and how such error can impact almost any system.

HAZID/MHS

Many companies and facilities use the term HAZID or Hazard Identification for preliminary studies. Generally, HAZIDs are less formal and thorough than a full HAZOP, and are often conducted during the early stages of a project when it is important to identify major potential problems, without having to go into a lot of detail.

There is no single standard concerning how a HAZID should be conducted; many facilities choose to use a "slimmed down" HAZOP approach, i.e., the analysis is conducted by a multidisciplinary team that uses the deviation guideword approach that was described above. The team focuses on identifying major hazards that could materially affect cost or schedule; the nodes are generally much bigger than in a HAZOP (typically each P&ID represents a node), and only those guidewords that are likely to be relevant are used. For example, the process analyzed during one HAZID did not have any heaters, coolers, or chemical reactions. Therefore the guidewords "High Temperature" and "Low Temperature" were excluded from the discussion (although any team member was free to raise these guidewords if he or she saw fit). As a rule of thumb, a HAZID will take about 20% of the time for a full HAZOP of the same facility.

An MHS or Major Hazards Analysis is a form of HAZID; it provides a preliminary safety review during the early phases of a project and is often conducted using either the What-If or Checklist techniques. An MHS can provide an excellent opportunity for identifying and then eliminating hazards entirely and for making fundamental changes to the process to achieve an inherently safer design. For example, a hazardous catalyst may be replaced with one that is more benign. Or it may be found that some equipment can be entirely eliminated, thus reducing the risk associated with it to zero. The analysis may also note that some critical information, say to do with the flammability of the chemicals being used, is not available.

A key feature of an MHS is that the team looks for consequences before causes (Baybutt, 2003). In a standard analysis, the team first identifies the causes of say high level in T-100 and then identifies the possible consequences for each cause. In an MHS, the opposite approach is used; the team only discusses causes for high level if they believe that these consequences are serious enough to warrant further analysis.

The MHS should be conducted by individuals with a high level of experience both in the way processes operate and in HAZID. The hazards analysis team leader will often find that leading a hazards analysis for a new facility is more difficult than for an existing facility for the following reasons:

- Teams are often quite large, since many groups are involved in the design and construction of the plant.
- During the design analyses, team members may bring to the table many agendas and disputes, some hidden and others open. The leader's job is to make sure that these agendas do not get in the way of finding high-risk hazards.
- If the contract is fixed price, the client may want to "pile on" during the hazards analysis, whereas the design company will want to get the hazards analysis completed as quickly as possible, with a minimal number of design changes. However, if the contract is cost plus, the design company will be glad to add changes to the scope of work, since such changes are often high margin markup items.

- Problems to do with hurting the feelings of the design engineers can be an issue, since the designers are likely to be part of the hazards analysis team. (This is not usually the case with operating plants because the design team will have moved on to other projects.)

THE HAZOP METHOD

The HAZOP method is probably the most widely used hazards analysis method. Even those who are not familiar with the concept of hazards analysis will often have heard of the term HAZOP, even if they are not really sure what it means. For example, when the PSM regulations in the United States were being promulgated in the early 1990s, it was not unknown for a plant manager to say "I know what PSM is, it's HAZOPs!" In fact, the HAZOP method is just one-seventh of one of the fourteen elements of PSM listed in the OSHA standard. These managers were, however, somewhat justified in what they said because they knew that, unless they could identify hazards, they could not reduce risk, and they knew that the HAZOP technique was widely accepted. Furthermore, both regulators and legal advisors generally support use of the HAZOP technique because of its reputation and because it is so thorough. Selection of the HAZOP technique is very defensible if a company is challenged regarding its safety performance, particularly in a legal dispute.

As a result of its widespread use and acceptance, large numbers of people are now trained in the use of the HAZOP method, and many of those are also trained as leaders/facilitators. Furthermore, a HAZOP infrastructure has developed. Many consulting companies offer HAZOP facilitation services; other companies provide special-purpose software.

The basic structure of a HAZOP is to divide the unit to be analyzed into nodes. A node represents a section of the process where a significant process change takes place. For example, a node might cover the transfer of material from one vessel to another through a pump. In this case, the process change is the increase in pressure and flow that occurs across the node. Another node might include an overhead air cooler on a distillation column. Here the temperature and phase are the process variables that change.

Although the strength of the HAZOP method lies in its clear organization, it is important not to allow the analysis to become too rigid. If the team finds that it is talking about "Reverse Flow" even though the current guideword is "High Flow," the leader should probably let the discussion continue. If he or she were to postpone the discussion until the "right" guideword, the current thinking and creativity may be lost. However, the leader must also keep the discussion focused on the issue at hand and should prevent too many digressions.

The steps that the HAZOP team works are as follows:

1. Select a node, define its purpose, and determine the process safe limits
2. Select a process guideword
3. Identify the hazards and their causes using the deviation guidewords
4. Determine how the hazard is "announced," i.e., how the operator knows a safe limit has been exceeded
5. Estimate the consequences of each hazard

6. Identify the safeguards
7. Estimate the frequency of occurrence of the hazard
8. Risk rank the hazard, with and without safeguards
9. Develop findings and potential recommendations
10. Move on to the next process guideword or to the next node if the guideword discussion is complete

STEP 1. NODE SELECTION AND PURPOSE

A node represents a section of a process in which conditions undergo a significant change. For example, a pump system will be a node because liquid pressure is increased, a reactor is a node because chemical composition changes, and a heat exchanger is a node because it causes changes in fluid temperatures.

In practice, a single node will frequently involve more than one process change. For example, the node for a chemical reactor will include changes to pressure, temperature, and composition. The decision as to how big a node may be will depend on the experience of the team, the degree to which similar process systems have already been discussed, the complexity of the process, and the judgment of the leader.

Figure 5.13 shows how the Standard Example can be divided into three nodes. Each node has been circled with a cloud line.

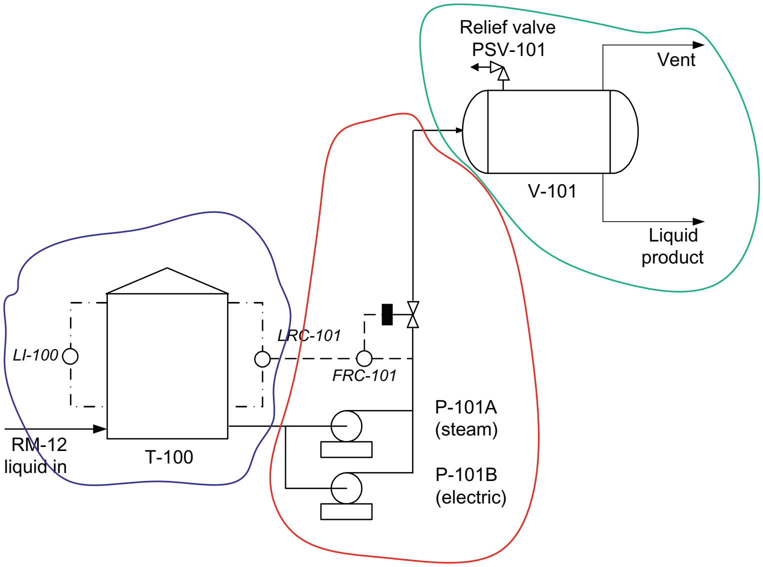


FIGURE 5.13

Example of node selection.

- Node 1 is the Tank, T-100, with its associated equipment and instrumentation (the process change is level in the tank).
- Node 2 includes the two pumps, P-101 A/B, and the flow control valve, FCV-101 (the process changes are flow rate and liquid pressure).
- Node 3 includes the pressure vessel, V-101, with its associated relief valve, and other instrumentation (the process changes are pressure, chemical composition, and level).

Often, node sizes increase as the HAZOP progresses because many of the identified hazards are repeated. For example, if a process includes several sets of similar tank/pump/vessel systems then the team may divide the first discussion into three nodes, as shown, but then treat subsequent systems as single nodes.

Once the team meetings start, the scribe will place a set of full-size P&IDs, with the nodes marked out, on the wall of the conference room (or they will be projected). These master P&IDs will be the focus point for the team discussions and will serve as the official record of the discussions. Team members can also be issued with a set of smaller, or shot-down, P&IDs for personal use.

Most team leaders use highlighter-type pens to define the boundaries of each node. Different colors are used so that the interfaces between the nodes are easily seen. Although the choice of color is not usually significant, some colors may have designated meanings. For example, the color blue may mean that the sections so highlighted were not discussed because they had been covered by a previous HAZOP. The color brown may designate items of equipment and piping that are deliberately being excluded from the current HAZOP discussion. Yellow may indicate that a node has been defined but not yet discussed. At the conclusion of the analysis all nodes should have been colored out, thus confirming that no equipment or piping items were overlooked.

Selection of Nodes

In order to save time, the leader and scribe may preselect the nodes. In a very simple process, this decision may make sense. Generally, however, the team as a whole should decide on the nodes, partly because all hazards analysis decisions are team decisions, and partly because the definition and selection of a node often is affected by the discussions that have taken place with regard to earlier nodes. Also, if the leader and scribe are from outside the local organization, they may not fully understand all the process parameters that could affect node selection.

For each node, the process engineer, and others who have knowledge of the system, will explain to the team the purpose of each node. Table 5.8 provides examples of purpose descriptions.

The scribe will enter the node description into the hazards analysis software. The start and stop points for the node should all be identified, as discussed above. Operations and maintenance experts will then provide some history and operating experience about it. Any relevant documentation to do with that node, such as equipment data sheets or MSDSs, should be put before the team at this time.

All control valves have a fail position. In the event of a power failure and/or loss of instrument air, the valve's spring operator will cause the valve to fail open, fully closed, or remain in its current position. A useful task for the team is to check the fail position of each control valve, and to ask What-If questions as to whether the designers "got it right." An analysis of this type is particularly valuable if more than one accident scenario has to be considered, and if the different scenarios call for different valve positions.

Table 5.8 Node Purpose Descriptions

Node Number	Name	Purpose
1	Tank, T-100, and associated instrumentation	T-100 contains a working inventory of liquid RM-12, which is supplied by tank (rail) cars from outside suppliers. The node does not include the tank loading systems
2	Pumps, P-101 A/B, including flow control valve, FCV-101	P-101 A/B transfer liquid RM-12 from Tank, T-100, to Vessel, V-100. Flow is controlled by FRC-101, whose set point is provided by LRC-100 (Node 1). One pump is operating; the other is on stand-by. A is steam driven; B is electrically driven. B is usually on stand-by
3	Pressure vessel, V-101, including relief valve, PSV-101	Liquid RM-12 flows into this vessel from various sources. V-101 provides surge capacity, thus smoothing out fluctuations in flow. A vent line removes residual quantities of inert gas

Once the node is defined and described, the team discusses deviations from design or operating intent following the steps given in Table 5.8.

Pressure/Spec Breaks

The HAZOP team should check that piping pressure breaks are located correctly (strictly speaking, this is a design function, but it is so important that it behooves the HAZOP team to double check). The general procedure is as follows:

- Ensure that piping is rated for the maximum source of pressure that it can be exposed to, or ensure that appropriately sized relief valves are installed.
- Assume that:
  - Check valves will leak
  - Control valves and block valves will be in the position that will create the maximum pressure possible
  - Relief valves and rupture disks always work
- Trace the line upstream from a relief valve to the near block or control valve (assumed to be closed)
- Check that the pipe system is rated for the relief valve's set pressure

STEP 2. PROCESS GUIDEWORD/SAFE LIMITS

A HAZOP looks at deviations from design or safe process conditions, so the first decision is to select the process parameters that are germane to the facility under discussion. Generally, the following parameters will be used:

- Flow rate
- Flow quantity (for batch operations)

- Pressure
- Temperature
- Level (when vessels and tanks are a part of the node)
- Composition
- Phase

It will often be found that two parameters are related to one another. For example, the deviation of “high temperature” can create “high pressure.” It is not important which of the two parameters is selected by the team as the basis of the ensuing discussion.

The parameters listed above can be supplemented with more specialized parameters, such as viscosity, color, surface tension, and density. These secondary parameters will not generally be needed since they are dependent on the first set. For example, the density of a liquid is likely to be a function of temperature and composition. Therefore, the discussions to do with temperature and composition deviations will incorporate any concerns to do with density.

The safe limit values for each guideword should be established wherever possible.

STEP 3. IDENTIFICATION OF HAZARDS AND THEIR CAUSES

Once the nodes have been defined, and the safe operating limits identified, the hazards are determined. A hazard is a deviation outside the safe operating limit that is identified through the use of deviation guidewords. The most commonly used deviation guidewords are:

- High (more/too much)
- Low (less/too little/not enough)
- No
- Reverse
- Misdirected
- Wrong (other than)

Some teams use the term “Loss of Containment” as a guideword. Given that the ultimate purpose of a process safety program is to make sure that hazardous materials remain confined in the pipes, tanks, and vessels that they are intended to be in, it could be argued that *all* deviation guidewords result in “Loss of Containment,” and so there is no need to handle this term separately. For example, High Temperature in a reactor is not, in and of itself, a hazard; it becomes a hazard only if it generates a pressure so high that containment is lost (exacerbated by weakening of pressure vessel walls at the higher temperature). Similarly, “High Flow” is not usually a hazard except that it may lead to a tank being filled too rapidly, thus generating a “High-Level” scenario, which then can lead to “Loss of Containment” due to overflow of the tank. Another example is “Wrong Composition” in T-101 that can lead to loss of containment if the seal on P-101A fails.

Most of the discussion to do with events and their causes will be associated with the node itself. For example, a leak from a pump may be caused by a seal leak at that pump. However, the team should always be looking for causes from other areas of the plant. For example, if a new chemical is inadvertently introduced into the system at another location, that chemical could cause the seal to leak.

If the consequence of a hazard has an effect on another node, the team leader and scribe should postpone the relevant discussion until that node is reached by the team.

Table 5.9 Hazard Causes

Node	Process Variable	Deviation	Causes
1	Level	High	1. High flow into T-100 2. Failure of the T-100 level control system 3. P-101A and B both stop
		Low	1. Low flow into T-100 2. Failure of the T-100 level control system
	. . .	. . .	. . .
2	Flow	High	1. Failure of level control system in T-100 2. Pump overspeed
		Low/no	1. Failure of level control system in T-100 2. Pump mechanical problems
		Reverse	1. Pump failure (with check valve failure)
	. . .	. . .	. . .

Table 5.10 HAZOP Matrix

	Flow	Pressure	Temperature	Level	Composition	Phase
High	🟨	🟨	🟨	🟨		
Low/no	🟨	🟨	🟨	🟨		
Reverse	🟨					
Misdirected	🟨					
Wrong					🟨	🟨

The actual guideword selected depends on team preference and company tradition. For example, the word “more” is used in traditional HAZOPs to describe an excess of some parameter. However, many teams prefer to use the word “high.” An even better term is “too much” because it implies an undesirable situation—the parameter in question has gone outside its safe limit range. After all, “high flow” is often a good thing because it suggests that the facility is making more product and more money.

Table 5.9 provides potential hazards for two of the variables: level in T-100 and flow from T-100 to V-101.

Some hazards have more than one cause. For example, High Level in T-100 is given in Table 5.10 to have three potential causes:

- High flow into the tank
- Failure of the level control system of the tank
- Pumps P-101 A/B stop

The process and deviation guidewords are organized into a matrix, as shown in Table 5.10. The shaded boxes in this matrix are to be discussed by the team. The empty boxes (such as “Reverse Phase” and “Misdirected Temperature”) are not discussed because they do not have physical meaning.

Table 5.11 HAZOP Steps—Using "High Flow" as an Example

- What is the quantitative definition for "High Flow?" (i.e., what is the Safe Upper Limit for flow in this node?)
- What are the causes of "High Flow?"
- How would an operator know that "High Flow" is occurring? How is this hazard "announced?"
- What are the consequences (safety, environmental, economic) of "High Flow?"
- What safeguards are in place to prevent "High Flow?"
- What is the predicted frequency with which "High Flow" is expected to occur, both with and without safeguards?
- What is the risk associated with the hazard just identified (evaluated from a risk matrix such as Table 5.2)?
- Does the team have any findings or recommendations?

In Table 5.10, the deviations "Low" and "No" are merged since they often lead to essentially the same discussion. However, they should be used separately where appropriate. For example, "Low Level" in a tank may lead to little more than production problems, whereas "No Level" in that tank could create major hazards such as pump cavitation and air ingress into the tank.

The choice of terms can vary according to the practice and culture of the facility. For example, some companies use the terms "As Well As" or "Contamination." These are equivalent to the term "Wrong Composition" in Table 5.10. Sometimes, the guideword combination "Reverse Pressure" is used to cover situations where operating pressures are below ambient.

Having determined which node parameters are to be used, the team discusses the hazards associated with each (shaded) square, using the prompt questions shown in Table 5.11—which uses the term High Flow for illustration.

The team will find that many hazards, causes, and consequences are similar to one another as the discussion moves from node to node.

Teams can sometimes become tangled up when hazards have effects outside the current node. For example, the team may be discussing "Low Level" in Tank, T-100. The cause of low level in the tank may lie within the node itself: a leak through the tank base, for example. However, "Low Level" is more likely to be caused by loss of flow of RM-12 into the tank, i.e., the cause is "Low Flow" in an upstream node. Similarly, deviations in the current node can create hazards in other nodes. "Low Level" in T-100 could lead to seal failure of P-101A, which is in the next node.

STEP 4. "ANNOUNCEMENT" OF THE HAZARD

The team should ask how each deviation outside the safe limits "announces" itself. Usually high and low alarms are built in to the critical variable instrumentation. These alarms tell the operator that an unsafe condition has occurred, or is developing. In the standard example, a high-level alarm incorporated into LRC-100 would warn the operator of high level in T-100.

If the team finds that there is no obvious way for an operator to know that a safe limit has been exceeded, then the hazards analysis will probably recommend the installation of additional instrumentation to provide warnings and alarms.

STEP 5. CONSEQUENCES

Having identified the hazards, the team should then determine the consequences of those hazards, with and without safeguards in place. Consequences can be safety, environmental, or economic.

Table 5.12 Consequences

Node	Process Variable	Value	Consequences
1	Level	High	1. Overflow could cause injury to operator in area 2. Overflow would be contained by secondary containment system—no environmental hazard identified
		Low	1. Possible damage to Pump, P-101, impeller, leading to vibration and leak and personal injury
	. . .	. . .	. . .
2	Flow	High	1. None identified
		Low/no	1. High level in T-100 and/or low level in V-101
		Reverse	1. Overflow of T-100
	. . .	. . .	. . .

Table 5.13 Hazards Analysis Assumptions

- The facility has been designed and engineered properly based on legal requirements, design/engineering codes, industry standards, and good engineering practices
- The process will not be operated above design rates
- All equipment will be well maintained
- Appropriate instrument and control system test procedures will be followed
- Alarm and shutdown set points will not be set out of range or disconnected to avoid nuisance trips or other problems
- Control valve bypasses will not be used unless the control valve is blocked out
- Rupture disks will be monitored
- If a double relief valve system is used, at least one will be in service when the facility is operating
- Relief device bypasses, vents, and drains not normally opened during operation will remain closed
- Pressure safety relief valves will not open except on demand
- Inadvertent opening or closing of locked/car sealed valves or blinds during maintenance
- With all safeguards, particularly those that rely on human performance, it is useful to keep in mind the proverb "Controls corrode faster than steel"

Table 5.12 illustrates some consequences for the standard example using the hazards listed in Table 5.10.

It can be seen from Table 5.13 that the term "None identified" is entered into the notes when the team was unable to think of a significant consequence associated with that hazard. Use of this term assures readers of the final report that the team did discuss potential consequences, but were unable to come up with issues of significance; they did not simply forget to examine this scenario.

STEP 6. IDENTIFICATION OF SAFEGUARDS

The topic of safeguards is discussed on page. Some teams choose to list the safeguard-type assumptions that are made during the analysis. Table 5.13 is an example of such a list.

Table 5.14 Sample Frequencies

Node	Process Variable	Deviation	Frequency without Safeguards (yr^{-1})	Frequency with Safeguards (yr^{-1})
1	Level	High	0.1	0.01
		Low	0.5	0.05
		. . .	. . .	. . .
2	Flow	High	0.05	0.01
		Low/no	1.0	1.0
		Reverse	0.01	0.01
		. . .	. . .	. . .

Table 5.15 Example of Hazard Frequencies

Hazard	Cause #	Consequence #	Frequency #	Risk
1	1.1	1.1	1.1	1.1
	1.2	1.2	1.2	1.2
2	2.1	2.1	2.1	2.1
3	3.1	3.1	3.1	3.1
	3.2	3.2	3.2	3.2
	3.3	3.3	3.3	3.3

STEP 7. PREDICTED FREQUENCY OF OCCURRENCE OF THE HAZARD

Estimated frequency values for each hazard are generally stated in terms of events per year or yr^{-1}. Sometimes they are in units of events per mission or events per batch operation. Table 5.14 provides some estimated frequency values for the hazards in the standard example.

Taking the deviation "High Level" in T-101 as an example, the anticipated frequency of this event is 0.1 yr^{-1} or once in 10 years. If credit is taken for the safeguard (high-level alarm on LRC-101) and the probability of this alarm failing is say 0.1, then the anticipated frequency of high-level drops to 0.01 yr^{-1}, or once in a 100 years.

If a hazard has more than one cause, a frequency for each can be provided in the same way as was done for consequences in Table 5.13. The full hazard/cause/consequence/frequency layout can be structured as shown in Table 5.15.

Hazard #1 could be, say, "High Level in Tank, T-100." The first cause for this hazard (#1.1) is "High Flow into T-100." The consequence associated with this failure is "Overflow of tank leading to operator injury." The predicted frequency of this event, taking credit for safeguards, is once in a 100 years or 0.01 yr^{-1}.

The second cause (#1.2) for Hazard #1 is the failure of LRC-101, the T-100 level control system. In this case, the consequence (#1.2) may be a small spill from the tank that is handled by the drain system, thus avoiding an environmental problem. The predicted frequency for this event (#1.2) is once in 20 years.

Table 5.16 Presentation of Findings

Finding Number	Node	Finding	Risk Rank	Suggested Recommendations	Drawings/Documents

STEP 8. RISK RANK

Once the hazards have been identified, and their causes, consequences, and frequencies discussed, the team should risk rank each identified hazard scenario. If a risk matrix is used then the estimated risk values for the two scenarios are "B" and "C," respectively.

Formal risk ranking can help reduce the number of findings. Hazards analysis teams have a tendency to be conservative and to generate a recommendation for every identified hazard without a great deal of scrutiny. Formalizing the risk helps cut out those recommendations that are really not justifiable.

STEP 9. FINDINGS

Those hazards that have a risk level above the facility's acceptable risk level generate a finding which will then become a recommendation.

Findings and their associated information should be summarized and presented in an overview form as illustrated in Table 5.16. Generally, findings are listed in the order in which they were created. The order in which the findings are listed is not significant in terms of risk level or follow-up priority.

On a long HAZOP, the team may find that certain findings are repeating themselves. For example, it may be that all centrifugal pumps of a certain type have an unusually high rate of seal failure. In such cases, the team should develop generic findings and recommendations.

STEP 10. NEXT PROCESS GUIDEWORD/NODE

Having completed the discussion to do with a process guideword, the team moves on to the next guideword, or to the next node if all of the guidewords have been discussed until the HAZOP is concluded.

EFFECTIVENESS OF HAZOPs

The HAZOP method is probably the most thorough hazards analysis technique, and the one which has the largest number of experienced users and trained leaders. Therefore, it is likely to the method which offers the greatest assurance that major hazards have been identified.

Skelton conducted some studies with different teams of students to compare their different findings. He observed a high level of consistency; in particular, it was unusual for a team to miss a high-consequence vent. One reason for this is that such an event can be identified from multiple keywords. For example, a "High-Pressure" scenario may be missed, but then picked up under the term "High Temperature." The only area where the teams seemed to miss events are what the article refers to as "domino events." For example, an explosion at another unit could send projectiles into the unit under study, thus leading to vessel rupture.

Given that these studies were conducted by students, it is likely that teams composed of personnel with extensive industry experience would be even more reliable in spotting high-consequence hazards. The paper concludes with the following quotation:

> There is no sure way of ensuring that a particular study will identify all significant deviations but, if it is conducted by an experienced leader and a team with a good spread of experience and expertise the probability of identifying all significant deviations and at least 80% of all deviations, other than those caused by the domino effect, is very high.

CHECKLISTS

The Checklist Method uses a set of prewritten questions to stimulate discussion and thinking, often in the form of a What-If discussion. The questions are developed by experts who have conducted many hazards analyses and who have extensive experience to do with the design, operation, and maintenance of process facilities. Checklists are not comprehensive—no hazards analysis method can make that claim. Nevertheless, they should make sure that a complete range questions is asked and that nothing that would be regarded as obvious is overlooked.

The checklist approach is generally part of other hazards analysis techniques. The HAZOP method itself is a form of checklist, and FMEAs use a set of checklist questions.

CHECKLIST CATEGORIES AND GUIDEWORDS

When used on a stand-alone basis, checklist questions are organized into categories, such as those shown in Table 5.17.

Table 5.18 provides a list of checklist guidewords that can be used, particularly in the early design stages of a project.

STRUCTURE OF A CHECKLIST

A checklist generally has two sections as illustrated in Figure 5.14 which is for a "Chemical Storage Checklist."

The top section provides information as to how the checklist is being used. The company, facility, and location are all identified. If some of the information for the checklists answers comes from discussions and interviews with personnel at the site, their names are entered here. The titles of all the documents that were reviewed are also entered in the top section of the checklist.

Table 5.17 Checklist Categories

- Equipment
- Pumps
- Compressors
- Pressure vessels
- Storage tanks
- Piping
- Valves
- Utilities
- Steam (various pressure levels)
- Cooling water
- Refrigerated water
- Process/service water
- Instrument air
- Service air
- Boiler feed water
- Nitrogen
- Other utility gases
- Fuel gas
- Natural gas
- Electrical power
- Pressure relief
- Relief valves
- Rupture disks
- Flare header and flare
- Instruments and controls
- Local instruments
- Board mounted instruments
- Distributed control system (DCS)
- Control loops
- Emergency loops
- Emergency systems
- Fire water
- Firefighting equipment
- External fire
- Runaway reactions
- Human factors
- Operating procedures
- Training
- Chemicals
- Siting

The bottom section of the checklist consists of the questions themselves. The response can be "Yes," "No," or "Not Applicable." Discussions and background information are entered into the Notes column.

THE WHAT-IF METHOD

The What-If method (spelled here in the same way as it is printed in the OSHA PSM regulation, i.e., hyphenated but with the question mark omitted) is the least structured of the hazards analysis techniques. This method also takes the least amount of time.

A What-If analysis is conducted by a team of very experienced analysts, engineers, and operations experts. They are adept at the identification of incident scenarios based on their experience and knowledge. Because it has relatively little structure, the success of a What-If analysis is highly dependent on the knowledge, thinking processes, experience, and attitudes of the individual team members. The method does, however, allow the team members to be creative—the very lack of structure allows them to expand their horizons. Since there is relatively little prompting from formal guidewords, it is vital that the team members prepare very thoroughly before the meetings start; the free-ranging nature of the discussion will require that everyone be up to speed on the process and its general hazards before the meetings start.

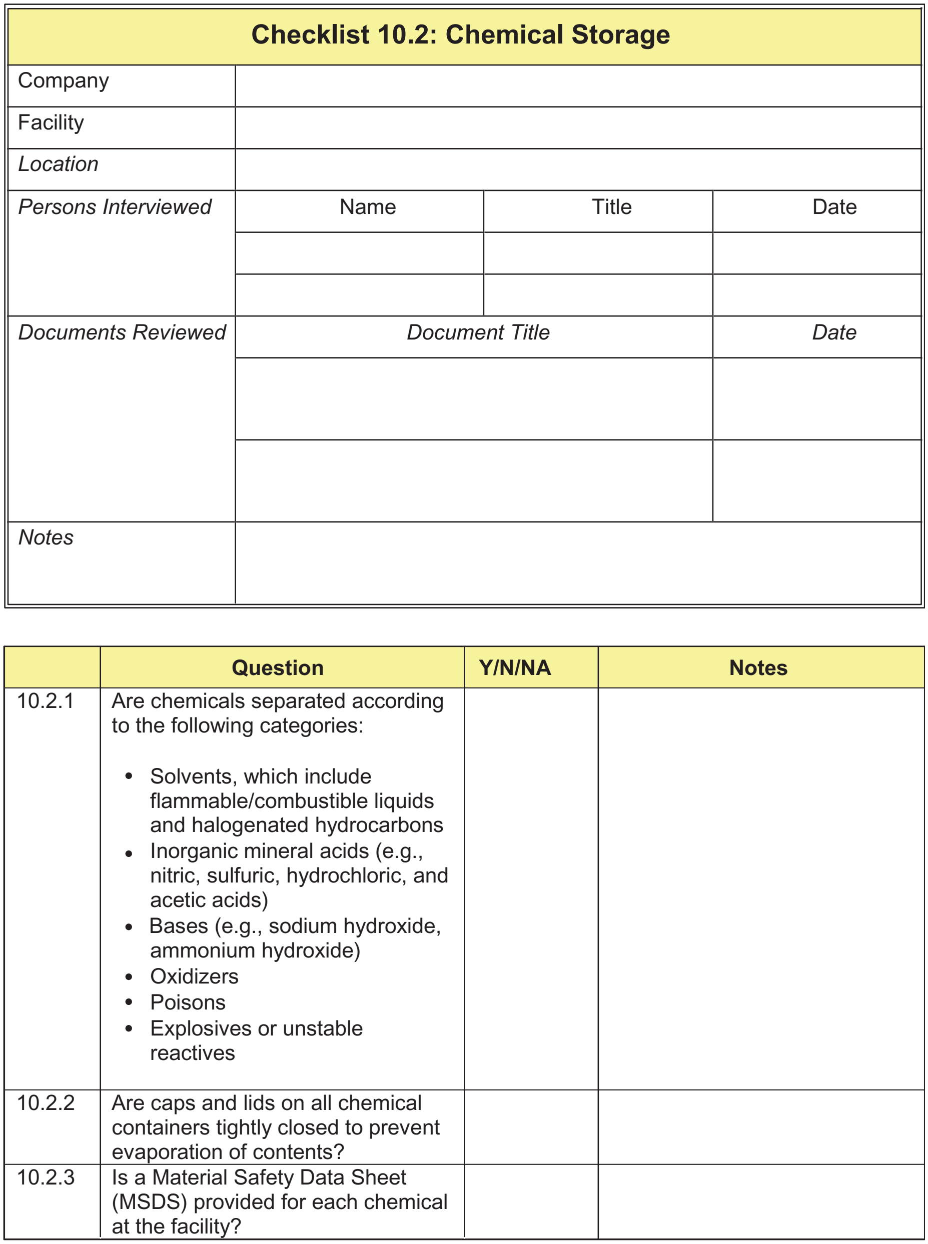
Issues that can be discussed during a What-If review include the following:

- Emergency shutdown systems
- Vents

Table 5.18 Checklist Guidewords

- Standards
- Deviation
- Innovation
- Philosophies (operation, maintenance, safety, relief, venting)
- Materials (hazardous chemicals, radioactive)
- Hazardous areas (for electrical equipment and other ignition sources)
- Emergency (ESD, subsea isolation valve, fire and gas, evacuation)
- Vents
- Flares
- Ventilation
- Effluents
- Drains
- Winterization (lagging, tracing, walkways)
- Noise
- Inventories
- Corrosion
- Low temperature
- Leakage
- Ignition
- Separation
- Safe havens (integrity)
- Control rooms (integrity)
- Buildings
- Explosion
- Collision
- Fire
- Instrument control
- Electrical control
- Utilities (steam, air, nitrogen, water, fuels)
- Machinery
- Mechanical handling (cranes, hoists, forklift trucks)
- Dropped loads
- Interfaces
- Ambient temperature
- Barometric pressure
- Freezing fog
- Chill effects wind
- Prevailing wind
- Tides
- Wave height
- Rainfall
- Flooding
- Earthquake
- Subsidence

- Flares
- Piping systems
- Electrical classification areas
- Truck/rail/ship/barge movements
- Effluents and drains



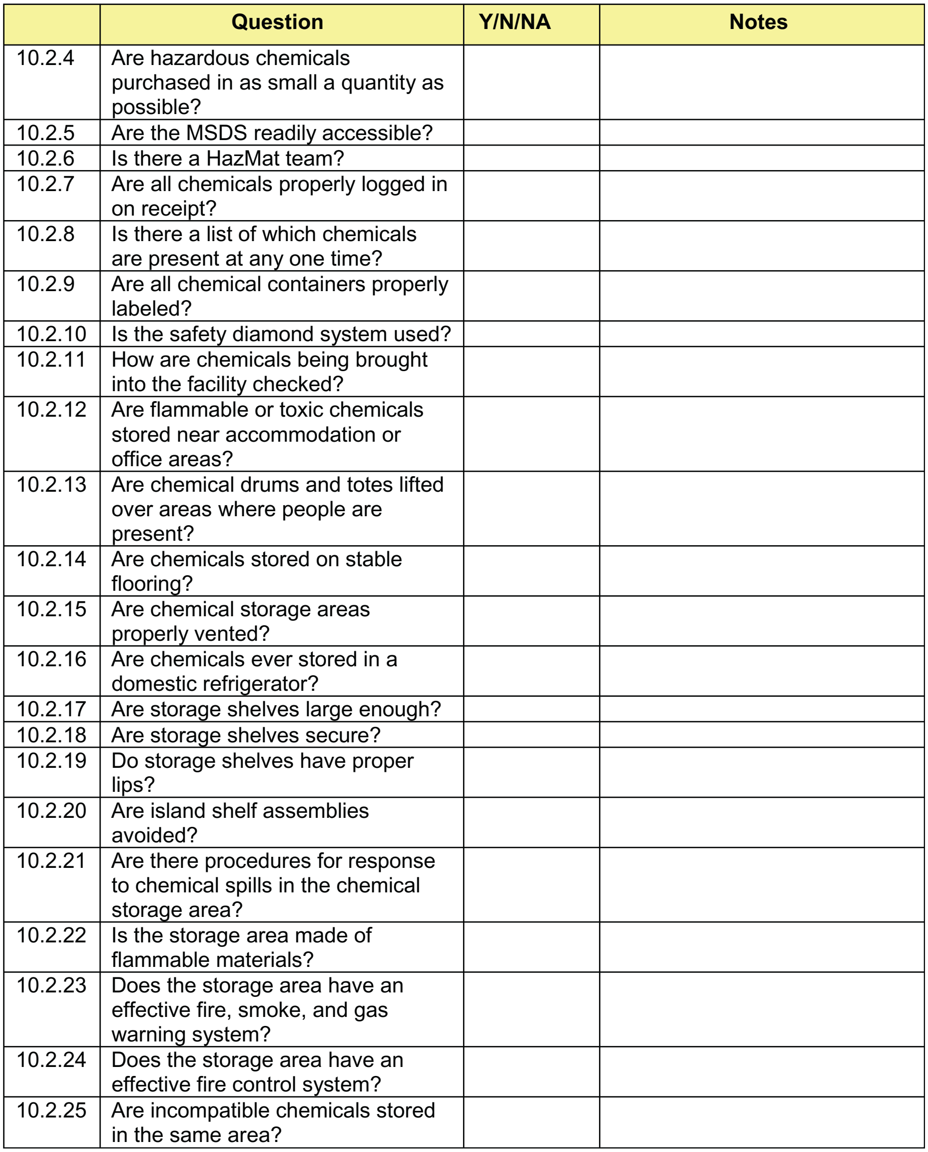
Checklist 10.2: Chemical Storage

Company			
Facility			
Location			
Persons Interviewed	Name	Title	Date
Documents Reviewed	*Document Title*		*Date*
Notes			

	Question	Y/N/NA	Notes
10.2.1	Are chemicals separated according to the following categories: • Solvents, which include flammable/combustible liquids and halogenated hydrocarbons • Inorganic mineral acids (e.g., nitric, sulfuric, hydrochloric, and acetic acids) • Bases (e.g., sodium hydroxide, ammonium hydroxide) • Oxidizers • Poisons • Explosives or unstable reactives		
10.2.2	Are caps and lids on all chemical containers tightly closed to prevent evaporation of contents?		
10.2.3	Is a Material Safety Data Sheet (MSDS) provided for each chemical at the facility?		

FIGURE 5.14

Chemical storage checklist.



	Question	Y/N/NA	Notes
10.2.4	Are hazardous chemicals purchased in as small a quantity as possible?		
10.2.5	Are the MSDS readily accessible?		
10.2.6	Is there a HazMat team?		
10.2.7	Are all chemicals properly logged in on receipt?		
10.2.8	Is there a list of which chemicals are present at any one time?		
10.2.9	Are all chemical containers properly labeled?		
10.2.10	Is the safety diamond system used?		
10.2.11	How are chemicals being brought into the facility checked?		
10.2.12	Are flammable or toxic chemicals stored near accommodation or office areas?		
10.2.13	Are chemical drums and totes lifted over areas where people are present?		
10.2.14	Are chemicals stored on stable flooring?		
10.2.15	Are chemical storage areas properly vented?		
10.2.16	Are chemicals ever stored in a domestic refrigerator?		
10.2.17	Are storage shelves large enough?		
10.2.18	Are storage shelves secure?		
10.2.19	Do storage shelves have proper lips?		
10.2.20	Are island shelf assemblies avoided?		
10.2.21	Are there procedures for response to chemical spills in the chemical storage area?		
10.2.22	Is the storage area made of flammable materials?		
10.2.23	Does the storage area have an effective fire, smoke, and gas warning system?		
10.2.24	Does the storage area have an effective fire control system?		
10.2.25	Are incompatible chemicals stored in the same area?		

FIGURE 5.14

(Continued.)

- Noise
- Leaks
- Operating procedures
- Maintenance procedures
- Machinery, including cranes, hoists, and forklifts
- Public access and perimeter fencing
- Adjacent facilities
- Buried cables
- Overhead cables
- Special weather problems, including freezing, fog, winterization, rain, snow, ice, high tides, and high temperatures
- Toxicity of construction materials
- Demolition safety

A What-If analysis can be organized in one of two ways. The first is to divide the facility into nodes, rather like a HAZOP, except that the nodes are typically bigger and more loosely defined. The second approach is to organize the analysis by major items of equipment rather like an FMEA, and then to discuss the different types of failure mode for each. These two approaches are discussed below. Guidance to do with utilities, batch processes, operating procedures, and equipment layout is also provided.

NODE/FUNCTIONAL AREA REVIEW

Nodal analyses are usually organized around major sections of the process such as a distillation column or a pig launching system. Team members ask questions such as "What-If there is high pressure?" or "What-If the operator forgets to do this?" or "What-If there is an external fire in this area?"

Using this approach, many of the individuals on the team will probably find themselves instinctively following the HAZOP guideword approach. Consequently, a What-If analysis of this type tends to take the form of a faster-than-normal HAZOP. However, the scribe will not need to take notes for every deviation guideword—only meaningful discussions will be recorded. Also, this type of What-If discussion will jump around from node to node more than would be normal in a HAZOP, thus placing greater pressure on the leader and scribe to achieve results and to come to relevant conclusions.

Some What-If questions that can be used for a nodal analysis are listed below.

- What-If the system is bypassed?
- What-If the flow stops?
- What-If there is contamination?
- What-If there is a power failure?
- What-If there is corrosion or erosion?
- What-If there is an external impact?
- What-If the operator fails to pay attention?

- What-If the operator skips a step?
- What-If there is an instrument error?
- What-If an interlock is bypassed?

EQUIPMENT AND FUNCTION REVIEW

In the second approach to a What-If analysis, the hazards analysis discussions are organized around equipment types and their function. Examples of equipment type are listed below.

- Pressure vessels
- Pump fails
- Compressors
- Distillation columns
- Absorbers
- Storage tanks
- Vents
- Flares
- Piping systems
- Heat exchanger fouls
- Internal coil leaks
- What-if a hose or hose fitting leaks?
- What-if a pump seal leaks?
- What-if a rupture disk fails open?
- What-if a valve is left open?

IGNITION SOURCE CONTROLS

- What-if there are errors with regard to electrical classification?
- What-if there are problems with hot work?
- What-if there is a vehicle spark?
- What-if there are electrical grounding problems?
- What-if there is a lightning strike?
- What-if there are problems with continuous bonding?

What-if questions to do with issues such as leaks and overpressure can be asked for each equipment type.

INSTRUMENTATION AND CONTROL SYSTEMS

- What-if the control valve sticks?
- What-if the level indicator fails?
- What-if the instrument malfunctions?
- What-if there is a loss of power to the control systems?

- What-if there is alarm flooding?
- What-if interlocks, trips, and shutdowns fails?
- What-if gas detection for flammables or toxics fail?

HUMAN FACTORS

- What-if there are distractions?
- What-if valves can be confused with one another?
- What-if the operator fails to detect a deviation?
- What-if the operator does not diagnose a problem correctly?
- What-if there is a deviation from an operating procedure?
- What-if there are simultaneous operations?
- What-if there is an incorrect response to an alarm?
- What-if there are communication breakdowns between workers?
- What-if there are communication breakdowns between shifts?

PROCESS UPSETS

The What-If discussion can also revolve around process upsets, such as the following:

- Overfill/overflow
- Inadvertent mixing or reactions
- Interruption of utilities
- Valve in wrong position
- Misdirected flow
- Instrument malfunction
- Contamination
- Reverse flow
- What-if a relief or vent header is overpressured?

SITING

- What-if there is an impact from outside the battery limits?
- What-if there are egress problems?
- What-if there are problems with drainage?

STRUCTURED WHAT-IF

The Structured What-If Approach is considered to be a combination of the What-If and the HAZOP approaches to PHA. It is considered to be applicable to well understood processes and it adds some structure to a What-If without approaching the detail of a HAZOP.

Philley (2011) lists the following strengths and limitations of the technique (Table 5.19).

Table 5.19 Strengths/Limitations of Structured What-If

Strengths	Limitations
Widely applicable	Requires an experienced and capable facilitator
Rapidly identifies major risk and hazards	Team composition and experience are critical
Focus on systems	Can lack sufficient detail
Good screening technique for risks that might need more in-depth analysis	Potential for wasted time if steam strays off scope
Useful for nonsafety issues	

UTILITY SYSTEMS

The analysis of utility systems such as steam headers and instrument air systems can be difficult because it is not always clear where the nodal boundaries are located. A discussion that starts in one area can become very far-reaching and include almost the entire facility.

Utility systems have a large number of connections with the process, any of which could leak. Sometimes the leak will be from the utility into the process; in other cases, the leak will be from the process to the utility. Either way, it can be difficult to detect the source of a problem.

One way of analyzing utility systems is for the team leader and scribe to note potential interface problems as they are discussed during the process analysis. These notes can then be discussed as a group when the utilities themselves are being analyzed.

BATCH PROCESSES

PHA methodologies were developed initially for large, continuous processes such as petrochemical plants and refineries. However, many plants are smaller and operate primarily in a batch mode. Batch plants are often found in the pharmaceuticals and food processing industries. Even processes which are primarily continuous generally have some batch operations, such as truck loading and unloading.

Because batch processes are dynamic (time is a variable) an analysis of their operation is more complex than for a steady-state process. One way of handling this additional complexity is to systematically work through the operating procedures using a What-If approach—in which deviation guidewords serve as prompt questions. For example, if the instruction is, “Add 100 liters of water to V-100,” the team might ask questions such as given below:

- What-if the vessel is over-filled (high level)?
- What-if the liquid is not water (contamination)?
- What-if there is less than 100 liters of water available (low flow)?
- What-If V-100 is overpressured (high pressure)?
- What-If the water is added too soon (high flow)?
- What-If the water is added too late (low flow)?
- What-If the step is omitted altogether (low flow)?

Once the discussion for this step is complete, the team can then analyze the next step in the operating procedures.

Other "step" questions include the following:

- Step done early
- Step done late
- Step omitted

Once the discussion for this step is complete, the team can then analyze the next step in the operating instructions.

OPERATING PROCEDURES

Before conducting a What-If analysis on operating procedures, an experienced technician should mimic the actions specified and make sure that they can be carried out and that they are in the correct sequence.

A What-If analysis of procedures it a team exercise. The team works through each step of the procedure asking a series of What-If questions, including the following:

- What-If the instruction is missed/overlooked/ignored?
- What-If two instructions are done in the wrong order?
- What-If this step is done out-of-sequence (early)?
- What-If this step is done out-of-sequence (late)?
- What-If this step is done too slowly?
- What-If this step is done too quickly?
- What-If the instruction is carried out partially (such as a valve being only partly closed)?
- Does the operator have the information that he or she needs to conduct this step? For example, can all relevant gauges be read?
- Can this step be performed at night?

LAYOUT REVIEWS

When evaluating the risks associated with the layout of equipment issues to consider include the following:

- Ease of escape in the event of a fire or other serious event
- Noise zones
- Vehicle movement
- Accessibility for emergency vehicles
- Dropped objects from cranes and other lifting equipment

A detailed discussion of equipment layout is provided in *Plant Design and Operations*.

WHAT-IF/CHECKLIST METHOD

The What-If/Checklist method is basically a combination of the two methods that have just been discussed. The hazards analysis team works through a checklist. However, instead of merely answering "yes" or "no" to the questions, the team leader generates a relatively unstructured What-If discussions around each of the questions.

FAILURE MODES AND EFFECTS ANALYSIS

One hazards analysis technique used to analyze equipment items is FMEA. The method examines the ways in which an equipment item can fail (its *failure modes*) and examines the *effects* or consequences of such failures. If the criticality of each failure is to be considered, then the method becomes a Failure Modes, Effects and Criticality (FMECA) Analysis. The consequences can be to do with safety, reliability, or environmental performance.

An FMEA is a bottom-up approach to hazards analysis. When linked with a top-down method (such as FTA) a powerful synergy can ensue. The top-down method will highlight those areas which pose the greatest risk; the FMEA can then be used to investigate those areas in greater detail. Like other types of hazards analysis, an FMEA should be carried out by a team. In most cases, however, only two or three team members—who are specialists in the required fields—are involved.

Historically, the FMEA technique has been extensively used in the aerospace, automotive, electronics, and defense industries because they all require analysis of complex mechanical systems and because the failure of an equipment item can have such catastrophic consequences. The FMEA method has not been used much in the process industries because most serious incidents are caused by problems with the chemical and refining processes themselves rather than simple equipment failure. (The same criticism is sometimes made of FTA.) In point of fact, neither the FMEA or FTA methods need take a lot of time it is just that the level of detail that is necessary for the analysis of a say a nuclear reactor or airplane wing is much greater than that needed for a pump in a refinery because the immediate consequences of a failure impact are likely to be so much greater.

The following are components of a typical FMEA:

- Determine the failure modes of the selected equipment item
- Determine the effects of each failure
- Determine the criticality of that failure
- Identify the indications that the failure has occurred
- Estimate the rates (either over time or per mission) for that failure mode
- Identify the failure compensation mechanisms

The causes of equipment failures are not failure modes *per se.* For example, fouling of the tubes of a heat exchanger is not a failure, but it leads to the failure mode of insufficient cooling.

The guidewords in Table 5.20 provide suggestions for general failure modes.

The consequences of failures need to be developed in as much detail as possible. For example, if the failure mode is "Pump fails to run," there is a world of difference between the pump tripping out for a few moments and a complete loss of pumping capability due to massive corrosion of the pump's impeller.

Table 5.20 FMEA Keywords

Rupture	Crack
Leak	Plugged
Failure to open	Failure to close
Failure to stop	Failure to start
Failure to continue	Spurious stop
Spurious start	Loss of function
High pressure	Low pressure
High temperature	Low temperature
Overfilling	Hose bypass
Instrument bypassed	

In general, the FMEA method does not consider the following issues:

- The reason for the occurrence of a particular failure mode
- Time dependency and dynamic conditions
- Human error
- A sequence of events

Table 5.21 provides some failure modes that can be considered for various equipment items.

The FMEA method can be illustrated using the second example to do with the shell and tube heat exchanger. Possible failure modes for the exchanger include the following:

- Tubes fouled on the tube side
- Tubes fouled on the shell side
- Plugged tubesheet
- Shell leaks to the atmosphere
- Cracked tube
- Tubesheet leak

These failure modes generally need to be defined more precisely. For example, a leak to the atmosphere might be a tiny flow of hydrocarbon that poses no danger. However, the leak could result from a catastrophic failure of the heat exchanger shell leading to a major fire.

The FMEA scribe will complete a form such as that shown in Table 5.22, which uses the heat exchanger example. In practice, an actual FMEA form would be considerably more detailed than what is shown in Table 5.22.

BOW TIE ANALYSIS

The bow tie technique is being used increasingly within the process industries not only to analyze risk but also to communicate hazard and risk findings to a broad audience. It can be used not only in hazards analysis but also in incident investigations.

Table 5.21 Failure Modes

- Automated valves
- Fail open
- Fail closed
- Fail late
- Fail erratically
- Partial failure
- Fail present position
- Cyclic operation
- Stem leaks
- Material in body cavity
- False position indication
- Pumps
- Fail to operate
- Fail to stop
- Partial failure
- Wrong impeller size
- Cavitation
- Seal leaks
- Run backwards
- Reverse flow
- Deadheaded
- Starved suction
- Plugged strainers
- Solids
- Water present (often after turnaround)
- Heat exchangers
- No flow on shell side
- No flow on tube side
- Partial flow
- Fouling shell side
- Fouling tube side
- Fouling tubesheet
- Leak shell to tubes
- Leak tubes to shell
- Overpressure
- Temperature measurement
- Wrong material
- Badly welded thermowell
- Incorrect calibration
- Fouled thermowell
- Element partially out of thermowell
- Air leakage into thermowell
- Bad transmitter
- Bad setpoint
- Bad controller
- Incorrect alarm/interlock values
- Manual operation
- Flow measurement
- Wrong material
- Wrong calibration
- Plugged orifice taps
- Wrong-size orifice plate
- Orifice backwards
- Corroded/eroded orifice plate
- Transmitter error
- Wrong scale
- Wrong setpoint
- Drift
- Manual operation
- Alarms
- Wrong setpoint
- Faulty reading
- Operator out of sight/earshot
- Alarm silenced/bypassed
- Level controls
- Stuck float
- Missing float
- Wrong calibration
- Broken sightglass
- Wrong setpoint
- Plugged taps
- Wrong seal leg fluid
- Seal leg fluid in process
- Freezing
- Pressure controls
- Plugged tap
- Wrong setpoint
- Corrosion
- Wrong calibration
- Weight sensors
- Wrong calibration
- Drift
- Wrong scale (English/Metric)
- Distillation towers
- Tray damage
- Tray pluggage
- Missing trays
- Missing internal manways
- Flooding
- Downcomer damage/plugging
- Loss of reflux
- Corrosion
- Leaks in
- Leaks out
- Overpressure
- Loss of condensing
- Loss of feed
- Polymerization

Table 5.21 Failure Modes *Continued*

- Vessels
- Leaks
- Overflow
- Overpressure
- Vacuum
- Flammability of vapor
- Loss of purge
- Compressors
- Deadheading
- Surging
- Solids in feed
- Leaks
- Lube oil leaks in
- Lube oil leaks out
- Overpressure
- Reactors
- Runaway reaction
- Overpressure
- Loss of agitation
- Overtemperature
- Overfilling
- Catalyst high
- Catalyst low

Figure 5.15 shows the structure of a bow tie diagram. It consists of a fault tree (the left-hand side) and an event tree (the right-hand side). (These techniques are described in detail in Chapter 15.) At the center of the diagram is an undesirable Top Event. Using the standard example from Chapter 1 to do with high level in Tank, T-100, the Top Event would be “High Level in T-101 leading to overflow of RM-12.” To the left of the Top Event are threats, i.e., conditions that could cause the Top Event to occur. In the case of high level in T-100, threats will include instrument failure and operating error.

Using the T-100 example once more, the control maybe a high-level switch that shuts off the incoming flow. The “demand” would be a requirement that the switch be activated when the liquid in T-100 reaches a certain level. If this control fails then the likelihood of a tank overflow occurring is increased because this barrier has been overcome.

Returning to Figure 5.15, once the Top Event has occurred, a series of recovery or control steps are in place to reduce or eliminate the consequences. For T-100, one of the consequence of “Tank Overflows” is that toxic RM-12 may enter the drainage system and cause a serious environmental problem. This is “Consequence 1” in Figure 5.15. Two control measures are available. The first is a hazardous drain system that diverts spilled material to a special treating area. If the drain system does not work—say because it is plugged—then a second control is the use of a vacuum truck to suck up the spilled RM-12 before it enters the general drainage system.

INDEXING METHODS

Comparative risk levels can be evaluated using indexing methods. Each design is scored on a variety of factors contributing to overall risk. For example, a design that uses highly toxic chemicals will score negative points, whereas a facility that is located away from populated areas receives positive points. Credit is also provided for the use of control and mitigation measures.

Three commonly used indexing methods are as follows:

1. The Dow Fire and Explosion Index (Dow, 1994)
2. The Dow Chemical Exposure Index (Dow, 1998)
3. The Pipeline Risk Management Index (Muhlbauer, 2003)

Table 5.22 FMEA Analysis of Heat Exchanger

#	Failure Mode	Cause(s)	Indications/ "Announcement"	Predicted Frequency	Consequences	Risk
1	Tube failure	Corrosion from fluids (shell side)	Odors at the cooling tower Hydrocarbon detector on the tower	Frequent—has happened twice in 10 years	Hydrocarbon is at higher pressure than the cooling water. Therefore flammable materials could enter the cooling tower and cause a major fire	A
2	Tubesheet failure	See tube failure. Vibration of the tubes may cause the sheet to fail even if the tubes hold up	See #1	Rare	See #1	B
3	Relief valve fails open	1. Mechanical failure 2. External impact	Hydrocarbons to atmosphere—fire and environmental hazard	Rare	Serious	C
4	Relief valve fails closed	1. Mechanical failure 2. Polymer buildup	None (passive failure)	Uncommon	Critical	B
5	Erosion of tubes	High velocity of cooling water	See tube failure	Rare	Critical—see tube failure	B
6	Vent valve fails open	Mechanical failure	See relief valve fails open	Rare	Serious	C

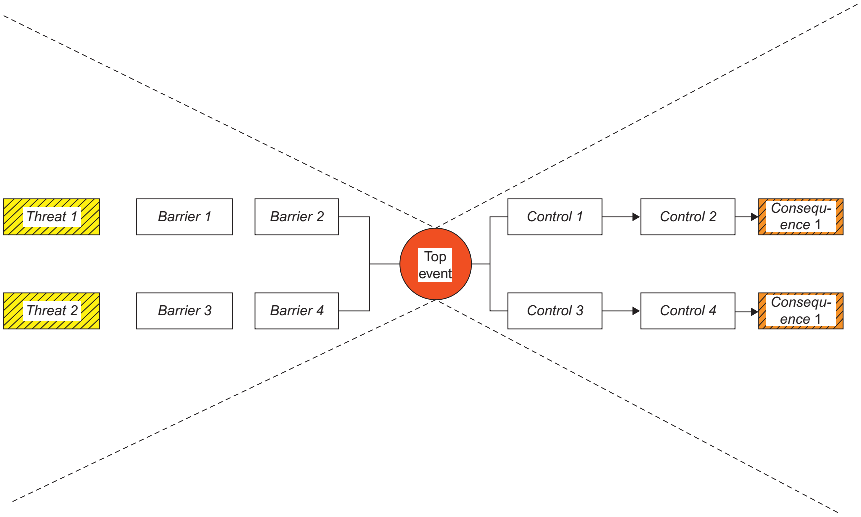


FIGURE 5.15

Bow tie diagram.

INTERFACE HAZARDS ANALYSIS

Most hazards analyses review a subset of a larger system. For example, a refinery hazards analysis team may carry out a hazards analysis on just the catalytic cracking unit, a pipeline company may analyze just the marine loading operations, or an offshore team may analyze just one platform in a larger complex. Yet these subsystems are part of larger systems, which means that hazards can be transferred to or from the other units across the interfaces.

One large oil production facility, e.g., had both onshore and offshore operations. An operator was carrying out a routine pigging operation on a line that came from an offshore platform to the onshore gas processing plant. He inadvertently misaligned the valves around the pig trap and caused a high-pressure surge to flow back along the line coming from offshore. This mishap had no significant effect on the onshore operations themselves, but the pressure surge caused the offshore platform to shut down, which triggered a chain reaction that caused many other offshore platforms in the complex to shut down in sequence. In the end, many millions of dollars of production were lost, and the company was lucky not to have had a safety or environmental incident. Because management and the technical staff had not conducted an IHA, they did not understand the interactions between the different operating units.

Another example of interface operations concerns truck operations. Many process facilities use trucks from third party companies to bring in chemicals and to export products and waste streams. It is generally a good idea to invite a representative of the trucking company to the pertinent PHA. That way each party can assure itself that the chances of a mishap are small. The process facility,

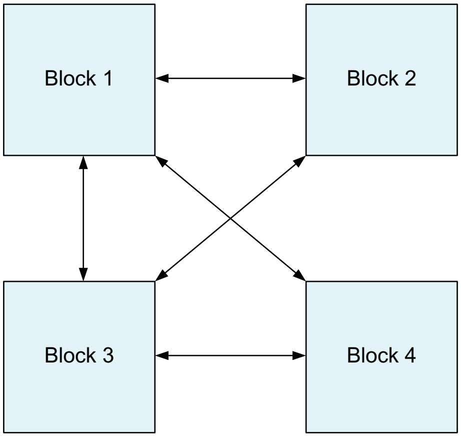


FIGURE 5.16

Interconnectivity.

e.g., can evaluate the procedures to make sure that delivered chemicals are what they should be; the trucking company representative can check for the possibility of reverse flow of process chemicals on to their truck.

An IHA can usually be structured into three areas:

1. Process fluids (wrong hazards analyses/reverse flow/wrong composition)
2. Instrument signals
3. People interfaces

No established methodology exists for analyzing system connectivity—for conducting what is, in effect, an "IHA." However, such a system can be viewed as being a collection of black boxes—where each black box represents an operating unit, each of which has been thoroughly analyzed individually. These black boxes are like nodes in a PHA.

Figure 5.16 shows a system consisting of four operating units, each of which can be connected to each of the others in some manner, except that there is no link between Block 2 and Block 4. (All the arrows are two way meaning that connectivity problems can flow in either direction.)

For a system containing N blocks, the total number of connections is $2 \times 3 \times (N-1)!$ (The number "2" represents the fact that each connection is two way. The number "3" represents that fact that there are three types of connection, as discussed above.) Therefore, in the case of Figure 5.15, the total number of potential interfaces is $2 \times 3 \times 3!$, which is 36. (30 if the missing connection between "2" and "4" is considered.)

One way of conducting an IHA is with the "What-If" approach. A hazards analysis team can use a flowchart of the overall process to ask "What-If" questions such as the following:

- What if the flow in this line is stopped suddenly (a pipeline issue)?
- Can the operators on Unit A shut down any of the equipment on Unit B (an instrumentation issue)?
- What does Unit B do if Unit A has a fire (a human communication and response issue)?

At each interface, the analyst will ask questions such as the following:

- How do we know?
- What is the consequence?
- Are the safeguards adequate?
- What is the effect of an upset on other units?

In the context of offshore operations, an IHA could be structured as follows:

1. Each company—operators, contractors, and vendors—that has anything to do with a rig or platform conducts its own, internal PHA.
2. Representatives from the companies attend a joint Systems Hazards Analysis in which each PHA is treated as a black box.
3. The team leader conducts an IHA. The team works through the dozen elements of SEMS; at each one they ask "What-If" questions to see if they are all in alignment.

Most of the "What-If" questions would be to do with:

- Wrong material
- Reverse flow
- High temperature
- High pressure
- No flow

Examples could include the following:

- In an emergency (Emergency Response and Control) Operator A may call for Valve 100 to be open, whereas Operator B may expect it to be closed.
- Vendor M may be concerned that a particular tote tank will be delivered to the wrong location (Safety and Environmental Information).
- Operator C may have an excellent MOC program, but fail to consider the impact of changes on Contractor D (MOC).

CHAPTER

6 OPERATING PROCEDURES

CHAPTER OUTLINE

Process Risk and Reliability Management. DOI: http://dx.doi.org/10.1016/B978-0-12-801653-4.00006-0

INTRODUCTION

All regulations and rules to do with process risk and safety management require that operating procedures, along with the associated training, be written and followed. No matter how automated operations may become, a human–machine interface will always exist, and that interface will be controlled through the use of procedures and training.

Moreover, many companies are now required either by law or by industry consensus standards to write thorough, up-to-date operating procedures. Typically, these regulations and standards do not provide much detailed guidance on how procedures should be written but they do put managers' feet to the fire—they have to get procedures written and their technicians trained in order to stay in compliance with the rules (and also to minimize potential liability problems).

Figure 6.1, which is taken from National Transportation Safety Board data, shows the dramatic improvement in airline safety over the past 60 years. The ordinate (y axis) shows the number of fatal accidents per million scheduled departures. In the past 50 years the value has dropped from 2.8 to 0.2. (The data from 2000 to 2005 show a leveling out, which is analogous to the occupational safety rate in the process industries shown in Chapter 1.)

Grimes (2008) attributes this impressive trend to four factors, which are as follows:

1. Standardization of procedures
2. Training
3. Behavioral observations
4. Human factors

He states that procedures should be:

- Clear and concise—getting directly to the point and avoiding wordy sentences. Standard operating procedures (SOPs) should be communicated in the fewest possible words, phrases, and paragraphs. In some situations, pictures may help
- Complete—containing all the necessary information to perform the procedure

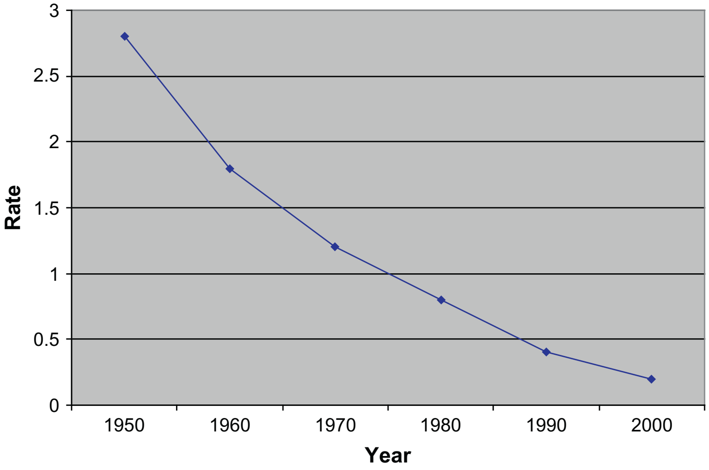


FIGURE 6.1

Airline safety.

- Objective—containing facts, not opinions
- Coherent—showing a logical thought process and sequentially listing all steps necessary to complete the procedure

Not only can high-quality procedures help managers and workers achieve safe and efficient operations, but it is typically found that the process of writing the procedures will itself identify better ways of operating and running the operations that they cover. For example, on a multishift system it is common for the personnel on each shift to develop their own ways of running the unit. Each method of operation may be quite acceptable and safe, and the differences between them may be minor. Nevertheless one method will be, *ipso facto*, superior to the others. The act of writing the procedures can help determine which method to choose.

Properly written procedures also help establish accountability within an organization. The procedures will make it clear as to who is responsible for executing which tasks. The operators and maintenance technicians must understand that operating procedures are *instructions*—they are not suggestions, guidance, or good ideas. Failure to follow written procedures can ultimately be grounds for discipline. This means that, if an operator or maintenance technician believes that an instruction in a procedure is incorrect, then it should be changed *via* the management of change (MOC) system. He or she cannot arbitrarily choose not to follow the procedures—with the possible exception of an emergency situation where quick decision-making may be required. On one facility, e.g., an operator failed to follow a standard procedure regarding locking out a piece of equipment. As a result of his error an incident occurred in which he suffered a serious injury. In spite of the suffering that he endured, he was still required by his management to take time off without pay because he had failed to follow instructions. This management decision may seem harsh, but it was probably just.

However, just as operators and maintenance technicians must follow the procedures, so management is responsible for providing procedures that are clear, succinct, accurate, and easy to use; and then for training the operations and maintenance personnel in their use. Hence, if there is an incident that is attributed to an operator failing to follow procedures, it must first be established that the procedure was actually available; that it was useful, correct, and usable; and that the operator had been properly trained in its application. Only then is it fair to take disciplinary action.

It may be thought that the increased use of automation reduces the need for procedures and training; yet the opposite is usually the case—for three reasons. First, a process that relies on manual operations is likely to be much less complex than one that is automated. Hence, it will be easier for the operators to learn how to run the facility without even needing procedures. Second, when operators are continuously carrying out manual operations, they learn what to do just through experience and repetition—hence procedures are not normally needed. The operators develop a sixth sense as to how to respond to upsets and problems based on their hands-on experience. The third reason for needing procedures on highly automated facilities is that instrument and control systems must be told exactly what to do; they themselves need procedures. Moreover, these procedures must be absolutely thorough and accurate. Whereas human beings are capable of filling in gaps in written procedures with a mix of experience, reasoning, and common sense, instrument systems are totally dumb; they need to have every step explained to them fully and in detail.

In spite of their importance the operating and maintenance procedures in many facilities are inadequate. All too often they are difficult to use, not detailed enough (or too detailed), out of date, and incomplete (or even missing altogether). These difficulties have been observed by the regulatory agencies. For example, up to the year 2009 Operating Procedures were the element of Process Safety Management (PSM) most cited by the Occupational, Safety and Health Administration (OSHA) as part of their National Emphasis Program (Dreux, 2009).

One reason for such deficiencies is that procedures are only rarely actually *needed* to run a facility. Most of the time, the operators and maintenance personnel know what to do and they can figure out how to respond to new circumstances. Consequently, the effort needed to write procedures tends to be given low priority; their development tends to be put off until “we have sufficient time.” Even when good procedures have been prepared, their update and maintenance tends to be of low priority. Hence, they fall out of date, and operators and maintenance technicians lose confidence in them.

Another reason for difficulties with procedures is that their writing, publication, and maintenance is often more difficult, time-consuming and expensive than what the management expects. At first sight, it would appear as if writing procedures, particularly for a facility that is already in operation would be quite simple. All that is needed—it would seem—is to write down how the facility is currently being operated and maintained, and then to format the resulting material using a standard protocol. However, those who actually write procedures find that the task is not so simple. In particular, extracting and organizing information can be surprisingly difficult. Doing so involves reviewing engineering documentation (which may be missing, out of date, or hard to locate), interviewing technicians (who are not always effective at articulately explaining their work and responsibilities), and observing actual operations that can be difficult to follow. Information to do with safe operating limits can be particularly difficult to obtain. Yet it is important to know those limits, particularly when writing troubleshooting and emergency procedures.

Because writing and publishing procedures tends to be more time-consuming and expensive than “it should be”; management often fails to dedicate sufficient resources to the effort.

For example, they may ask an engineer or supervisor to work on the procedures "in your spare time." Such an approach is virtually certain to fail. It is vital that the writing and maintenance of procedures be treated as a full-fledged project that is assigned a budget, a schedule, and a properly qualified team.

Another challenge regarding the writing of procedures for process facilities is that it is often not possible to "test them out." If the procedure is wrong the resulting actions could result in a serious safety or economic incident. Much of the published literature to do with procedures writing is written for the software business. In that environment it is feasible to write procedures, and then test them to "see what happens." If the user really messes up then the worst that happens is that the software has to be reinstalled or backup data used. Such an approach obviously does not make sense when operating a refinery or when drilling a high-pressure gas well. Serious mistakes are not reversible in such circumstances; therefore, the procedures must be correct the first time that they are used.

There are no rules as to how procedures for process facilities should be written. Nor should there be; there cannot be a single "one-size-fits-all" format and style. Different companies have different needs and goals; the procedures should be designed to meet those needs and goals. For example, procedures for batch processes will be different from those for continuous processes, procedures for a food-processing facility will differ from those for petrochemical facilities, and procedures for highly regulated industries will look different from those where there is relatively little regulatory pressure. Moreover, the goals of the procedures will differ from facility to facility within the same industry. Sometimes, their primary purpose is to provide experienced operators with checklists for activities that they already know how to perform very well indeed. In other facilities, the procedures will serve more as a training manual for new employees.

Factors that affect the design and content of the procedures include the following:

- The hazards associated with the chemicals that are handled at the facility
- The experience and knowledge of the workforce
- The complexity of the technology being used
- The degree to which the processes are automated
- Whether the process is a continuous or batch operation
- The regulatory environment

Because there can be no single standard for procedures only, general principles are provided in this chapter; these principles can then be transformed into guidance and rules that are relevant to the needs and requirements of specific facilities and projects. So, e.g., it is suggested in this chapter that a distinction be made between *instructions* and *information*. However, such a division is not a requirement; it is merely a suggestion. What is important is that managers and technicians go through the thinking process as to how procedures and information are to be organized and linked to one another.

Having freedom with regard to the choice of the design and structure of operating procedures does not mean, however, that the people who write those procedures have a license to write any way they choose, regardless of what their colleagues in other units are doing. Each facility needs a standard, which, once established, must be followed by everyone—for two reasons. First, a standardized format helps technicians when they transfer from one area of the facility to another because they will be already familiar with the organization of the procedures.

The second advantage of standardization, and the one that is actually the more important, is that standardization makes the writing process much easier. Instead of having to create instructions from nothing and then write those instructions on to a blank sheet of paper, the writers of the procedures, at least to a certain extent, merely have to follow a prescribed formula, thus reducing potential problems associated with writer's block. Most people find it much easier to "fill in the blanks" than to write creatively on a blank piece of paper. (The avoidance of writer's block is one of the reasons for stressing the usefulness of having a SOPs library. The use of such a library can help create a situation where the procedures writers are doing little more than filling in the blanks.)

Procedures and training are opposite sides of the same coin. Procedures are of no value if the technicians are not trained in their use; equally, it is not possible to train operators and maintenance technicians until the appropriate procedures have been written. Most of the above comments to do with procedures apply equally well to training. In particular, the training program should be consistent and should be oriented toward to the needs and of the technicians.

DEFINITION OF OPERATING PROCEDURES

The definition of operating procedures used in this chapter is as follows:

> Operating procedures are written instructions that, when carried out by the operations personnel, will minimize deviations from design or operating intent.

The key terms used in this definition are discussed below.

OPERATIONS

Operating procedures should be written for operators, supervisors, and line managers. Other users, such as engineers, auditors, and technical experts may use the procedures, but generally their requirements are secondary; the operators are the primary customers of the procedures.

In practice, operating procedures are usually expected to serve different goals. There is nothing inherently wrong with this requirement, as long as the nature of the separate goals is understood and the manual is organized so that they are handled appropriately. The following is a list of some of the varied goals that a manual is often expected to address:

1. Provide brief, checklist-type instructions to operators who are fully trained and who are very familiar with the facility and its operation.
2. Provide detailed instructions for operators who are experienced in general facility operations, but who do not know the particular unit for which the procedures were written.
3. Provide background and reference information, such as Material Safety Data Sheets (MSDSs) and safe operating limit values.
4. Describe what to do in the event of a major emergency.
5. Describe what to do in the event of an environmental upset, including the procedure for contacting the appropriate regulatory agencies.

As well as understanding the profile of the person(s) who will be using the procedures, it is also important to understand the physical and social context in which the manual will be used. For example, operators and maintenance technicians often work outside, where they have to contend with high or low temperatures, wind, rain, and snow. If they work indoors noise and confined space access could be an issue. The operating and maintenance manuals should be written and published in a manner such that it is useful to the operator in his or her workplace.

In many cases, the operator using a manual will not be sitting at a desk with the book directly in front of him; instead he or she will often be at a control panel trying to following instructions from a manual that is placed on a table at some distance, or he may be attempting to read the manual while repairing a piece of machinery. In cases such as these, it makes sense to print the instructions in large type so that they can be read at a distance.

A manual is judged not by its appearance, the quality of its written English, the exactitude of the contents, or the sophistication of the software used to deliver those contents—such attributes are merely factors affecting the ultimate usefulness of a manual; instead, an operating manual is judged by its usefulness to the persons using it. Hence, a shabby, old-fashioned, battered, and coffee-stained manual that is frequently used is better than a slick, colorful, and user-friendly document that stays on the shelf. If the operators choose not to use a manual, then they will not use it; it cannot be forced upon them. Therefore, it is the responsibility of those who are writing and publishing the manual to develop a product that is genuinely useful.

WRITTEN INSTRUCTIONS

Operating procedures must be written down (either on paper or in an electronic file). Sometimes the operators may have a good set of informal, oral procedures that has never been committed to paper. In these situations, the procedures-writing project consists largely of writing down that informal information in a clear and organized manner.

DESIGN OR OPERATING INTENT

Before procedures can be written, management and the operators must clearly define how the facility is to be run; in other words, they must determine the design or operating intent for their unit. In particular, target conditions for all flows, pressures, and temperatures have to be specified, along with the allowable deviations from those target conditions.

Design and operating intent must be quantified. For example, the following instruction (which is somewhat tongue in cheek) is totally qualitative, and so is not of much value to the operator who is expected to follow it.

> Increase the bottoms temperature gradually until the overhead pressure is about normal.

The above instruction can be rewritten more precisely as follows:

- Increase the bottoms temperature by 5°C every 10 minutes as measured by TI-213.
- When the overhead pressure reaches 3.4 barg as measured by PIC-221, stop the temperature increase.

The permissible overhead pressure range is 3.0–4.0 barg. If the pressure deviates outside this range, refer to Instruction XYZ.

The adverb "gradually" in the first text box has been replaced with numerical rate values. The word "normal" has been replaced with a number and a safe range.

In the same vein, terms such as "crack the valve open" are unhelpful because they are nonquantitative. Even a phrase such as "open the valve two turns" could lead to an error were the valve trim to be changed. It would be better for the procedures to read, "Open the valve so that the liquid flow, as measured by FR-203, is in the range 90–100 gpm."

DEFINITION OF MAINTENANCE PROCEDURES

The definition of maintenance procedures used in this chapter is as follows:

Maintenance procedures are written instructions that, when followed by the maintenance personnel, will ensure that equipment operates as designed within safe operating limits.

The above definition follows the same approach as that used for operating procedures. Equipment and facilities must operate in the safe range. Preventive maintenance helps ensure that equipment stays in that range; repair maintenance restores equipment to its normal function.

Many of the techniques described in the previous section can be useful in the preparation of maintenance procedures—however, maintenance tasks are not usually so concerned with a long sequence of activities, and they tend to benefit more from the use of equipment sketches and pictures than do operating procedures.

TERMINOLOGY

A chronic vexation for those who write procedures is the lack of an agreed-upon standard for the meaning of words and phrases such as "manual," "procedure," "task," and "SOP." Different companies, organizations, and operating facilities apply different meanings to such terms.

A set of definitions is provided below in Table 6.1. These definitions are neither official, nor are they universally applied—they merely describe the convention used in this chapter. The manner in which the terms in Table 6.1 fit with one another is shown in Figure 6.2.

Figure 6.2 shows the overall structure for an operating manual. The maintenance procedures are shown as being part of the operating manual structure.

ENGINEERING THE SOLUTION

The purpose of this chapter is to provide guidance and assistance with the writing of procedures that encourage a safe and efficient operation. However, it is very important not to place too much responsibility on the procedures, or on the people who use them. In the words of the proverb, "Red lights don't stop cars—brakes stop cars." No matter how well written a procedure may be,

Table 6.1 Terminology

Term	Explanation
Operating manual	An operating manual provides a complete set of procedures for running a major unit within a facility. For example, the title of an operating manual could be “Operation of the Powerhouse.” Such a manual would contain all the instructions for starting, stopping, and running the Powerhouse—along with the associated troubleshooting and emergency procedures. The operating manual may also contain the associated maintenance procedures. If the procedures are located on the company’s intranet, the “manual” consists of all the web pages to do with that set of procedures.
Operating procedures	An operating procedure consists of a set of instructions for carrying out a specific assignment. In general, a procedure should not contain more than around 20 instructions, and should not be more than two pages long. If it is longer than this, it should generally be broken down into a set of shorter procedures. The following are examples of operating procedures: • Start Pump, P-100. • Check the bearings on Compressor, C-201. • Collect samples for lab analysis. If the operating manual is on a web site, each procedure becomes a page on that site.
Operating task instruction	A task instruction consists of a single sentence describing just one action that is to be carried out. The instruction should start with a verb in the imperative tense. Examples are: • Measure the temperature. • Fill the truck. • Read the logbook. • Report to the supervisor. There should be no more than one instruction per sentence. Hence: • Open the valve, then stop the pump. Should be written as: • Open the valve. • Stop the pump.
Troubleshooting procedures	Troubleshooting procedures help an operator respond to a nonstandard operation that is not an emergency.
Emergency procedures	Emergency procedures describe the actions to be taken when a major event such as a fire has occurred. They are discussed in Chapter 11.
Maintenance procedures	Like an operating procedure, a maintenance procedure is a collection of instructions that describe an overall activity, such as repairing a pump or checking the set point of a relief valve.
Checklists	Operators and maintenance technicians do not usually use procedures on a regular basis, particularly for routine work. However, they will use summary checklists to make sure that nothing was overlooked while carrying out a sequence of tasks.
Standard operating procedures	An SOP describes a generic set of instructions for tasks such as starting pumps, lighting burners, or filling vessels. The SOPs can be used as the foundation of specific procedures. For example, the SOP, “How to start a centrifugal pump” can be used as the basis for the specific procedure, “How to start centrifugal pump, P-100.”

Table 6.1 Terminology ***Continued***

Term	Explanation
	The use of SOPs can greatly improve the quality of the final procedures, and can drastically reduce the development time for the complete manual. Quality is improved because the generic SOP can be very carefully reviewed by all the pertinent disciplines (operations, process, electrical, and maintenance) to ensure that it represents the very best understanding of how to perform this particular task. Development time for equipment-specific procedures is reduced because the persons writing them only have to edit a "go-by"; they do not have to start from scratch.
Job safe practices	JSPs are similar to SOPs except that they are more oriented toward the means by which maintenance tasks can be carried out safely. JSPs are often associated with the interface between operations and maintenance. Typical JSP titles are: • Use of torque wrenches • Operation of portable air movers • Opening hydraulically operated valves

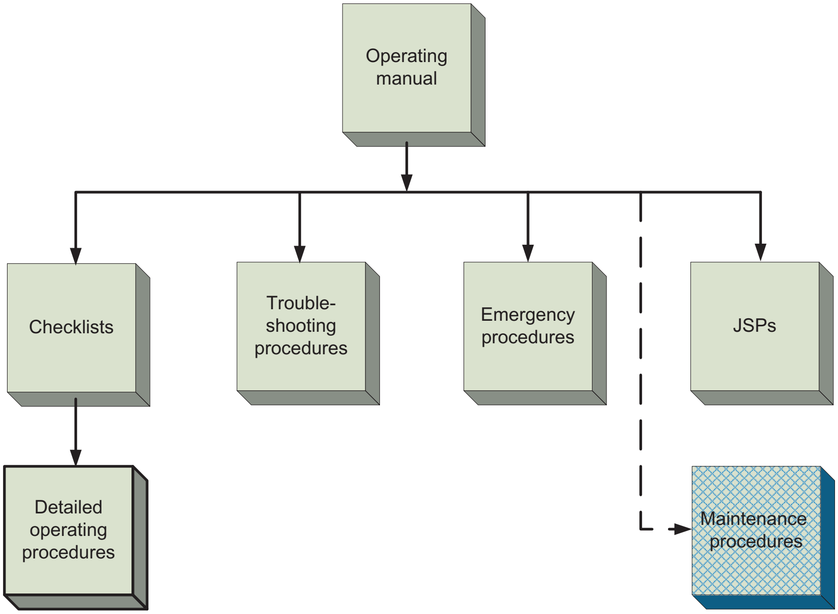


FIGURE 6.2

Structure of an operating manual.

and no matter how well trained the operator or maintenance technician may be, the chance of a slip or mistake will always exist. In particular, any procedure that requires a Danger or Warning notice is likely to be inherently too risky—the system itself should be reengineered.

The first step in the procedures/training program is simply to determine whether the tasks that they covered can reasonably be executed by an operator in a safe and efficient manner. If not then the system itself needs to be made inherently safer or more operable. Generally, the best way of improving operability and safety is to engineer the problem away.

On one facility, e.g., a certain process used both sodium hydroxide solution and sulfuric acid. As is well known, the inadvertent mixing of these two substances can create a violent and dangerous chemical reaction. The chemicals were stored in tanks as shown in Figure 6.3. The tanks were filled by trucks that used hoses connected to fill nozzles. (There were many other pipes in the area, so the situation was actually considerably more complex than what is shown in the sketch.)

A set of procedures was written to guide the operators and truck drivers through the connection, filling, and disconnection steps. In addition, warning signs were posted to make sure that the correct tank was filled. However, it was obvious that the situation shown was fundamentally too risky. Sooner or later someone is going to connect a hose to the valve that is immediately in front of the tank that is to be filled, and an accident will occur.

In such a situation, too much reliance was placed on the procedures. What was needed was an engineering solution. The company made the following two changes:

1. The tanks were separated; one of them was placed at another location in the facility.
2. Different types of connections were used for the two chemicals.

If there is absolutely no choice but to rely on procedures in such situations, then the following actions can help reduce the risk.

- Have two operators involved in the loading process, so that there is a cross-check.
- Color code the valves corresponding to the chemical being fed.
- Develop detailed checklists that require the operator to double-check his or her actions.

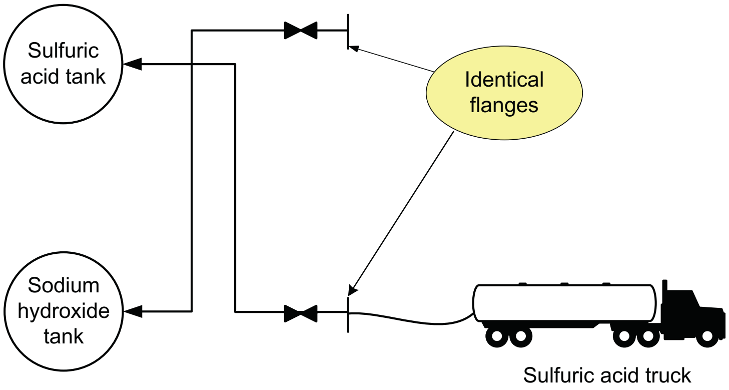


FIGURE 6.3

Potential for incorrect tank filling.

Not only is it unreasonable to expect procedures to address poorly engineered systems but also operators and maintenance technicians are less likely to execute procedures properly if conditions such as the following exist:

- Poor communication with supervision or with other operators
- Sloppy housekeeping
- Too many mental tasks to perform
- Too many physical tasks to perform
- Inadequate tools
- Extended, uneventful vigilance
- Inadequate breaks and rests

QUICK ASSESSMENT OF OPERATING PROCEDURES

For those facilities that already have operating procedures, it is useful to carry out a quick assessment to determine the present status of the procedures and to provide guidance as to what needs to be done. Some quick assessment questions are provided in Table 6.2. The answers to the questions can help an organization determine how good its procedures are, and which areas need the most work. The questions in Table 6.2 are not an audit protocol—they simply provide guidance as to the current state of the procedures. There is no pass or fail associated with these questions.

Table 6.2 has two columns. The first column provides the questions to be used in the assessment. A "Yes" answer to the questions indicates that the procedures are likely to be satisfactory.

Table 6.2 Quick Assessment—Overall Organization

Question	Y/N
Does the manual have a clear structure and organization?	
Does each procedure have a unique and clear title?	
Are the operating and training manuals separate documents?	
Are informational materials and procedures kept separate from one another?	
Can operators quickly find the instructions that they need?	
Does the manual have a Table of Contents?	
Does the manual have an index?	
Is the manual complete?	
Are the procedures linked with the other elements of PSM?	
Are temporary procedures clearly identified?	
Do temporary procedures have a termination date/time?	
Is the person responsible for performing each step identified?	
Are procedures laid out in the correct sequence?	
Does every procedure have a unique and permanent number or name?	
Is each procedure dated and signed?	
Are the procedures free of handwritten notes?	

Table 6.2 **Quick Assessment—Overall Organization** *Continued*

Question	Y/N
Do most procedures have revision dates that are less than a year old?	
Do individual procedures contain just one instruction?	
Do multiuser procedures include a sign-off process?	
Is the active voice used?	
Is the writing style simple?	
Do the operating instructions avoid the use of vague statements?	
Is a consistent format and layout used?	
Are colloquialisms avoided?	
Is the use of redundant words such as “next” and “then” avoided?	
Is the use of potentially ambiguous words avoided?	
Does the writing style avoid ambiguity, discursiveness, complexity, verbosity, long-windedness, and needless erudition?	
Are sketches, drawings, and pictures used?	
Are cautions and warnings placed immediately before the step to which they apply?	
Can instructions be found quickly?	
Do the procedures avoid the use of “soft” materials?	
Is the manual physically easy to use?	
Is the manual physically complete and undamaged?	
Are procedures written to the correct level of detail?	
Are jargons and acronyms avoided?	
Are conditional criteria placed ahead of the procedural step?	
Is all necessary information included or referenced in the procedure?	
Does the procedure match the way the task is done in practice?	
Is each procedure written so that the detail is appropriate to the complexity of the job?	
For complicated or critical calculations is a formula or table included or referenced?	
Is there plenty of white space?	
Are consistent formatting and layout styles used?	
Is a clearly readable font used?	
Is the use of capital letters minimized?	
Is text left justified?	
Is the use of nonobjective or nonquantitative criteria avoided?	
Are steps which can be carried out simultaneously identified?	
Are operating or maintenance limits defined quantitatively?	
Are measurements provided in engineering units?	
Are regulatory issues addressed?	
Is there a system for addressing new regulatory requirements?	
Is an organization for writing, maintaining, and updating the manuals in place?	

THE USERS

As already noted, an operating/maintenance manual has many potential users, some of whom are listed below.

EXPERIENCED TECHNICIANS

Experienced operating and maintenance technicians will not normally need detailed procedures, but they will find summary checklists to be useful. They may also need help with troubleshooting in order to address situations that they have not seen before.

Increasingly the senior technicians function as supervisors for computer control systems such as Distributed Control Systems (DCS) or Supervisory Control and Data Acquisition Systems (SCADA). These technicians need procedures that help them work with the electronic interface, generally as troubleshooters for when the electronic systems go awry, or for when the control systems fail.

LESS EXPERIENCED TECHNICIANS

Technicians who are new to the facility need detailed step-by-step procedures. They will also need thorough training in the use of the procedures.

ENGINEERING/MANAGEMENT

The technical staff use the procedures as a framework within which they can conduct facility tests and assist with troubleshooting. Management may also use the procedures when planning large projects such as a turnaround or revamp. In such situations, it is likely that many temporary procedures will have to be written.

DCS/SCADA PROGRAMMERS

Those responsible for developing DCS and by SCADA software (information technology professionals and operating personnel) develop and write the instructions to be followed by the automated equipment.

AUDITORS, REGULATORS, AND INSPECTORS

Regulations from safety and environmental authorities almost invariably require that operating procedures be written and followed. Therefore, an auditor can be considered to be a user in this context; the procedures must address the requirements of the regulations, and the company’s own internal standards, where applicable.

TRANSLATORS

Many manuals are written by an engineering company for use by a client in a different country. This means that the first “user” or “customer” of the manual will be a translator. Should this be the case, it is particularly important to avoid very technical terms, jargon, ambiguity, and convoluted sentence structures. All material must be explicit; there must be no latitude for "reader interpretation," inference, or reading between the lines.

ELEMENTS OF OPERATIONAL INTEGRITY MANAGEMENT

Operating procedures have links to most of the other elements of an operational integrity program (Table 6.1). They have particularly strong links with the following:

- Workforce Involvement
- Knowledge Management
- Hazard Identification and Risk Management
- MOC
- Operational Readiness
- Emergency Management
- Technical Information

They are discussed below.

WORKFORCE INVOLVEMENT

Participation, leadership, and accountability are at the heart of any successful process safety program. In the context of operating and maintenance procedures, participation means that the persons who will be using those procedures are fully involved in their preparation and in the subsequent training.

Management must provide leadership by organizing the procedures-writing program, and ensuring that sufficient funds, people, and other resources are made available for the work. They must also ensure that sufficient time is provided for the training that follows the publication of the procedures.

Finally, accountability should be built into the procedures-writing program. Management is accountable for providing the procedures; operators and technicians are accountable for following those procedures, and for making suggestions for improvements.

KNOWLEDGE MANAGEMENT

Operating and maintenance procedures should tell the technicians how to run the facility for which they are responsible—no more, no less. In practice, many operating manuals are used to store technical information such as P&IDs (Piping and Instrument Diagrams) and MSDS. The mixing of instructions and information in this manner generally reduces the effectiveness of the procedures. Technical information should be available in its own, separate, and stand-alone manual.

Nor should technical information be allowed to clutter up the operating instructions themselves. A simple way to decide whether a sentence belongs in the procedures or to an information manual is to see if the sentence has the form of an instruction, i.e., does the sentence start with a verb in the imperative tense? Sentences such as the following belong in the procedures because they are all "do" items.

- Open the valve.
- Measure the temperature.
- Inform the supervisor.

The following statements, however, do not belong in the operating manual.

- The valve is made of 316 stainless steel.
- The maximum allowable temperature is 165°C.
- The refinery can process 100,000 barrels per day of crude.

The first edition of an operating manual often contains excessive technical information because it is written while the facility is still in the design or construction phase. These procedures are typically written by design engineers who know the process and equipment but who do not necessarily have much operating experience. Hence they may describe the material of construction and the design parameters of a pump in some detail, but provide little or no information on how to actually operate that pump.

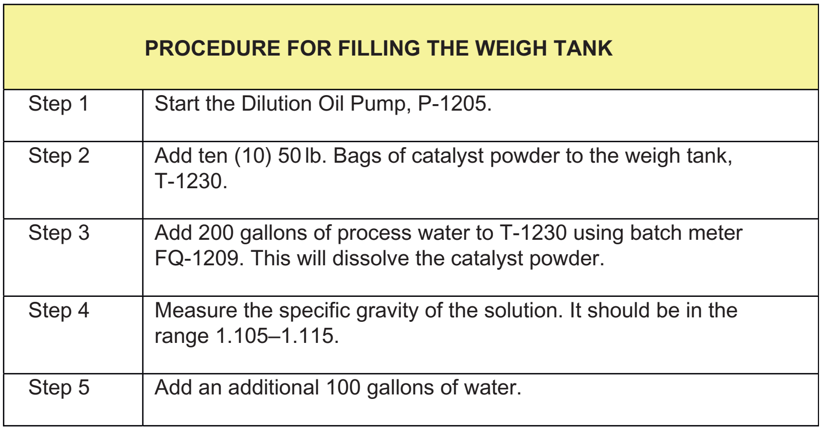
Evidence of the problem of having design engineers write procedures can be seen in statements such as:

> Pump, P-100, is designed to transfer 100 gpm.

The writer is describing an equipment that does not yet exist. Yet, when an operator has to start P-100, the pump is installed and operational. A more appropriate phrase for the operator would be:

> Pump, P-100, has a capacity of 100 gpm.

Figure 6.4 provides another example as to how procedures can be mixed up with information, potentially creating a confusion of purpose for the operator who is using the procedures to help him or her carry out a set of tasks.



PROCEDURE FOR FILLING THE WEIGH TANK	
Step 1	Start the Dilution Oil Pump, P-1205.
Step 2	Add ten (10) 50 lb. Bags of catalyst powder to the weigh tank, T-1230.
Step 3	Add 200 gallons of process water to T-1230 using batch meter FQ-1209. This will dissolve the catalyst powder.
Step 4	Measure the specific gravity of the solution. It should be in the range 1.105–1.115.
Step 5	Add an additional 100 gallons of water.

FIGURE 6.4

Example of confusion of purpose.

Strictly speaking, the second sentence in Step 3—"This will dissolve the catalyst powder"—is redundant because it is not an instruction. The sentence is actually an item of process information, and should be located elsewhere. In its present position, it is merely diluting the operating procedures.

Although a single instance of putting information in an operating manual as shown in Figure 6.4 is trivial, the repeated occurrence of such instances can seriously degrade the usability of the manual.

HAZARD IDENTIFICATION AND RISK MANAGEMENT

The purpose of a hazards analysis is to identify those hazards that pose an unacceptably high level of risk, and to ensure that corrective actions are taken.

A hazards analysis can be used to systematically review the operating instructions using a What-If approach. The team works through the procedures asking What-If questions regarding each instruction. The questions include the following:

- What-If the instruction is missed/overlooked/ignored?
- What-If the instruction is carried out partially (such as a valve being only partly closed)?
- What-If two instructions are executed in the wrong order?

Also, the team will try to identify actions that are carried out in the field but that are not recorded in the instructions.

MANAGEMENT OF CHANGE

On facilities that are already operating, most revisions to the operating procedures will come through the MOC process. Generally, someone on the facility will want to either change the operating conditions (e.g., by raising reaction temperatures to gain more production), or they will want to modify an equipment or instrument item. Most MOCs require that the procedures be updated because the procedures represent the operator−equipment interface. Therefore, any change to either the operation or the equipment will require a change to the procedures.

OPERATIONAL READINESS

After a change has been implemented following the use of the MOC process, it is important to conduct an operational readiness or prestartup safety review (PSSR) immediately prior to starting the changed equipment or operations. An important part of any PSSR is to ensure that the operating and maintenance procedures have been updated, and that the affected technicians have been trained.

EMERGENCY MANAGEMENT

The operating manual will generally include the procedures for handling a process-related emergency.

TECHNICAL INFORMATION

It has been stressed that operating instructions and operating information should be segregated from one another. However, critical operating information should be readily available to the operators and maintenance technicians.

TYPES OF OPERATING PROCEDURE

Six types of operating procedure are discussed here. They are as follows:

1. Steady-state operations
2. Start-up
3. Shutdown
4. Temporary operations
5. Batch operations
6. Standard operations

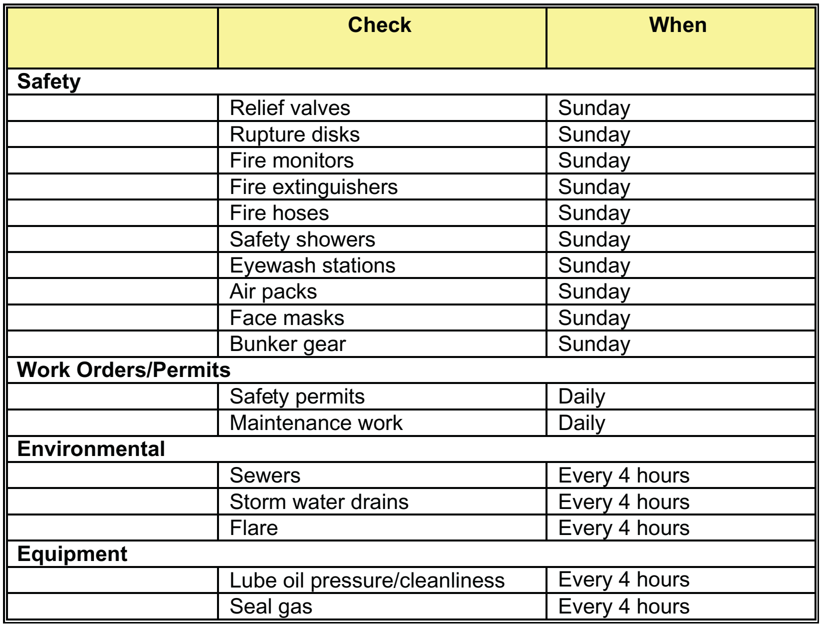
STEADY-STATE OPERATING PROCEDURES

Steady-state procedures cover those actions that are to be carried out during normal operations (as distinct from during a start-up or shutdown). During steady-state operations the facility is under the immediate control of the instrument systems; the role of the operator is to monitor the overall operation and to respond to alarms. Hence, the operating procedures are much more like checklists than statements of actions required. The inside technician checks the instrumentation to make sure that operating targets are being met; the outside technician conducts routine rounds to check that equipment is performing correctly.

TYPES OF STEADY-STATE PROCEDURE

Steady-state procedures that require routine operator intervention can be either event- or time-based. Event-based procedures are usually performed in response to a system change or condition. For example, with regard to the cooling tower example, the facility may have event-based procedures to handle issues such as adding chemicals to the water, or controlling the temperature of the water. Time-based procedures are those that are to take place at a specified time interval. For example, the operator may have to catch a sample of the cooling water every 4 hours in order to check the chemical concentrations in the water. Many maintenance-related activities, such as checking the lube oil level in pumps, are time based.

Figure 6.5 lists typical time-based duties and responsibilities for a particular job.



	Check	When
Safety		
	Relief valves	Sunday
	Rupture disks	Sunday
	Fire monitors	Sunday
	Fire extinguishers	Sunday
	Fire hoses	Sunday
	Safety showers	Sunday
	Eyewash stations	Sunday
	Air packs	Sunday
	Face masks	Sunday
	Bunker gear	Sunday
Work Orders/Permits		
	Safety permits	Daily
	Maintenance work	Daily
Environmental		
	Sewers	Every 4 hours
	Storm water drains	Every 4 hours
	Flare	Every 4 hours
Equipment		
	Lube oil pressure/cleanliness	Every 4 hours
	Seal gas	Every 4 hours

FIGURE 6.5

Example of a routine task list.

SHIFT CHANGE

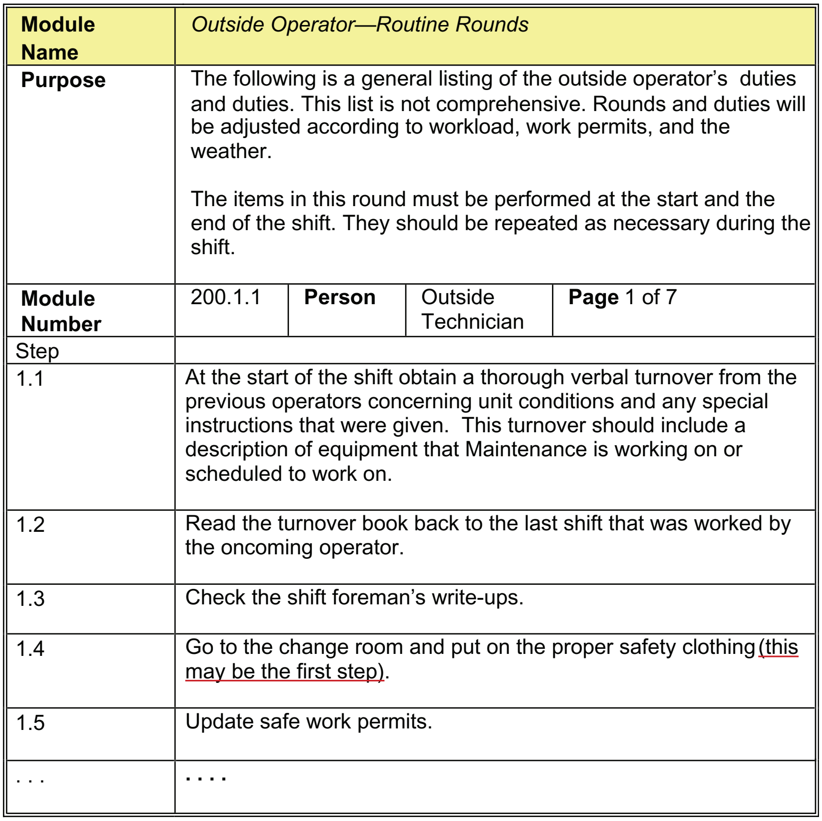
Many accidents occur at the time of shift change. Therefore, it is very important that handover procedures and checklists be written and followed during the handover. Nimmo (2006) suggests that the handover information be organized according to the following topics:

1. Safety
2. Environment
3. Quality
4. Production
5. Reliability

Other topics to be reviewed include maintenance and upcoming work. A routine rounds procedure is shown in Figure 6.6. It is to be followed by the outside operator at the start and end of each shift.

START-UP PROCEDURES

Once the operational readiness review described in the previous chapter is complete the facility can be started up. Start-up phase is often a hazardous time because the facility is in a dynamic state with conditions varying all the time, and because management and the operators may not have



<table>
<tr><td><b>Module Name</b></td><td colspan="4"><i>Outside Operator—Routine Rounds</i></td></tr>
<tr><td><b>Purpose</b></td><td colspan="4">The following is a general listing of the outside operator's duties and duties. This list is not comprehensive. Rounds and duties will be adjusted according to workload, work permits, and the weather.
The items in this round must be performed at the start and the end of the shift. They should be repeated as necessary during the shift.</td></tr>
<tr><td><b>Module Number</b></td><td>200.1.1</td><td><b>Person</b></td><td>Outside Technician</td><td><b>Page</b> 1 of 7</td></tr>
<tr><td>Step</td><td colspan="4"></td></tr>
<tr><td>1.1</td><td colspan="4">At the start of the shift obtain a thorough verbal turnover from the previous operators concerning unit conditions and any special instructions that were given. This turnover should include a description of equipment that Maintenance is working on or scheduled to work on.</td></tr>
<tr><td>1.2</td><td colspan="4">Read the turnover book back to the last shift that was worked by the oncoming operator.</td></tr>
<tr><td>1.3</td><td colspan="4">Check the shift foreman's write-ups.</td></tr>
<tr><td>1.4</td><td colspan="4">Go to the change room and put on the proper safety clothing (this may be the first step).</td></tr>
<tr><td>1.5</td><td colspan="4">Update safe work permits.</td></tr>
<tr><td>. . .</td><td colspan="4">. . . .</td></tr>
</table>

FIGURE 6.6

Example of a unit tour module.

much experience of what to do. Ironically, the improvements in system reliability brought about by risk management programs means that may quite experienced personnel may never have actually been through a full start-up because the facility can run for years without a full turnaround.

Some of the various levels of start-up are listed below.

Level 1 A brand new facility is being started for the first time.

Level 2 The facility is being started following a major turnaround. Equipment is still open for entry, blinds are still in place, electrical equipment is locked out, and instrument loops may not be in service.

Level 3 Maintenance has been completed; the facility has been buttoned up, with all blinds and lockouts removed; solid catalyst beds have been recharged. However, the equipment contains air and possibly small amounts of water from the clean-out following the turnaround work. Process equipment is at ambient temperature and pressure.

Level 4 The facility has been inventoried with hydrocarbons and process chemicals; all equipment is air free and ready to be operated. However, temperatures and pressures are close to ambient. This is the normal condition before a start-up if the facility was shut down for reasons other than major turnaround.

Level 5 The facility is on standby or "static operation." All equipment is operable and inventoried with the correct process materials in each piece of equipment (but probably not within specification). Pressures and temperatures are close to operating levels. This is the condition following a temporary shutdown that lasted for just a short period of time. Start-up from this condition is sometimes referred to as a "hot start" or a "rolling start."

During the start-up, technical support may be required in order to address unexpected issues as they arise. The technical support team will generally consist of the following personnel:

- A process or facilities engineer
- An instrument engineer
- Operations specialists

Depending on the scale of the project work and the complexity of the start-up it may be necessary to have a team of people representing the above disciplines working on a 24-hour shift cycle until the facility is properly lined out.

Even if 24-hour coverage is not considered necessary, discipline specialists should be available on call.

SHUTDOWN PROCEDURES

Procedures for (planned) shutdowns have the same features as start-up instructions, except that they are carried out in the reverse order. The starting point is the facility in full operating mode; the end point is having the facility shut down, with equipment cleared of chemicals so that maintenance can work on it. In many cases, shutdowns are only partial; e.g., if a pump seal has failed, and the pump has to be isolated, the facility may be put in a standby condition in which temperatures and pressures are maintained, and only the section to do with the pump is actually shutdown.

One important difference between shutdown and start-up is that, if something goes wrong during a start-up, particularly in the early stages, it is possible to stop further action and to take time to correct what has gone wrong. The system is probably in a safe condition at that point. For example, if the first step in the start-up of a distillation column is to put feed into the tower, a failure of the feed pump will mean that the tower will remain in a deinventoried condition. With shutdowns, however, equipment problems can create hazardous situations. For example, if the distillation column is being deinventoried into a holding tank, and the tank is being pumped out to another section of the facility, failure of the tank pump could lead to the tank overflowing.

The potential hazards associated with shutdown are analogous to flying an airplane. If, during the "start-up" of an airplane something goes wrong, such as the engines fail to start or the brakes will not release, the plane will remain on the ground in a safe condition until the problem is fixed. However, if the engines fail on a plane that is coming in to land, or if the brakes fail after landing, an accident will ensue.

LEVELS OF SHUTDOWN

If operating conditions deviate sufficiently from the safe state, various levels of automatic shutdown can be implemented. The following system is representative.

Standby

A facility is said to be on standby operation when most of the equipment is running normally. Only the items that are being worked on are actually shut in. During standby operation no feed is entering the unit, nor is any product being made. As far as possible, operating conditions are kept as close to normal as possible so that the facility can be restarted with minimal effort. For example, distillation columns are put on total reflux, vessels are operated at their normal level and rotating equipment is kept running. Only the items that are actually being repaired are taken out of service.

Unit Shutdown

A normal shutdown is that state where all rotating equipment, heaters, and other unit operations are stopped. No attempt is made to keep the unit in a partially operating state. However, equipment is not deinventoried, nor is anything purged—except for the equipment that is being worked on.

This type of shutdown is one that affects just a local operating unit. Equipment in that unit should be brought to a safe state, but it will be on standby, i.e., ready for immediate restart once conditions are back to normal. Normally, other units in the facility, including the utilities area, will continue operations at this level of shutdown. However, quick action may be required before the local shutdown leads to a shutdown of the whole process.

Facility Shutdown

When the whole facility or plant is to be shut down, additional ripple effects can be caused by issues such as the following:

- Loss of instrument air pressure
- Loss of control hydraulic pressure
- Loss of main electrical power
- Operator invention
- High liquid level in the flare knockout pot

Emergency Shutdown

An emergency shutdown is initiated when either an operator or the safety instrumentation system detects a situation that is critical enough to cause immediate injury to personnel. It will be initiated by actions such as the following:

- Manual action—usually through use of a remotely operated pushbutton
- Confirmed gas detection any nonhazardous area
- Confirmed toxic gas detection in nondesignated areas
- Confirmed fire detection in specific areas

An emergency shutdown will operate all automatic safety valves and blowdown inventories to a safe location (such as the flare) according to the cause-and-effect charts. Similarly, utilities will be de-energized, although the cause and effect charts may call for some systems—such as electrical power—to remain active. Fire pumps, emergency generators, and other emergency equipment will be brought online using their dedicated fuel supply (such as diesel) as called for.

Some facilities—particularly those offshore—require personnel to evacuate during an emergency shutdown. The emergency systems continue to operate, but the personnel abandon the facility by lifeboat or helicopter.

Turnaround

When a facility is shut down for turnaround, it is completely deinventoried and purged. Blinds are installed and instruments are disconnected and safety systems bypassed. Generally, all vessels are made ready for maintenance and personnel entry. Control of the facility is transferred from the operations department to the maintenance or project department.

TROUBLESHOOTING PROCEDURES

Once a facility has been started up, and brought into a stable operating condition, it is not likely that the procedures will change much—except as the MOC program calls for modifications to the way equipment is operated, or to the sequence in which procedures are carried out. Moreover, once the operators have been trained, and have gained day-to-day working experience on the unit, they are not likely to need the procedures, except in a checklist format. However, it is likely that during normal operations the facility will experience a variety of upsets and problems. These non-critical upsets do not constitute an emergency, but they can lead to economic losses and environmental damage, so it is useful if troubleshooting guidance is available. Such guidance is particularly useful to experienced operators because it is the one area in which they can never have sufficient knowledge. Even the most experienced person cannot have seen all the possible upsets that can occur.

It has been stressed that operating procedures are instructions that must be followed. Such is not the case with troubleshooting procedures, which typically provide guidance and suggestions, rather than "must do" instructions. Indeed, a troubleshooting "procedure" can provide two or more responses that address the same issue, such as why a particular pump is not putting up the expected discharge pressure. Such guidance can legitimately involve disparate opinions, hunches and feelings, thus making it very distinct from other types of operating procedure.

Although facility upsets that lead to a need for troubleshooting are fundamentally different from those that require an emergency response, it is not always clear to an operator as to which situation he or she may be in. For example, high temperature in a furnace may just be "trouble," leading to say excessive energy consumption. However, that same high temperature may be an indicator that a tube may soon rupture leading to an uncontrolled firebox fire, which in turn could lead to injuries, fatalities, and catastrophic loss. A good set of operating procedures gives as much help as possible in this situation by providing assistance on how to diagnose what has gone wrong, and what the immediate response ought to be.

In most troubleshooting situations, time is not of the essence; management and the operators have time to consider what is the best action to take. A troubleshooting scenario suggests problems such as the following:

- Changes in feedstock composition leading to the potential for off-spec product or unusual operating conditions
- Harsh environmental conditions, such as a hurricane or a hard freeze
- Equipment operating in a degraded condition
- Apparently inexplicable changes in a distillation column temperature profile

It is critical that an operator understand the distinction between troubleshooting and emergencies. Were he or she to handle an emergency as if it were only an operational problem, the consequences could be catastrophic. However, the opposite situation can be almost as bad. If the operator erroneously decides that an upset that is really *trouble* is actually an *emergency*, not only will his or her subsequent actions lead to unnecessary production and productivity losses, they may actually create an emergency. For example, tripping a motor-operated valve to its closed position in response to a misdiagnosis of an emergency could cause hydraulic and thermal shocks in other parts of the process that, in turn, could create an upstream flange to spread, leading to a possible release of toxic or flammable chemicals. Even if the consequences of the action do not lead to such extreme consequences, the sudden shutdown will likely cause irreversible degradation. For example, catalyst activity may be permanently reduced, equipment will be physically stressed, and the operators themselves will be tired and probably more prone to making mistakes in the time immediately following the false emergency.

ELEMENTS OF TROUBLESHOOTING PROCEDURES

Some of the distinctive elements of troubleshooting procedures, and the manner in which they differ from normal operating procedures and from emergency procedures are described below.

- Normal operating procedures are “closed,” that is they fully describe a particular operation. Troubleshooting, on the other hand, is an open-ended activity. An almost infinite number of potential problems exists. Therefore, the manual can never be comprehensive or definitive; all it that it can do is to offer guidance in the form of suggestions and ideas based on experience and brainstorming [such as would come from a process hazards analysis (PHA)]. There is a wide range of possible actions for any troubleshooting situation; many of the actions will be new and untried.
- It has been stressed earlier in this chapter that operating procedures are instructions that must be followed. Such is not the case with troubleshooting procedures, which typically provide guidance and suggestions, rather than “must do” instructions. Indeed, a troubleshooting “procedure” can provide two or more responses that address the same issue, such as why a particular pump is not putting up the expected discharge pressure. Such guidance can legitimately involve disparate opinions, hunches, and feelings, thus making it very distinct from other types of operating procedure.
- Development of a troubleshooting response often requires insight and imagination because there is rarely any predefined “correct” response; each situation possesses unique qualities. This aspect of troubleshooting is one of the reasons for stressing the education, as distinct from

training, of the senior operators. Training teaches them how to do a particular task, education teaches them the principles on which the facility is running and how to think through problems.

- Troubleshooting often involves the handling of differing opinions, many of which will conflict with one another, and none of which are necessarily absolutely right or wrong.
- Troubleshooting procedures are organic. As more and more operating experience is gained from the facility, so the amount of useful troubleshooting material will increase. Their usefulness depends on the commitment that facility personnel make toward recording their experiences whenever a problem arises.
- There is an element of creativity in troubleshooting. When solving problems, an operator will often reason by analogy, i.e., he compares the present situation with a similar, but not identical, situation that occurred at some other time and place. He then has to decide if the analogy is appropriate, and what action should be taken as a result of this reasoning. There is no place for this type of approach in the emergency response procedures.

STRUCTURE OF TROUBLESHOOTING PROCEDURES

The use of a modular design structure is stressed throughout this chapter. With regard to troubleshooting procedures such rigor is not so necessary. The procedures are, by their very nature, going to be somewhat open-ended. Therefore, they can be written in a more discursive manner.

TEMPORARY OPERATING PROCEDURES

A temporary operation is one that is carried out for a short period of time and then may never be carried out again. Many temporary operations are associated with equipment breakdown. For example, if a pump fails, management may decide to install a portable pump in the same service, or to install a temporary bypass while the repair is being carried out. Hence temporary operations can often be identified by their frequent use of phrases such as “hot-tap,” “flex-hose,” “overtime,” and “vacuum truck.”

Items to watch for during temporary operations include the following:

- Sudden changes in utilities consumption
- Inventories of intermediate chemicals
- Changes in flow rates

It is important to distinguish between “temporary operations” and “rare permanent operations.” If an operation is to be carried out just once with no anticipation that it will ever be repeated, then it is “temporary.” If, however, it is anticipated that the operation will be repeated, then it is “rare permanent,” and will have its own associated procedures as part of the operating manual. For example, if a vessel is to receive a special chemical treatment say once every 3 years, then that operation is “rare permanent.”

Temporary operations, and their associated procedures, have the following features.

- The operation lasts for only a finite period of time; at the conclusion of that time, the facility is returned to normal operation and the temporary procedures that had been implemented are withdrawn. This means that all temporary operating procedures must contain a built-in expiration date or time.

- Temporary operations are often carried out in a hurry—particularly if the facility has been brought into standby mode due to failure of an equipment item, and management wants to correct the problem before having to implement a more complete shutdown. The urgent nature of such operations is potentially risky; management and supervision are often under pressure "to get back up to speed as quickly as possible," so they are tempted to cut corners by, among other things, not bothering to write a temporary operating procedure. They may also be tempted to skip the all-important PSSR step.
- Operating procedures for temporary operations are difficult to write because the normal procedures-writing support systems and personnel may not be available when they are needed.
- Probably the most critical feature of operating procedures for temporary operations is to recognize that they must be written. Yet, in spite of their importance, it is frequently an area of manual writing that gets overlooked. The temporary nature of this type of work can generate a "Let's just get on with it attitude." Statements such as, "It will take longer to write the procedure than to do the job" are often made. Such statements may indeed be correct, but they do not justify skipping writing the procedure before the work starts.

Once the temporary operation has been completed its associated procedure must be removed from the manual. If it is intended to make the operation permanent, then the procedure should be edited and then incorporated into the normal operating procedures manual.

A policy regarding the retention of temporary procedures once they have expired is required. As already noted, the procedures must be removed from the operating manual to minimize the chance of someone using them inadvertently. However, many technicians and managers not unreasonably like to keep copies of the old temporary procedures because they can serve as worked examples, or "go-bys," in the event that a similar procedure has to be written at a later date.

BATCH PROCEDURES

A batch operation is one in which the operating conditions change over time. Typically a series of steps are followed, the product is transferred to the next phase of the operation and the process starts over.

The distinction between continuous and batch operations is not as great as is sometimes thought. All steady-state processes include a variety of batch operations such as filling tanks from trucks and catching samples according to a predetermined schedule. Moreover, the sequence of instructions within a procedure or module is essentially the same as the sequence of instructions in a batch process.

Operating procedures for batch facilities are generally more complicated and difficult to write than for steady-state facilities because time is a factor. In addition, many batch facilities are designed to make multiple products from the same items of equipment at different times. Therefore, two or more procedures are needed for the same equipment items, creating the possibility of mix-ups and misunderstandings.

Some batch operations involve the use of calculation sheets. For example, an operator may add a bag of chemicals to a reactor and then add a second chemical. The ratio of the second to the first should be exact—say 1.8—1. The operator will weigh the first bag, calculate the weight of the second chemical needed, and proceed to weigh out that chemical. A calculation sheet is needed to determine the requirements for the weight of the second chemical. Furthermore, a calculation sheet may also be needed if different types of product are being made and operating conditions vary accordingly.

STANDARD OPERATING PROCEDURES

The term “SOP” is often used to describe all types of operating procedure (indeed, it is used in this manner in the EPA’s Risk Management Program rule). However, it is suggested here that a *standard* operating procedure should actually be what it says it is: a standard or a template upon which the *equipment* and *unit-specific* operating procedures can be built.

The use of a library of generic or SOPs makes sense because many operations and tasks are very similar to one another; hence one template can provide a foundation for many specific procedures.

The benefits to this approach to the writing of SOPs include the following:

- It will take much less time to write the equipment-specific procedures because most of the material will already have been written. To a large extent, the writing of the specific procedures will consist of little more than filling in the blanks in the generic procedure.
- The equipment-specific procedures will be of high quality because their framework will have been developed by such a highly qualified team.
- By forcing the writers of the procedures to fill in the blanks in the generic procedure (the SOP) there will be less chance of a step being overlooked or of a mistake being made.
- Problems associated with writer’s block will be minimized.

If a clear distinction between equipment-specific and generic procedures is made then the writing of procedures proceeds in two steps. First, the generic library of SOPs is created. Then the unit-specific and equipment-specific procedures can be written.

For example, a facility may have many centrifugal pumps, all operating at similar conditions and all manufactured by the same vendor. Management can create a team consisting of the following personnel to write the centrifugal pump SOPs:

- One or more senior technicians who have extensive experience in the operation of pumps at that facility
- An experienced representative from the maintenance department who would provide expertise on how a centrifugal pump should be operated in order to keep it in good working order
- A process engineer with a knowledge of pump theory
- A representative from the company that manufactures the pumps that are used at the facility
- A safety expert who has a broad grasp of the issues to do with pump operations

This team can create a set of SOPs for starting, running, and stopping centrifugal pumps. Using the appropriate SOP (sometimes referred to as a “go-by”), the writers of the procedures for each specific pump will have little more to do than fill in the blanks. In the case of the SOP for starting a centrifugal pump, e.g., the blank areas that would require pump-specific information include the following:

- The discharge pressure of the pump
- The expected amperage that the pump will pull
- The location of the suction and discharge valves

Representative titles for an SOP library are provided in Table 6.3. (This Table is not intended to be complete—it merely provides an outline for a full set of procedures.)

Table 6.3 Standard Operating Procedures

- 100—NORMAL OPERATIONS
  - 101—Routine Rounds
    - 101.01—Taking Outside Readings
    - 101.02—Taking Inside Readings
    - 101.03—Rotating Equipment Checks
  - 102—Equipment Checks
    - 102.01—Rotating Equipment
    - 102.02—Fin Fan Heat Exchanger
    - 102.03—Shell and Tube Heat Exchanger
  - 103—Equipment Operation
    - 103.01—Switching Centrifugal Pumps
    - 103.02—Filling a Vessel
    - 103.03—Emptying a Vessel
- 200—START-UP
  - 201—General
    - 201.01—Air Free the System
    - 201.02—Drying Equipment
    - 201.03—Nitrogen Purging
  - 202—Rotating Equipment
    - 202.01—Centrifugal Pump Initial Start-Up (1 of 2)
    - 202.02—Centrifugal Pump Initial Start-Up (2 of 2)
    - 202.03—Centrifugal Pump: Normal Operations
    - 202.10—Steam Turbine (Condensing) (1 of 2)
    - 202.11—Steam Turbine (Condensing) (1 of 2)
    - 202.12—Steam Turbine (Noncondensing)
    - 202.13—Steam Turbine (Pressure Lubricated)
    - 202.20—Reciprocating Pump
    - 202.30—Reciprocating Compressor
  - 203—Equipment
    - 203.01—Distillation Column (1 of 2)
    - 203.02—Distillation Column (2 of 2)
    - 203.05—Distillation Column, Fired Heater Reboiler

Table 6.3 Standard Operating Procedures *Continued*

- 203.10—Stripper
- 203.20—Incinerator
- 203.21—Fired Heater

- 300—SHUTDOWN
  - 301—Rotating Equipment
    - 301.01—Centrifugal Pump
    - 301.02—Steam Turbine
    - 301.03—Centrifugal Compressor
    - 301.10—Reciprocating Compressor
  - 302—Equipment
    - 302.01—Vessel
    - 302.05—Distillation Column
- 400—EMERGENCY OPERATIONS
  - 401—Emergency Shutdown
  - 402—Emergency Response
    - 402.01—Fires and Explosions
    - 402.02—Release of Toxic Gas
  - 410—Response Following an Emergency
    - 410.01—Clean-Up Following an Emergency
    - 410.02—Start-Up Following an Emergency Shutdown
- 500—TROUBLESHOOTING
  - 501—Compressors
    - 501.01—Reciprocating Compressors (1 of 2)
    - 501.02—Reciprocating Compressors (2 of 2)
    - 501.05—Centrifugal Compressors
  - 502—Pumps
    - 502.01—Centrifugal Pumps (1 of 3)
    - 502.02—Centrifugal Pumps (2 of 3)
    - 502.03—Centrifugal Pumps (3 of 3)
    - 502.04—Reciprocating Pumps
- 600—OPERATIONS/MAINTENANCE
  - 601—General
    - 601.01—Turnover of Equipment to Maintenance
    - 601.02—Turnover of Equipment from Maintenance
    - 601.03—Changing Filters
  - 602—Valves and Piping
    - 602.01—Putting a Relief Valve in Service
    - 602.02—Taking a Relief Valve out of Service
  - 603—Instrumentation/DCS
- 700—PRECOMMISSIONING
  - 701—Mechanical and Equipment Check

Table 6.3 Standard Operating Procedures *Continued*

- 701.01—Steam Turbines
- 701.02—Steam Systems (1 of 2)
- 701.03—Steam Systems (2 of 2)
- 701.04—Steam Turbines
- 701.05—Steam Traps
- 701.06—Centrifugal Pumps Mechanical Check
- 702—Water Flushing
  - 702.01—Overview
  - 702.02—Centrifugal Pumps
  - 702.03—Piping
  - 702.04—Shell and Tube Heat Exchangers
  - 702.05—Control Valves
  - 702.06—Steam Traps
  - 702.07—Completion
- 800—COMMISSIONING
  - 801—Utility Systems
    - 801.01—Facility and Instrument Air
    - 801.02—Cooling Water
    - 801.03—Natural Gas
    - 801.04—Fuel Gas
    - 801.05—Firewater
    - 801.06—Steam Headers
    - 801.07—Steam Equipment Lines
    - 801.08—Lube Oil Systems
    - 801.09—Seal Oil Systems
    - 801.10—Steam Turbines
    - 801.11—Flare
    - 801.12—Steam Tracing
    - 801.13—Drying and Inerting a System
  - 802—Feed Preparation Unit
- 900—MISCELLANEOUS
  - 901—Vehicle Movement
    - 901.01—Verification of Truck Documents
    - 901.04—Loading a Truck
    - 901.05—Unloading a Truck
    - 910.01—Changing Filters
  - 920—Pipelines
    - 920.01—Pigging a Line
    - 920.02—Checking Cathodic Protection

MAINTENANCE PROCEDURES

Most of the concepts that have been described in the previous chapters to do with operating procedures can also be applied to maintenance procedures. The major differences between the two types of procedure are as follows:

1. Maintenance procedures are generally carried out on a stand-alone basis whereas operating procedures are usually part of an overall sequence of instructions.
2. Maintenance procedures focus on equipment and instruments rather than on operating systems.
3. Illustrations and pictures are very useful in operating procedures; in maintenance procedures their presence is essential.

Maintenance work is, by its very nature, hazardous. Workers maintain equipment that is opened or disassembled, thereby exposing those workers to a wide range of potential hazards that stem from toxic chemicals, heat, electricity, moving machinery, hydraulics, pneumatic equipment, falling objects, springs and coils, and falls from equipment. In addition, maintenance workers may be asked to work at heights, in confined spaces, or in other unsafe locations. Therefore, first goal of any maintenance procedure is to ensure that the work can be carried out safely.

JOB SAFE PRACTICES

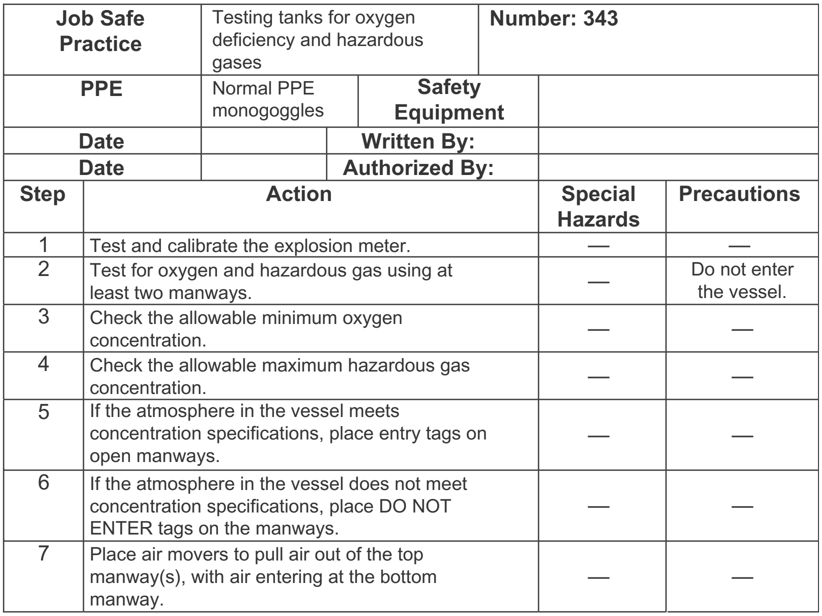
SOPs, described above, provide general instructions for a task; they are used as the foundation of job-specific procedures. Job Safe Practices (JSPs) are a special type of SOP used for carrying out hazardous tasks.

Figures 6.7 and 6.8 are examples of JSPs. In practice, much more detail than is shown here would be needed, particularly with regard to the specific hazards associated with the process being worked on.

Figures 6.7 and 6.8 also illustrate how maintenance procedures can be organized and published. The actions to be performed are listed sequentially; potential hazards and precautions associated with each step are also shown.

SOFTWARE ANALOGY

The terminology used when developing and using operating procedures is typically based on the writing and publishing business. Words such as “page,” “binder,” “write,” and “print” all evoke a world of books. Yet an operating manual is not really a book in the same manner as a textbook or a novel. In fact a well-organized manual is much closer in structure to a computer program than it is to a book. Therefore, if the manual is designed and developed as if it were a piece of software rather than as a written text the procedures-writing effort is more likely to be successful and effective.



Job Safe Practice	Testing tanks for oxygen deficiency and hazardous gases	**Number: 343**	
PPE	Normal PPE monogoggles	**Safety Equipment**	
Date		**Written By:**	
Date		**Authorized By:**	
Step	**Action**	**Special Hazards**	**Precautions**
1	Test and calibrate the explosion meter.	—	—
2	Test for oxygen and hazardous gas using at least two manways.	—	Do not enter the vessel.
3	Check the allowable minimum oxygen concentration.	—	—
4	Check the allowable maximum hazardous gas concentration.	—	—
5	If the atmosphere in the vessel meets concentration specifications, place entry tags on open manways.	—	—
6	If the atmosphere in the vessel does not meet concentration specifications, place DO NOT ENTER tags on the manways.	—	—
7	Place air movers to pull air out of the top manway(s), with air entering at the bottom manway.	—	—

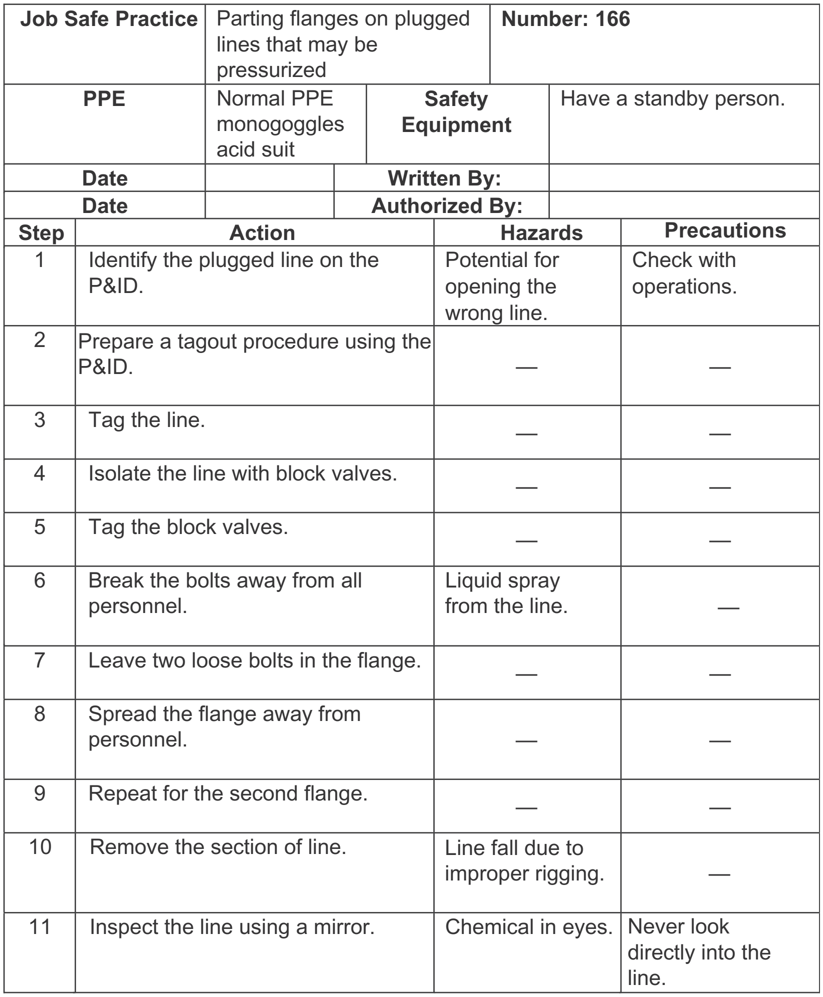
FIGURE 6.7

Sample JSP—testing tanks for vessel entry.

Moreover, books are usually written in a sequential manner with a beginning, a middle, and an end. Not only is this true of novels, mystery stories, and biographies, it is also true of technical works, such as this one. Typically, they start with an introductory chapter, which is then developed in greater detail in the subsequent chapters, with a final chapter providing a review and conclusion. Operating and maintenance procedures, however, are not written in a narrative form because they are not read straight through like a book. Instead, procedures are much closer in form to random access databases because the operators use the information in them eclectically, i.e., they go to the section that addresses their needs, regardless of its location within the manual. Moreover, one piece of operating information, such as starting a particular pump, may be used in more than one operating sequence. This characteristic—multiple uses of one information set—is fundamental to database design. As with software, it is particularly important that an operating manual have a good index so that the users can quickly find the instructions that they need.

The following concepts are central to the development of operating manuals based on the approach used in the software business:

- Modular design
- Database structure
- Top-down development
- Prototyping



Job Safe Practice	Parting flanges on plugged lines that may be pressurized	**Number: 166**	
PPE	Normal PPE monogoggles acid suit	**Safety Equipment**	Have a standby person.
Date		**Written By:**	
Date		**Authorized By:**	
Step	**Action**	**Hazards**	**Precautions**
1	Identify the plugged line on the P&ID.	Potential for opening the wrong line.	Check with operations.
2	Prepare a tagout procedure using the P&ID.	—	—
3	Tag the line.	—	—
4	Isolate the line with block valves.	—	—
5	Tag the block valves.	—	—
6	Break the bolts away from all personnel.	Liquid spray from the line.	—
7	Leave two loose bolts in the flange.	—	—
8	Spread the flange away from personnel.	—	—
9	Repeat for the second flange.	—	—
10	Remove the section of line.	Line fall due to improper rigging.	—
11	Inspect the line using a mirror.	Chemical in eyes.	Never look directly into the line.

FIGURE 6.8

Sample JSP—parting flanges on plugged lines that may be pressurized.

MODULAR DESIGN

When writing a computer program, the programmer first creates a high-level structure; then he or she writes modules that fit into that structure. Depending on the computer language being used, these modules are called subroutines, functions, or procedures. Within each of the software modules are lines of code.

The schematic shown in Figure 6.9 illustrates the use of this approach. To the left of the sketch is a sequence of computer instructions—the flow of the program is from top to bottom. One of the steps requires that two numbers, X and Y, be added to one another to give the answer Z. To do

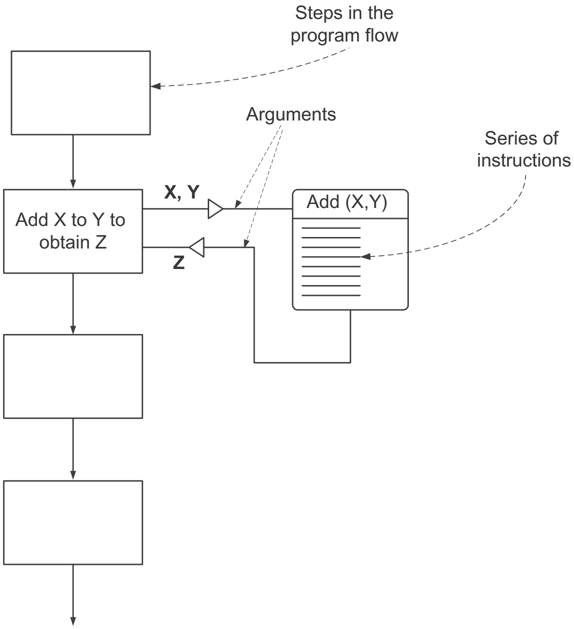


FIGURE 6.9

Computer subroutine.

this, the main program calls a subroutine with the title ADD. The numbers X and Y are fed as arguments to the subroutine, which adds them to one another, and then returns the answer Z as an argument to the calling program.

If it is decided to make a change to the above program, say by giving the ADD module the capability of adding three numbers instead of two, then all that needs to be done is to pull that particular module out of the system, modify it, and then reinsert it into the overall program. No other part of the program is affected. In particular, other parts of the program that use the ADD subroutine are not affected in any way, so there is no need for them to be rewritten.

Connecting the Modules

One of the cardinal rules to do with a modular system is that each module can only be entered through its Title Block. Figure 6 (the computer subroutine) shows that the incoming numbers “X” and “Y” (the arguments) must enter through the title block of the module as shown. With regard to operating procedures, only the whole module can be called, not the individual instructions within the modules. The flow of information always goes to the top of the module/procedure. Hence, if a writer wants to change a module all he or she has to do is pull out the affected module(s), modify it, and then reinsert it into the system with full confidence that nothing else has changed.

Figure 6.10 looks very similar to Figure 6.9. However, it illustrates an *incorrect* way of linking procedures. The arguments “X” and “Y” enter the body of the module ADD (X, Y), not the title block.

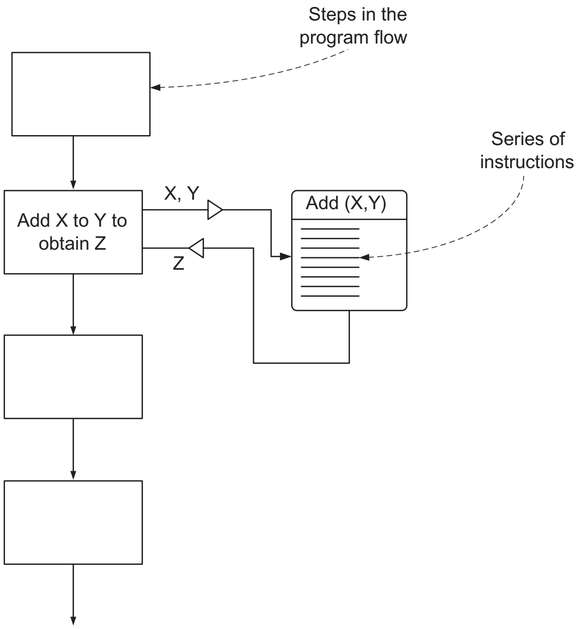


FIGURE 6.10

Example of incorrect linkage.

If/Then/Else Instructions

Although a procedure must be entered through its title block, it can be exited before it is complete. In particular, if a procedure contains an IF/THEN/ELSE sequence, the work flow may jump away from the procedure before it is completed, as illustrated in Figure 6.11.

Modular operating manual

The principle of modularity can be used for designing an operating manual, with its associated procedures and instructions. Under this paradigm, the overall computer program becomes the operating manual, the subroutines within the program are the operating procedures, and the lines of code are the task instructions.

The terms used by the software and operating manual businesses are compared in Table 6.4.

The advantage of a highly structured approach to software development is that, if a module has to be changed, its internals can be updated and modified—"privately maintained"—without having any impact on the overall structure. As long as the title of a module is not changed, a writer is free to change the contents of a module without having to worry about system-wide implications.

Figures 6.12 and 6.13 which illustrate the use of modularity in the development of an operating manual.

Figure 6.13, which is based on Figure 6.11, shows an incorrect linkage.

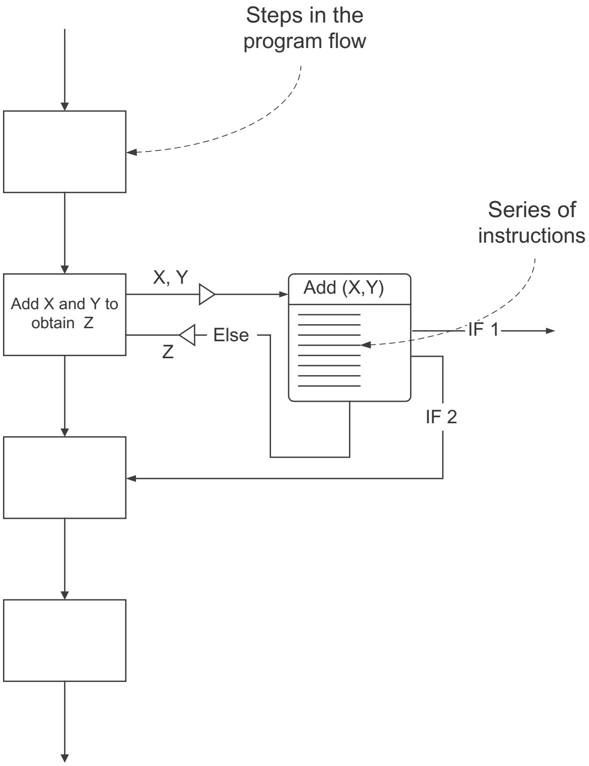


FIGURE 6.11

Use of conditional instructions.

Table 6.4 Terminology

Software	Operating Manual
Program	Operating manual
Subroutine/procedure/function	Operating procedure
Line of code	Task instruction

DATABASE STRUCTURE

The software analogy applies also to manner in which the modules (procedures) are organized. Technicians need the procedures right away. Therefore, the manual needs to be organized like a database; in particular the manual must be carefully indexed so that information and instructions can be reached as and when needed.

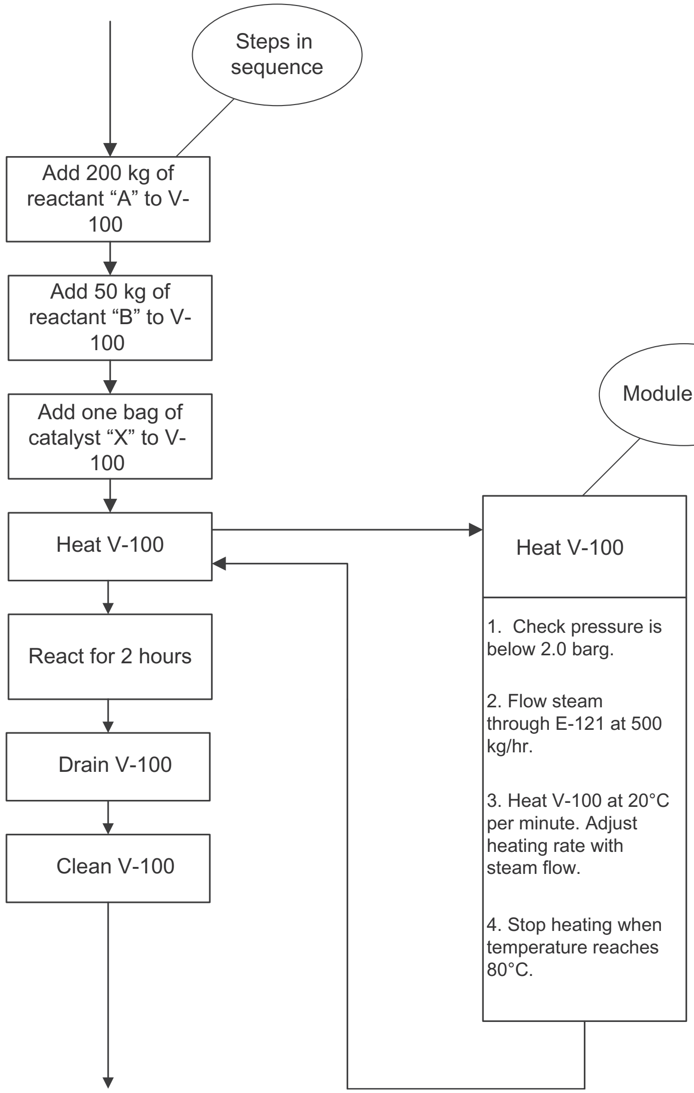

Steps in sequence
Add 200 kg of reactant "A" to V-100
Add 50 kg of reactant "B" to V-100
Add one bag of catalyst "X" to V-100
Heat V-100
React for 2 hours
Drain V-100
Clean V-100
Module title
Heat V-100
1. Check pressure is below 2.0 barg.
2. Flow steam through E-121 at 500 kg/hr.
3. Heat V-100 at 20°C per minute. Adjust heating rate with steam flow.
4. Stop heating when temperature reaches 80°C.

FIGURE 6.12

Subroutine analogy.

TOP-DOWN DEVELOPMENT

The development of an operating manual should be a highly structured activity that is properly planned before the first words are written. The first modules will be broad in scope with very little detail. As more specific instructions are written, so they can be plugged into the overall structure, which will develop in ever-increasing levels of detail. At all times, the people writing the

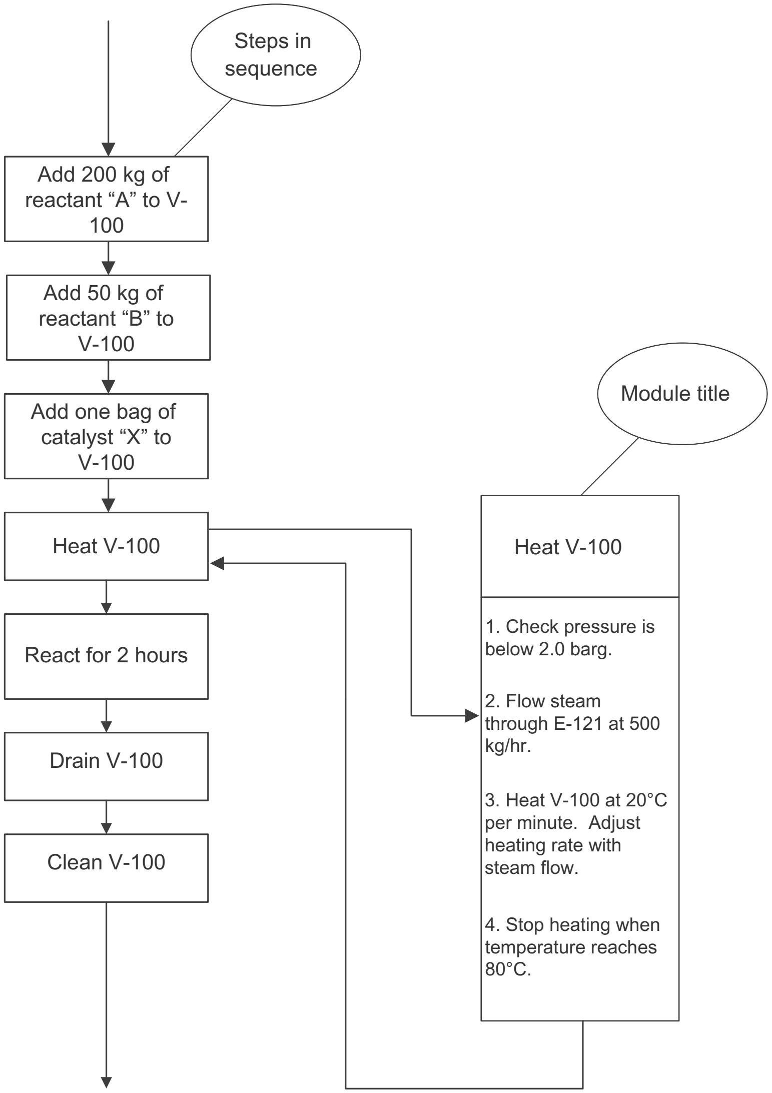

Steps in sequence
Add 200 kg of reactant "A" to V-100
Add 50 kg of reactant "B" to V-100
Add one bag of catalyst "X" to V-100
Heat V-100
React for 2 hours
Drain V-100
Clean V-100
Module title
Heat V-100
1. Check pressure is below 2.0 barg.
2. Flow steam through E-121 at 500 kg/hr.
3. Heat V-100 at 20°C per minute. Adjust heating rate with steam flow.
4. Stop heating when temperature reaches 80°C.

FIGURE 6.13

Subroutine analogy with incorrect linkage.

procedures have the big picture in front of them, and look at the manual holistically. In other words, "The manual is always complete."

Yet the manual will never be truly finished; there is always more information that can be added. However, by having the overall structure in place, the procedures writers are always working with a complete product; they are not just "writing procedures"—they are contributing material that

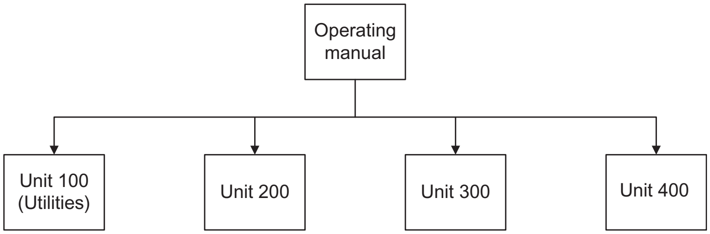


FIGURE 6.14

Top-down development 1.

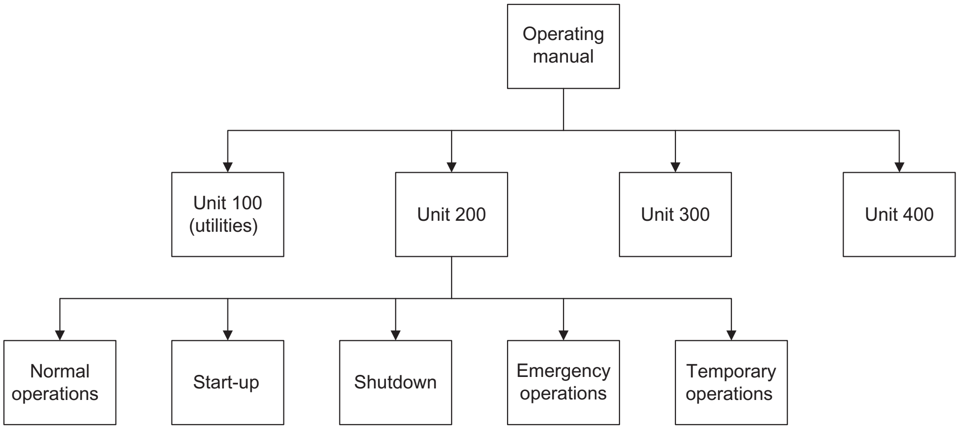


FIGURE 6.15

Top-down development 2.

forms part of the overall operating manual. In other words, "The manual is always complete but the manual is never complete."

The development of a top-down system is illustrated in Figures 6.14–6.17.

Figure 6.14 shows that the operating manual has been divided into four major sections: Units 100–400. At this stage the manual is, of course, of little practical value. However, it is complete, accurate, and up to date.

Figure 6.15 illustrates the development of the section of the manual to do with Unit 200 (the comparable divisions for the other units have been omitted in order to save space). The Unit 200 operating manual has been divided into the five categories shown.

Once more, the manual has little practical value. However, its overall organization is coming into focus.

Figure 6.16 is a development of Figure 6.15. The start-up section for Unit 200 has been expanded. It consists of eight blocks, one of which, Block 3, has been identified as "Start Compressors." Blocks 4 and 5 can be carried out in parallel with one another.

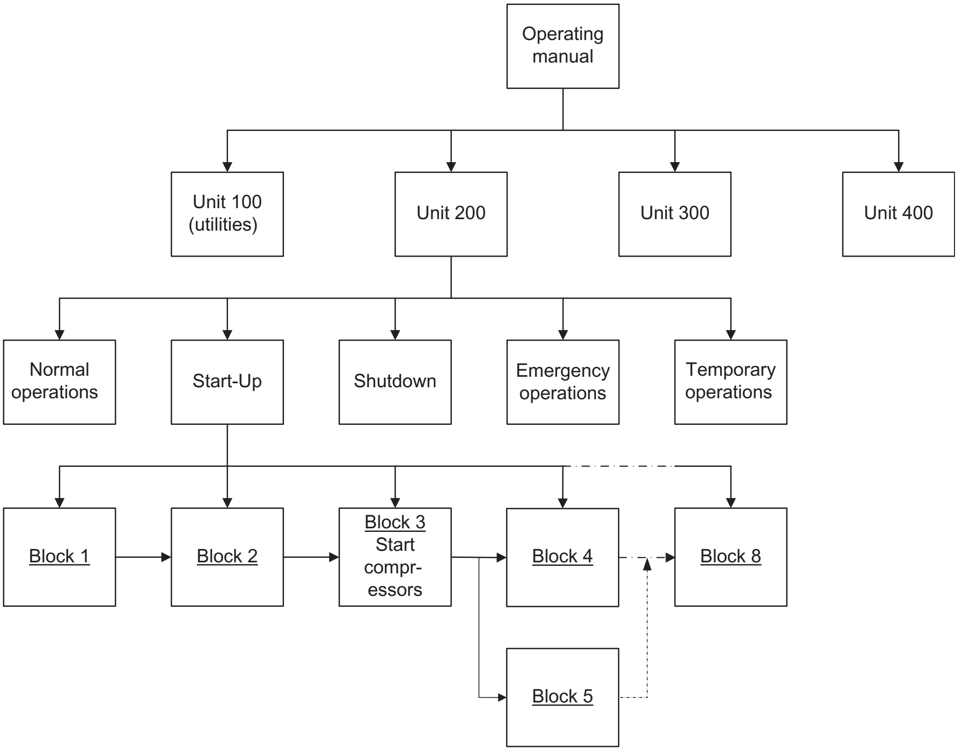


FIGURE 6.16

Top-down development 3.

Figure 6.17 shows the final development in the sequence. Block 3 is expanded into actual modules or operating procedures, of which there are four in this case: Modules 3-1 to 3-4.

PROTOTYPING

Although a top-down approach to developing a manual is a good way of managing and controlling a procedures-writing project, it sometimes makes sense to develop one or two of the procedures in detail as prototypes early on in the project for the following reasons:

1. A prototype provides management with a better understanding as to how much time and effort will be needed for the complete project.
2. It gives everyone, particularly the operators, a chance to work with, and to critique the format. It is much easier to comment on a worked example than to try and create something new. If this step goes well, everyone is much more likely to buy into the overall project. If there are problems with the structure, design, or level of detail they can be addressed at this stage before too much time and effort has been misdirected.

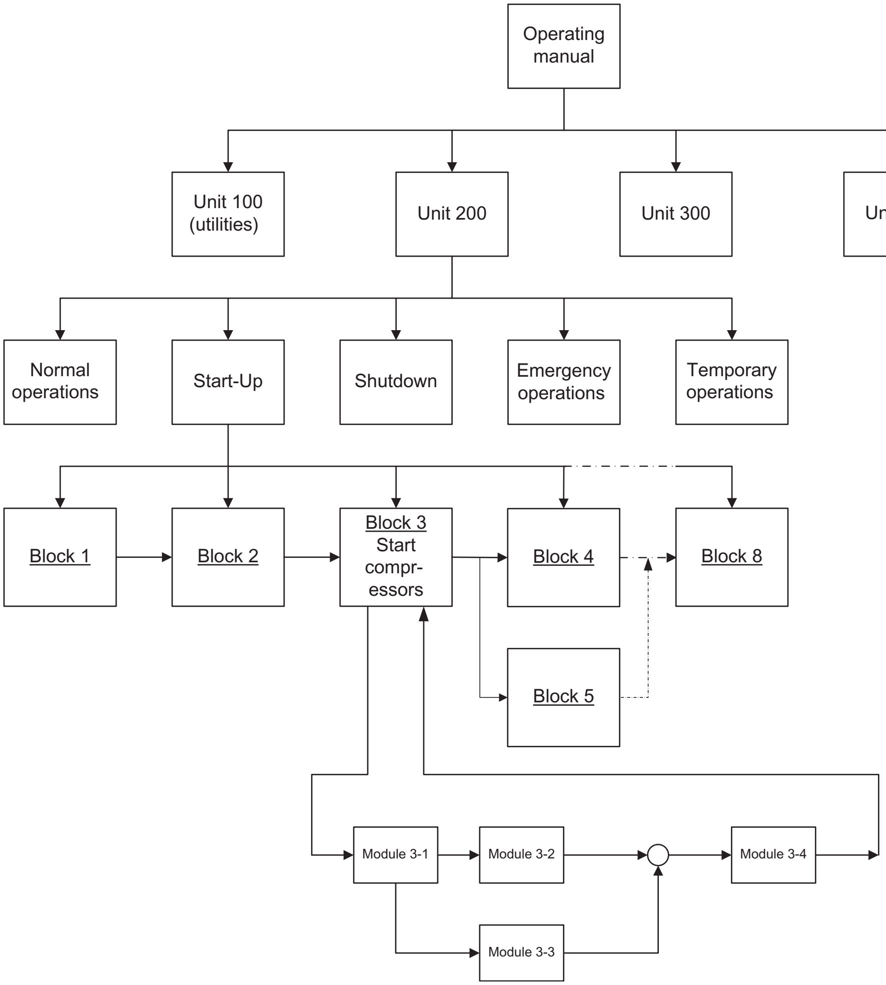


FIGURE 6.17

Top-down development 4.

3. It highlights any problems that are likely to arise, such as missing information or difficulties with the information-gathering process.

The publication of the prototype using a "drill-down procedure" will be the first time that the future users will actually see the product, so it is important that both the contents and the appearance are first class. It should not be treated as "just a draft." In the words of the proverb, "You don't get a second chance to make a first impression."

Another reason for creating some early detailed procedures is in response to incident in particular areas or on particular types of operation.

LIMITATIONS OF MODULARITY

Although modularity has many benefits, perfect modularity is difficult to achieve, particularly when changes are made to facility-wide systems, such as utilities. For example, a pump driver may be changed from a steam turbine to an electric motor. Apparently the only modules that are changed are those that concern the normal operation, start-up, and shutdown of that pump. Yet, placing a new turbine on the steam header may lead to steam availability problems that have system-wide effects and that affect many other equipment items. Hence the modules for all the other affected equipment items may require updating.

DESIGN OF AN OPERATING MANUAL

Figures 6.18–6.22 illustrated the use of the top-down concept in the creation of operating procedures. At the start of the procedures-writing project a high-level structure is developed; increasing levels of detail are then added within that structure. At all times, the people writing the procedures have the big picture in front of them; they can look at the manual holistically. By having the overall

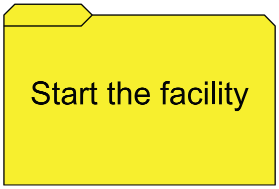


FIGURE 6.18

Level 1 of the manual.

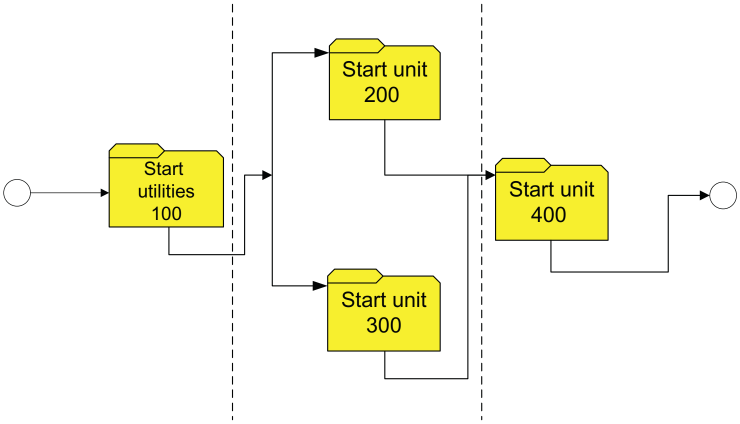


FIGURE 6.19

Level 2 of the manual.

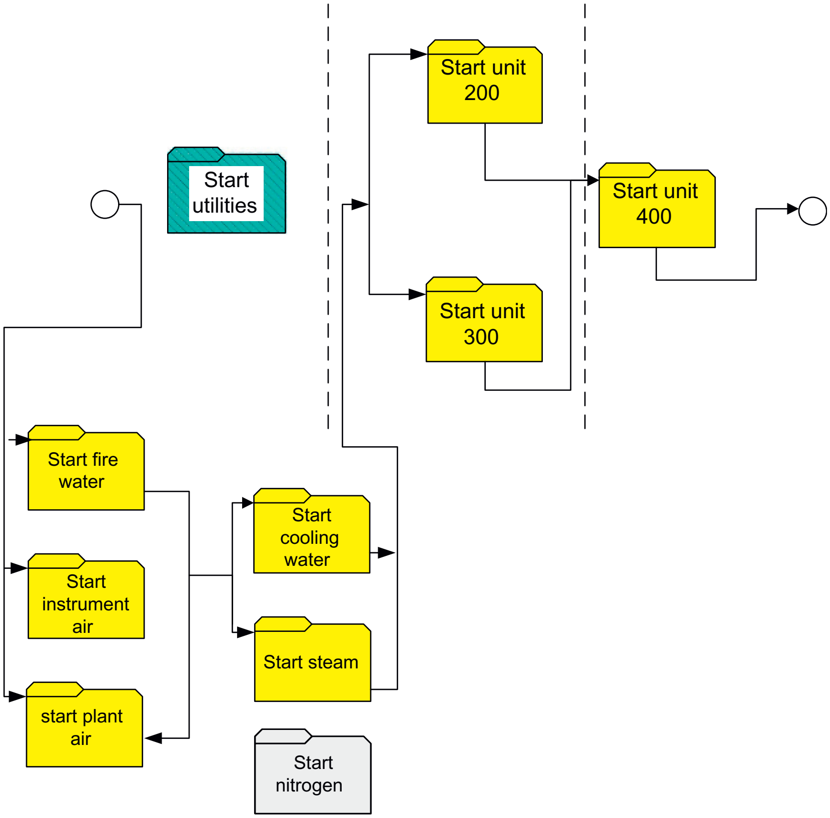


FIGURE 6.20

Level 3 of the manual.

structure in place, the procedures writers are always working with a complete product; they are not just "writing procedures"—they are developing an integrated operating manual.

The top-down concept is illustrated with a second example, starting with Figure 6.18. The start-up procedures for a facility are developed, with the procedures for starting the cooling tower shown in greater detail.

At the very top level—Figure 6.18—the operating manual consists of but just three words: "Start the Facility." Obviously the manual at this stage has no practical value. However, it *is* complete, accurate and up to date, and it does provide the starting point for the development of more detailed procedures.

To show how Figure 6.18 can be further developed, it is assumed that the facility has four operating areas.

1. Area 100 (Utilities)
2. Area 200

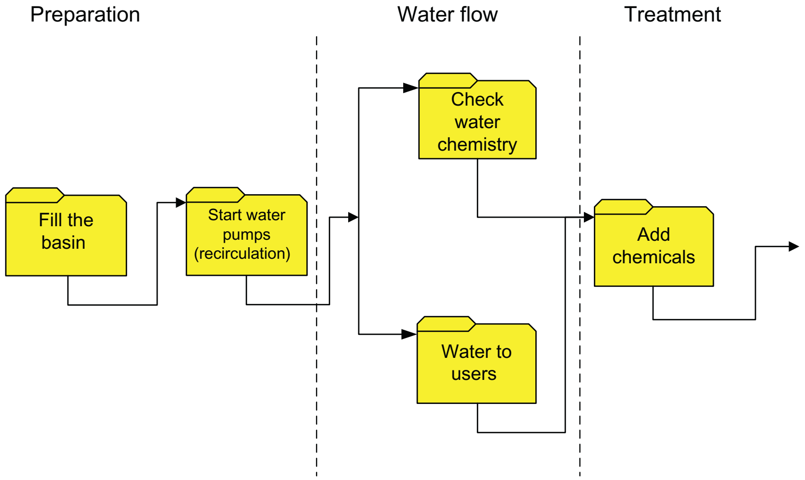


FIGURE 6.21

Level 4 of the manual (start the cooling water).

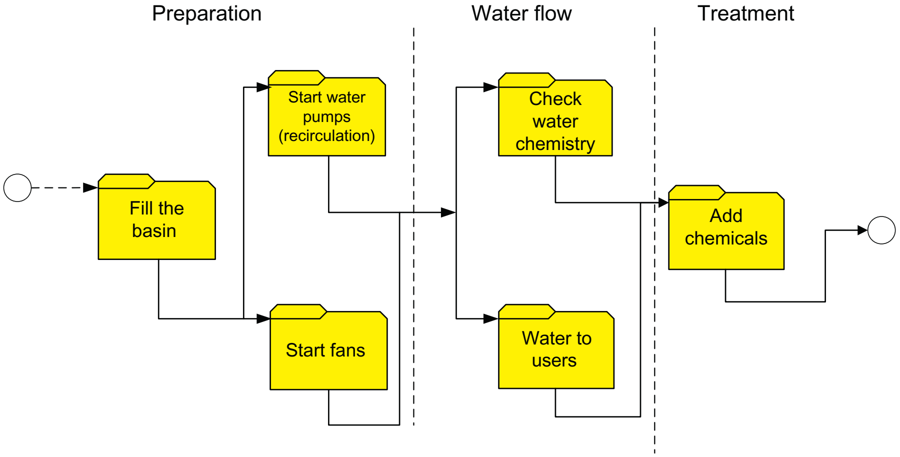


FIGURE 6.22

Sequential layout with new procedure.

3. Area 300
4. Area 400

The first step in the start-up is to get the utility systems started. Then Units 200 and 300 are started in parallel. When they are both up and running, Unit 400 can be started. This sequence is illustrated in Figure 6.19.

Once more, Figure 6.19 represents a complete operating manual; one that is complete, accurate and up to date. Although no detail is provided, even at this stage some useful guidance is provided: the operators know not to start Unit 400 until Units 100, 200, and 300 are up and running.

Figure 6.19 is further expanded in Figures 6.20 and 6.21.

The module "Start Utilities" has been expanded, although the icon labeled "Start Utilities" remains on the drawing for completeness. However, it has been shaded out and the connecting lines to and from it have been removed to indicate that it is no longer functional. It has been divided into six separate utility systems. The logic of Figure 6.20 shows that neither the cooling water nor the steam systems can be started until the firewater, instrument air, and facility air systems are operating.

One section of the facility—the nitrogen system—is not connected to the other modules because nitrogen system is not currently in use. However, plans are in place to use nitrogen at a later date; consequently, a place holder for the procedures to do with nitrogen is provided in Figure 6.20.

The structure shown in Figure 6.20 continues to be developed in greater levels of detail until all the operating modules have been identified. For example, the module "Start Cooling Water" can be developed as shown in Figure 6.21.

Figure 6.18 shows that the "Start the Cooling Water" section of the manual now consists of five modules or file folders. Each folder represents a module within the overall system structure for starting up the cooling tower. The folders themselves have been divided into three groups: Preparation, Water Flow, and Treatment. Each of the file folders or modules shown in Figure 6.18 is an operating procedure made up of operating or task instructions.

The first two modules (Fill the Basin/Start the Water Pumps) are in the "Preparation" section. The modules must be carried out in the sequence shown, i.e., filling the basin of the tower must be done before any other actions are taken. It must then be followed by the starting of the main cooling water pumps on recirculation (i.e., water from the pumps flows immediately back to the cooling tower without going to any of the users).

The next two modules (Check Water Chemistry/Water to Users) fall into the "Water Flow" section. These two modules can be executed in parallel, i.e., the order in which they are carried out relative to one another is not important. However, both have to have been completed before moving on to the "Treatment" section, which contains just one module—"Add Chemicals."

It is possible for one module to be called upon by many different operating sequences. Indeed, it is this capability that provides one of the strongest incentives for the use of a modular system. For example, the troubleshooting procedures for any of the shell and tube heat exchangers in the system can call on the "Check the Water Chemistry" module. That module is "publicly available" to any other sequence of operating tasks.

ADDING AND REMOVING MODULES

One of the advantages of having a clearly defined structure for the operating manual and its component procedures is that it is quite simple to add or remove modules. For example, in the case of Figure 6.21 it may be decided that a new procedure entitled "Start the [Cooling Tower] Fans" is needed. This new procedure will be carried out in parallel with the existing "Start Water Pumps" procedure. It must be complete before the "Water Flow" set of procedures can be started. The updated structure is shown in Figure 6.22.

Table 6.5 Names and Numbers for Start-Up Modules

Operating Procedure	Number
Start the utilities	1.100
Start the cooling water	1.100.4
Fill the basin	1.100.4.1
Start the water pumps	1.100.4.2
Start the fans	1.100.4.3
Check the water chemistry	1.100.4.4
Flow water to the users	1.100.4.5
Add treatment chemicals	1.100.4.6

NUMBERING THE MODULES

Each module/procedure is given a unique number and name. For this example, all start-up modules begin with the number "1"; the numbers for steady-state procedures, shutdown, and emergency procedures are "2," "3," and "4," respectively. Modules in the utilities system start with the number "100"; those to do with the cooling tower use the number "4." Hence, any procedure to do with the start-up of the cooling tower will have the numerical prefix "1.100.4." The numbers for the modules shown in Figure 6.22 are provided in Table 6.5.

The first two procedures—"Start the Utilities" and "Start the Cooling Water"—are shown in strikeout format to indicate that they do not actually appear in the operating manual. They have been developed into the more detailed procedures shown below them.

Once a module has been assigned a number then that number always stays with it. If additional modules are added, they are given the next numbers in the sequence. If a module is removed, then its number is "retired" in the manner in which the numbers of famous sports players are retired.

The manner in which operating procedures can link to one another is illustrated in Figure 6.23. In the case of the cooling water example, the module 1.100.4.4—Check the Water Chemistry—will have a series of instructions to do with checking the chemical composition of the cooling water. IF the composition is not what it should be THEN the sequence of will flow to the module 1.100.4.6—Add Treatment Chemicals—ELSE the sequence will flow on to the next set of modules.

MODULE DESIGN

Almost all operating procedures (either paper- or web-based) are organized into the following three sections:

- A Title Block
- The Operating Instructions
- An Authorization Block

The title block provides a name and unique identifier for the procedure, the operating instructions tell the operator what actions to take, and the authorization block provides information to do with signature authority and release dates.

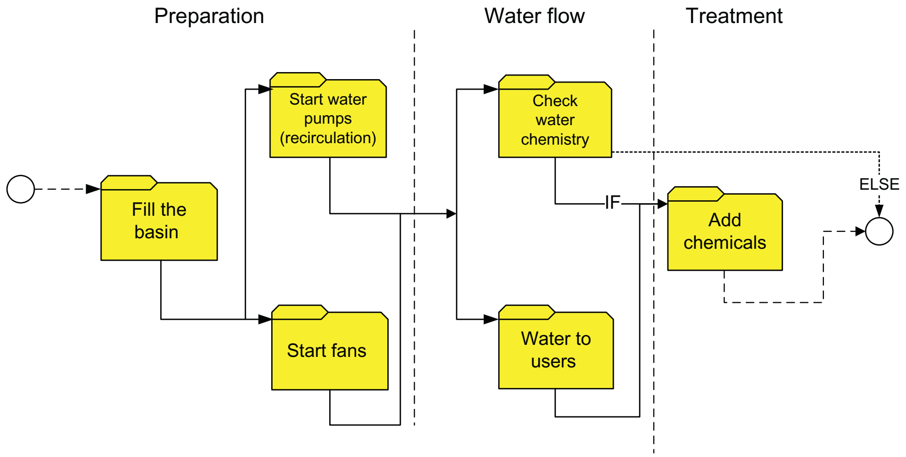
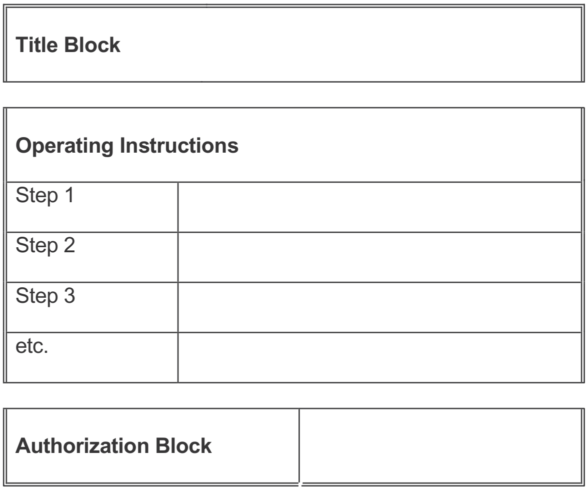


FIGURE 6.23

Use of conditional instructions 2.



Title Block	

Operating Instructions	
Step 1	
Step 2	
Step 3	
etc.	

Authorization Block	

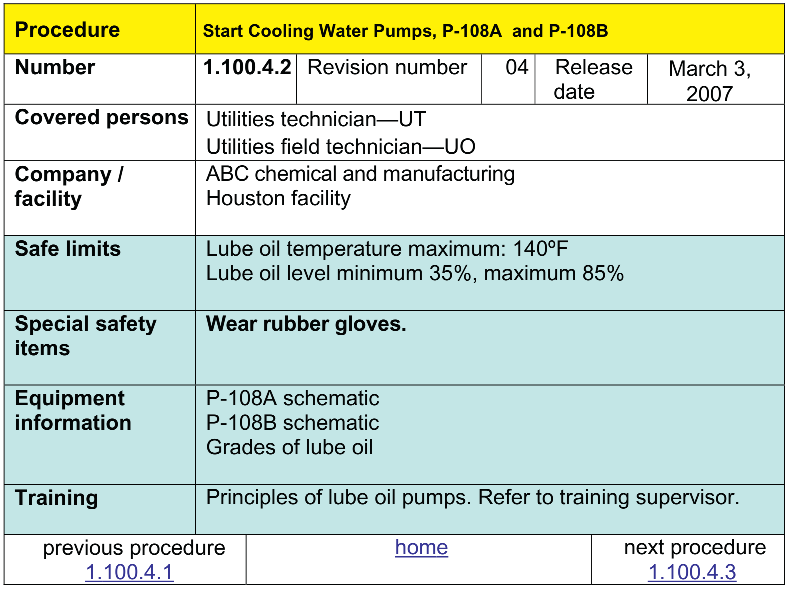
FIGURE 6.24

Three-section module layout.

The way in which the three sections can be laid out is illustrated in Figure 6.24. The location of the boxes on the page is not critical. For example, some companies prefer to place the authorization block at the top of the page (or else they group the authorization blocks in a separate section).

THE TITLE BLOCK

The Title Block can contain the following elements. (In practice, it will not usually be necessary to include them all, but they are shown here for completeness.)



Procedure	**Start Cooling Water Pumps, P-108A and P-108B**				
Number	**1.100.4.2**	Revision number	04	Release date	March 3, 2007
Covered persons	Utilities technician—UT Utilities field technician—UO				
Company / facility	ABC chemical and manufacturing Houston facility				
Safe limits	Lube oil temperature maximum: 140°F Lube oil level minimum 35%, maximum 85%				
Special safety items	**Wear rubber gloves.**				
Equipment information	P-108A schematic P-108B schematic Grades of lube oil				
Training	Principles of lube oil pumps. Refer to training supervisor.				
previous procedure 1.100.4.1	home		next procedure 1.100.4.3		

FIGURE 6.25

Example of a title block.

- Module name
- Purpose of the module
- Special safety considerations
- Discussion
- P&IDs and other reference documents
- Company/Facility
- Module number
- Page number/Date of issue

One of the practical problems that procedures writers face is how much detail to include in the Title Block. It is tempting to include a large amount of information, particularly concerning safety issues. However, if the amount of information becomes so large as to make the actual operating procedures difficult to use, then the net effect on the operation may be deleterious.

The Title Block not only names the procedure that is being described, it also provides background information and precautions to do with that procedure. Figure 6.25 is an example of a complete Title Block.

Procedure name

The procedure name should accurately and completely describe the purpose of the module. The name must be unique; and no other title name should be identical, or closely similar. The name should be as descriptive as possible and should contain as much detail as possible. For example, "*Add water treatment chemicals to Cooling Tower, CT-108*" is a more helpful and precise title than "*Treating Cooling Water.*"

It is suggested that a procedure name contain the following three parts:

1. The first part of the name is a verb that describes the action to be taken (in this example, the operative verb is the word "Start"). The verb can be either in the imperative tense (as in this example), or could express continuous action—which in this case would be "Starting." Either is acceptable, but a consistent approach should be followed throughout.
2. The second part of the title refers to what is being acted upon. In this example, the treatment chemicals are being added to the cooling tower basin, so they are the object of the verb "Start."
3. The final part of the title describes where the action is to take place. This part also provides pertinent equipment numbers.

In spite of the general need to minimize the number of words in a procedure, it is suggested that the full name and number for each equipment item be used every time that it is referred to. The avoidance of ambiguity is more important than minimizing the number of words.

Module number

Each procedure must have a unique number. In this example, the first number "1" indicates a start-up procedure; the number "100" refers to the utility area; the number "4" refers to the cooling water system; the final number "2" refers to this particular procedure.

Purpose of the procedure

Although not shown here, a block can be used to provide an overview as to why the procedure has to be carried out, and what its purpose is.

Revision number

The module in this example corresponds to Revision 04. This does not mean that all the other modules are reissued at the same time. It is quite likely that other modules in this set will have different revision numbers because the revision applies only to that module, not to the complete manual. The location of the sections that have changed as a consequence of the revision is shown by putting the revision number in the appropriate column of the instructions.

Although not done in this example, it is possible to include the Revision Purpose at this point, i.e., to describe what has changed since the last update to the procedure.

Date of revision

The date of revision is the date of *issue*, not the date on which the module was *written*. Temporary procedures should also include an expiration date. This line could also contain the date by which the module must be checked and/or revised. If the company is following the OSHA PSM standard, the module will require a review every 12 months.

Covered persons

This procedure involves two persons: the Utilities Technician (UT) and the Utilities Field Technician (UO).

The assignment of responsibility is particularly important when working with technicians from other units or with outsiders, such as truck drivers.

Company/Facility

This section of the Title Block provides detail as to which particular process and facility site is covered by these procedures. This is important if a company has more than one location because, once a standard design for procedures has been adopted, the procedures from different units will all look very similar to one another, and it is important to make sure that they do not get mixed up.

Safe upper and lower limits

One of the most important features of any operating procedure is a statement of the Safe Upper and Lower limits. In this example, a safe upper limit for lube oil temperature is provided, along with the upper and lower limits for the lube oil level.

Special safety items

A commonly occurring problem with respect to operating procedures is that the writers feel obliged to include all safety considerations in each procedure. Since most of these considerations are general, there is really no need to repeat them in each and every procedure. For example, if technicians are required to wear hard hats whenever they are outside, then stating the hard hat requirement in each procedure is redundant, and is against the spirit of minimalist writing. Indeed, the rule about wearing hard hats is not really a procedure—it is a condition of employment that should be covered in basic training.

If a particular operation has special safety considerations, then such considerations can be included within the title block, as shown. In this example, the biocide chemical has corrosive properties, so the operators need to wear rubber gloves to protect their hands and arms in the event of a minor spill of the chemical.

Equipment information

It can be useful to show the pertinent P&ID numbers and information concerning other reference documents in the Title Block. In this example, the relevant P&ID number is provided, along with the two MSDS for the two treatment chemicals.

Training

The final section of the Title Block provides information about basic training materials as they pertain to this procedure.

THE OPERATING TASK INSTRUCTIONS

The next section of the module shown in Figure 6.26 consists of the actual operating instructions in which the instructions are laid out in columns. As with the Title Block, in most cases it will not be necessary to use all of these columns. For example, if all of the actions in a procedure are carried out by one person, there is no need to have the “PERSON” column. Instead, the person carrying out the instructions can be identified in the Title Block just once.

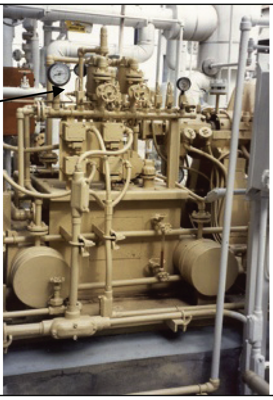
	By	Action	√	Discussion/Illustration
8		. . .		
9	UO	Check the lube oil temperature using TI-7103A-2. TI-7103A-2		
			Never start the lube oil pump if the lube oil temperature is above 150°F.	
10	UO / UT	If the lube oil temperature is above its safe limit THEN 1. Stop this procedure **AND** 2. Inform the powerhouse technician		Information regarding troubleshooting lube oil systems is provided in procedure 01-GEN-34.
11		. . .		

FIGURE 6.26

Example of operating task instructions.

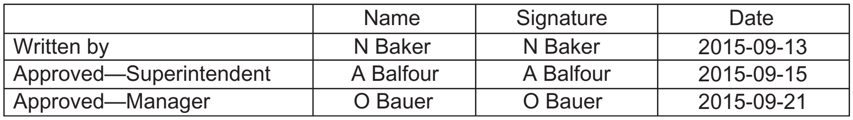
Figure 6.26 shows just a few of the sequential instructions. The full procedure will have all of the instructions included.

Step number column

The first column contains the step number. The order in which the instructions are listed is usually critical, i.e., they must be carried out in the sequence shown, unless stated otherwise.

Person

The second column identifies the person who has to perform the action. In this example, the symbols used for the job classifications involved in this procedure are explained in the section to do with "covered persons" in the Title Block.



	Name	Signature	Date
Written by	N Baker	N Baker	2015-09-13
Approved—Superintendent	A Balfour	A Balfour	2015-09-15
Approved—Manager	O Bauer	O Bauer	2015-09-21

FIGURE 6.27

Example of an authorization block.

If all of the instructions in one module are to be carried out by just one person, then this second column in the operating instructions can be removed, and the person(s) responsible for the actions can then be identified in the title block.

Action

The action column tells the operator what to do. The following guidelines are suggested.

- Only one action is listed for each instruction. If there are two or more action steps, they should be separated and each given its own row in the module.
- All instructions should, where possible, be single sentences, starting with a verb in the imperative tense.
- Adverbs such as "slowly," "gradually," "soon," and "quickly," should be avoided. It is much better to replace adverbs with quantitative terms such as "5 minutes" or "10 degrees per hour." The use of scale values such as "roots" of flow should be avoided.

Discussion/Illustration

The fourth column provides some general discussion to do with the step just described. In addition, troubleshooting information can be provided in this column, which can also be used to describe the anticipated response of the system to the action taken. For example, if the instruction is to do with starting a pump, then the response could be that the discharge pressure should be above a certain value, and that the pump motor should be drawing a specified number of amps. If actual results do not correspond to these anticipated values, the operator knows that he needs to identify the cause of the discrepancy.

The Discussion/Illustration column can also be used for general discussion and explanation. For example, it is a convenient place to provide discursive information that may be useful to an inexperienced technician but that the experienced technician does not need. Graphics and pictures can also be located in this column.

THE AUTHORIZATION BLOCK

The third section of the module shown in Figure 6.24 provides the authority associated with its issue. Figure 6.27, which is an example of this block, has just three rows.

The process for the signing of procedures can often constitute a bottleneck. There are usually three reasons for this difficulty.

1. Too many people are asked to sign the procedure. Hence it takes a long time for the procedure to wend its way through the system. The stated reason for having many signatures is that multiple checks are put into place. However, if the issuance of the procedure is seriously

delayed, safety and efficiency could be compromised. A balance must be struck between thoroughness and speed.

2. The people who know the unit well, and whose signature is therefore of the highest importance, are also the people who are likely to have the most to do with other activities. They will put off signing the procedures until "they are not busy."
3. The person who signs a procedure as being correct and complete is putting himself and his company in potential legal jeopardy. If an accident occurs, and errors with the procedures are implicated in the cause of the accident, then the signer may be challenged in court (either criminal or civil). For these reasons, managers are often reluctant to sign procedures until they are absolutely sure that those procedures are correct.

Because the signing-off process can be so time-consuming, it is important to pay considerable attention to its design and implementation. Basically, there are three types of signature authority.

The first signature is from the person(s) who actually wrote the material. This person could be both the subject matter expert (SME) and the technical writer (if used). Their signature states that they have prepared a set of instructions to the best of their ability, and that the instructions are, as far as they can ascertain, accurate, complete, and usable.

The second signature comes from someone who knows the process being described extremely well indeed. Often this will be a supervisor or senior technician. Their signature states that they have reviewed the written procedure and that, as far as they can determine, it is accurate and complete.

The third signature is that of the facility or operations manager. He or she is not likely to know the process well enough to comment on the technical content. What their signature states is the management systems for writing procedures are in place, that these management systems address all appropriate regulations and standards, and that the systems were followed during the execution of this assignment.

The three rows in Figure 6.27, which are discussed below, illustrate the concepts just described.

Written by

The first line provides space for the name of the writer(s) of the procedure. The term "writer" in this context refers to the technical expect (usually an operator or supervisor) who provided the technical knowledge for the procedure. By signing this box, Mr. Baker is saying, in effect, "I am technically knowledgeable about the operation described in this procedure, and the instructions in the procedures represent, to the best of my knowledge, a safe and effective way of conducting this operation."

Note that the writer does not claim that the instructions are accurate—he merely states that they are accurate to the best of his knowledge.

Approval—superintendent

The second signature certifies that a technical check was made on the procedure—ideally by walking it through step-by-step in the field. In this example, the Area Superintendent, Mr. Balfour, provides the certification.

Approval—manager

In this example, the Area Manager, Mr. Bauer, is stating that the correct process for writing and publishing procedures was followed, and this particular procedure conforms to the requirements of the PSM standard (and any other pertinent rules that may apply).

Authorization sheet

In order to save space, the authorization blocks can be removed from the individual modules and put on a single sheet, as shown in Figure 6.28. This sheet can be stored in a separate place from the working procedures.

OVERALL MODULE

Figure 6.29 is the overall operating module, incorporating the Title Block, the Instructions, and the Signature Sheet.

Various features of Figure 6.29 are illustrated through the use of callouts. An explanation for each of these callouts is provided in Table 6.6.

LINKS TO OTHER PROCEDURES AND MANUALS

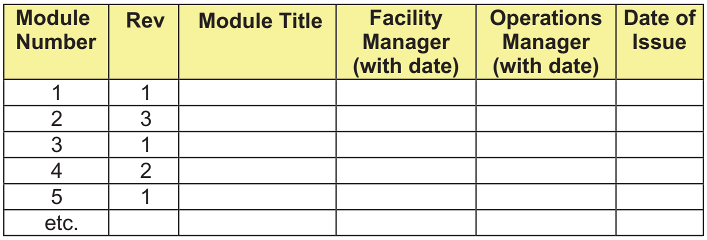
Many operating procedures are to be used as part of an overall start-up or shutdown sequence. In order to minimize the chance of a procedure being overlooked, forward and backward links to other procedures can be provided as shown at the bottom of Figure 6.29.

As has already been discussed, most technicians need checklists more than they need detailed procedures. Therefore, the instructions in Figure 6.29 can be quite short and even somewhat cryptic. If the operator would like to have more detail, all he or she need do is click on the appropriate hyperlink and more information will appear in a pop-up window.

A link to the home page for the operating manual is also provided.

LINKS TO TECHNICAL INFORMATION

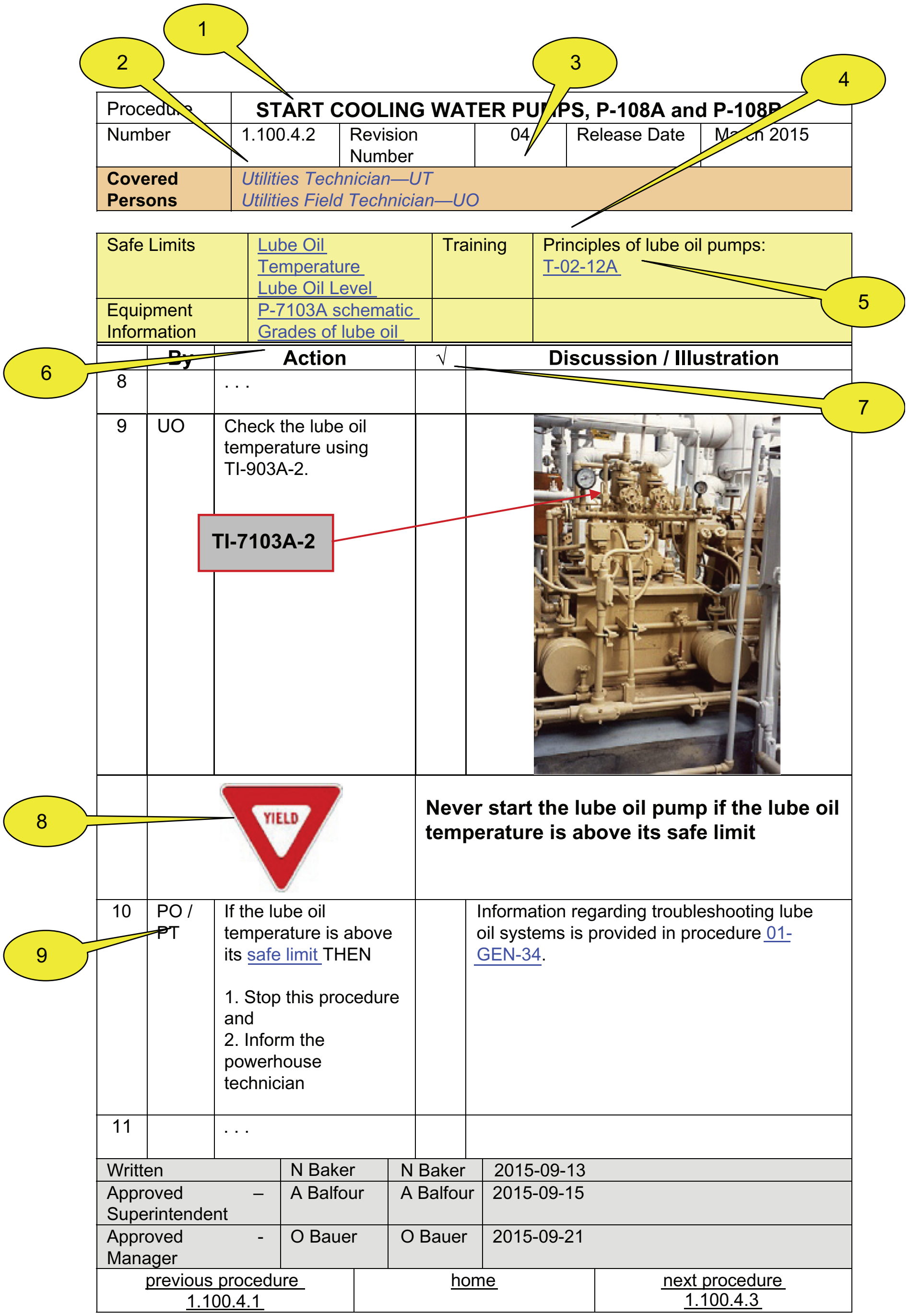
Providing links to technical information as shown in the Title Block of Figure 6.26 means that it only need be updated in one location. For example, with paper procedures, if a pressure vessel is rerated to a higher pressure someone will have to go through all the procedures related to that vessel to make sure that the new value has been corrected wherever it is used. With hyperlinks such an effort is not needed because the link will direct the operator to the latest information.



Module Number	Rev	Module Title	Facility Manager (with date)	Operations Manager (with date)	Date of Issue
1	1				
2	3				
3	1				
4	2				
5	1				
etc.					

FIGURE 6.28

Authorization sheet.


1
2
3
4
5
6
7
8
9
TI-7103A-2
YIELD

Procedure	**START COOLING WATER PUMPS, P-108A and P-108B**				
Number	1.100.4.2	Revision Number	04	Release Date	March 2015
Covered Persons	*Utilities Technician—UT* *Utilities Field Technician—UO*				

Safe Limits	Lube Oil Temperature Lube Oil Level	Training	Principles of lube oil pumps: T-02-12A
Equipment Information	P-7103A schematic Grades of lube oil		

	By	Action	√	Discussion / Illustration
8		. . .		
9	UO	Check the lube oil temperature using TI-903A-2.		
				Never start the lube oil pump if the lube oil temperature is above its safe limit
10	PO / PT	If the lube oil temperature is above its safe limit THEN 1. Stop this procedure and 2. Inform the powerhouse technician		Information regarding troubleshooting lube oil systems is provided in procedure 01-GEN-34.
11		. . .		

Written	N Baker	N Baker	2015-09-13
Approved – Superintendent	A Balfour	A Balfour	2015-09-15
Approved - Manager	O Bauer	O Bauer	2015-09-21

previous procedure 1.100.4.1	home	next procedure 1.100.4.3

FIGURE 6.29

Example of a full module.

Table 6.6 Annotations for Figure 6.29

Call Out	Discussion
1	The procedure has a unique name that fully describes its purpose and intent
2	The procedure also has a unique number that can be called from other procedures
3	The revision number and the date of release are shown. Policy regarding training should be established also, i.e., management must decide if a procedure is "released" if not all the operators have been trained in it
4	The persons who are expected to know the procedure are identified
5	A link to a Training Module is provided
6	Links to information are provided (equipment integrity and safety information) are provided. The hyperlink will take the operator to relevant documents such as engineering data sheets or MSDS. With a paper-based system the practical difficulties of finding such information means that the operator is less likely to make the effort to go look for it
7	The operator enters a response or sign-offs in this column
8	The warning precedes the instruction to which it appertains
9	Safe Limit values are provided in the header of the procedure, and also in the body, as required. A link to troubleshooting information is provided on the same line of the procedure
10	Links to other procedures are provided

Some typical technical information sources may be called for by the operator are as follows:

- Equipment Information
- Safe Upper and Lower Limits
- Drawings, particularly P&IDs
- MSDS
- Personal Protective Equipment (PPE)

The above list is not all-inclusive—additional types of information will be needed at different times. However, most of the needed information will probably fall into one of the five categories shown.

TRAINING

Training can be integrated with the modular concept of operating procedures. Along with the Action and Response columns, there can be two training columns: one of them called "Why?" and the other "How?" The "How?" column provides more detail as to how to do a task. The Response/Discussion column alluded to in the previous chapter can fill this role. The "Why?" column provides an explanation, and so is education rather than training.

TWO-PAGE MODULES

When an operator opens an operating manual, he or she is looking at two pages. Therefore, as a means of structuring the manual, it makes sense to organize the procedures and instructions into modules that take up just two pages. If a procedure is too big for just two pages then it can be broken down into two smaller modules.

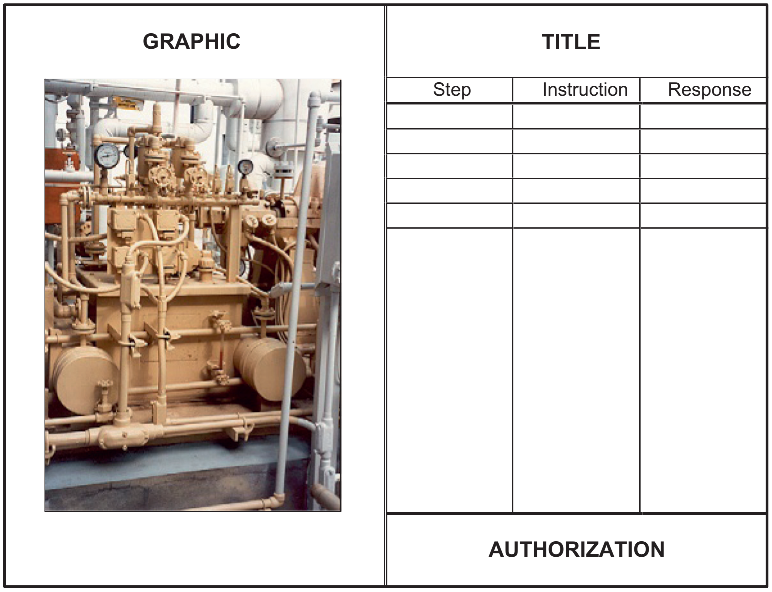


FIGURE 6.30

Example of a two-page module.

One way of achieving the goal of two-page modularity is to have a page of text and a page of graphics facing one another. (A *page* refers to one side of paper, a *sheet* is the physical piece of paper; it has two pages—front and back.) The text is put on the right-hand side because it is where most readers automatically look for written material (it is how single-page reports are laid out, for example). Therefore, each module actually consists of a total of four pages—with the two interior pages containing the instructions and graphics to do with that module. Figure 6.30 illustrates the two-page concept.

Placing text and graphics opposite one another in this fashion means that two sheets of paper are used. Therefore, a complete module has four pages. The first page of the first sheet shows the title of the module. The second page of the first sheet has the graphic on it, as shown. The first page of the second sheet has the text. The second page of the second sheet (the fourth page of the complete module) is used for overflow text.

If a change is to be made to this particular procedure, all that has to be done is to pull out this two-sheet/four-page module, rewrite it, and reinsert it. *Nothing else changes*. This approach to modularity matches the software subroutines analogy discussed earlier in this chapter. The maintenance of operating procedures now requires much less effort than the normal process of removing pages, changing them, and then reinserting them, all the time hoping that it will not throw the complete page-numbering system off. If a module changes no other module is affected or needs to be changed.

One of the reasons for using the text-graphic layout shown in Figure 6.30 is that, before the introduction of modern word processing and publishing software, it was difficult to integrate the two on the same page. The page has to be formatted with space for the graphic, the graphic has to be inserted in that space, and then the combined elements have to be copied. This is a labor-intensive process. Modern software now makes the integration of text and graphics considerably easier, hence the incentive for the two-page concept is not as strong as it was. Nevertheless the two-page approach does provide a convenient, prestructured format that all the writers can follow.

CONTENT DEVELOPMENT

Having designed the overall system, and developed a template for each procedure, the next step in the procedures-writing process is to develop the content, i.e., to prepare the actual operating instructions that are to go into the procedures. The development of high-quality content is the most important part of an operating manual project. If the content is correct, but the appearance of the manual is shabby, or the instructions are difficult to follow, the manual can still assist the operator to do his or her job. However, if the content is incorrect, or if it is missing crucial information then no amount of window dressing will make the manual valuable to the operator. The content of an operating manual must be complete, accurate, and up to date.

LEVEL OF DETAIL

It is not always clear as to how much detail should be provided. Many writers of operating procedures do not know how much detail to provide. Instructions can range all the way from high-level procedures such as, “Fill the Tank,” all the way to detailed valve-by-valve and step-by-step instructions.

In practice, the problem of how much detail is needed often tends to resolve itself naturally. During the writing process, the operators will describe the operations at the level of the detail that they need. If they are writing about the unloading of a truck of highly hazardous chemicals, or the start-up a high-pressure reactor, the operation will be described minute detail. However, procedures for checking pressure gauges in a utility system will probably be quite brief. The level of detail will also depend on the user. A trainee who has very little facility experience will need considerable detail. An experienced technician, on the other hand, needs little more than high-level checklists to help him work through tasks with which he is already very familiar.

Operating instructions are generally written at one of the following three levels of detail.

Level 1—overview/checklists

At the first level, the manual contains just broad, general statements, such as “Commission the Condenser” or “Load the Truck.” Little or no facility-specific detail is provided. This level of detail roughly corresponds to the module titles.

Once a procedure has been written, it is normal to develop a matching checklist. Given that the operator has been trained in the use of the procedure, the checklist is what will actually be used in the field, and in the control room. The Operating Procedures will then serve essentially as reference documents.

One of the strongest justifications for the use of a checklist is that it can help make sure that an action is actually carried out. By marking the check box, the operator states that he actually has performed the required action, and has not overlooked or accidentally skipped the step. The use of checklists can also help ensure that actions are taken in the correct order.

Checklists also provide a means for the operator to communicate with his supervision. For example, he might note that there was a difficulty with one of the steps in the module, although it was not of such severity to prevent the action sequence from being continued. For example, the operator may note that the pump cavitates while he is carrying out the following instruction: "Open the bypass around FCV-121." Therefore, he could write on to the check list that he had noticed a problem.

A checklist will look similar to the Operating Procedure, except that the Response/Discussion and Revision Number columns can be omitted. Most of the information in the Title Block can be omitted.

In general each step in a checklist will have a small number of associated task instructions. For example, if the checklist instruction states, "Check the tank level," the detailed procedures may provide a set of task instructions to do with which instrument to use, what the level should be, and what to if the level is out of range.

Level 2—equipment description

The next level of detail for operating instructions, which is probably the most widely used, is to have instructions that are at the equipment level. The procedure provided in Figure 6.29 shows this level of detail.

Level 3—valve detail

The final level, which is uncommon on process facilities (although it is standard in nuclear facilities) provides exact step-by-step instructions concerning opening and closing valves, and pressing instrument or DCS buttons. This level of detail may be found on process facilities when providing instructions for the handling of very hazardous chemicals, e.g., the unloading of hydrogen fluoride from a tank truck or trailer.

If it is decided to write procedures at this level, a valve/pump checklist such as that shown in Table 6.7 can be useful, and often has to be developed anyway when working out instrument logic. It shows the status of each control valve and pump on the unit at the conclusion of each operation for each P&ID. Even if this type of list is not included in the final product, it is useful for the procedures writers to develop one as a check on their own work. Table 6.7 is also handy for catching oversights, such as forgetting to turn on a pump before filling a vessel.

Table 6.7 Valve/Pump Checklist

P&ID	Step	1	2	3	4	5
1000	P-100	Off	On	On	On	On
1000	P-101	Off	Off	Off	Off	Off
1001	PCV-103	Closed	Closed	Open	Open	Open
...	...	...	...	...	...	...

SOURCES OF INFORMATION

Those developing the content of an operating manual have various potential sources of information, including the following:

- Existing procedures
- Interviews and discussions with experienced technicians
- Engineering information
- Vendor manuals
- PHA

Existing procedures

For facilities that are already operating an existing set of procedures is usually in place. These procedures may be out of date, incomplete, and difficult to use (which is why new procedures are being written). Nevertheless the content of the old procedures is often of great value, even though all the instructions in them will have to be checked before they are incorporated into the new manual.

If the manual is being written for a new facility, it is often possible to obtain the procedures from other, similar facilities. These borrowed procedures can serve as a useful starting point.

Technician interviews

On facilities that are already in operation much of the information needed for the manual will come from the operators who are working with the unit on a daily basis. The writer's biggest challenge will be to organize the operator's thoughts and experience, and to have him verbalize on actions that he carries out on a routine basis.

For example, on one facility, a highly experienced supervisor stated that, at the start of each shift, he climbed to the top of one of the highest distillation columns in the unit so that he could look around to make sure that, "Everything was OK." The challenge that the procedures writer faced was to determine exactly what was meant by the term "OK." The supervisor was actually carrying out a check to make sure that there were no obvious problems such as leaking lines, improperly controlled maintenance tasks or inappropriate vehicle movements. But, until the procedures-writing project came along, he had never verbalized these thoughts, or written them up in the form of a checklist.

Engineering information

Engineering information in the form of equipment data sheets, instruments specifications, and maintenance instructions provide a necessary background to the operating instructions.

Vendor manuals

Vendor manuals can be an excellent source of material that can be used in the development of operating manuals. Typically, the information that they provide is more oriented toward maintenance than operations.

Process hazards analyses

The purpose of a PHA is to identify hazards that could lead to major incidents. A PHA can also serve as a means of developing the information needed in operating procedures, particularly with respect to troubleshooting and emergency conditions.

A PHA can also be useful for identifying the safe upper and lower limits. It is often difficult to actually determine those limits—particularly on facilities that are more than a few years old, and for which the original design bases are no longer available or valid. During the course of the PHA discussions, experienced operations, and maintenance personnel will often relate their own experiences of incidents and near-misses. For example, they will say something like, "We once got the reactor temperature above 350°C, and had a high pressure excursion." This experience indicates that 350°C represents a safe upper limit for temperature.

THE PROCEDURES-WRITING TEAM

Traditionally procedures are written by technical specialists, often chemical engineers working in the process engineering group. These people are likely to have an excellent understanding as to how the process works, but they may not be as knowledgeable about the actual operations. The best manual is one that is written by those who will use it, i.e., the operators and the maintenance technicians, supported by the process engineers.

A facility that has multiple shifts will find that there are differences of opinion as to the best of operating. Therefore, when writing the manual, the workers on each shift should be provided with an opportunity of discussing how they would run the unit; out of the ensuring discussions, it is to be hoped that the best type of operation will be uncovered. Although management will give responsibility for creating the procedures to an operations team, the actual writing of the manual should still be done by someone who is good at writing and editing.

WRITING AND PUBLISHING

The process of writing the procedures can raise a subtle, yet profound difficulty: those who write the procedures may not communicate in a manner that reflects the way the operators actually think and work. For example, if the procedures are written in a rigid and highly structured manner by an engineer, an experienced operator may feel that they do not really express how he actually runs the unit. Many operators tend to work a relatively eclectic manner—they perform numerous tasks in parallel depending on what "feels" right at that point in time (of course, they still have to carry out tasks in a safe manner). This approach to operations is not inherently worse or better than the more formal or linear approach; it is just different. It is the responsibility of the people writing the procedures to make sure that not only are the procedures correct and well written, but also that they reflect the way in which the operators actually work and think.

Generally, the ownership and maintenance of procedures is seen as a responsibility of the operations department. However, this department is not likely to have a built-in writing staff.

Moreover, their key people are usually very busy with their other work, and so they tend to put off the writing of procedures almost indefinitely. Nevertheless, it is vital that the needs of those in the operations and maintenance departments are met and that the manual addresses their knowledge, goals, concerns, opinions, and needs. Ownership is always important, everyone likes to feel involved in what is going on and to feel that they are being listened to—that is basic human nature. In the case of an operating manual, if the operators feel responsible for its creation and for its ongoing upkeep, they will be much more willing to use it and to improve it than if it is merely provided to them by another group of people such as their technical staff or an outside consulting company. If it is accepted that the operators do indeed own and create the manual, then the task of everyone else (management, engineers, writers, and consultants) is to provide assistance to the operators in the development of *their* manual—not the other way around.

PROJECT ORGANIZATION

The writing of an operating manual is a project just as installing a new piece of equipment is a project. Therefore, standard project management issues such as defining the scope of work, creating a budget and tracking progress must be followed. The development of an operating manual can be divided into the following seven steps:

1. Define the scope of work.
2. Create the team.
3. Develop a detailed plan.
4. Collect information.
5. Write the procedures.
6. Review and sign.
7. Publish.

1. DEFINE THE SCOPE OF WORK

As with any project, it is vital that the scope of work be properly defined, otherwise the project team and the final customers will be in constant confusion, and misunderstandings will abound. The responsibility for defining the scope of work lies primarily with the client—in this case, the operations or maintenance department that will be using the procedures once they are written and published.

The following are key elements in understanding the scope of work:

- The physical area and equipment covered
- The needs of the users of the published procedures
- Types of procedure required
- Pertinent regulations and standards to be addressed

PHYSICAL AREA/EQUIPMENT COVERED

Usually procedures are written for a specific area, such as the boilers or the reaction section. Generally, defining the covered areas is not a problem. However, it is important to understand where the boundaries lie, particularly with regard to utility systems. It is also important to ensure that the procedures link properly with the procedures in the adjacent areas.

USERS

As already discussed, the manual has many potential users, so it is important to define who they are, and what they want. Most manuals are written in the form of checklists for the experienced technicians, and more detailed instructions for those with less experience.

TYPES OF PROCEDURE

The types of procedure to be written have to be listed. For example, if a troubleshooting manual is to be written the scope of work will increase substantially. Also the required level of detail must be thought through before the project starts. Clearly an operating manual that provides instructions at the valve level is going to take much longer to write than one that discusses major equipment items only.

JOB TASK ANALYSIS

The purpose of a Job Task Analysis (JTA) is to analyze some particular action in depth, so that effective procedures for that job can be written. Typically, JTA has been used most in high hazard industries, such as the operation of nuclear power facilities.

A JTA usually works by asking the following questions in the context of a particular task, or assignment.

1. What is being done?
2. Who is doing it?
3. When is it done?
4. What skills, abilities and training are needed?
5. How is information communicated?

For those companies that are developing a brand new operating manual (or who are essentially starting over), it makes sense to develop the overall structure of the Manual, as discussed in earlier sections of this book, before starting on detailed JTA. JTA is time-consuming and expensive, and it is important to make sure that it is done only on those tasks that are properly defined and understood. Also, the writing of JTAs provides an opportunity for management to improve and upgrade the way in which tasks are carried out. The upgrade analysis should be deferred until the overall structure of the operating manual is developed.

DESIGN OF THE MANUAL

The overall design for the manual and procedures must be decided upon at the beginning of the project. The modular, top-down concepts that have been discussed in previous pages stress the importance of developing the design before starting the actual writing process.

REGULATIONS/STANDARDS

If the facility for which procedures are being written is covered by a regulation such as OSHA's PSM standard, it is important to ensure that the design and content of the manual addresses the specific regulatory requirements.

WRITER'S GUIDE

The Writer's Guide is used by the project team to direct their work. The Guide includes the information described above; it also provides the rules to do with formatting, layout and writing style.

2. CREATE THE TEAM

The writing of an operating manual is a team activity. It is highly unlikely that one person will possess the all of project management, operating, technical, and publishing skills that are required to prepare a good manual. Also interaction between the team members will improve the quality of the final product and will maximize employee participation.

A typical operating procedures team consists of the following personnel (in practice, one person is likely to fill two or more of the roles, but it is still important to clearly distinguish between these responsibilities).

- Steering Committee
- Project Manager
- Project Lead
- Operations Expert(s)
- Technology Expert(s)
- Interviewer-Writer(s)
- Publisher/Webmaster
- Reviewers/Signers

STEERING COMMITTEE

The elements of a PSM program, including operating procedures and training, are often sponsored by a management group, often known as the "steering committee." The project manager for the procedures-writing effort reports to this committee. The purpose of the committee—which typically includes representatives from operations, maintenance, and safety—is to ensure that the needs of the users of the operating manual are met.

The committee will issue the project team with a charge or scope letter describing the goals and objectives of the procedures-writing project, and outlining the project management parameters (particularly budget and schedule). The committee will also ensure that the appropriate links with the other elements of PSM are in place, and that the appropriate risk management criteria are being used.

If the procedures-writing team wishes to make a significant change to the way the project is being handled, such a change will have to be approved by the steering committee.

PROJECT MANAGER

The project manager is in charge of the overall project. He or she is responsible for all facets of the work, including technical quality, financial control, gathering resources, and scheduling. He does not necessarily have to be an expert on procedures or on the unit being described, unless he also serves as the project lead. The project manager must also have a global view of the procedures; he or she should understand as to how the procedures fit into the overall operational integrity management program.

One of the most important characteristics of the project manager is the ability to resist pressures and demands from other departments and managers, particularly with respect to the availability of experienced personnel. The experts working on the procedures are likely to be in high demand to perform their normal operations and maintenance tasks as well as helping with other activities such as hazards analyses. The project manager must resist the demands that will be made on the time of the experts, and make it clear that the writing of procedures is also a high-priority activity.

PROJECT LEAD

The project lead—who may be the same person as the project manager—is responsible for creating the operating manual, and for ensuring that the final product meets the needs of the operators and other users. For this reason, the lead will generally come from the operations department. The lead's particular responsibility is to ensure that the procedures are technically correct.

For all but the smallest project, the lead should be assigned to the writing of procedures on a full-time basis; he or she will have no other assignments until the procedures are finished.

TECHNICIANS

Assuming that the procedures are being written for a facility that is already in operation, one or more senior technicians or supervisors will be assigned to the team. A retiree often makes a good choice because he will not have scheduling conflicts and can be brought into the project on an as-needed basis. For the same reason someone who is on light duty can make a good team member.

If the facility for which the procedures are being written is new, or has been substantially altered from its previous mode of operation, it may be possible to borrow technicians from other facilities that use similar technology.

TECHNOLOGY EXPERT

Technology experts and SMEs understand the basic theory and design of the process. They do not necessarily have a detailed knowledge of how the facility operates, but they can provide insights as to why a certain operation works in the way that it does. They are particularly useful for establishing operating and emergency limits. The technology expert will often be the process engineer assigned to the unit, but assistance may be provided by other departments such as maintenance, instrumentation, and environmental.

INTERVIEWER-WRITERS

An interviewer-writer obtains the information from the process and operations experts, then writes up that information in an organized, useful, and readable manner using an agreed-upon template. He or she will generally have a good working knowledge of process facilities in general but does not need to be an expert on the process in question. This person must also be skilled in technical writing. For these reasons, the interviewer-writer will often be an outside contractor.

The interviewer-writer asks the experts how they operate their facility. The questioning can be quite open-ended and relatively unstructured. Once the knowledge has been captured, the interviewer will then organize the information into a structure of linked modules, as discussed in the previous chapter. He or she will then print out an early draft of the procedures and ask the process and operations experts to review it. The process of reviewing drafts can be repeated until the experts are satisfied that what is written down is an expression of their intent. The writer will also collect information from other sources, such as existing procedures and engineering manuals. If the operators actually write the first draft of the procedures, it is the writer's job to organize and edit them.

The advantage of using interviewer-writers is that neither the operators nor the technology experts are required to actually *write* the procedures (unless they want to—a most unusual situation). However, although SMEs rarely enjoy writing, they usually enjoy talking about their work, and they have little trouble in reviewing the written work of others.

PUBLISHER/WEBMASTER

The publisher is responsible for ensuring that the procedures are formatted correctly using an agreed-upon template. If the procedures are to be accessed *via* a web site, the publisher will normally work very closely with the webmaster (assuming that the two jobs are separate).

3. DEVELOP A DETAILED PLAN

A common problem to do with the writing of procedures is that the activity is not treated as a project in the same way as say the purchase and installation of a new piece of equipment would be. All too often technicians, supervisors, and engineers are asked to write the procedures "as time permits." Yet the writing of a manual normally requires a considerable amount of time and money.

Table 6.8 Representative Schedule

Month	1	2	3	4	5	6	Total
Write	10	45	45	15			115
Reviewed		10	25	60	20		115
Signed					25	90	115

Hence a project structure, including the creation of budgets, schedules, and resource requirements, is required.

The writing of operating procedures is not usually a high-priority activity—unless the facility is responding to a regulatory citation, or there has been a serious incident. This means that management will be tempted to "borrow" the operations and technical experts from the writing teams because these people are often needed to address short-term operating problems. Similarly, the operators and other technical experts are asked to review the draft versions of the procedures during the "quiet times" on their shift, or when they have some "spare time."

The development of a high-quality manual can take a long time; management must be prepared to make a long-term commitment to the effort and to stay the course. Hence a formal project plan for the writing and publication of an operating manual has to be prepared and implemented. Therefore, once the scope of work has been defined, and the team put in place, the next step is to prepare a schedule, progress metric, and budget.

SCHEDULE AND PROGRESS METRIC

A convenient method of organizing a manual writing is to build the program around the number of procedures or modules. Of course, not all procedures are the same: they differ in length, are of different complexity and may require different levels of information gathering. Nevertheless, using the number of procedures completed provides a consistent and easy-to-follow means of measuring progress.

Table 6.8 shows how a project can be organized. A total of 115 procedures is to be written and published over a period of 6 months. (As the project proceeds it is likely that the number will change from the original estimate. However, experience of actual projects has shown that the initial estimate of the number of modules needed is often quite accurate.)

The schedule calls for each procedure to be written, reviewed, and signed according to the monthly schedule shown.

Table 6.8 shows that, in the first month the writers are expected to complete the first 10 modules, in the second and third months they do the bulk of their work, and in the fourth month they finish up. They should not be writing new procedures in months five and six—this is time for reviews and signatures.

Table 6.8 can be expanded to demonstrate actual *vs.* planned progress, as shown in Table 6.9.

The following conclusions can be gleaned from an inspection of Table 6.9.

- The writers stayed quite close to the schedule, although they got off to a slow start, and eight procedures had to be written in the fifth month.

Table 6.9 Representative Schedule and Progress

Month	1	2	3	4	5	6	Total
Write							
Plan	10	45	45	15			115
Actual	4	55	35	13	8		115
Reviewed							
Plan		10	25	60	20		115
Actual	2	8	25	60	20		115
Signed							
Plan					25	90	115
Actual					5	103	108

- The reviewers also stayed well on schedule.
- The signature process was delayed. Seven procedures had not been signed by the time the project was scheduled to be complete.

BUDGET

Writing an operating manual is expensive—both in terms of money and of the time of key personnel.

Usually, the largest single cost is paying for the time of skilled people. The total time that these people need will depend on the following factors:

- The number of units for which procedures are being written
- The size of each unit
- The complexity of each unit
- The quality of the existing procedures
- The level of detail of the procedures
- The scope of the project
- The published quality of the final product

There are other costs, such as the computers needed to do the work, but these are likely to be minor compared with labor costs.

Once more, a sensible way of budgeting procedures is to use the number of procedures metric discussed in the previous section to do with scheduling, and to determine the number of hours that each team member is likely to spend on each module. A multiplier can be applied to determine overall costs.

Table 6.10 shows the effort that may be involved in the development of a single module using fully burdened hourly rates. If a table such as this is prepared as a spreadsheet for each module, then Tables 6.9 and 6.10 can be linked to track the overall project cost.

Table 6.10 gives a total, burdened labor cost of $1,040 for each procedure. If an overhead factor of say 25% is added to that to cover items such as initial preparation time, travel expenses, and final publishing, the total cost becomes $1,300 per procedure. If the overall manual contains say 115 procedures (Table 6.9) then the total cost for writing the manual will be around $150,000.

Table 6.10 Example of Hours/Module

Person	Hours	Rate ($/h)	Cost ($)
Project manager	0.5	120	60
Operations lead	4	80	320
Operations expert	2	80	160
Technology expert	0.5	120	60
Interviewer-writer	2	65	130
Publisher	2	75	150
Reviewers	2	80	160
Total	13.0		1,040

PREPARE THE SOPs

If generic or SOPs are needed they should be prepared at this time, i.e., before the facility-specific procedures are written.

4. COLLECT INFORMATION

Before starting on the actual procedure writing, the project team will first gather the technical information that is needed. This information will include drawings, vendor instructions, photographs, and equipment/instrument data sheets. Operating information will also be provided through the use of interviews and discussions with experienced technicians, supervisors, engineers, and managers.

For facilities that are already operating, information for the procedures can come from various sources, such as the following.

OPERATOR INTERVIEWS

For facilities that are already operating, most of the information that will be written into the procedures will come from the operators who are working on the facility.

EXISTING PROCEDURES/VENDOR MANUALS

For facilities that are already operating some procedures usually exist. These procedures may be out of date, incomplete, and difficult to use. Nevertheless, they will still have value and can provide a good foundation for updated procedures.

As already noted, vendors can be an excellent source of material that can be used in the development of operating manuals. Typically, this information is more oriented toward maintenance than operations.

LOGBOOKS

Logbooks contain information that the operators thought it worth recording during the course of the shift. Since the logbooks often record the responses taken to unusual or hazardous situations, they can be a valuable source of guidance when writing Troubleshooting Procedures.

5. WRITE THE PROCEDURES

The next stage in the project is to write the procedures themselves. Those who are good writers of normal business correspondence such as reports and letters sometimes have trouble writing operating procedures because many normal writing rules are not effective for operating procedures. For example, in general business writing it is generally considered poor style to repeat a word too frequently. But there is nothing wrong with this practice when writing technical reports. Similarly, writers of reports are taught to avoid “cobblestone writing,” i.e., writing that consists of sentences of almost the same length that are strung together with no connecting materials to smooth the flow. Yet good operating procedures will often exhibit a cobblestone effect because each instruction is about the same length, and the connecting words do not add value.

The writing of procedures will have two major steps: (1) Develop the overall structure of modules and module linkage, and (2) Write the detailed procedures and task instructions.

DRAFT RELEASES

Although there is an argument to be made for releasing one or two prototype procedures, in general draft releases of the operating manual should be avoided. There is a saying in the consulting business that “draft reports don’t exist.” This insight stems from the fact that consultants, whose final product is usually a report, are often under considerable pressure to issue a first draft in the early phases before they are ready to do so. The client will state that he will ignore any superficial problems or omissions, and that the draft will be discarded once it has been read. This rarely happens. The first draft is often photocopied and widely distributed around the client company. It can make an indelible impression on the readers such that, no matter how many subsequent corrected and improved updates are issued, they fixate on their first impression. Any mistakes or omissions are pounced upon and remembered forever. The same principle applies to operating procedures.

In spite of the above reservations, there is an argument to be made for issuing draft procedures quickly so that people can become involved in the project and feel a sense of participation and ownership. Moreover management is probably investing considerable financial and human resources into the project so want to know how the money is being spent.

Therefore, one of the project manager’s ongoing problems is to resolve the tension between issuing drafts that are so preliminary as to cause more harm than good, and issuing them so late that people are not fully involved in the project. There is no simple answer to this dilemma, but the project manager does need to be sensitive to it.

Another decision concerning the release of the first draft is whether or not to issue it piecemeal. It is suggested that, as far as possible, this strategy should be avoided. It is important that the readers and reviewers see the procedures as an integrated whole. If individual modules are released, the reader will not have a good overall impression of where they fit in; thus, he is likely to become confused and unsure of the overall picture.

PLAN TO THROW ONE AWAY—YOU WILL ANYWAY

In the entertaining and insightful book to do with the development of computer software, *The Mythical Man Month* the author Frederick Brooks (2005) uses the phrase, "Plan to throw one away; you will, anyhow." His idea is that, no matter how well planned a software project may be, the changes that are made to a program during its design and development will be so significant as to eventually make modifications to the original structure almost impossible. Instead, the software writers will do much better to discard what they have done and to start again, with all the changes in specification incorporated into the new design.

Although the idea of throwing everything away sounds draconian and wasteful, it is, in fact, far more productive than trying to fix the existing structure to incorporate major changes, and it causes fewer project management problems than might be expected.

This approach can be applied to the writing of operating procedures. Many procedures-writing projects reach a point at which so many changes are required, and so much redesign of the modules and their linkage to one another is to be done that it is easier to start again. This does not mean that all the previous work is wasted; indeed, the opposite is the case. All of the information that has been gathered previously will be used, and will be connected into the system in a useful and coherent manner. Thus the decision to throw away the first version is not necessarily a sign of failure, but a sign of progress.

6. REVIEW AND SIGN

Once written, the procedures must be reviewed for technical content, grammatical correctness and overall appearance. There are two types of reviewers. The first type checks for technical accuracy and completeness. He or she is likely to be an experienced technician who was not involved in the procedures-writing project. The second type of reviewer will check the manual for writing accuracy, grammar, spelling, continuity, and overall consistency.

7. PUBLISH

The final step is the writing and publishing phase. In this context, the term "publishing" is likely to refer to the organization of a web site, rather than the printing of a paper manual. However, it is important to recognize that print does offer benefits, including the following:

- Print generally offers more attractive and readable design.
- It is easier for the reader to refer to any time, any place.
- The message has greater sense of permanence.
- Print can serve as a roadmap to what too often is online confusion (the way a TV guide does with television).

POTENTIAL DIFFICULTIES

In the *Mythical Man Month* Brooks provides the following five reasons as to why software programming projects often fall badly behind schedule:

1. Methods of estimating are poorly developed
2. Effort is confused with progress
3. Lack of firmness in telling senior management that the project cannot be speeded up
4. Poor monitoring techniques
5. Adding more people to reduce the slippage

Similar reasons can be used to explain why operating procedures projects tend to slip behind schedule. Some of the potential difficulties are described below.

POORLY DEFINED GOALS

The writing team must have a clearly defined scope—in particular the team members must have a clear idea at the start of the project as to what defines completion. An operating manual will never be finished, there are always additions and improvements to be made. Nevertheless, the team must have a clear definition as to what constitutes the end point for the project, otherwise the work will drag on forever, or else it will be canceled when the work is only partially complete.

TOO MANY PEOPLE

Slippage is not usually caused by some major predicament that everyone knows about. Indeed, problems of that magnitude can often be handled effectively because everyone knows about them, and it is clear that action must be taken. Usually slippage occurs due an accumulation of small problems, summarized in the expression:

> **Q:** How did this project get to be a year late?
> **A:** One day at a time.

In the event that the procedures-writing project does slip behind schedule, a makeup plan is needed. In order to address the slippage, management's first reaction is usually to add more people to the project. Such a reaction may not be effective, as illustrated in Figure 6.31. Initially adding more people may help, but it will be found that "adding people to a late project will make it later."

One reason for the absence of improvement is that many tasks demand a finite amount of time, regardless of how many people are put to work. Furthermore, as more people are added to the project, they spend more and more time communicating with one another and training newcomers rather than doing direct work. Also, it is likely that the newer people will have less experience and knowledge.

EXTENDED REVIEW CYCLE

No operating procedure will ever be perfect so it is possible that the review process will drag on for too long. One of the project manager's more important roles is to have control mechanisms in

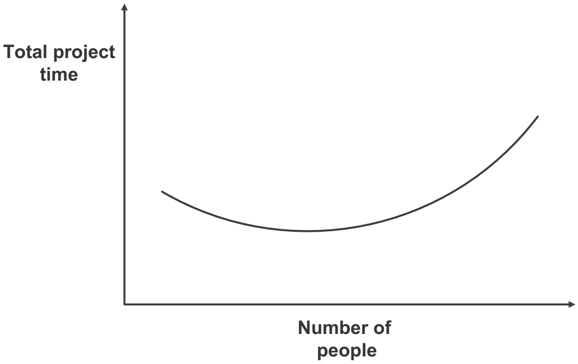


FIGURE 6.31

Effect of adding more people to a project.

place so that he or she knows when a review is taking too long, then stepping in to move the delayed procedure forward.

LACK OF SIGNATURES

The final publication of an operating manual is often delayed due to difficulties in obtaining managers' signatures. As already discussed, one reason for delays in obtaining management signatures is that the people involved are usually very busy running the facility so they tend to defer looking at the procedures "until they have more time."

A more fundamental difficulty with respect to signatures concerns legal responsibility. If a procedure contains an incorrect statement such as "close the valve" instead of "open the valve," and a serious accident occurs as a result of that error, the manager who signed the procedure could be held liable legally, and may even have to face criminal charges. Consequently, most managers want to make sure that the procedures are absolutely right before they sign them—which means that, all too often, the procedures do not get signed in a timely manner. To get around this difficulty, the project manager should make it clear to all concerned that the management signature does not mean that the manager has reviewed the actual procedure in detail; what the signature means is that a procedure for writing procedures is in place, and that it was followed.

MAINTAINING THE PROCEDURES

On all process facilities change is a constant. Almost every day there is a change to the equipment, the organization's structure or the operating targets. Many of these changes require that one or more of the operating procedures be modified or updated because the procedures represent the human–machine interface, and virtually all types of change affect that interface. This means that, all too often, the biggest management challenge to do with operating manuals is not the writing of the first edition, but keeping the contents up to date and current.

Writing procedures is challenging; keeping them up to date is much more challenging. Yet it is vital that the procedures are kept up to date. Not only could an incorrect procedure cause an operator to take the wrong action, if the operators find that the procedures do not reflect current reality, they will quickly lose confidence in all of the operating procedures because they will not know which ones to trust. Therefore, when organizing a procedures-writing project, it is critically important to make sure that the maintenance and updating process is built-in from the very start. In particular, it must be made clear who has ownership of the procedures, and who is responsible for their accuracy and completeness. The procedures-writing project does not terminate with the publication of the first edition of the manual; an ongoing effort to keep the procedures up to date and useful is needed.

Unfortunately, most traditional operating manuals do not readily lend themselves to being updated easily because of the system-wide impacts that are often created by even small changes. Even the task of simply identifying which procedures are impacted by a change to the operation can be formidable. Consequently, the chore of updating the procedures becomes a victim of procrastination. Even in those companies that have effectively internalized the principles of PSM there is a tendency to treat operating procedures as a nuisance, as something "that we will get to later—in the meantime we've got real work to do." It is easy to criticize such an attitude, but the reality is that most managers are under a lot of pressure to get things done quickly, so they are almost forced to postpone work on the operating procedures until "they have more time."

For example, in the cooling tower example, management may decide to change one of the treatment chemicals that are added to the cooling water. Apparently this change will affect only the instructions to do with chemical addition. However, the change could affect many other procedures, including those to do with truck movements (maybe the new chemical is provided by a different company), emergency response procedures (the new chemical may have different flammability or toxicity issues and new MSDS), and the troubleshooting guidance for those times when heat exchangers within the facility become fouled.

It can be seen that this apparently small change to one of the treatment chemicals involves not only operations in different areas; it also involves coordination with other management departments and managers. Hence, the impact of the change effort goes beyond simply rewriting one procedure—the change requires coordination with many other people, and could involve updating quite a large number of disparate operating procedures.

Due to the effort required to respond to even a minor change such as the one described above, many companies do not update their operating procedures in a timely manner. Therefore, after a few months those procedures are out of date; after a year or two, the procedures may be so badly out of date as to be unusable or untrustworthy. For these reasons, it is very important to design and organize the procedures for ease of maintenance and updating—in other words, to make the procedures modular. In the long term, this focus on ease of updating is likely to be more important and more valuable than expediting the writing and publication of the first edition of the manual.

A related maintenance problem concerns the handling and distribution of the updates. Often, there are multiple copies of the manuals in circulation. These may be temporarily lost, misplaced or buried in lockers. Also, many of the manuals will have "walked." Ensuring that the new pages are inserted and the old pages removed whenever a change is instituted is a challenging task, and provides a powerful incentive for using electronic distribution. Using a computer system, the master copy of the procedures can be stored on a disk. If an operator wants a paper copy of a procedure, he is welcome to print a copy of that procedure, use it and then throw it away. The master procedures will be read-only, and the printouts will be marked as uncontrolled, time-limited copies.

The updating process involves more than just rewriting an operating procedure—it frequently involves changing the links to many of the other elements of operational integrity. In particular, once a new procedure has been written and published, the operators will have to be trained in its use, and a prestartup review will have to be carried out before the procedure is actually implemented.

Once the first edition of the operating manual has been published, the team that executed the project will probably be disbanded. Control of the manual passes from the writing team to the operations and maintenance departments. It is important to have a proper handover for two reasons. First, handover represents a formal and even legal transition—the writers are saying that the procedures are, to the best of their knowledge, accurate, and complete, and the operations department is saying that they are satisfied with the product that they have been given.

PROCEDURES MODIFICATION PROCESS

A process that can be followed for updating procedures is shown in Figure 6.32.

ORGANIZATION

If the procedures are to be kept up to date, and if they are to maintained to a standard format, it is suggested that a one person be given the job of "Operating Manual Coordinator"—or some

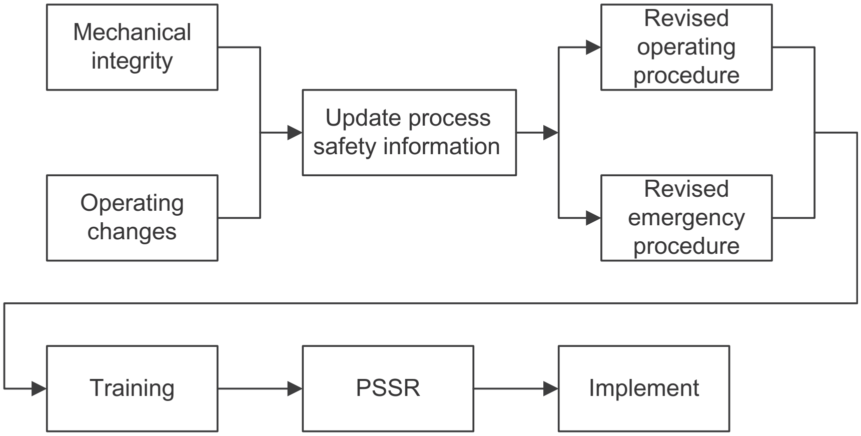

Mechanical integrity
Operating changes
Update process safety information
Revised operating procedure
Revised emergency procedure
Training
PSSR
Implement

FIGURE 6.32

Procedures modification process.

equivalent title. This position may not be full time, but it is important to have someone dedicated to keeping the procedures up to date. The responsibilities of this person include the following:

- Ensure that individual procedures are updated and certified according to schedule (facilities covered by OSHA's PSM standard have to certify their procedures annually).
- Ensure that all updated procedures to conform to the agreed-upon layout and formatting standards.
- Ensure that the procedures are technically correct.
- Maintain links between the procedures and other elements of process safety, particularly operating information (safe limits), MOC, and training.

The attributes of this person include the following:

- The ability to organize large amounts of information.
- Good working knowledge of facility operations at that site.
- Project management skills—particularly the ability to keep to define the scope of work, stay on schedule, and keep within a budget.
- Ability to work effectively and tactfully with senior operators and supervisors—in particular, the ability to "interview" them so as to capture their knowledge as to the details of the process.

WRITING GUIDELINES

This book does not provide instruction on how to write English; such a goal would be presumptuous. Those who wish to write well need do little more than read the classic *Elements of Style* by Strunk and White, first published in the year 1918, and the well-known *Chicago Manual of Style*. Nor does this chapter provide guidance to do with technical writing. Many books on technical writing are available. However, given that the writing of an operating manual requires different skills and techniques from those needed for writing reports or books, some thoughts as to the actual writing of procedures are provided in this chapter.

People who are good writers of normal business correspondence such as reports and letters sometimes have trouble writing effective operating procedures because many of the normal rules and style guides that they follow are not appropriate. For example, it is generally considered poor style to repeat a word too often. A grammar school teacher would say that a broader and more subtle range of words should be used. But there is nothing wrong with simplicity and repetition when writing procedures. Similarly, it is often considered poor style to use simple words such as "good," "big," and "have" on the grounds that they are insufficiently precise. Such a nuanced approach is not needed when writing procedures. An operating manual is intended to help the operators do their job efficiently and safely, not to provide them with a "good read" or to demonstrate the writer's prowess in the English language.

Issues to consider when developing writing guidelines include the following:

- Vigorous writing
- Writing style
- Vocabulary
- The use of graphics

These topics are discussed below.

VIGOROUS WRITING

In the book *Elements of Style*, the author, Professor Strunk (1869−1946), states:

> Vigorous writing is concise. A sentence should contain no unnecessary words, a paragraph no unnecessary sentences, for the same reason that a drawing should have no unnecessary lines and a machine no unnecessary parts. This requires not that the writer make all his sentences short, or that he avoid all detail and treat his subjects only in outline, but that every word tell.

It is telling that Professor Strunk makes a direct comparison between writing and the design of engineered systems. Operators and maintenance technicians need procedures that are as predictable, efficient, and reliable as the instruments and machines for which they are responsible.

Elements of a vigorous writing style as applied to procedures include the following:

- Minimalist writing
- The use of short, pithy instructions
- Avoidance of the repetition of instructions
- Omission of needless words
- Omission of adverbs
- Use of short and old words
- Avoidance of wordy phrases and padded syllables

MINIMALIST WRITING

An operating manual should be written using a minimalist style of writing. There are various elements to minimalist writing, not all of which are usable, or even safe, were they to be applied to the process industries. Nevertheless the concept of minimizing "soft" materials in the manual is particularly germane. Minimalist writing eliminates all extraneous material. It is not quite the same as writing with just a few words—if many words are needed then many words should be used. But every word must help the operator run his or her unit. All extraneous materials should be ruthlessly purged. Every word must tell.

Many operating manuals are cocooned in a cloud of "soft" materials such as introductions, summaries, generic safety instructions, and company mission statements. None of these materials help the operator do his or her work more efficiently or more safely; instead they pad the manual with material that gets in the way, thereby increasing the time it takes find the pertinent instructions. In response to this concern, the minimalist approach eliminates these soft materials. An operating manual should tell the operator how to operate the unit—no more, no less. All other material should be located in other documents.

For example, if it is policy that persons working outside must always wear a hard hat, no matter where they are or what they are doing, then there is no point in inserting that requirement in every operating procedure. The requirement to wear a hard hat is a condition of employment—not an operating instruction. However, if a particular task requires that the operator wear goggles then it is perfectly in order to include that requirement in the procedure itself.

SHORT, PITHY INSTRUCTIONS

A minimalist approach condenses the style of writing. When describing the execution of a particular task, an operator may *say*:

> Next, you need to go over to Pump P-100 and get it started.

The corresponding minimalist instruction would read:

> Start Pump P-100.

All redundant words and phrases have been removed.

Procedures written by engineers are sometimes verbose, and are often written in the passive tense. As already noted, engineers have an unfortunate tendency to write "instructions" such as,

> Having started P-100, flow 1,000 kg/h of condensate into V-100 using FCV-121, first making sure that the pressure in V-100 is not greater than 20 barg.

The above sentence can be collapsed into the following five separate instructions:

1. Start Pump, P-100.
2. Measure the pressure in V-100.
3. If the pressure in V-100 is greater than 20 barg, transfer control to Procedure ABC.
4. Start the flow of condensate from P-100 to V-100.
5. Adjust the flow rate to 1000 kg/h as measured by FCV-121.

AVOID REPETITION OF INSTRUCTIONS

Generally, there should be no need to repeat an instruction. If a task is so critical or so confusing that the writer feels a need to repeat the pertinent instruction, then it is likely that too much reliance is being put on the procedures and the operators. Rather than repeat the instruction, it would be better to redesign the operation itself, or to modify the equipment, so that is not so subject to the vagaries of human error.

There is one important exception to general rule about repeating instructions—particularly with respect to maintenance procedures. Pictures and sketches often provide a very useful supplement and alternative to the written text.

OMIT NEEDLESS WORDS

The above phrase (which is also from Professor Strunk's book) is one of the keys to minimalist writing.

Table 6.11 illustrates how needless words can be removed; the phrases in the first column are all unnecessarily lengthy, and can be shortened to the phrase in the second column.

OMIT ADVERBS

The fourth example in Table 6.11—Close the valve carefully—is worth additional discussion. The word "carefully" is adding no value to the instruction. This can be seen by considering the

Table 6.11 Needless Words

Original	Minimalist "Translation"	Comment
Next, go over to the valve and get it closed	Close the valve	The original version is similar to what a person would say during a discussion. However, it is too wordy for a procedure
The valve should be closed	Close the valve	Use of the passive tense creates uncertainty as to whether the operator is to check on the status of the valve or take action. Also, the word "should" is ambiguous
You must close the valve	Close the valve	The words "you" and "must" are redundant
Close the valve carefully	Close the valve	The inappropriate use of adverbs in operating procedures is discussed below

Table 6.12 Use of Short Words

Original	Replacement
Accomplish	Do
Attempt	Try
Utilize	Use
Construct	Build
Deficiency	Lack
Equitable	Fair
Infrequent	Rare
Occurrence	Event
Terminate	End/finish
Requisite	Required

opposite instruction, "Close the valve recklessly." Obviously no one would write such an instruction. Therefore, it can be seen that words such as "carefully" are adding no value. Like all adverbs when used in procedures, it should either be dropped, or replaced with quantified statements.

In the case of the instruction in Table 6.11, the writer probably used the word "carefully" to warn of some hazardous condition that might arise from the closing of the valve. For example, the valve may be on a feed line to Tank, T-100. If the valve is closed too quickly, the level in the tank may fall below a safe limit. Therefore, the instruction "Close the valve carefully" becomes:

1. Close the valve.
2. Ensure that the level of liquid in Tank, T-100, does not fall below 3 meters.

SHORT AND OLD WORDS

When writing procedures short words are preferred over long words. Some examples are provided in Table 6.12.

Table 6.13 Wordy Phrases

Original	Replacement
On the order of	About
In the nature of	Like
In view of the fact that	Since
Give encouragement to	Encourage
Make an adjustment in	Adjust

Table 6.14 Syllable Padding

Original	Replacement
Administrate	Administer
Discontentment	Discontent
Experimentalize	Experiment
Irregardless	Regardless
Orientated	Oriented
Preventative	Preventive

The English language often has two words that mean roughly the same; one derives from Saxon and the Germanic languages, the other from Latin and the romantic languages. Generally, the Saxon words, which are typically older, are preferred. Saxon words tend to be shorter than their Latinate equivalent. Most of the words in the right-hand column of Table 6.13 are of Saxon derivation, whereas those on the left are largely Latinate.

In other words, the procedures writer should always select short, simple words where at all possible. As Winston Churchill once said, “The short words are best, but the old words are best of all.”

AVOID WORDY PHRASES AND PADDED SYLLABLES

Wordy phrases and padded syllables should also be avoided, as shown in Tables 6.13 and 6.14.

WRITING STYLE

With regard to writing style, the following guidance will generally result in procedures that are easier to use.

- Use the imperative tense.
- Use the active voice.
- Write to eighth grade reading level.

- List instructions singly.
- Avoid implied instructions.
- Use bulleted lists.

IMPERATIVE TENSE

Operating instructions and not guidelines or suggestions—they are *instructions*. Hence operating instructions should start with a verb in the imperative tense followed by the name of the object that is being acted upon. Therefore, referring to Table 6.11, the following sentence is correct:

Open the valve.

The following would normally be incorrect.

You must open the valve.
Having opened the valve,. . .

Other examples of the above principle (with the action verbs shown in bold and small capitals) are:

- **FILL** the Waste Water Tank, T-109, to a level of 5 meters.
- **REPORT** the level in the Waste Water Tank, T-109, to the supervisor.
- **WAIT** 5 minutes.

Some verbs are not specific enough to be used in procedures. For example, the instruction,

Ensure that the level in the Waste Water Tank, T-109, does not go above 5 meters.

is too vague; the word "ensure" is too abstract. The following is a more specific explication of the above instruction:

1. Fill the Waste Water Tank, T-109, to a level of 5 meters as measured with LI-109A.
2. IF the level in the Waste Water Tank, T-109, goes above 5.5 meters, THEN. . . (do something).

ACTIVE VOICE

Generally, procedures should be written in the active voice. For example, the statement, "The engineering department installed the drain valve in 1988" is better than, "The drain valve was installed by the engineering department in 1988." The first sentence, which is in the active voice, is more direct and shorter.

Passive writing of the type,

The pump is started

should be avoided because it is not clear whether this is intended to be an instruction or a statement. The phrase should either be:

Start the pump.

or

The pump will start.

READING GRADE LEVEL

In general, operating procedures should be written at an eighth grade level (U.S. system). This is roughly the level to which the newspaper *USA Today* is written. Of course, most technicians have a higher reading capability, but the aim of an operating manual is to communicate instructions quickly and clearly—not to provide the operator with a meaningful reading experience, nor to challenge him or her to parse or interpret the text.

Various techniques for analyzing the readability of written material are available. For example, the "Fog Index" by Gunning is calculated for a 100-word passage from the following equation:

$$G = 0.4 \times (W + \mathrm{HW}) \tag{6.1}$$

where

- G is the educational grade level of the written material,
- W is the average number of words per sentence, and
- HW is the percentage of words with three or more syllables (with some exceptions).

Procedures that are written as short, simple instructions, as discussed above, will almost certainly meet the Fog Index threshold value.

The algorithm shown in Eq. (6.1) is built into many widely available word processors, often under the "readability statistics" section. The word processor package may also make suggestions for improvements, although their suggestions tend to become rather repetitive and boring after a while. They can also be rather patronizing in tone, and sometimes they are simply wrong.

The text shown in Table 6.15 has a Fog Index of 13.2.

Table 6.15 High Fog Index

The intent of this policy is to (a) maximize the strategic value of the systems and the data by promoting its effective use in management decisions, daily operations, and analyses being conducted by faculty, staff, and students, (b) provide clear assignment of responsibility for protection against unauthorized use, and (c) promote security measures for the purpose of maintaining the integrity of the systems and the data.

This policy addresses access to and data residing in computerized administrative systems (hereafter referred to as the systems and the data) supported by Administrative Information Services (AIS). This includes but is not limited to Financial and Student systems. It does not include institutional reporting databases (i.e., FRDB, RRDB, and SDRDB), departmental systems, hard-copy files, or systems or databases maintained by any unit other than AIS. It does not supersede applicable statutes that guarantee either the protection or accessibility of data.

The text shown in Table 6.16 has a Fog Index of 8.4.

Table 6.16 Medium Fog Index

The Fog Index is a proven method of analyzing written material to see how easy it is to read and understand. The steps you can use to calculate the Fog Index are outlined below. The numbers in the right column are based on this paragraph. When using these steps to analyze your writing, choose a sample that contains at least 100 words. The "ideal" Fog Index level is 7 or 8. A level above 12 indicates the writing sample is too hard for most people to read.

LIST INSTRUCTIONS SINGLY

Each instruction should be given its own sentence on its own line. So the phrase:

> Open the valve, start the pump and measure the temperature.

should read:

1. Open the valve.
2. Start the pump.
3. Measure the temperature.

IMPLIED INSTRUCTIONS

A common problem with manuals is that instructions are implied, rather than stated right out. For example, the phrase, "Make sure that the pump is turned off," can be interpreted in one of two ways. Either it means, "Turn off the pump," or else it means "Check that the pump is turned off." The operator should not be required to make a judgment call in this situation.

BULLETED LISTS

Bulleted lists are an excellent way of organizing instructions, particularly if a modular concept is not being used. For example:

- Instruction 1
- Instruction 2
- Instruction 3

CONDITIONAL INSTRUCTIONS

Operating procedures often contain conditional instructions, i.e., the person following the instructions will be required to take different courses of action depending on the current operating conditions.

The U.S. Department of Energy Writer's Guide provides some rules and guidance for the use of conditional statements. It suggests that the use of the following words is acceptable:

- IF
- THEN
- WHEN
- AND
- OR
- NOT

The following words should be avoided:

- FOR EXAMPLE
- EXCEPT
- BUT
- ONLY IF

The Guide also suggests that conditional words should be written in underlined uppercase letters (the underlining convention is not followed in this chapter). Finally, a conditional phrase, and the action that follows it should be on separate lines. For example:

WHEN the temperature reaches 120°F
THEN line up the steam trap

Tortuous or confusing logic should be avoided. For example, the following instruction can be interpreted in one of two different ways.

WHEN the temperature reaches 120°F AND the flow is 66,000 lb/h OR the pressure is 100 psig
THEN line up the steam trap.

would be better written as follows:

- WHEN the temperature reaches 120°F AND the flow is 66,000 lb/h,
- THEN line up the steam trap.

or

- WHEN the temperature reaches 120°F AND the pressure is 100 psig,
- THEN line up the steam trap.

Generally, the process industries do not use such a tightly structured and formalized approach. Nevertheless, the clear logic paths that result from use of methods such as those described above does provide a good framework for the operating procedures.

To illustrate the above points, consider the following instruction:

Next, after measuring the reactor temperature, and making sure that is not above 210°C, open the discharge valve.

should read:

- Measure the reactor temperature.
- IF it is above 210°C, go to Module XYZ.
- ELSE open the discharge valve.

POSITIVE/NEGATIVE INSTRUCTIONS

Instructions are more likely to be understood and followed if they are written in a positive manner. For example, it is better to write,

Keep the flow rate below 2000 lb/h.

than

Do not let the flow rate go over 2000 lb/h.

VOCABULARY

Guidance regarding the words used in the procedures is provided in this section. Once more, it must be stressed that this guidance is for the writing of instructions, not necessarily for the writing of discursive text such as would be used in a report.

IDENTIFICATION OF EQUIPMENT

It is vital that there be no confusion about equipment identification within a set of operating procedures. A phrase such as,

> Start the Boiler Feed Pump

could be misinterpreted if the facility has more than one boiler, or more than one pump feeding a particular boiler. To eliminate potential confusion it is suggested that equipment always be identified with its official name (as shown on the P&ID), and its official number. So, the above phrase becomes,

> Start the Waste Heat Boiler Feed Pump, 12-P-103

Although the second example has more words than the first, the additional words add genuine value—hence they do not conflict with Professor Strunk's rule about omitting needless words.

Sometimes equipment items are given nicknames, often derived from the name of the manufacturer of the item. Such nicknames should not be used in operating procedures. Nicknames lack engineering integrity, and they may change over time. In general, all jargon, slang, and other uncontrolled words should be excluded from the operating procedures.

CONSISTENCY

Consistency of terminology is important. Not only must the manner in which capital letters and abbreviations remain the same throughout the manual, words themselves must be used consistently. For example, a "Column" should not be later called an "Absorber."

SHOULD/WOULD/COULD

The words "should," "would," and "could" often create ambiguity. Hence their use in operating procedures is generally undesirable.

It is best simply not to use the word "should" in operating instructions. For example, the phrase "the pump should be started" could mean:

- Start the pump.
- The pump is likely to be already running.
- The pump might not be running.
- Someone else will have started the pump.
- If you haven't started the pump yet, you're in trouble.

Similarly the statement:

> The valve should be opened before measuring the temperature.

could mean:

- The valve can be expected to be in an open position—but it might not be—either way it doesn't matter.
- The operator is expected to open the valve.

- Someone else should have opened the valve.
- Regardless of the valve status, the temperature must be measured.
- The temperature should be measured only if the valve is in an open position.

What the writer probably meant to write was,

1. Open the valve.
2. Measure the temperature.

Use of the word "would" can also create a sense of ambiguity or lack of assertiveness. For example, the statement, "Were the valve to be open, then the water would flow out of the tank" is better written as, "If the valve is open, water will flow out of the tank."

Finally, the word "could" can also create vagueness. For example, the statement, "If the valve could be opened, then fill the tank," seems to suggest that the operator ought to open the valve, but it does not matter if he cannot. There is no place for such ambiguity in an operating manual.

THE WORD "YOU"

Generally, the word "you" should not be used in operating procedures because its use is generally not minimalist. For example, it is better to write "Close the valve" rather than "You must close the valve."

THE WORD "THIS"

Use of the word "this" can create vagueness. "This" is a pronoun, hence, if two or more nouns are in use, confusion can arise as to which noun is being referenced. For example, in the sentence, "Measure the temperatures in Reactor 1 and in Reactor 2. If this is below 200°F, then start the steam flow," the word "this" could refer to either of the individual reactor temperatures or to both. The sentence is better written as:

1. Measure the temperature in Reactor 1 with TI-101.
2. Measure the temperature in Reactor 2 with TI-102.
3. IF the temperatures in both Reactor 1 and Reactor 2 are below 200°F, THEN start the steam flow.

ARABIC NUMERALS

Numerical information should generally use Arabic numbers, i.e., 1, 2, 3... Roman Numerals, either upper or lower case, e.g., i, ii, iii, iv and I, II, III, IV, can be confused with letters and are best avoided in operating manuals.

ADVERBS AND ADJECTIVES

Adverbs are words that qualify verbs. They are commonly used in discursive text but, as discussed earlier, they rarely have a place in operating procedures. Words such as "quickly," "slowly," and "carefully" lack precision. Wherever possible words such as these should be replaced with quantified statements. Measurements should be provided in engineering units such as °F or kg/h.

Similarly, adjectives, which are words that qualify nouns, are generally ambiguous or imprecise, and should be avoided. Statements such as, "Fill the tank to the correct level" are too vague. The instruction should read, "Fill the tank to a level between 5.5 and 6.0 meters."

ARTICLES

The importance of writing minimally provides no excuse for dropping definite and indefinite articles (the words "the" and "a"). Therefore, the following instruction:

> Start Waste Heat Boiler Feed Pump, 12-P-103

should be written as:

> Start the Waste Heat Boiler Feed Pump, 12-P-103

HUMOR

There is no place for humor in operating procedures for the following reasons.

1. Humor relies on surprise to make its effect. Operating procedures are intended to be used frequently; therefore, the surprise effect will be lost and the humor will become tedious, tendentious, and distracting.
2. Humor does not tell an operator how to carry out a task, hence it contravenes the principles of minimalist writing.
3. Humor can have unfortunate, unintended side effects because what is funny to one person may be tasteless or offensive to another. People of a different ethnic and national background from the writer of the procedures may interpret the humor in ways that were never intended but which, nevertheless, cause offense. Even simple technical words can have unanticipated meanings. For this reason, English and American engineers working in one another's countries need a quick course in *double entendre*.
4. Humor can be perceived as being patronizing.
5. Humor can trivialize the importance of the instructions.

SPELLING

All modern word processing packages incorporate comprehensive spell-checkers; they should be used. Technical and facility-specific words can be added to the spell-checker. There is no longer any excuse for misspellings, nor for misspellings.

Most word processors also contain a thesaurus that will suggest alternative words that have similar meanings to the one just entered. Not only will this sometimes provide a better choice of word to express an idea, it will also liven up the writing by adding variety to the vocabulary.

The correct spelling of potentially troublesome words that are frequently used in operating manuals is shown in Table 6.17. In all cases the Webster dictionary was used.

Table 6.17 Spellings

Start-up	Inline	Bypass
Shutdown	Knockout	Handvalve
Troubleshooting	Feedstock	Pipeline
Precommissioning	Setpoint	Off-spec
Stand-by	Flowrate	Seawater
Bypass (verb)	Firewater	Checklist
By-pass (noun)	Feedwater	Run-in
Online	Makeup	Sight glass
Halfway	Tie-in	Nonoperating
Handswitch	Backup	

Table 6.18 Internal Dictionary

Start-up	Shutdown
Troubleshooting	Precommissioning
Stand-by	Bypass (verb)
Bypass (noun)	Online
Inline	Knockout
Feedstock	Flow rate
Firewater	Feedwater
Makeup	Handvalve
Tie-in	Backup
Handswitch	Pipeline
Non-operating	Halfway
Off-spec	Seawater
Checklist	Run-in
Setpoint	

The operations in many facilities often require the use of specialized words, or the use of normal words in a specialized context. Since many writers of operating procedures may not know how to spell such words, or given that legitimate disagreement may exist as to how the words should be spelled, it can be useful to create an internal dictionary for the procedures-writing project. Such a dictionary can be particularly useful if the people writing the procedures do not speak English as a first language.

Table 6.18 provides an example of some of the spellings agreed upon by a team of about 20 writers who were working on one project.

The essential point about Table 6.18 is not that the selected spellings are "right" or "wrong" or that they meet the dictionary definition. These were the spellings were agreed upon for this particular project.

LATINATE ABBREVIATIONS

Latin abbreviations are often used in procedures. Since Latin is a foreign language, these terms should be shown in italics (as should all foreign language words and abbreviations).

Table 6.19 Examples of Ambiguity

Ambiguous Instruction	Nonambiguous Version
Add more catalyst to the Batch Reactor, R-200	Add 200 kg of catalyst RM-12 to the Batch Reactor, R-200
Use gasket specification GR-201A, or similar	Use gasket specification GR-201A, or GR-201B, or GR-300
Remove all the blinds from Batch Reactor, R-200	Remove the blinds listed below: [a list of blinds and their location follows]

Three Latinate abbreviations that are commonly used in procedures are: *etc.*, *i.e.*, and *e.g.*

The first of these terms is "etc.," which is short for the Latin word "etcetera," is used when referring to a list of objects. For example, a manual may contain the following list:

P-101, P-102A, P-102B, and P-104.

If this list is repeated, then it is proper to use P-101, *etc.* However, it is not correct to use the term *etc.* if the full list has not been spelled out at least once at an earlier point in the document.

The terms *e.g.* and *i.e.* tend to be confused with one another, yet they have different meanings. *e.g.*, which is Latin for *exempli gratia*, means "for the sake of an example," whereas *i.e.* stands for *id est*, which means "that is."

The following sentence shows how each term could be used within the context of an operating manual.

Centrifugal pumps, e.g., Pump, P-101A, contain an impeller.

P-101A is a centrifugal pump, i.e., it contains an impeller.

APOSTROPHES

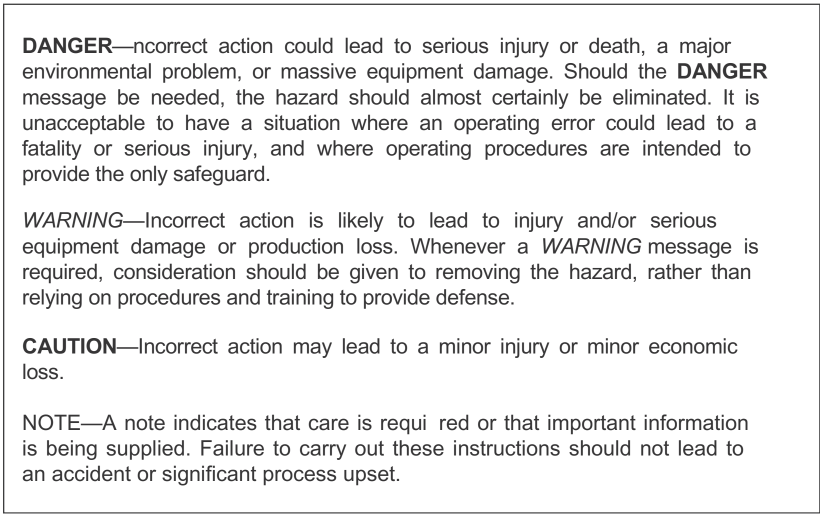
An apostrophe before or after the letter "s" at the end of a word is used to indicate possession (and also when words are merged). At other times, the apostrophe should be avoided. Hence the phrase, "The facility was modified in the 1980s" is correct; the phrase, "The facility was modified in the 1980's" is incorrect.

AMBIGUOUS WORDS

Operating procedures are instructions. Hence they must always be clear, precise, and unambiguous. Some examples of ambiguity have already been provided. Other words that can create ambiguity are:

- More
- Less
- Equivalent to
- Similar to
- All

In general, such words should be replaced with a quantified instruction, or with a list of items. Some examples are provided in Table 6.19.



DANGER—ncorrect action could lead to serious injury or death, a major environmental problem, or massive equipment damage. Should the **DANGER** message be needed, the hazard should almost certainly be eliminated. It is unacceptable to have a situation where an operating error could lead to a fatality or serious injury, and where operating procedures are intended to provide the only safeguard.

WARNING—Incorrect action is likely to lead to injury and/or serious equipment damage or production loss. Whenever a *WARNING* message is required, consideration should be given to removing the hazard, rather than relying on procedures and training to provide defense.

CAUTION—Incorrect action may lead to a minor injury or minor economic loss.

NOTE—A note indicates that care is requi red or that important information is being supplied. Failure to carry out these instructions should not lead to an accident or significant process upset.

FIGURE 6.33

Dangers, warnings, cautions, and notes.

REPETITION OF MESSAGES

The writers of an operating manual have to decide how much repetition of a message is appropriate. For example, if a text-graphics approach is used, there is some built-in redundancy. Generally, it is desirable to have at least some repetition for the following reasons:

- A second message will have some differences from the first one. The difference will provide the reader with a better understanding of the instruction. This is particularly true if one message is text and the other is graphics.
- If one message contains errors, it will show up as a discrepancy when compared with the other.
- Repetition will help reinforce critical statements.

DANGER, WARNING, CAUTION, NOTE

The writers of the procedures should use a consistent and systematic method of highlighting problems and dangers, particularly for those situations where a single error could cause some type of accident.

The Danger/Warning/Caution/Note terminology used in this book, and defined in Figure 6.33 is derived from military standards.

All messages to the operator must precede the instruction with which they are associated. There is no value in telling someone about the hazards associated with an action after they have taken that action.

Warnings, Cautions, and Notes should provide information only. They should not contain actual operating instructions.

Table 6.20 Common Proofreader Marks

Mark	Explanation
¶	New paragraph
/	New line. For example, • Open the valve/measure the flow is equivalent to: • Open the valve • Measure the flow
stet	Let it stand
—	em dash
–	en dash
©	Copyright
®	Registered
™	Trade mark
#	Insert space
ˆ	Insert here or subscript
ˇ	Insert here or superscript

PROOFREADER MARKS

When editing a document, it is sensible to use standard proofreader's marks—a complete list of which is provided in the *Chicago Manual of Style* and in Webster's Dictionary. These marks will be understood by professional editors and printers, and provide consistency among all editors. Some of the more common marks are listed in Table 6.20.

When editing a procedure with a highlighter pen it is useful to assign different meanings to different colors. One system is shown below:

- *Blue*

  Delete
- *Yellow*

  Checked, the information successfully cross-checked with information in another document
- *Red*

  Change—the new words replace the old words

ILLUSTRATIONS

Where possible, the written procedures should be supplemented with graphics. Not only do graphics provide additional information and explanation, they also make the manual more attractive. This is important because a manual that is attractive and easy to read is more likely to be used. The following types of graphics can be used:

- Photographs
- P&IDs

- Personalized sketches
- Iconic flow diagrams
- Maps/plot plans
- Calculation sheets (usually to go with batch operating procedures and/or checklists)
- Equipment drawings
- Distillation column temperature and pressure profiles

PHOTOGRAPHS

Photographs are most effective when describing equipment detail. Therefore photographs are particularly useful in maintenance procedures.

The use of photographs can cause difficulties when coordinating procedures updates with the MOC program because extraneous background detail may be included. For example, the photograph may be of Pump, P-100. But, in the background, is a Vessel, V-100. If V-100 changes, it may not occur to anyone to change out the picture of P-100 in its module.

P&IDs

A P&ID provides detailed engineering information such as line sizes, material specifications, insulation requirements, and all control loops. They are not to scale, nor do they show equipment layout. They can be used in operating procedures to illustrate complex operations, such as the lineup of a certain flow path where there is a complex network of piping. They can also be used where detailed information is needed, such as in the preparation of blind lists.

ICONIC FLOW DIAGRAMS/SCHEMATICS

Most people who work on facilities often prepare a personalized set of sketches and drawings that provide information on exactly what they need to do their job. These sketches are usually an informal mix of Block Diagrams, Process Flow Diagrams, P&IDs, and the Process Plot Plan.

Sketches such as these are unofficial and unauthorized; therefore, they will not have been reviewed for accuracy or completeness. Indeed, it is almost certain that many items will be missing from them because the person who drew it will have written down only those items that were of particular interest to him. For example, the sketch may show just one valve in a certain line because that was the only one of interest to that person. If there are, in fact, two valves in that line, then an operating instruction that used this sketch could be misinterpreted, and the operator might close the wrong valve.

The writer of an operating manual is faced with a dilemma regarding personalized sketches. However, there is no question that they are very useful in operating the facility. Yet, their lack of engineering integrity could lead to errors and confusion if they are incorporated into the operating manual. This means that the review of these sketches before they are included in the manual has to be very thorough.

One solution to this dilemma is to develop *Iconic Flow Diagrams*. An Iconic Flow Diagram is basically a Block Flow Diagram with some process information added, and with detail regarding many of the minor items omitted. It helps an operator to follow the principal flows through a unit or to follow the path of a start-up. It has more engineering detail than a Personalized Sketch but less than a full P&ID.

Figure 6.34 is an Iconic Flow Diagram for Truck and Barge Movements. Valves that are to be closed are shown as solid; valves that are to be open are shown in clear. Alternatively, color can also be used to identify which valves on a drawing should be opened or closed.

MAPS/PLOT PLANS

Maps are used when it is important to locate a piece of equipment. They are particularly useful for showing the location of safety equipment, such as fire hoses and first-aid stations. They are often found in emergency procedures.

Maps are also handy for operations involving vehicle movement. If, e.g., a truck of hazardous chemicals arrives at the gate of the facility, the security guard can provide the driver with a map of the roads to the location where he is to unload. Maps can also show the layout of safety equipment such as fire monitors and extinguishers.

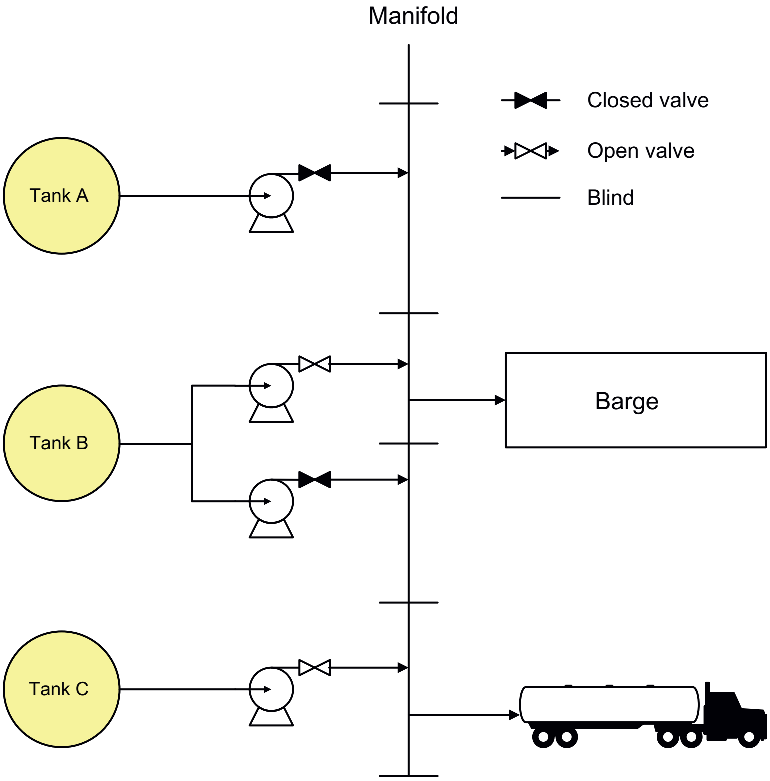


FIGURE 6.34

Example of an iconic flow diagram.

PUBLISHING

Once the procedures are written they must be published. Most people involved in writing procedures have a technical background, hence they may fail to recognize the importance of the publishing process. They believe that the words “speak for themselves” and that appearance is not all that important. Yet the operators who are asked to use the procedures live in a world where most of what they read and view is of very high quality. They go home, turn on the television, and watch news programs that use state-of-the-art graphics techniques; they then pick up a magazine such as *Time, Newsweek*, or *National Geographic*, and read stories and articles that are profusely and richly illustrated. They then check in with their favorite web site and are presented with carefully researched site designs that possess an immediate appeal. The next morning, they pick up a copy of *USA Today*, and are once more provided with a copy that is colorful, strong on white space, and attractively laid out. Then, those same technicians come to work and are provided with an operating manual that is just black and white text, has no color, is not appealingly written, and weighs 3½ pounds. It is little wonder that the operators are tempted to ignore such procedures.

In order to improve on this situation, the writers of operating manuals must understand that their competition is not the chemical facility, refinery, or gas facility down the road. Their “competition” is the world of attractive and appealing published documents available to the public.

COLOR

Most operating procedures are published using black ink on white paper. However, the advent of low-cost color printers and color photocopiers is changing this situation. The sensible use of color highlights important information in procedures and makes them look more attractive. It also enhances the quality of the information and makes it easier to follow a sequence of steps. Color can also be used to identify original documents (assuming that the company does not use color copiers). If an original has say a red title block, and is then copied, the copy will not show the color, and so is identified as not being an original. This is a technique that some quality standards, such as ISO 9000, can use to identify any illicit photocopies.

Color should be used sparingly, and should be used only to contrast different sections of the page. Color should not be used in operating procedures only to make the document look interesting or attractive.

It is important to choose colors that contrast with one another tastefully. The choice is usually made through use of a color wheel. The major colors, moving clockwise, are Violet, Blue, Green, Yellow, Orange, and Red. Colors from opposite sides of the color wheel should not be placed next to one another on the printed page. Doing so can cause a perception of shimmer or vibration. Selecting colors that are near to one another on the color wheel creates a sense of harmony. Colors that have three other colors between them provide a strong sense of contrast.

Color photographs are generally a better choice for graphic illustrations than black and white, even when the final, published copy is to be monochrome, because a process facility tends to offer a very sharp contrast between the dark outline of the equipment and the light background (often the sky.) This strong contrast has the effect of creating a profile, with the equipment being in deep shade and all detail being lost. Color pictures provide for a smoother transition; the contrasts are not so extreme.

WHITE SPACE

It is important to provide plenty of white space in the manual. People do not read text word by word, they read groups of words together. The correct use of white space will help the reader create the right groupings of words, and so facilitate the reading. White space also serves as a formatting device; if a section of text is isolated from the text surrounding it by a large amount of white space, the reader knows that it is being highlighted.

FONTS

A font is a set of letters, numbers, punctuation marks, and symbols that share a unified design. Modern software has made a huge number of fonts available to writers. This choice can help make written text (including operating procedures) look attractive. However, if fonts are not mixed properly their use can make reading more difficult. For example, the mixing of fonts on the same page, is generally not recommended, unless the writer has training in artistic effects.

Font size is defined in *points*, where a point is 1/72 of an inch. Most texts use 11 or 12 point (this chapter is written in 11 point, except for the headings, which are 14 and 12 points, respectively). With regard to operating procedures, a larger font size may be a better choice because it will make the manual easier to read from a distance; technicians are not always sitting down at a desk when they need the manual. They may have to read the manual while they are located at the control panel, for example.

The style of the font can be normal, bold, or italics. As discussed below, bold can be a problem because it is not always clear which texts have been bolded, and which have not. Italics is a better choice for emphasizing text in an operating manual.

Serif refers to the small extensions or projections that are used in some fonts. Generally, serif fonts make the text seem to flow more naturally. *Sans serif* (without serif) may be a better choice for titles and headings. Examples of fonts are provided in Figure 6.35.

The fonts of choice for most operating manuals are Times New Roman and Arial (most of this chapter is printed in Times New Roman).

PARAGRAPH FORMATTING

Modern word processors all give the option of justified printing. This means that the words on a line are spaced so as to completely fill the line. Because some letters, such as "A" take up more space than others such as "j," the amount of space allotted to the letters is automatically adjusted

Serif	Sans Serif
Times New Roman	Arial
Bookman Old Style	**Arial Black**
Courier New	Tahoma

FIGURE 6.35

Sample fonts.

so as to create a pleasing effect. Nevertheless, justified text can still be a strain to read, particularly when there is a small number of long words on a line. Therefore, many writers choose "ragged right margins" in order to eliminate these potential problems.

Another choice is whether to start each paragraph with an indent. If the indent is not used, as with this book, some space is saved. Otherwise, it is really a matter of taste.

EMPHASIS TECHNIQUES

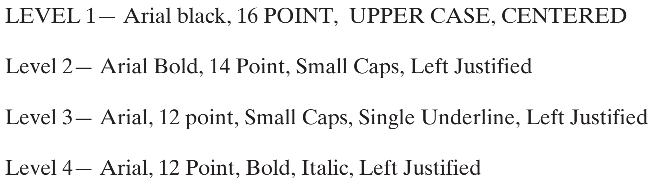
The most commonly used methods for emphasizing text are CAPITALIZATION, **bold**, underline, *italic*, emphasis boxes, color, font changes, and white space. They are generally used to highlight critical information. Once a method of emphasizing the written material has been selected, it should be used consistently throughout the manual. No more than 10% of the material should be emphasized.

The following suggestions are provided regarding the use of emphasis techniques:

- CAPITALIZATION should generally be avoided except to emphasize single words or very short phrases. Strings of uppercase letters are hard to read and give the impression that the writer is shouting or expressing emotion.
- **Bold** printing should normally be avoided because it might not be sufficiently distinct, particularly if the toner in the laser printer is low.
- Underlined text is an effective means of emphasis. It is clear to see but is not intrusive. However, many people now interpret an underline to indicate a hyperlink.
- *Italicized* is an effective way of creating emphasis, but, like bolding, it might be overlooked if the printer does not make the font distinctive enough.
- Emphasis Boxes are effective, but they also take a lot of space. Their use is generally confined to Warnings, Cautions, and Notes.
- Color is discussed in a later section of this chapter.

HEADING

For those parts of the manual which are discursive, it is important to have a standardized heading style. Modern word processors can automatically create the correct formatting for each heading. The heading style used in this chapter is shown in Figure 6.36.



LEVEL 1— Arial black, 16 POINT, UPPER CASE, CENTERED

Level 2— Arial Bold, 14 Point, Small Caps, Left Justified

Level 3— Arial, 12 point, Small Caps, Single Underline, Left Justified

Level 4— Arial, 12 Point, Bold, Italic, Left Justified

FIGURE 6.36

Heading styles.

PAGE NUMBERING

It is important to have some type of numbering system with an associated index, so that any missing procedures can be identified. However, if a strict modular approach is used, there is no need for an overall page-numbering scheme, thus making it simple to add and remove new procedures, as needed.

SINGLE-SIDED VERSUS DOUBLE-SIDED PRINTING

It is necessary to decide if the manual is to be printed single-sided or double-sided, i.e., whether the reverse side of each piece of paper is to be left blank. Single-sided pages are easier to read. However, they do bulk up the manual, and are contrary to the paper-saving policies that many companies follow.

INDEXING

A good index is an important part of any manual, yet it is rarely provided. There are two types of index: the Table of Contents at the beginning of the manual, and the topic index at the end. The Table of Contents shows the organization of the manual; but it does not purport to provide much detail. It gives the reader an idea as to what the major topics are, and where they are to be found. The index identifies the location of specific topics and words. Each piece of information in the manual should be indexed in as many different ways as possible so that it can be accessed by different approaches.

GLOSSARY

A glossary is used to define technical terms and abbreviations; it will not always be required. The glossary should not overlook simple terms. An experienced technician does not need to be told the difference between a compressor and a pump, but an outsider, such as an auditor might not know.

THE BINDER

The first impression that a reader of the operating manual is created by the binder; therefore, it is worth devoting considerable attention to its design. This will often include the company logo and some appropriate graphics.

It is suggested that the emergency procedures be put in their own binder, the Emergency Manual, that has a distinctive, bright color (usually red), thus allowing the operators to locate it quickly, at a time when they are under considerable stress. The emergency manual will also provide the information that they need without it being cluttered up with other, nonemergency operating information. Included in the emergency operating procedures are plans for activities such as evacuation, major fires, communication with other refineries and agencies, and public relations.

Where funds permit, it is suggested that the binder should be silk-screened, with customized graphics on both the cover and spine.

MULTIPLE LANGUAGES

The discussion up to this point of the book has been premised on the assumption that the procedures are to be written in a single language. In fact, many facilities are operated by personnel with different first languages, and many of these people may not be fluent in reading the facility's primary language. For example, in the United States, English is the official language in virtually all facilities, yet many of the operators and maintenance personnel come from cultures where other languages, particularly Spanish, are primary.

OSHA alludes to the multilingual issue in the PSM regulations. They make it clear that it is the management's responsibility to make sure that the procedures and the training program are provided in the language that the operators speak.

In practice, most facilities will require that employees in responsible positions be able to speak, write, and read the primary language. However, those writing the procedures must take care to ensure that what they write is clear and unambiguous to all readers.

CHAPTER

7 TRAINING AND COMPETENCE

CHAPTER OUTLINE

There's No Substitute for Knowing What You're Doing

Bumper Sticker

INTRODUCTION

All aspects of operational integrity and process safety come down to people working with systems; and people—including contract workers—need to be trained in running those systems. Training is expensive and time-consuming, but, in the words of Zig Ziglar, "The only thing worse than training your employees and losing them is NOT training your employees and keeping them." But getting the right person for the job also remains critical. In the words of the proverb, "You can train a turkey to climb trees, but it's better to hire a squirrel."

There is an important distinction to be made between training and education. Training refers to the ability to carry out a routine and predefined task in a safe and efficient manner. For example, an

Process Risk and Reliability Management. DOI: http://dx.doi.org/10.1016/B978-0-12-801653-4.00007-2

operator may be *trained* in how to start Pump, P-100 (described in the first standard example). The training will list a set of precise instructions that will, when followed, lead to the pump being started in a safe and orderly manner. Education, however, provides an understanding of basic principles. If the operator who is starting P-100 has been *educated* as to the basic theory of pump operation, he or she may be able to determine what to do if the pump behaves in an unusual manner—say if the discharge pressure is less than what it should be, or if the bearings make a strange noise.

Training and procedures are opposite sides of the same coin. If a facility does not have good procedures, then its people cannot be trained. However, there is no point in having good procedures if people are not trained in their use. Therefore, in the context of this chapter, training can be defined as follows:

> Operators and maintenance technicians are trained to carry out the tasks and instructions described in the operating and maintenance procedures.

Training is an integral part of all process safety management (PSM) standards. The regulators recognize that the effectiveness of all other elements of a management system depends on the manner in which they are implemented.

LEVELS OF COMPETENCE

Most companies build their training programs around levels of competence. As operators and maintenance technicians move into increasingly responsible positions, their training moves from basic and introductory to task specific.

One company's structure for operator training is organized at three levels.

LEVEL 1—BASIC SKILLS

This will be oriented toward someone who is new to the company, or who has been transferred to a technology that is very different from what he or she is used to. A Level 1 operator will have had basic classroom training; he or she will assist in performing routine tasks, but will be under constant supervision of a Level 3 or higher operator. Once qualified an operator at this level can carry out routine tasks such as catching samples. He or she is also capable of recognizing unsafe conditions.

Documentation will consist of standard publications on topics such as safe work practices, work permits, overviews of the processes, and the use of material safety data sheet (MSDS). This person will be given generic equipment training on issues such as how centrifugal pumps work, how to read a distributed control system (DCS) screen, and the internal operation of relief valves.

Many companies use local junior colleges for this type of training. When an operator qualifies, he often has a 2-year degree in plant operations.

LEVEL 2—CERTIFICATION

The Level 1 operator moves on toward certification as a technician. The foundation documents for this work are the plant-specific operating procedures. So, at the basic level, there will be a procedure on how to start a centrifugal pump, say. The trainee will also learn specific operating procedures and will be tested on his or her knowledge of those procedures (and the corresponding checklists). The trainee technician will also be trained in emergency procedures and response.

Once an operator is certified, he or she can assume day-to-day control of the pertinent section of the facility, its equipment, and instrumentation.

LEVEL 3—MASTER TECHNICIAN

Someone qualified at the technician level can move on to master technician. The emphasis up to this point has been on training, as distinct from education (a distinction that is discussed below). A person is trained in how to execute a task; he does not necessarily have a grasp of why he is doing the task, or what to do if things go wrong. For example, an operator may be trained on how to start a pump, but will not necessarily know what to do if something untoward happens, such as the pump blowing a seal, pulling too many (or too few) amps, making strange noises, or vibrating. To address issues such as these, the technician needs education into the principles of pump operation. He or she can try to figure out what is going wrong and what corrective action should be taken. Education is the foundation for troubleshooting skills.

Someone at this level can also serve as a team leader in special areas such as emergency response.

ELEMENTS OF A TRAINING PROGRAM

A training program can be organized into the following categories:

1. Orientation
2. Initial or basic training
3. Site training
4. Abnormal situation management
5. Refresher training

ORIENTATION

Everyone who enters a facility that handles flammable or toxic chemicals must have basic orientation. If the facility is onshore, then this orientation is often carried out at the guard house at the entrance gate and last for around 30 minutes. The visitor is shown a video that provides information on topics such as the following:

- Entry and exit procedures for the facility.
- Rules of the road for anyone driving a vehicle inside the facility, including speed limits, where to park, and whether to leave the keys in the ignition when no one is in the vehicle.
- How to respond to an emergency.
- Basic rules such as not allowing drugs, alcohol, or weapons on the facility.

At the conclusion of the orientation, the newcomer should take a test that shows his or her understanding of basic safety issues. Questions to ask include the following:

1. How do you know that an emergency has been declared (usually through the use of sirens and a public address system)?

2. Where do you go if an emergency is announced?
3. To whom do you report in the event of an emergency after you have reached your assembly point or muster area?
4. What is the signal for the all clear?
5. If you see an emergency situation (such as someone falling), how do you declare an emergency so as to get help?
6. Which areas on the facility are restricted to visitor access and how do you know which they are?
7. What is the facility speed limit?
8. What are the rules regarding alcohol, drugs, and weapons?

INITIAL/BASIC TRAINING

Initial or basic training is designed for people who have little or no knowledge as to how process facilities work. It teaches basic operations (such as how to open a valve or turn on a pump) and covers standard safety practices. This type of training is not specific to any company, facility, or technology. Indeed, in areas where there are high concentrations of process plants (such as the U.S. Gulf Coast), various colleges and institutes provide basic training that is accepted by most of the facilities in the area. This approach is efficient and minimizes differences between companies.

Initial training has a high educational component. Trainees learn about a wide variety of topics such as pumps, valves, electrical motors, instruments, and heat exchangers. It will also cover basic tasks such as how to read a DCS screen, how to light a fired heater, the principles of relief valve operation, and how to read an MSDS. Basic training also covers company-specific issues such as the facility's organizational structure, the products it makes, emergency response plans, departmental functions, chemicals used, and policies to do with safety, environmental, maintenance, and regulatory work practices.

Some of the components of the basic training program are as follows:

- *Safety policies*. This will be concerned principally with occupational or "hard hat" safety.
- *Emergency response and emergency operations*. The new operator will be made familiar with the facility emergency systems, and what his or her role will be should an emergency occur. Training as to how to run particular units during an emergency will come later.
- *Company structure*. This part of the training will provide an overview of the different departments at the site, and what their responsibilities are. It will also explain the lines of authority, both in normal operation and at times of emergency and how the various departments coordinate with one another.
- *Permit to work program*. The basic training will include a thorough explanation of the permit to work system, including lockout/tagout, hot work procedures, and vessel entry procedures. The training should focus on the interface between operations and maintenance. It is essential that the operator trainee knows where the lines of responsibility lie.
- *Personal protective equipment (PPE)*—when and where it is to be used.

- *Special safety equipment*. The operator will be introduced to special safety equipment, such as self-contained breathing apparatus (SCBA) and chemically resistant clothing, and be trained in its use.
- *Regulatory issues* covering environmental policies and procedures, Occupational Safety and Health Administration (OSHA) regulations to do with hot work, lockout/tagout, confined space entry and hearing protection, and HAZWOPER and HAZCOM requirements.

SITE TRAINING

Site training instructs the operators on how to perform specific tasks to do with the equipment for which they are responsible. Training at this level is a mix of classroom work, computer-based training, on-the-job training, and job shadowing. The trainee will also perform simple tasks such as completing log sheets and catching samples for the lab. One company allocates 3 years to this phase of the training, during which the new operator rotates through at least four units.

Some of the components of site training are listed here:

- *Facility and operating units.* Provides the trainee with an understanding of the overall process and of the operating units within it.
- *Major equipment*. Provides an overview of how equipment items work, and how to operate them. The equipment covered will typically include pumps, heat exchangers, distillation columns, compressors, and valves. Generic procedures will include items such as starting pumps, opening and closing valves, and catching samples.
- *Emergency response.* This training covers the emergency response systems that are used within the facility.
- *Instrumentation and safety systems*. The trainee will be provided with an explanation of the facility's instrumentation, computer control systems, and emergency shutdown systems. The principles of measurement and control, including proportional, differential, and integral controllers, are explained.
- *Regulations.* Provide information to do with safety and environmental regulations.

ABNORMAL SITUATION MANAGEMENT

Completion of the site training means that an operator can conduct normal tasks reliably and efficiently. It also means that he or she knows how to handle an emergency. The next level of training/education is to teach the senior operators how to handle process upsets and how to carry out troubleshooting. An important part of this training involves reviewing records of upsets, incidents, and near-misses, and learning how to respond should similar events recur. (The topic of "Abnormal Situation Management" is discussed in Chapter 12.)

REFRESHER TRAINING

Training is not a one-time affair; it has to be ongoing. Refresher training can come from activities such as the use of simulators, drills, participation in hazards analyses, and classroom sessions.

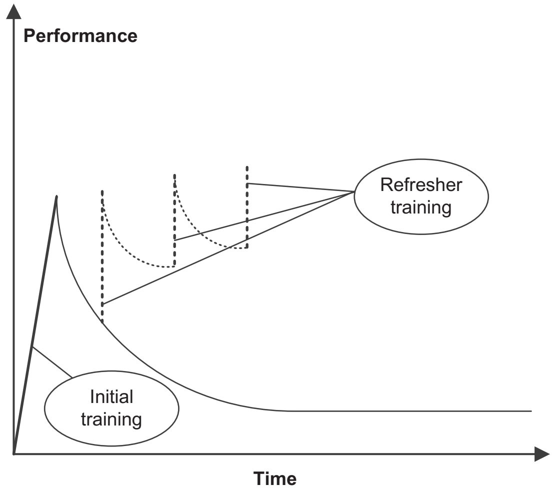


FIGURE 7.1

Training cycles.

The impact of refresher training on performance is illustrated in Figure 7.1

The first step in Figure 7.1 is the initial training. During this period, the trainee's performance improves rapidly. However, if no further training is carried out, performance slips to the lower level shown by the solid curve. Therefore, refresher training is needed. But, after each training session, performance drifts down again, as illustrated by the sawtooth line.

At the conclusion of each refresher training session, performance is greater than the previous peak. This is because the refresher training is being provided on top of the previous training and supplements the hands-on experience and general understanding that is being acquired. Therefore, if refresher training is conducted regularly, the technician's performance will reach higher and higher levels.

SEMS (BSEE)

The Safety and Environmental Management System (SEMS) requirements to do with offshore training are described and discussed in Table 7.1 (some formatting changes have been made). Additional information to do with offshore training is provided by the American Petroleum Institute (API) (2001).

PSM (OSHA)

The training element of the OSHA PSM standard is given in Table 7.2. Once more, the standard is shown in the left column and discussion is provided in the right column.

Table 7.1 SEMS Training Requirements

7.1 General	
The management program should establish and implement training programs so that all personnel are trained to work safely and are aware of environmental considerations offshore, in accordance with their duties and responsibilities. Training should address the operating procedures, the safe work practices, and the emergency response and control measures.	This paragraph identifies the strong link between procedures and training. They are basically two sides of the same coin. There is little point in having procedures if the affected employees are not trained in their use. Equally, it is impossible to provide equipment-specific training without having good quality procedures. Many organizations, including the API, provide training materials and courses. These are referenced in RP 75.
Any change in facilities that requires new or modification of existing operating procedures may require training for the safe implementation of those procedures. Training should be provided by qualified instructors and documented.	Although this paragraph does not use the term "management of change," it is what it is about.
7.2 Initial Training	
7.2.1 Basic Training	
Due to the nature of offshore operations, certain training elements should be provided for the basic well-being of personnel and protection of the environment. Certain examples of appropriate training are: (a) All personnel should receive orientation training per API RP T-1, Recommended Practice for Orientation Program for Personnel Going Offshore for the First Time (latest edition) or the equivalent, prior to their first work assignment offshore.	Many of the men who died in the Piper Alpha catastrophe were trapped in the Living Quarters and had not received the basic safety training described here.
(b) All personnel regularly assigned offshore should receive training, as applicable, in nonoperating emergencies per API RP T-4, Recommended Practice for Training of Offshore Personnel in Non-Operating Emergencies (latest edition), rescue of persons in the water per API RP T-7, Recommended Practice for Training of Personnel in Rescue of Persons in Water (latest edition), and firefighting per API RP 14G, Recommended Practice for Fire Prevention and Control on Open Type Offshore Production Platforms.	This requirement does not apply to visitors.
(c) Appropriate personnel, regularly or occasionally assigned as required by the circumstances, should be trained for safe work practices (e.g., hot work, hot tapping, safe entry, lockout/tagout), simultaneous operations planning, and hazards communication.	
(d) All regularly assigned offshore personnel should be trained as appropriate per applicable governmental regulations.	

Table 7.1 SEMS Training Requirements *Continued*

7.2 Initial Training	
7.2.2 Qualification Criteria	
The management program should require that qualification criteria be developed and implemented for operating and maintenance personnel, as applicable. Procedures should be developed to ensure that persons assigned to operate and maintain the facility possess the required knowledge and skills to carry out their duties and responsibilities, including startup and shutdown. Some examples of appropriate training are: Safety and antipollution device training per API RP T-2, Recommended Practice for Qualification Programs for Offshore Production Personnel Who Work with Anti-Pollution Safety Devices (latest edition), for those who maintain and test safety valves and controls. Crane operation and maintenance training per API RP 2D, Recommended Practice for Operation and Maintenance of Offshore Cranes (latest edition), for those who operate platform cranes.	In addition to generic training, personnel need to be trained in the facility's operating procedures—both standard and task specific. SEMS refers to many of the well-established API documents to do with training.
Well control training per API RP T-6, Recommended Practice for Training and Qualification of Personnel in Well Control Equipment and Techniques for Completion and Workover Operations on Offshore Locations (latest edition) or the equivalent, API RP 59, Recommended Practices for Well Control Operations (latest edition), safe drilling of wells containing hydrogen sulfide per API RP 49, Recommended Practice for Drilling and Well Servicing Operations Involving Hydrogen Sulfide (latest edition), if well target is to or through horizons suspected of containing hydrogen sulfide; production operations where hydrogen sulfide is known to be present per API RP 55, Recommended Practices for Oil and Gas Producing and Gas Processing Plant Operations Involving Hydrogen Sulfide (latest edition). Operating and maintenance training may utilize API recommended training modules and films, or equivalent, and should be reinforced by appropriate demonstrations and "hands-on" training. Reinforcement through on-the-job training is permissible if under the supervision of a knowledgeable operating/maintenance person of proven performance. If hydrogen sulfide is present at levels that require training, appropriate training is required for all personnel, including visitors.	

Table 7.1 SEMS Training Requirements *Continued*

All regularly assigned personnel, as applicable, should be trained in environmental protection and pollution control.	For most personnel, this requirement involves little more than making sure that everyone knows that it is completely unacceptable to spill liquids or drop objects overboard. Senior operators and supervisors need to be aware of the allowable limits for discharges of materials such as produced water, and they must know when they seem to be not in compliance with those limits.
7.3 Periodic Training	
Refresher training should be provided to maintain understanding of and adherence to the current operating procedures. Procedures should be established, such as periodic drills, to verify adequate retention of the required knowledge and skills.	
7.4 Communication	
The management program should require that whenever a change is made in the procedures recommended in other sections, personnel will be trained in or otherwise informed of the change before they are expected to operate the facility.	
7.5 Contractor Training	
Contractors should train their personnel in the work practices necessary to perform their jobs in a safe and environmentally sound manner. The training provided to contract personnel should include applicable site-specific safety and environmental procedures and rules pertaining to the facility and the applicable provisions of emergency action plans. This paragraph applies to contractors performing operating duties, maintenance or repair, turnaround, major renovation, or specialty work at the facility.	Although contractors are responsible for training their people, the ultimate SEMS responsibility for safe operations rests with the facility operator.
Contractors providing incidental services that do not influence operation of the facility, such as janitorial work, food and drink services, laundry, delivery, and other supply services should be trained to perform their jobs in a safe and environmentally sound manner. They should also receive training in transportation safety, emergency evacuation, and other applicable safety and environmental procedures.	
The operator should verify contractor training utilizing a variety of methods, which may include audits of the contractor's environmental, health, and safety training programs; and operator observation of contractor work performance.	

Table 7.2 OSHA PSM Training Standard

(1) Initial Training	
(i) Each employee presently involved in operating a process, and each employee before being involved in operating a newly assigned process, shall be trained in an overview of the process and in the operating procedures as specified in paragraph (f) of this section. The training shall include emphasis on the specific safety and health hazards, emergency operations including shutdown, and safe work practices applicable to the employee's job tasks.	Once more, a clear link between operating procedures and training is spelled out.
(ii) In lieu of initial training for those employees already involved in operating a process on May 26, 1992, an employer may certify in writing that the employee has the required knowledge, skills, and abilities to safely carry out the duties and responsibilities as specified in the operating procedures.	This is a historical issue that is not likely to be relevant any more.
(2) Refresher Training	
Refresher training shall be provided at least every 3 years, and more often if necessary, to each employee involved in operating a process to assure that the employee understands and adheres to the current operating procedures of the process. The employer, in consultation with the employees involved in operating the process, shall determine the appropriate frequency of refresher training.	
(3) Training Documentation	
The employer shall ascertain that each employee involved in operating a process has received and understood the training required by this paragraph. The employer shall prepare a record which contains the identity of the employee, the date of training, and the means used to verify that the employee understood the training.	

PROCEDURES AND TRAINING

It has already been pointed out that there is a very strong link between procedures and training. Indeed, some companies refer to their operating manual as the training manual. This is probably not a wise choice. The two documents are different and serve different goals. An operating manual describes how to carry out specified tasks; the training manual provides much greater details and explanation.

One way of linking procedures with training is to provide a training video that shows an experienced operator actually working through the steps in the appropriate module. While describing what he was doing for each of the steps, the words and actions would be recorded on a video. The tape/DVD would then be kept in the control room so that the operators could review it at any

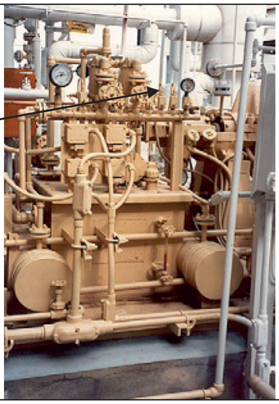
	By	Action	√	Discussion/Illustration	How	Why
8		. . .				
9	UO	Check the lube oil temperature using TI-7103A-2.				
	YIELD		NEVER START THE LUBE OIL PUMP IF THE LUBE OIL TEMPERATURE IS ABOVE 150F.			
10	UO / UT	If the lube oil temperature is above its safe limit **THEN** . . .		Information regarding troubleshooting lube oil systems is provided in procedure 01-GEN-34.		

FIGURE 7.2

Example of operating task instructions.

time. It could also be used to describe incidents that have occurred in the past relating to this step and he could also use it to show visually any difficulties or special features of the operation. Such a video would provide a fine foundation for a troubleshooting program.

Training can be integrated into the modular concept of operating procedures, as described in Chapter 6—*Operating Procedures*. Along with the action and response columns, two additional columns can be inserted: one of them called "How?" and the other "Why?"—as illustrated in Figure 7.2. The "How?" column (training) provides a link to task instructions. The "Why?" column (education) provides a link to background information.

MANAGEMENT OF A TRAINING PROGRAM

The management of a training program typically has the following three key elements:

1. Development of a training matrix that identifies training needs by job description.
2. Preparation of a schedule and budget.
3. Progress measurement.

	Initial	Task	Facility-Specific	Refresher
Operations	X	X	X	X
Maintenance	X	X	X	X
Administrative staff	X			X
Contractors	X	X		X
Technical staff	X		X	X
Management	X			X

FIGURE 7.3

Training matrix.

TRAINING MATRIX

Most organizations develop a training matrix such as that shown in Figure 7.3 to determine who needs training in which topics. A matrix such as this allows management to structure a career and development path for each employee, thus avoiding the "spray and pray" concept in which everyone receives the same training, regardless of their needs or the requirements of their work.

An "X" in Figure 7.3 indicates that training is required for persons in that job category. Figure 7.3 shows that all personnel, no matter what their role, must receive refresher training on a regular basis.

Supporting the high-level matrix shown in Figure 7.3 will be submatrices, typically one for each training category. Figure 7.4, e.g., shows just some of the elements of the initial training; it also shows which persons need to take which training elements.

The following conclusions can be gleaned from Figure 7.4:

- The training program has been organized into three categories: safety, system (i.e., the overall process), and equipment.
- All persons must know how to report an incident.
- Specialized topics (such as how to use the one call system) are assigned only to those who need to know about them.
- In general, supervisors need the most training.

Many of the topics listed in Figure 7.4 can themselves be broken down into even more detailed matrices. For example, the "incident reporting" section can range from basic, "how to report a fire" all the way to, "communicating with the media." Also, some of the training will be restricted to a small audience. For example, only those involved with onshore pipelines will need to know about the "one call system."

BUDGET ALLOCATION

A budget breakdown for training could be as follows:

- New hires: 20%
- Outside operators: 25%
- Control room operators: 35%
- Supervisors: 20%

	Safety			System			Equipment		
	Basic first aid	*Incident reporting*	*Other . . .*	*Tank farm*	*One-call system*	*Other . . .*	*PSV testing*	*Compressor ops*	*Other . . .*
Operations									
Supervisors	X	X		X			X	X	
Level 1 technician	X	X		X			X	X	
Level 2 technician	X	X		X				X	
Level 3 technician	X	X		X					
. . .									
Maintenance									
Supervisors	X	X		X			X		
Level 1 technician	X	X		X			X	X	
Level 2 technician	X	X							
. . .									
Administrative staff									
Office worker		X							
Casual contractor		X							
. . .									
Contractors									
Supervisors	X	X							
Fitters		X							
Riggers		X							
. . .									
Geotech supervisor		X			X				
Compressor specialist		X						X	
. . .									

FIGURE 7.4

Initial training matrix.

Difficulties to do with training often involve budget cutbacks. If a facility finds that it is behind its financial targets, the management will try to cut back on "nonessential" items. Training is often one of those items because the benefits of training tend to be long term.

MEASURING PROGRESS

When managing a training program, it is useful to keep track as to who has been trained on what using a matrix such as that described for operating procedures. Table 7.3 is an example of such a

Table 7.3 Training Progress

	Number of Operators	Days/ Operator	Total Man-Days	Man-Days Completed	Progress
Basic					
Utilities	20	3	60	20	33%
Unit 100	16	3	48	25	52%
Unit 200	12	3	36	25	69%
Unit 300	12	3	36	25	69%
Unit 400	20	3	60	25	42%
Unit 500	8	3	24	24	100%
Total	**88**		**264**	**144**	**55%**
Detailed					
Utilities	20	10	200	100	50%
Unit 100	16	9	144	25	17%
Unit 200	12	12	144	25	17%
Unit 300	12	4	48	25	52%
Unit 400	20	3	60	0	0%
Unit 500	8	8	64	25	39%
Total	**88**		**660**	**200**	**30%**
Certification					
Utilities	16	1	16	0	0%
Unit 100	12	2	24	1	4%
Unit 200	12	1	12	0	0%
Unit 300	12	1	12	0	0%
Unit 400	20	1	20	0	0%
Unit 500	8	1	8	8	100%
Total	**80**		**92**	**9**	**10%**
Overall			**1016**	**353**	**35%**

matrix. It shows, e.g., that 20 operators work in the utilities area, that each of these operators requires 3 days of training giving a total of 60 man-days of required training. In this example, 20 man-days have been completed, so this section of the program is 33% complete.

ECONOMICS OF TRAINING

Although everyone agrees that operators and maintenance workers must be trained, the scope of the training program is often open for discussion. Ultimately, of course, the workers must be trained so that the facility is safe and profits maximized. Such goals are difficult to determine for qualitative issues such as training, but every effort should be made to organize the training program so that it is economically effective.

A rough estimate as to the cost of *not* training personnel is to review the facility's incident register and the associated root cause analyses to see how much the lack of training contributed to those incidents.

For example, a process facility may send a sample of each product batch to the lab for testing before that product is shipped to customers. Investigation of incidents to do with shipping off-quality material shows that, during the last financial year, the lab approved two shipments that were, in fact, off-spec. The cost of each incident was approximately $20,000. In each case, the incident could be attributed to lack of training. Hence the justification for an upgraded training program for the lab technicians is in the region of $40,000 per annum.

PROCESS SIMULATORS AND EMULATORS

Computer-based training is widely used in many industries, particularly aerospace and nuclear power, to increase the effectiveness and efficiency of the training program. Although the use of simulators has been less widespread in the process industries, they are becoming more widely accepted because of the similarities between the process industry and airlines and nuclear power facilities. These similarities include the following:

- The use of complex and sophisticated control systems.
- High capital costs, which means that economic losses can be very high.
- High operating costs.
- The potential for major loss of life in the event of a major accident.

FEATURES

Ayral and de Jonge (2013) note that a computer-based training should possess the following features:

- The simulator should show to the trainee the same equipment and control systems as the real facility.
- The training environment should be very similar to that of the control room.
- The models used by the simulator should be accurate and events should happen at roughly the same speed as they would in the facility.
- The model should allow the instructor to make sudden changes to the process conditions, such as stopping a major equipment item "out of the blue."
- Trainees should be able to operate the simulator without the instructor being present.
- The simulator should be kept up to date to reflect changes that are made to the actual facility.

BENEFITS

There are four major benefits to the computer-based training, which are as follows:

1. The number of operator errors should be reduced, thus reducing maintenance costs and increasing onstream times. For example, computer-based training is seen as being a significant

factor in a 10% increase in the availability of French nuclear power facilities over a 10-year period.

2. The operating team will develop the skills needed to optimize the performance of the unit that they are running.
3. Process plant operations are generally much more smooth and reliable than they were some years ago. One downside to this situation is that operators have less experience than they had in the past of running the process under upset conditions. They can gain some of this experience through the use of simulated upsets.
4. Related to the above point, operators can also be trained to respond to major emergencies.

SIMULATOR DESIGN

The basic concept behind simulation is shown in Figure 7.5.

It is possible to develop generic models for processes that are found in many companies—most of the operations in a refinery, e.g., are similar, regardless of the location. In these cases, an emulator can be developed. Even though it does not precisely mimic the behavior of a specific unit, an emulator is good for training new operators. The emulator does not have to be in the control room. Indeed it could be off-site. (Some of them are owned and operated by local colleges.)

The right side of Figure 7.5 shows the actual facility operation. The operator runs the facility through a DCS terminal. On the left side of Figure 7.5 is the simulator. This is a mathematical

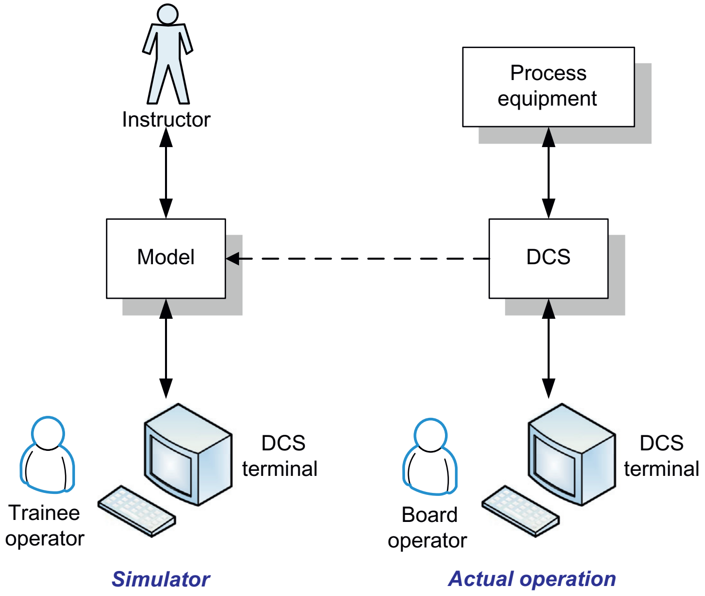


FIGURE 7.5

Simulation.

model of the facility that is loaded on to a stand-alone computer. The simulator interface looks and feels exactly like the actual DCS terminal. “Behind” the simulator is an instructor who creates upset conditions to which the trainee operator must respond. The simulator is essentially a video game and is highly analogous to pilot flight simulators. The operator learns how to troubleshoot and thus save a lot of money for the facility.

Figure 7.5 shows a one-way flow of information from the DCS to the model (the line is dashed to indicate that this capability is not always provided). Actual data from the facility enters the simulator, thus allowing the trainee operator to work with live information. The information flow is most definitely one way. There is no way in which the trainee operator can affect actual operations.

Simulators are not only used to train operators, they can also be used by operations management and engineering to see what happens if they want to try new operating conditions. It is important, however, to treat the predictions of such a simulation with care, particularly if the model is extrapolating rather than interpolating, as illustrated in Figure 7.6, which shows the reaction rate for a particular chemical reaction as a function of temperature.

Points A and B represent the range of current, normal operation. By drawing a line through them, it is possible to predict the reaction rate at temperature C and to determine if the operation at that point is safe.

The problem with extrapolation is that the forecast may fail to predict the introduction of some new function that creates a nonlinear change in the dependent parameter. In Figure 7.6, it can be seen that the chemical reaction rate starts to rise quite rapidly between temperatures B and C. Clearly some change in the reaction chemistry has taken place in this temperature range. If the new reaction is not known about, then the simulator algorithm will not accurately predict the fact that, because the reaction rate increases exponentially, the reaction will be higher than anticipated.

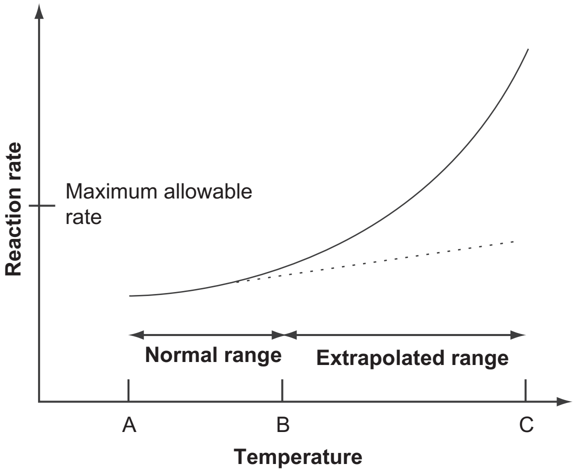


FIGURE 7.6

Interpolation and extrapolation.

TESTING AND CERTIFICATION

Once an operator or maintenance technician has completed a training program, he or she has to be tested to make sure that they understood what they were taught. Testing is not an option; only if people pass the appropriate tests can management be sure that their employees know enough to operate the facility safely. At every step in the training process, the operator must be tested against some objective standard, with a clearly defined measure as to the distinction between passing and failing.

The tests can be highly structured, using a computer-based input. But less formal tests may be even better. For example, a supervisor may walk around the unit with the trainee operator. During the walk around, the operator is asked to show how he or she would carry out a particular task or respond to a change in operating conditions. On one refinery, a supervisor told his trainee operators that they would be asked to draw a sketch of the unit from memory, and then, also from memory, show the location of all the firefighting equipment. The trainees knew about the question ahead of time, but it was not open book; they could not look at notes, and they could not look at the unit through the window.

A good test question has the attributes listed in Table 7.4.

Each facility must decide on its policy concerning "grandfathering," i.e., whether or not it is acceptable for a very experienced operator who has not participated in the most recent training program, and who has not taken the tests associated with that program, to avoid having to take the test on the grounds that his experience makes it unnecessary. This can be a very delicate topic; if an operator has worked on a unit for a long time, the idea of being tested can be very threatening. Yet, it might be that management has to insist on his taking the test, because it could be, that, in spite of his experience, the operator really is not properly trained, especially in emergency operations.

Once the employee has passed the tests for an area and for a job class, the facility may choose to certify him or her. The exact meaning of the word "certification" in the context of process safety is open to interpretation and will vary from site to site. It can also have legal implications, e.g., in the negotiation of union contracts.

Table 7.4 Effective Questions

Attribute	Discussion
Simply worded	The purpose of the question is to test the technician's knowledge, not his or her language skills.
Well defined	The questions should be clear, with no potential for ambiguity or multiple correct answers (unless an "All of the above" option is provided). Where possible, a quantitative answer should be called for.
Reasonable	The person taking the test must have a reasonable chance of getting a correct answer. At the same time, the questions should be challenging; they should not be too easy.
Relevant	The questions should be relevant to the topic that the technicians are learning about.
Demanding	The questions should be thought-provoking in order to show understanding. Demonstration of the correct thought process is sometimes more desirable than simply knowing the right answer (c.f., the difference between training and education). Ideally, the test questions themselves will contribute toward the learning process.

SAFEGULF

SafeGulf is a program for training workers in the offshore industry. It defines its role as follows:

> A volunteer organization comprised of operating companies, industry associations, and educators with the purpose of having a standardized orientation which sets minimum requirements for the US Offshore E&P Industry.

Operator members include the following:

- PEC Safety
- BP America Production Company
- Chevron
- ExxonMobil U.S. Production Company
- Hell Exploration and Production Company

Under this program, all contractors must fulfill minimum Health, Safety, and Environmental (HSE) training requirements prior to working on operator premises in the Gulf of Mexico. A database is maintained for all those who have had this training.

Topics covered by SafeGulf include the following:

- Incident Reporting and Investigation
- Accident Prevention Signs and Tags
- Hand Safety
- Back Injury Prevention
- Behavioral Safety
- Bloodborne Pathogens
- Confined Space
- Lockout/Tagout
- Drug and Alcohol
- HazCom
- HAZWOPER (First Responder)
- Electrical Safety (Non-Qualified)
- Intervention
- Fire Prevention and Portable Fire Extinguishers
- Walking Working Surfaces
- Job Safety and Environmental Analysis
- Offshore Orientation and Emergency Evacuation
- Personal Protective Equipment, Respiratory
- Prevention of Workplace Violence
- Marine Debris
- Fall Protection: Introduction
- Permitting
- SafeGulf Maritime Security

The SafeGulf basic training is supplemented by specialized training, as needed. Some of this specialized training takes the form of industry certification programs.

PIPELINE OPERATOR TRAINING

Specific issues to do with the training of pipeline operators are listed here:

- Pipeline shutdown and startup
- Pipeline pigging
- Electric arc welding
- Atmospheric corrosion
- Electrical insulator inspection and casing testing
- Oxygen/acetylene welding
- Locating and marking pipelines
- Basic Supervisory Control and Data Acquisition Systems (SCADA)
- Pressure testing for steel and plastic pipelines
- Hot tapping and stopping
- Characteristics and properties of natural gas
- Excavation safety
- Compressor operation
- Pipeline purging
- Valve maintenance
- Cathodic protection
- Inspection and testing of relief valves, regulators, and control valves
- Pipeline crossings
- Protective coatings
- Natural gas operations and maintenance
- Internal corrosion monitoring
- Installation of anodes;
- Cathodic protection troubleshooting
- Leak survey and classification
- Emergency plans and public relations
- Odorization
- Pipeline leak repair

CHAPTER

8 PRESTARTUP REVIEWS

CHAPTER OUTLINE

INTRODUCTION

The purpose of a prestartup review (PSR) is to ensure that initial start-ups, or start-ups following major project work, proceed safely and smoothly. Alternative names for the same activity are prestartup safety review (PSSR) and operational readiness review. As with most process safety activities, a PSR will generally be performed by a small team made up of representatives from operations, maintenance, engineering, and safety.

The review has two major components, which are as follows:

1. Ensure that all action items and recommendations from hazards analyses and other reviews such as management of change (MOC) have been completed as required.
2. Ensure that no changes that could affect safety or operability have crept into the system during the construction or equipment installation phases of a project.

The review represents the last chance to catch any problems. Therefore, it should be led by the personnel who will be required to run the modified system.

Generally, the following issues will be covered by the review team:

- Equipment and instrumentation items that have been changed are installed and commissioned in accordance with design specifications.

Process Risk and Reliability Management. DOI: http://dx.doi.org/10.1016/B978-0-12-801653-4.00008-4

- Safety, operating, maintenance, and emergency procedures are in place and are adequate.
- All findings from hazards analyses, MOC evaluations, and other types of review have been closed out properly.
- All affected personnel have been trained in the new or modified operation.

Readiness reviews are important because projects frequently fall behind schedule and/or run over budget, thus creating pressure on the project team to eliminate or postpone the installation of any items that are not absolutely necessary for the start-up. If not controlled properly, this can lead to corner-cutting—either intentional or inadvertent—which may in turn jeopardize the safety or operability of the modified facility. The review gives the operations department the authority to refuse to accept "care, custody, and control" of a facility that they judge to be unsafe or difficult to operate. In effect, a PSR provides a breathing space for everyone to make sure that the plant that they are about to start is safe.

It is not the purpose of a readiness review to replace this normal "punching out" of the facility that is done during the turnover phase of the project (Chapter 18).

A PSR has the form of an audit but it is not a formal audit. The purpose of the review is to make sure that all work that had to be done prior to start-up was in fact done; it is not the purpose of the review to evaluate the work itself. Therefore, the review can be more flexible than an audit. For example, on one facility, there had been times when operations personnel, acting on their own initiative, had bypassed by certain instruments without going through proper procedures. During a turnaround, the interlock system was upgraded in order to prevent such unauthorized overrides. Part of this facility's review was to have a knowledgeable and determined operator try to override the new interlock (while the plant was shut down), in order to see if he could "beat the system." This type of activity would not be carried out during a conventional audit.

Readiness reviews cover not only equipment but also "soft" issues, such as operating procedures and training. These are particularly important with regard to restart reviews—it is vital that the operating procedures be updated to reflect the changes that have been made, and that the operators are then trained in the new procedures before they start work on the modified facility.

Readiness reviews sometimes identify problems with respect to documentation and records. During the construction and commissioning of a plant, there is usually considerable pressure just to get the plant completed and up and running. Hence the record-keeping part of the project may slip. If, in the judgment of the review team, some of the missing documents are important to safety, then the team must insist that those documents are completed and issued before the plant is started.

WHAT THE REVIEW IS NOT

It is tempting to treat a PSR review as a chance to catch up on activities that should have been carried out earlier in the project. This temptation must be avoided. Particular concerns include the following:

- A PSR is not a last-minute hazards analysis. The review team must check that the right types of hazards analysis were carried out at the right times, and that the quality of those analyses is satisfactory. The team must also check that all the findings were implemented or closed out in a professional manner. But the team does not actually analyze the new system for hazards.

- The review team does not check basic design standards or calculated values. It may check that the appropriate rules and standards were followed, but the review does not perform actual engineering work.
- The review is not part of the MOC process. It is carried out once the MOC procedures have been completed.

REGULATIONS

PSSRs are an integral part of all process safety management (PSM) regulations. In the United States, the PSSR requirements from Occupational Safety and Health Administration (OSHA) and Environmental Protection Agency (EPA) are very similar. Offshore facilities are regulated by the Bureau of Safety and Environmental Enforcement (BSEE) in their Safety and Environmental Management Systems (SEMS) rule. They use the term PSR.

OSHA'S PSM

The OSHA standard is discussed below, as being representative of regulations to do with operational readiness and PSRs. It is to be found in paragraph (i) of the regulation as given in Table 8.1. The agency's guidance on the topic is provided in Table 8.2.

The first paragraph of the regulation states that a PSSR is needed whenever process safety information is changed. Since virtually all changes result in updates to the facility documentation, particularly piping and instrument diagrams (P&IDs), the effect of this requirement means that virtually all changes will have to be reviewed by a PSSR. There are very few changes that do not require some information changes to do with topics such as safe limits, engineering drawings, and equipment lists.

(i) Construction and equipment

Paragraph (i) of the standard requires that construction and equipment is in accordance with design specifications. PSSR team members can carry out spot-checks of the installed piping and equipment, and compare it with the piping lists and equipment data sheets.

Table 8.1 OSHA PSM Regulation

The employer shall perform a PSSR for new facilities and for modified facilities when the modification is significant enough to require a change in the process safety information.

The PSSR shall confirm that prior to the introduction of highly hazardous chemicals to a process:

(i) Construction and equipment is in accordance with design specifications.
(ii) Safety, operating, maintenance, and emergency procedures are in place and are adequate.
(iii) For new facilities, a process hazard analysis has been performed and recommendations have been resolved or implemented before start-up; and modified facilities meet the requirements contained in MOC, paragraph (l) (of this regulation).

Table 8.2 OSHA PSM Guidance

For new processes, the employer will find a PHA helpful in improving the design and construction of the process from a reliability and quality point of view. The safe operation of the new process will be enhanced by making use of the PHA recommendations before final installations are completed. P&IDs are to be completed along with having the operating procedures in place and the operating staff trained to run the process before start-up. The initial start-up procedures and normal operating procedures need to be fully evaluated as part of the PSR to assure a safe transfer into the normal operating mode for meeting the process parameters.

For existing processes that have been shut down for turnaround, or modification, etc., the employer must assure that any changes other than "replacement in kind" made to the process during shutdown go through the MOC procedures. P&IDs will need to be updated as necessary, as well as operating procedures and instructions. If the changes made to the process during shutdown are significant and impact the training program, then operating personnel as well as employees engaged in routine and nonroutine work in the process area may need some refresher or additional training in light of the changes. Any incident investigation recommendations, compliance audits, or PHA recommendations need to be reviewed as well to see what impacts they may have on the process before beginning the start-up.

Table 8.3 SEMS Rule

Your SEMS program must require that the commissioning process includes a prestartup safety and environmental review for new and significantly modified facilities that are subject to this subpart to confirm that the following criteria are met:

a. Construction and equipment are in accordance with applicable specifications.
b. Safety, environmental, operating, maintenance, and emergency procedures are in place and are adequate.
c. Safety and environmental information is current.
d. Hazards analysis recommendations have been implemented as appropriate.
e. Training of operating personnel has been completed.
f. Programs to address MOC and other elements of this subpart are in place.
g. Safe work practices are in place.

(ii) Procedures

Paragraph (ii) requires that the facility's procedures reflect the manner in which the facility is to be operated after the process changes have been made. The PSSR should check that safety, operating, and emergency procedures for the new operation have been written down, and that they accurately describe what has to be done. This paragraph does not mention training, but it can be assumed that operators and maintenance workers must be trained in the use of the new procedures.

(iii) New/modified facilities

The regulation requires that new facilities conduct a process hazards analysis (PHA). The PSSR team should check that the PHA was, in fact, carried out, and that its recommendations were either resolved or implemented. During the pressure of construction, there is sometimes a tendency to postpone some of the PHA recommendations until "there is sufficient time." The PSSR should check that the recommendations have, in fact, been closed out properly.

SEMS

The SEMS rule for offshore safety in the U.S. waters is given in Table 8.3.

TYPES OF REVIEW

The size and scope of the PSR will be adjusted according to the size and complexity of the changes that were made. The following four categories are representative.

REVIEW NOT REQUIRED

Not all start-ups require that a review be carried out. The following are examples:

- Immediate start-up following utility failure where no equipment maintenance or opening of equipment has been performed.
- Start-up following short duration shutdown (less than 30 days) for inventory management.
- Start-up of existing equipment where the work permit system and the unit local procedure are sufficient for safely managing the activities involved.
- Restart of equipment post online cleaning.

SMALL PROJECTS/ENGINEERING CHANGES

Reviews at this level are limited in scope; they apply only to small projects and process equipment or procedure changes. Generally they follow on from the MOC process.

MEDIUM SIZE

The second level of review applies to the start-up of a unit after a maintenance turnaround has been completed or the unit has been down for a significant time period. It also applies to small project or hardware change involving the construction and start-up where:

- It is necessary to make significant revisions to the operating procedures or develop new operating procedures.
- Training is required for operations, maintenance, and engineering personnel because new equipment has been installed.
- There is significant impact (not major) on utilities, environmental operations, and maintenance.
- Start-up after shutdown for turnaround activities.
- Start-up after shutdown for catalyst change or catalyst regeneration activities.
- Start-up after shutdown of a group of equipment for maintenance or cleaning where coordination of several disciplines is required.
- Start-up after shutdown following a significant incident such as fire, release, or explosion.
- Start-up after a significant natural event such as an earthquake or storm that resulted in equipment shutdown.
- Long-term shutdown (greater than 30 days).

LARGE PROJECTS

Large reviews apply to major projects that involve the construction and start-up of an entire process unit or a significant portion of a process unit where:

- It is necessary to make major revisions to or develop several new operating procedures.

- A substantial amount of training is required for operations, maintenance, and engineering personnel.
- There is a major impact on utilities, environmental operations, and maintenance.
- The project will interface with several units either by piping connections or by the need to communicate operating activities.

A very large project may not require that a PSSR be carried out because it will have its own precommissioning, commissioning, and start-up procedures. However, a PSSR may be used to coordinate changes with other operating units.

RESTART REVIEWS

PSRs should also be conducted on equipment that have been idle for an extended period, even if it has not been intentionally modified. The team should also check on any MOCs that were issued while the equipment was down and then check that they were closed out properly.

The following are reasons for conducting a restart review:

- If a plant has been shut down for a long time, changes may have been made to it. In particular, personnel from other departments may have cannibalized the shutdown equipment for spare parts. Also, a unit that is down for an extended period may be changed inadvertently. For example, it may be decided to add nitrogen padding to some equipment. This is a change that has to be reviewed.
- If equipment is not used for a few weeks or months, and is then restarted, it may be found that it may not work as it should. For example, pump shafts may have bent out of alignment, pockets of corrosive materials may have formed at the base of storage tanks, instruments contacts may have covertly failed, equipment and piping may have corroded, rotating equipment shafts may have bent, and seals may be degraded.
- During the shutdown period, external factors may have changed. For example, the composition of the streams feeding the unit may be different, or the utilities that it uses may have changed properties.
- It is unlikely that the operations and maintenance personnel will have been retained to work on the unit while it was shut down. Therefore, on restart, new people will have to be brought in, and experienced personnel brought back up to speed.

ORGANIZATIONAL RESPONSIBILITY

Since the primary purpose of a readiness review is to ensure that the operations department receives a unit that is safe to operate, it is their responsibility to accept or reject the system that is turned over to them. Therefore, it is suggested that the leader of the review team should be the operations manager or superintendent who has line responsibility for the safe operation of the unit on restart. Others, such as the process safety specialists, support this person by providing checklists, conducting the detailed reviews, and preparing final reports. However, the final decision as to whether or not the plant is safe to operate rests with the operations manager.

TIME REQUIRED

When estimating the time, it will take to conduct a readiness review factors such as the following should be considered:

- Number of P&IDs
- Number of pressure vessels
- Number of storage tanks
- Number of items of rotating equipment
- Complexity of the control scheme
- Materials of construction
- Number of underground lines

TEAM STRUCTURE

A readiness review is a team activity. The leader of the team must be someone who represents the operations department because, as already discussed, the whole purpose of the exercise is to ensure that the operations people are provided with a plant that is safe. Contractor employees and representatives may assist the team, but basically the work should be organized and run by the operating company.

The review team can include the following personnel, depending on the size and nature of the project:

- A review team leader—usually the person who will be charged with starting up the new system
- Plant personnel—particularly those on the start-up team
- The project manager or technical lead
- A safety representative
- The construction lead
- A representative from the hazards analysis team

The leader should have sufficient authority to delay the start-up if he or she identifies a significant deficiency. Given that such a delay could lead to the loss of thousands of dollars of production, the leader may find himself or herself under very strong pressure to let things go ahead as they are. He or she must have the personality and the organizational authority to resist such pressures.

USING THE ELEMENTS OF PSM

One way of organizing a readiness review is to structure it according to some of the elements listed as Table 8.4, which gives the elements that generally require the greatest attention during a readiness review.

KNOWLEDGE MANAGEMENT

The review team will determine if all documentation such as P&IDs and material safety data sheet (MSDS) have been updated.

Table 8.4 Elements of OIM

- Process Safety Culture
- Compliance
- Competence
- Workforce Involvement
- Stakeholder Outreach
- Knowledge Management
- Hazard Identification/Risk
- Operating Procedures
- Safe Work Practices
- Asset Integrity/Reliability
- Contractor Management
- Training/Performance
- Management of Change
- Operational Readiness
- Conduct of Operations
- Emergency Management
- Incident Investigation
- Measurement and Metrics
- Auditing
- Management Review

OPERATING PROCEDURES

The focus of most projects is on getting the equipment built, installed, and commissioned. There is a tendency to put off writing the operating procedures until the last minute. This raises the potential for having sections of the plant for which procedures have not been written at all, or where the quality of what has been written is low.

It is particularly important to carefully evaluate operating procedures during a restart safety review. In such situations, the plant is only being modified, and it is likely that there is already a set of operating procedures. However, the project changes may lead to substantial changes in the way the facility is operated and so in the content of the operating procedures.

ASSET INTEGRITY/RELIABILITY

The operations team must be sure that the equipment that has been installed or changed will perform properly and that it meets all the pertinent design specifications.

Inspection reports, which are an integral part of the mechanical integrity program, should be reviewed because they demonstrate that the plant was constructed according to the design standards.

TRAINING/PERFORMANCE

As with procedures, there is a danger that training could be delayed and deferred because everyone (including the operators) is so busy getting the facility physically ready. Therefore, the readiness review team should pay particular attention to the quality of the training program.

CHAPTER

9 ASSET INTEGRITY

CHAPTER OUTLINE

As mentioned in the Preface to this book, a companion volume entitled *Design and Operation of Process Facilities* is under preparation. One reason for creating a second volume was that the bulk of *Process Risk and Reliability Management* was becoming so large as to make it unmanageable. Much of the material that was in this chapter—asset integrity—has been transferred to the new book. What is provided here is a review of the process risk and safety management principles to do with the design and management of equipment and instrument systems.

INTRODUCTION

An asset integrity program seeks to ensure that all equipment, piping, instrumentation, electrical systems, and other physical items in a unit are designed, constructed, inspected, and maintained to the appropriate standards. The term "mechanical integrity" is used by some organizations—particularly OSHA. However, the term "asset integrity" is used here in order to ensure that nonequipment items—particularly instrumentation—are included in the program.

ENGINEERING STANDARDS

The use and application of engineering standards is crucial to having an effective asset integrity program. The development and organization of these standards is discussed in Chapter 2.

Process Risk and Reliability Management. DOI: http://dx.doi.org/10.1016/B978-0-12-801653-4.00009-6

INHERENT SAFETY

A concept that threads throughout this book is that of inherent safety. The basic idea is that, were a system to fail, it would end up in a safe state regardless of the existence and effectiveness of safeguards. (The term “inherent safety” is actually a little misleading. Risk can never be zero, and perfect safety can never be achieved. Hence the term “inherent*ly* safer” is probably a better choice.)

For example, a facility may use a chemical additive as part of a reaction control system. The chemical additive can be supplied either in water solution or in hydrocarbon solvent. The water is nonflammable, whereas the solvent can burn. Therefore, with respect to fire, the first is inherently safe, the second is not. (The water-based additive is not inherently safe in all of its properties. For example, if the additive is toxic, then it poses a threat to any person who may ingest it.)

Inherent safety is usually divided into different categories such as those in the following. They are generally addressed in the order shown, i.e., those at the top of the list provide greater security than those toward the end.

1. Eliminate
2. Minimize (intensify)
3. Substitute (attenuate)
4. Moderate (limit effects)
5. Simplify (error tolerance)

Although these principles can be followed at any time, they are generally most effective when used in the design stage of a project.

ELIMINATE

The only way of reducing risk to zero is to remove the hazard that creates that risk. (“If a tank’s not there, it can’t leak.”) For example, in the standard example, liquid is transferred from a tank to a pressure vessel with a pump. The pump contains hazards such as the possibility of a seal leak or the possibility that it may fail at a critical phase of the operation. If the design can be changed such that the liquid flows under gravity, then all the hazards associated with the pump will disappear.

Changes to the operation may also help eliminate an activity. If the liquid does not need to be transferred on a continuous basis, it may be possible to wait for time periods when the downstream pressure is zero, so no pumping of any kind is needed.

With regard to the standard example, if the process can be operated without needing Tank, T-100 at all, then all of the hazards associated with that tank simply disappear.

Another way of eliminating risk is to eliminate an activity and so removing the change of that activity going awry.

General questions to do with the elimination of risk include the following:

- Can a hazardous material be eliminated?
- Can a flammable material be eliminated?
- Can an additive be removed?
- Can equipment no longer in use be removed?
- Can piping no longer in used be removed?

Remove equipment

The decision to remove equipment may be resisted by operations personnel. For example, a process may have two operating units. Unit A produces an intermediate chemical that is stored in a tank that has say 1 hour of holding capacity. The chemical is pumped from the tank to Unit B that carries out further reactions and processing. This simple system is illustrated in Figure 9.1.

The purpose of the tank is to dampen out swings in flow rates. If Unit A is producing more chemical than Unit B needs for a short period of time, then the level in the tank is allowed to rise, and vice versa. Eliminating the tank may appear to make the system safer. However, operations could become more difficult and safety in other areas could be compromised. This is an example of the law of unintended consequences (discussed below).

When considering the "eliminate" option, the following checklist questions should be considered:

- Can a hazardous material be eliminated?
- Can a flammable material be eliminated?
- Can an additive be removed?
- Can equipment no longer in use be removed?
- Can piping no longer in used be removed?

Remove people

"If a man's not there, he can't be killed." The risk associated with a system can be moderated by moving personnel away from the equipment. Ideally, people will not be present at all.

An excellent example of the effect of removing people occurs almost every year in the Gulf of Mexico. Typically three or four destructive hurricanes enter the Gulf each year. These hurricanes can and do cause serious damage to platforms. Yet the number of people who are killed or injured is zero because the platforms are always evacuated well before the hurricane arrives.

In many cases, it may not be possible to entirely eliminate a hazard, but it may be feasible to substitute a high-risk hazard with one that has inherently less risk, thus improving "inherent safety." For example, if the hazardous chemical RM-12 in the standard example can be replaced with another chemical that is less toxic and flammable, then the consequences of an overflow are reduced. Examples of substitution are given in the following sections.

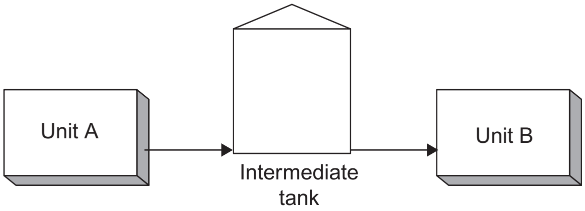


FIGURE 9.1

Intermediate storage tank.

MINIMIZE

Where possible, smaller quantities of hazardous materials should be used. This philosophy comes in part from the Bhopal tragedy. The facility stored large quantities of the intermediate compound methyl isocyanate that created the toxic cloud. Had the facility been designed so as to greatly reduce this inventory—a technically feasible solution—then the consequences of the event would have been much less severe.

General minimization questions include the following:

- Can inventories be reduced through the use of just-in-time management?
- If inventories are held by a supplier or vendor, are their risk management procedures better than those on site?
- Can the length of piping containing hazardous materials be reduced?

There is one situation where minimization may not be appropriate, and that is to do with adding overcapacity to equipment. Although the design engineers are under constant pressure to reduce the size of equipment so as to save costs, some overdesign can help take care of operational upsets and changes in performance. For example, adding extra tubes to a heat exchanger may help handle temperature surges and they may reduce the internal between exchanger cleanings, thus reducing the exposure of maintenance personnel.

SUBSTITUTE

The next step in addressing inherent safety is to replace a hazardous material with one that is less hazardous. Thus the consequences of a release are fundamentally less dangerous.

General questions to do with substitution include the following:

- Can less volatile or flammable solvents be used?
- Is it possible to replace powders or dusty solids with pellets?
- Can changes to piping design remove the need for nozzles, bellows, and expansion joints?

A classic example of substitution concerns the use of hydrogen fluoride (HF) as an alkylation catalyst in oil refineries. The properties of HF that make it such an effective catalyst also make it a highly solvent and toxic chemical in the event of a release. An alternative alkylation catalyst is sulfuric acid. Although sulfuric acid is also a hazardous material, it cannot cause a catastrophic accident when released in the way that HF can.

Another example of substitution includes the use of aqueous rather than anhydrous ammonia.

MODERATE

Moderation accepts that a certain condition exists but aims to reduce its impact. Safety through modification is generally achieved either by changing equipment or by increasing the spacing between equipment items, or by moving people away from the site of a potential incident. With regard to the pump example, another form of moderation would be to use a lower voltage of electricity for the pump motor. Doing so makes maintenance safer and reduces the chance of a fire-creating spark from being created.

Some checklist questions to consider for use with the “moderate” term include the following:

- Are pipe diameters as low as possible so as to minimize the size of a leak?
- Can the system be operated at lower temperatures and pressures?
- Can aqueous solvents be used in preference to hydrocarbon solvents?
- Can the facility be located so as to minimize the impact of a release?
- Can the facility be located so as to minimize the transportation of materials to and from it?
- Can barges be used in preference to tank cars, and tank cars in preference to tank trucks?

Equipment modification

In the case of the pump that is transferring liquid from one tank to another, it may be that the greatest risk occurs if the pump is blocked in while running and achieves deadhead pressure. In such a case, the risk can be moderated by using a lower pressure pump curve.

With regard to the pump example, another form of moderation would be to use a lower voltage of electricity for the pump motor. Doing so makes maintenance safer and reduces the chance of a fire-creating spark from being created.

Spacing

An important aspect of moderation concerns the use of space between equipment items. Blast overpressure and concentrations of toxic gas from releases fall off exponentially with distance. Inherent safety suggests that it is better to protect systems from the effects of an explosion by moving them apart from one another than by putting a blast wall between them. If equipment items are spaced well apart from one another, there is also less risk of a confined vapor cloud forming with its potential for a very destructive explosion.

Underground location

For onshore facilities, it is generally better to run utilities such as electrical cabling and instrument lines underground. This will protect them from fires and explosions (a particularly important consideration if some of the utility systems need to be kept in operation as part of the facility’s emergency response program). The protection of utilities is also important because it is often found that, following a major accident, large equipment items and piping are soon back in service, but it can take a long time to repair the damaged utility systems, particularly instrumentation runs.

Putting utilities underground does have drawbacks. There is an “out-of-sight, out-of-mind” problem—buried systems may not be inspected and checked as those above ground. They may also be more subject to corrosion than if they were above ground. A sensible compromise is to place utility lines below grade in open trenches.

SIMPLIFY

The final step in achieving inherent safety is to make systems as simple as possible.

The following are examples of simplification questions that can be asked:

- Can less volatile or flammable solvents be used?
- Is it possible to replace powders or dusty solids with pellets?
- Can changes to piping design remove the need for nozzles, bellows, and expansion joints?

An important part of simplification concerns making systems error tolerant in one or more of the following ways:

- A simple system is easier for operations personnel to understand. The chance of operating and maintenance errors is reduced. And, if things do go awry, the operators will probably have a better grasp of the situation.
- The system should be designed to reduce the chance of human error.
- The system should also be designed to be error tolerant such that, if a person does make a mistake, the system fails into a safe condition. For example, different types of hose nozzles are used for different chemicals. Therefore, if an operator tries to connect the wrong hose to a truck or rail car, the nozzle type will prevent him from doing so.

APPLYING INHERENT SAFETY

Project management is described in Chapter 18. The design phase of a project, particularly during Front End Engineering (FEED), is the best time for considering and applying the principles of inherent safety (Figure 9.2).

Up until about the end of the 1980s, the emphasis on most projects was on "fast-track" progress and on selecting just a few contractors and vendors as part of the core project team. Where possible, designs were repeats of earlier projects, thus reducing the amount of time and money that had

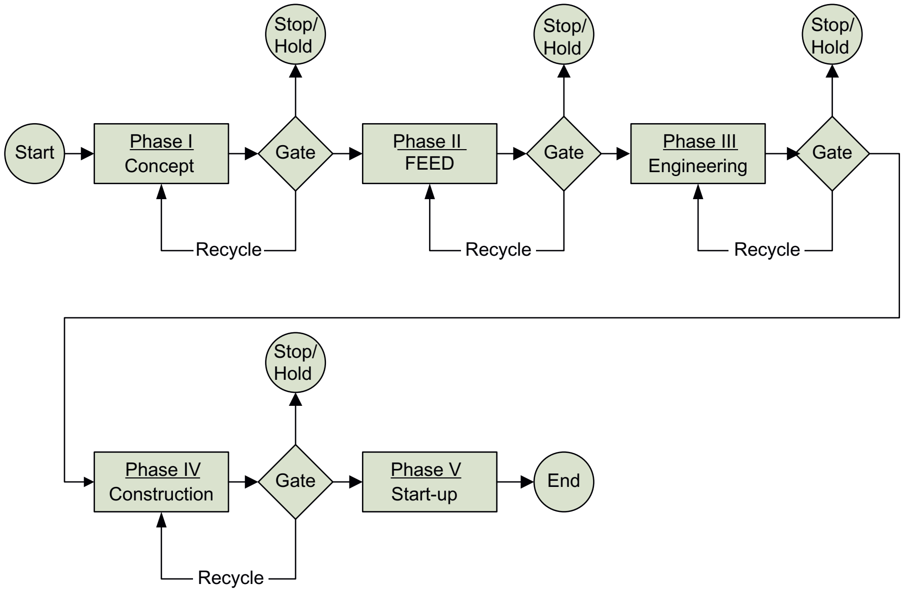


FIGURE 9.2

Project phases.

to be spent on engineering, and allowing for economies of scale with regard to purchased equipment. This approach to project management had a number of drawbacks, including the following:

- Money was being spent on designs and design changes at fairly late stages of projects because the project scope and plan had not been fully defined.
- The facility as built was prone to a high frequency of upsets and shutdowns with the associated high maintenance costs.
- The potential for serious incidents increased because personnel were having to respond to the high frequency of breakdowns without having had sufficient training or preparation—particularly if the facility start-up had occurred before all the “minor” equipment, such as instruments, had been installed.

In order to minimize problems such as the above, the concept of FEED was introduced. As much as 20% of the budget could be spent before the final cost estimate was prepared and the project presented to management for approval.

One advantage of spending resources at the FEED stage was that process safety management issues, such as the writing of operating procedures and the training of operators, could proceed at a measured pace in parallel with the design work. Also, the design would be carefully scrutinized multiple times through a series of hazard identifications (HAZIDs) and hazard and operability analyses (HAZOPs), thus minimizing the possibility of expensive design changes or safety add-ons at later stages of the project.

The first way of applying the concepts of inherent safety is work through the guidewords during each formal hazards analysis (HAZIDs and HAZOPs). Maher et al. (2011) discuss the use of HAZIDs to promote inherently safer designs.

LAW OF UNINTENDED CONSEQUENCES

Albert Einstein once said, “Everything should be made as simple as possible, but not simpler.” So it is with inherent safety. The use of one or more of the above precepts of inherent safety may have unexpected consequences that make safety worse than it was in the first place.

The law of unintended consequences is a term that is used, often ironically, to describe the above concept. The basic idea is that human intervention in complex systems may create a range of unexpected outcomes, most of which are assumed to be undesirable, and which could readily lead to losses which negate the benefits many times over. (The rabbit was introduced into Australia for food, but eventually became a highly destructive pest and has caused extensive habitat destruction.)

In the process industries, the replacement of HF with sulfuric acid (H_2SO_4) that was discussed above is considered be a fine example of the application of inherent safety. However, there are trade-offs. H_2SO_4 is less efficient as a catalyst in the alkylation process; hence, there have to be more truck movements to bring the material on site and to remove the spent acid. These additional truck movements create an increased likelihood of a vehicle accident leading to a spill in a populated area.

Unintended consequences can fall into one of three general categories.

Serendipity

The unexpected outcome is desirable. This concept is usually described as serendipity. In process facilities, a commonly desired serendipity is between equipment reliability and safety. If an equipment item is made more reliable, then safety will be improved because workers will not have to work in hazardous situations so often. (Also, operating costs will be reduced.)

Undesirable outcome

The unexpected outcome is undesirable. Using the same example to do with equipment reliability, it may be found that, because the workers now have to work on the item less frequently, they are less experienced when they have to do so, and they therefore are more likely to make a mistake resulting in an injury.

Such an outcome does not mean that the change should not be made, but additional precautions—such as increased worker training—may be called for.

Original situation worse

The third type of outcome is one that makes the original situation worse. Once more using an equipment item as an example, it may be found that making it more reliable not only increases the chance of an injury accident because the workers have less experience with regard to maintaining the item, it may also be found that excessively long repair times reduced the overall system availability.

One subtle example of how a situation could be made worse occurs when the risk is transferred from the facility to one of its suppliers. For example, instead of storing large quantities of a hazardous chemical on site, the company management may ask their supplier to do so, and then to ship the chemical as needed using a just-in-time management system. If it turns out that the supplier's risk management procedures are worse than those of the operating facility, then overall risks have increased.

PASSIVE SAFETY SYSTEMS

A passive safety system is one that brings an out-of-control condition back to a safe state without any action required from equipment, instruments, or facility personnel.

An example of a passive safeguard is to do with the containment (bund) walls that are typically located around storage tanks. If a storage tank is overfilled, some of its contents will spill to the ground, thus creating a safety and environmental problem. One response to this situation would be to install instrumentation that detects high liquid level and then opens a drain valve so that the tank's contents drain to a safe location. However, the instrumentation may not be totally reliable. A better approach would be to install a containment or bund wall around the tank, as shown in Figure 9.3. The wall is totally passive, requiring neither equipment nor human intervention in order to be effective. The wall will always be there, regardless of what else is going on.

Now if the tank leaks, the wall will retain the spilled liquid, regardless of instrument or operator response. (This safeguard is made more secure by the use of the appropriate engineering standard; in this case the standard calls for the retaining wall to hold 110% of the tank's volume, thus ensuring that the liquid will not escape to the environment.)

ACTIVE SAFETY SYSTEMS

Active safety systems require a mechanical or instrumentation system to take action on identification of an unsafe or out-of-range condition. Pressure relief valves are a standard example; if they

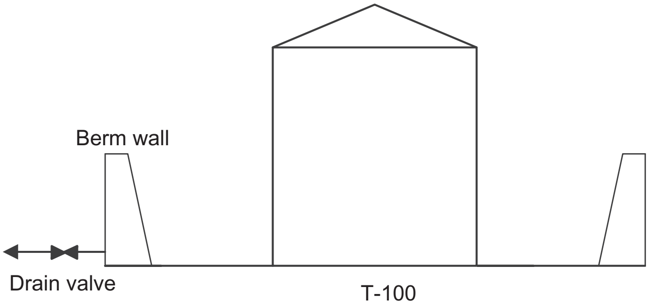


FIGURE 9.3

Retaining wall.

detect high pressure in the system, they open and discharge the high-pressure fluids to a safe location. Safety instrumentation is also an active safety system. On detection of an unsafe condition, the instrumentation opens and closes valves so as to remove the cause of that condition.

Because active safety systems rely on action being taken they are liable to failure. Therefore, they should only be used when the system cannot be made inherently safe or when passive safety systems cannot be used.

Human factors incorporate both active and passive safety. For example, placing a valve so that it is easy to identify and operate is a passive design feature; however, an operator control panel is more of an active safety system.

ADMINISTRATIVE SAFETY SYSTEMS

Administrative or procedural systems, such as operating procedures, training and the use of pre-start-up safety reviews are not generally considered during the design process. Their development gets under way once the front-end design is complete and the project is into the detailed design, fabrication, and construction phases.

SAFETY CRITICAL ITEMS

Equipment and instrument items can be organized according to their level of safety criticality. (It is important to use judgment when deciding on the level of criticality. Some apparently minor or unimportant instrument, e.g., may turn out to play a major role in the overall facility operation.)

Priority 1

An equipment item or instrumentation system is placed in this category if its failure would lead to an uncontrolled release of toxic or flammable materials. Primary containment systems such as tanks and vessels will generally fall into this category. However, the number of Priority 1 items should be small; the system should be designed that were there to be a failure then a backup safety device would control the situation and ameliorate the risk.

Priority 2

Failure of equipment or instrument systems at this level could cause an uncontrolled release. This category also includes vessels and tanks that contain relatively nonhazardous materials.

Priority 3

Failure of equipment or instrument systems at the Priority 3 level should not lead to an uncontrolled release of toxic or flammable materials.

RAGAGEP

With regard to acceptable risk in the context of engineering design, a term that is sometimes used is "recognized and generally accepted good engineering practice" (RAGAGEP). Such a practice establishes engineering performance criteria based on established codes, standards, and recommended practices.

> "Recognized And Generally Accepted Good Engineering Practices" (RAGAGEP)—are the basis for engineering, operation, or maintenance activities and are themselves based on established codes, standards, published technical reports or recommended practices (RP) or similar documents. RAGAGEPs detail generally approved ways to perform specific engineering, inspection or mechanical integrity activities, such as fabricating a vessel, inspecting a storage tank, or servicing a relief valve.

The development of RAGAGEPs for a particular company or facility typically includes the following steps:

- Identify the relevant federal, state, county, and local regulations
- Identify local codes and standards (such as building and fire codes)
- Identify the pertinent industry consensus standards
- Review all of the above with legal, safety, and environmental staff
- Incorporate proprietary experience and standards
- Finalize with engineering judgment

The final step—the use of engineering judgment—can be hard to define. Basically, such a judgment should determine if the RAGAGEP "makes sense" in the context in which its use is proposed, whether safety or environmental performance is truly enhanced, and whether regulatory exposure is reduced. A final and crucial step in a RAGAGEP program is to ensure that it is kept up to date as new standards, regulations, and practices are issued and adopted.

CHAPTER

10 MANAGEMENT OF CHANGE

CHAPTER OUTLINE

INTRODUCTION

The proper management of change (MOC) lies at the heart of any successful risk management program. It can be taken for granted that everyone associated with the design and operation of any industrial facility wants to do a good job—yet, in spite of their best intentions, accidents continue to happen; people get hurt, production is lost, and the environment is polluted. All of these undesired events are caused by uncontrolled change. Someone, somewhere moved operating conditions outside their safe range without taking the proper precautions, i.e., without implementing the MOC process.

Simply setting up an MOC system, with its accompanying forms and software, is not sufficient. The people who use the system must understand its intent and the manner in which it is to be used.

Process Risk and Reliability Management. DOI: http://dx.doi.org/10.1016/B978-0-12-801653-4.00010-2

A facility's MOC program may look good on paper, but, if the people working there do not understand its fundamental purpose then that program will not be effective. MOC is not just a program—it is a way of life for all employees and contract workers.

There is, however, one note of caution that should be sounded. It has been stressed throughout this book that a key to a successful process safety program is to develop a culture that encourages the involvement of all employees. In this respect, an MOC program is different. The program imposes a clear structure and discipline on all employees and discourages spontaneous actions.

The effort needed to properly manage change can be substantial. It has been reported (Bradley, 1996) that the number of changes that flow through the MOC system is typically around 250 per year for a medium-sized site (with say 140 employees) and up to 1,000 a year for a large site with say 2,000 employees. One world-scale refinery in Texas had 1,400 changes in 2008. About 75% of the changes were regarded as moderate, i.e., they were not perceived as materially affecting the safety of the unit; nevertheless, they had to be handled through the MOC system.

BENEFITS OF MOC

Many companies started their MOC programs in the late 1980s and early 1990s in order to comply with the newly introduced process safety management (PSM) regulations. Typically, these companies have now moved beyond mere compliance, and are looking for other benefits to be gained from properly managing change, some of which are listed below.

INCREASED PRODUCTION, PRODUCTIVITY, AND QUALITY

An effective MOC program will help increase production rates because there will be fewer direct losses from unscheduled downtime and from undesired events such as flaring or the recycling of off-spec product. Also, internal losses from problems such as reactor temperature excursions will be reduced.

Product quality and energy costs should also improve through the use of an MOC program. Fewer operational excursions result in fewer problems with off-spec products or missed delivery dates, and energy requirements for reprocessing will be reduced.

MAINTENANCE EXPENSE AND SAFETY

Uncontrolled change can result in equipment being operated outside its safe limits thus leading to damage requiring maintenance and/or repair work. Such work can be costly. Moreover, it can create safety problems because workers may need to perform unnecessary high-risk activities such as entering vessels, working on high-voltage electrical systems or moving heavy equipment items to correct the damage that has been done.

ENVIRONMENTAL PERFORMANCE

Most environmental problems stem from operational upsets. Indeed, if a facility is designed to meet the pertinent air and water quality standards then virtually all environmental problems will result from improperly managed changes that lead to upset operating conditions.

PERSONAL REPUTATION

The benefits of an effective MOC program extend beyond objective issues such as safety and profitability. If the manager who is responsible for running a facility can achieve a steady and stable operation with a minimal number of upsets then his or her personal reputation will be enhanced. Senior management typically wants an atmosphere of "no surprises." The proper control of change will help facility managers create such an atmosphere.

Likewise, the day-to-day lives of everyone associated with the facility will be more smooth and productive when the operations are stable. It is when there are upsets and unexpected problems that managers are subject to out-of-hours telephone calls from the facility, complaints from unhappy customers, and unsolicited offers of "help" from corporate headquarters. Moreover, if day-to-day operations are smooth, managers will be able to give more attention to long-range plans and strategic improvements.

DEFINITION OF MOC

The Canadian Chemical Producers Association has prepared a checklist for determining when MOC is needed. It is reproduced below in Table 10.1 (with some minor editorial changes). If, during the change evaluation process, a positive answer to any of the 12 questions in the checklist is generated, then the proposed change probably requires the implementation of the MOC process.

Table 10.1 CCPA Checklist

- Does the change involve different chemicals that could react with other chemicals (including diluents, solvents, and additives) already in the process?
- Does the new proposal encourage the production of undesirable byproducts either through primary reactions, side reactions, or introduction of impurities with the new chemical?
- Does the rate of heat generation and/or the reaction pressure increase as a result of the new scheme?
- Does the proposed change encourage or require the operation of equipment outside the approved operating or design limits of chemical processing equipment?
- Does the proposal consider the compatibility of the new chemical component and its impurities with the materials of construction?
- Has the occupational health and environmental impact of the change been considered?
- Has the design for modifying the process facilities or conditions been reviewed by a qualified individual using effective techniques for analyzing process hazards, particularly when the modifications are being made in rush situations or emergency conditions?
- Has there been an on-site inspection by qualified personnel to ensure that the new equipment is installed in accordance with specifications and drawings?
- Have the operating instructions and engineering drawings been revised to take into account the modifications?
- Have proper communications been made for the training of chemical process operators, maintenance craftsmen and supervisors who may be affected by the modification?
- Have proper revisions been made to the process control logic, instrumentation set points and alarm points, especially for computer control systems?
- Have provisions been made to remove or completely isolate obsolete facilities/equipment in order to eliminate the chances for operator error involving abandoned equipment?

The Center for Chemical Process Safety (CCPS) defines the topic as,

> A temporary or permanent substitution, alteration, replacement (not in kind), modification by addition or deletion of critical process equipment, applicable codes, process controls, catalysts or chemicals, feedstocks, mechanical procedures, electrical procedures, safety procedures, emergency response equipment from the present configuration of the critical process equipment, procedures, or operating limits.

A British Standard defines MOC as,

> The discipline of identifying the components of a continuously evolving system (taking into account relevant system interfaces) for the purposes of controlling changes to these components and maintaining integrity and traceability throughout the system life cycle.

DEVIATION BEYOND LIMITS

A more fundamental determination of looking at change is to decide if the process is to be taken outside its current, predefined, safe operating limits (Chapter 1). Therefore, another way in which change can be defined is as follows:

> A change occurs when a critical variable moves outside its predefined safe limits.

From the above definition for the word change the term "Management of Change" can be defined as follows:

> Management of Change is process to ensure that any proposal to move a critical variable outside its current safe limits is properly evaluated and that appropriate safeguards be put in place if the safe limit values change.

IMPACT ON OTHER PROCESS SAFETY ELEMENTS

Another way of defining the word change in the context of MOC is to determine if the proposed change affects any of the other elements of process safety. For example, if a new operating procedure has to be written then the MOC process must be followed. Similarly, if the proposed change means that updated P&IDs are needed, then the topic of knowledge management has been affected.

CRITICAL CHANGES

Changes are sometimes classified as being either "critical" or "noncritical." If it is believed that a proposed change could, if improperly managed, lead to a serious accident, then it is defined as being critical, and vice versa. Critical changes will receive a more thorough evaluation and scrutiny than those deemed to be noncritical.

Unfortunately, it is not always obvious when a change is critical, and when it is not. Indeed, one of the principal purposes of an MOC review is to determine the impact of a proposed change, i.e., to define its criticality. There is a danger of falling into the trap of circular logic:

- A critical change requires thorough analysis as part of the MOC process.
- A thorough analysis is needed to determine if a proposed change is critical.

This critique of the term "criticality" as used in this context is not just theoretical. Examination of actual incidents shows that many of them were triggered by an apparently noncritical change. Indeed, it could be argued that changes which are judged *prima facie* to be critical actually require *less* analysis because they will certainly receive considerable attention and analysis.

IN-KIND/NOT-IN-KIND CHANGE

The concept of "In-Kind/Not-In-Kind Change" is frequently used to determine if a proposed change should be handled by the MOC system. In-Kind changes are generally those to do with replacement and repair. If a replacement part is made to the same specifications as the one that it is replacing then the change is In-Kind, and so the MOC process need not be implemented. On the other hand, if equipment is being added, modified, installed, or removed, then the change is Not-In-Kind and the MOC process should be used.

Strictly speaking no two equipment parts will ever be truly identical. Any replacement part, even if built to the same specification, will differ from the original part. The replacement part was probably made at a different time, by different workers, possibly in a different factory, and stored in a different warehouse for a different length of time. When evaluated rigorously in this manner, all changes are Not-In-Kind. Of course, it is important not to push this argument too far. For example, if a piece of equipment is to be repainted it is theoretically possible that the new paint could contain a hazardous chemical that could start an accident sequence. However, few companies would seriously consider conducting an MOC on a repainting project just because a different brand of paint is being used.

The following criteria provide further guidance regarding when a change is to be considered In-Kind or Not-In-Kind.

SAME SPECIFICATION

If a replacement item has the same technical specifications as the original, then it is generally considered to be In-Kind. The replacement item should have the same materials of construction, rating (pressure, temperature, voltage, amperage, resistance, and reactance), function, capacity, electrical area classification, and settings.

The new item should be a genuine replacement—not an improvement on the old one. If the purpose of the replacement is to upgrade the operation in some manner then the change may not be In-Kind. For example, if a new vendor is used to supply a replacement part to the same specification as the old part then the change may be Not-in-Kind. After all, the reason for using the new vendor is that management wanted to make a change to the system (probably to reduce costs or improve system reliability). There must be some difference between the old and the new products in order to explain why the new vendor was chosen. For this reason, decision to change a vendor or a supplier should generally be validated using the MOC process.

SAME SERVICE AND MATERIALS OF CONSTRUCTION

The service in which the item is being used should not have changed. Process conditions, including pressure, temperature, and process materials, must be the same as for when the original item was in service. Nor should the inspection and maintenance requirements have changed.

Changes in materials of construction will always require MOC approval.

SAME STORAGE AND HANDLING PROCESS

The replacement item should be stored and handled in the same manner as that which it is replacing. On one facility, a very serious accident resulted when a supposedly In-Kind replacement gasket was inserted into a filter housing as part of a routine operation. The new gasket leaked, and a major fire ensued resulting in extensive equipment damage, and many weeks of lost production (fortunately no one was injured). After the accident, it was determined that the new gasket was not in fact identical to the old one, even though all parties concerned had thought that it was. An inadvertent change had occurred in the supply chain process.

It will never be possible to have absolutely identical storage and handling processes for all items, so some judgment is required. For example, changing the storage location from indoors to outdoors could have an effect on the stored items, as could the use or nonuse of air-conditioned facilities.

PROCEDURAL REPLACEMENT

Any action that follows normal operating or maintenance instructions is generally In-Kind. Similarly, the replacement of any equipment part should be In-Kind. Either the item is replaced as part of a preventive maintenance program, or experience has shown that it wears out within a known period of time and then must be replaced. However, if the original item is failing inexplicably, then simply putting in a replacement part is not sufficient. There must be some reason for the system failures—they could be occurring because the system has changed in some undetected manner. Hence, an MOC review is required.

PROCESS CHEMISTRY

If the change involves the introduction of a new chemical (or the removal of an old one) MOC will be required. New chemicals could create undesirable side reactions or change heats of reaction such that a hazardous situation is created. They may also require changes to the Emergency Response Plan.

INSTRUMENTATION AND CONTROL SYSTEMS

Usually, a proposal to change instrumentation systems will require that the MOC policy be followed. This is certainly true if alarm limits, interlock settings, or control logic are to be changed. Changing operating set points should not require a formal change approval as long as the new values stay within the safe operating range, as shown in Figure 1.9. Any changes to the emergency shutdown system and its associated interlocks will certainly need to go through the MOC process.

TYPES OF CHANGE

If change is to be managed properly, it is necessary to understand the types of change that are typically made on a facility—each will require its own response. Changes can be categorized as follows:

- Initiated equipment change
- Noninitiated equipment change
- Temporary change
- Emergency change
- Administrative and organizational change.

INITIATED EQUIPMENT CHANGE

An Initiated Change takes place when someone, usually a manager or an engineer, decides that he or she would like to modify the current operation so as to improve the facility's economic performance. This is the type of change that most people think of when they hear the term "Management of Change."

The following are examples of Initiated Change:

- A process engineer proposes an increase in reactor temperatures in order to achieve higher production rates.
- The operations manager plans to manufacture a new grade of chemical using existing equipment.
- A chemist suggests the use of a new additive to improve yields.
- An operator requests that the logic of a control loop on a distillation column be changed in order to minimize product quality variations.
- A maintenance engineer proposes that the size of a pump motor be increased in order to reduce the number of pump trips.

In each of these examples, the facility operations are being taken to a point that is outside the previous operating experience and possibly outside the predefined safe limits. In each case, the MOC process should be initiated so as to ensure that the new conditions are safe, and to make appropriate modifications as required.

Large and small changes

Large changes, which usually involve numerous modifications to equipment, instrument systems and administrative procedures, will almost always receive a full MOC review. Because they can be implemented quickly and easily small changes are often treated informally and tend to be subject to fewer checks and reviews. Some of the dismissive terms that are sometimes used to describe small changes, such as "quick and dirty," "one minute change," and "midnight engineering," are indicative of this way of thinking. A moment's reflection, however, shows that this line of reasoning is disingenuous. Indeed, experience has shown that it is often the small changes that lead to serious accidents (Sanders, 1992).

Turnarounds

When a facility is shutdown for turnaround the maintenance group may wish to make temporary changes to assist them in their work. For example, they may wish to run a line from one vessel to another in order to fill the second vessel with wash water more quickly. Once the work is finished, the line will be removed before the startup. Unless an area work permit has been issued, such changes must still be handled through the MOC process.

Field change

A field change often represents the specific application of a generically approved procedure. For example, a facility may have a standard procedure for steaming out pressure vessels before they are placed in service following maintenance. A field change will determine exactly how a particular vessel is to be steamed out in a specific situation. In spite of the fact that an MOC may not be needed, the work will still require that a job hazards analysis be performed for this type of change.

NONINITIATED EQUIPMENT CHANGE

Some changes are "noninitiated," i.e., they are not created through a person's conscious volition. Corrosion is a common example of noninitiated change; a vessel or a pipe may be gradually losing wall thickness due to corrosion without anyone knowing about it until the system fails catastrophically.

Increasing production rates can also lead to noninitiated change; as management gradually sets higher and higher target values, the facility, its equipment and its people are pushed to their limits: flows, temperatures, and pressures are all increased. Even if no specific safe limit is exceeded, the increased severity of operating conditions could lead to a failure.

Noninitiated changes cannot be controlled with the MOC program because no one knows about them until after an event. Instead, changes of this type are controlled by other elements of the risk management program such as asset integrity, process hazards analysis (PHA), and incident investigation.

Noninitiated changes can be categorized as:

- Overt
- Covert (both sudden and gradual)
- Ripple effect.

Overt change

An overt noninitiated change is one that is known about, and whose consequences can be mitigated before an accident actually takes place. For example, if a key variable such as a reactor temperature or a tank level is getting out of control but is being watched by an operator then the change is overt. Because someone is watching the change develop, there is time to propose a modification to the system so that appropriate action can be taken.

Covert change

A covert change is one that is not anticipated, and that comes as a complete surprise to the organization's personnel. For example, if a vessel is gradually corroding, and no one knew that corrosion was taking place until the vessel failed catastrophically, then the change was covert. Covert changes can be particularly hazardous because there may be no warning that a catastrophic incident is about to happen until it "announces itself"—possibly in the form of a serious accident. Furthermore, it is not possible to put safeguards in place because this type of incident is fundamentally unpredictable. Covert changes cannot be handled by the MOC system because no one is aware that a change has occurred.

Changes to passive safety systems such as the firewater and flare headers can lead to covert safety problems. As additional equipment is installed, these systems can be overloaded. The capacity of the flare system should be checked, but, if it is not, and since such systems are passive, there are no indications that they have become overloaded until they are called upon to operate.

Some covert failures are not anticipated because they are unusual. For example, one chemical plant used a series of large, liquid-filled reactors. A noble metal compound catalyst, which was in solution, was fed continuously into the reactors. Over a period of years some of noble metal came out of solution, and slowly formed a metal lining that was steadily growing in thickness on the inside walls of the reactors. The process and economic consequences of this problem had been analyzed and accepted. However, no one had considered the civil and structural engineering implications of this uncontrolled change: the fact that the reactors were slowly getting heavier, and possibly overloading their foundations.

Covert change sometimes occurs in the form of a ripple effect through utility systems. If a facility has multiple operating areas, each of which is connected to a common utility system, then each area may make properly controlled changes to its own operation but may not realize that it is having a system effect. An example of a ripple effect change that can occur in a utility system is shown in Figure 10.1.

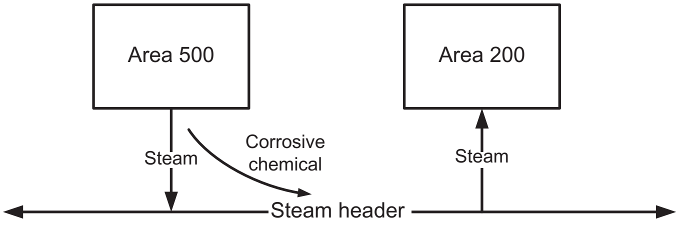


FIGURE 10.1

Covert change in utility system.

Area 100 generates steam, which flows to the steam header. Area 200 imports steam from the header. The process in Area 100 is modified such that a more corrosive chemical is used. The change is reviewed with the Area 100 MOC system, and is approved. However, if a heat exchanger tube in Area 100 fails, the corrosive chemical could enter the steam header, from where it will flow into Area 200, possibly leading to serious equipment damage.

The effect of changes such as this can be analyzed using an Interface Hazards Analysis.

TEMPORARY CHANGES

Temporary changes are those changes that incorporate within themselves a built-in termination date or time. Changes of this type are often implemented to keep the operation running while a piece of equipment is repaired or replaced.

From a safety and operational point of view, whether or not a change is permanent or temporary is merely a semantic matter—the system itself does not know or care that a change is intended to be temporary. Therefore, the fact that a proposed change is defined as being "temporary" does not mean that it can be handled less rigorously than a change that is intended to be permanent. Yet, because of the short duration of temporary changes, the personnel implementing them may be tempted to take shortcuts, particularly if going through the MOC process takes longer than actually making the change itself. There is a temptation to take an attitude of "let's just get on with it—why bother spending hours writing and reviewing a procedure for an operation that will only take a few minutes to carry out?"

An example of a situation that can tempt personnel to take an unacceptable shortcut is shown in Figure 10.2. A hazardous chemical is leaking to the atmosphere through a control valve's packing. Operations management decides to run a hose bypass around the valve, and to control the flow in the line using a manual valve. The leaking control valve can then be blocked in and repaired.

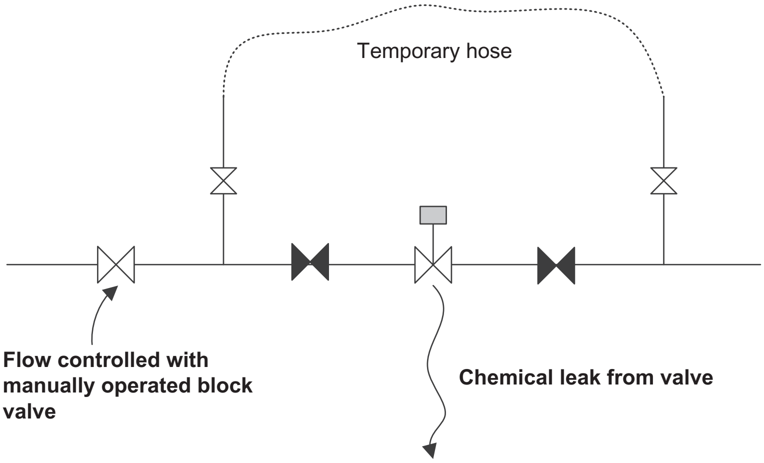


FIGURE 10.2

Example of temporary change.

This repair activity may take no more than 30 minutes. Yet it is a new operation, so the system has changed. Hence, the following steps should be followed:

- Conduct a safety analysis—probably using some type of What-If method. The analysis should focus on the feasibility of controlling the flow of chemical using a manually operated block valve.
- Write a temporary operating procedure.
- Train the operators in the new procedure.
- Prepare an emergency response plan in case the modification does not work properly.
- Make sure that the temporary hose is removed once the repair work is complete, that all valves are returned to their normal position and that blinds are installed.

These activities could take hours, far longer than the change itself, and so could easily engender the response, "Oh, let's just get on with it—we don't have time for all this bureaucracy."

Although it is easy to reproach someone who takes this point of view, it has to be recognized that temporary changes often need to be implemented quickly in order to avoid more serious problems from developing. Indeed, many temporary changes are also emergency changes.

It is important to distinguish between true Temporary Changes and those changes that have occurred at least once before and that are repeated at infrequent intervals. Such changes are "Infrequent Repeat Changes." If the change has been carried out before, and if it was properly managed, then, strictly speaking, it does not need to be put through the MOC system when it is carried out a second time.

This approach to the management of infrequent repeat change is only valid, however, if the change, when it was previously made, was properly controlled and documented. If the records are inadequate or incomplete then the MOC process will have to be implemented a second time. People may have memories as to what was done, but this is not sufficient; the information must be written down. Moreover, if the change has not been implemented for some time, there is a good chance that not all of the current personnel will have been trained to operate the facility in the new mode. Hence, in this situation, it is best to treat the change as if it is entirely new, and to train people again.

EMERGENCY CHANGES

Sometimes it is essential that a change be made very quickly. In these cases, the people wishing to make the change take the responsibility to go ahead and do what has to be done without invoking the full MOC process. This constitutes an Emergency Change. This type of change is justified when there is the potential for a serious short-term impact in areas such as the following:

- Danger to personnel
- Major equipment damage
- Major operational loss
- Serious environmental loss
- Community complaint
- Regulatory violation.

Generally, the justification for an emergency change is that a person in line authority—a shift supervisor for example—decides that the dangers associated with doing nothing are greater than those associated with the proposed change, even though that change has not been properly evaluated or authorized. Time is of the essence. For example, in the middle of the graveyard shift, a pump seal may start to leak, allowing flammable chemicals to escape into the atmosphere. The warehouse workers may report that they do not have identical seals with which to replace the leaking item, but they do have others which are very similar. In this situation, the operations and maintenance supervisors may decide to go ahead and make the change right away using the incorrect seal, even though they know that it is not a true In-Kind replacement. They decide that the risk associated with using a not-quite-the-same seal is less than that of the leaking vapors catching fire.

In spite of the fact the emergency changes bypass the full, formal MOC process it is vital that they always be subject to at least one review before being implemented. There may not be time to assemble a full MOC team; nevertheless, the change ought to be reviewed by at least three people. These people should represent different disciplines and departments, and should operate in the same way as the normal review team; i.e., they should systematically investigate the nature and consequences of the proposed change—probably using an abbreviated What-If approach. Only in a true life-or-death situation, where seconds or minutes count, can a single person assume full responsibility for making a change without having a team review first.

Every effort must be made to minimize the number of emergency changes because they bypass the normal systems for checking for hazards. This is why all employees should be thoroughly trained in the use of the formal system. Once it becomes familiar to them, and once they understand its importance, they will be less inclined to bypass it. Moreover, those who are familiar with the formal MOC process will tend to follow its precepts, even when they are in a hurry.

Following its implementation, an emergency change should be validated by a normal MOC review in order to make sure that no problems have been overlooked. Even if the emergency change can be shown to be safe in the long term, a full evaluation of what occurred may show that the action taken was not optimal. A more efficient or practical solution to the problem may be uncovered.

ADMINISTRATIVE AND ORGANIZATIONAL CHANGE

When MOC systems were first implemented they generally focused on physical items such as equipment and instruments. However, an effective MOC program will also consider the impact of changes to “soft” items, such as organization, operating procedures, and training, even though they are generally more difficult to categorize and define in terms of their impact on system safety. Indeed, in civilian nuclear power facilities in the United Kingdom, it is now a legal requirement to analyze organizational changes.

Managing organizational change is more difficult than managing technical change because it involves human behavior and feelings—issues which are difficult to understand and to predict. For example, a large theoretical gain in efficiency may be achievable if operators and maintenance personnel can share their work activities. Yet, such changes can generate concerns about job security and loss of seniority. The upshot may be that that overall efficiency and productivity may actually fall should that change be implemented.

The following are examples of organizational change that could have an impact on a facility's performance:

- A corporate directive calls for a reduction in the number of people employed at the site.
- The operations superintendent proposes to change the route that delivery trucks follow when moving within the facility boundaries.
- Shift workers vote for a change from 8- to 12-hour shifts.
- The engineering manager suggests that a different contract company be used to bench-test the facility's relief valves.
- The Information Technology department installs a new computer system for inventory control.
- A purchasing agent decides to use a different vendor to supply a critical spare part.

Reorganization

If a facility is reorganized, with job functions being assigned to different departments, then the MOC process should be used to make sure that all process safety issues have been properly considered.

If the change involves putting new people into existing jobs then it is likely that the new person will have less experience than the person being replaced. The replacement may be given some formal training for the new position, but generally the handover consists of working in tandem for a while with the person who is leaving the job. Whether or not such a change should be processed through the MOC system will probably depend on the criticality of the job in question.

Management by contractors

Increasingly, contracting companies are being assigned operational control of large facilities, with the host company acting as little more than a high-level observer. This means, therefore, that the contractor has full responsibility for running the MOC program. It is critical to ensure that the contractor understands this responsibility, and that he implements the program thoroughly and effectively.

On one large petrochemical facility, for example, a contractor was assigned full control over a demolition project. The contractor was fully responsible for all aspects of the project, including process safety (the contractor had "care, custody and control" of the facility). This responsibility was written into the contract with the client. Unfortunately, the contractor did not effectively implement MOC in one part of the project. This failure was a root cause that led to a serious accident in which two persons were severely burned. Moreover, one of the key personnel over the project was an employee of the operating company, but he was on loan to the contractor. The upshot was that everyone assumed that someone else was taking care of process safety. This assumption was obviously flawed.

INFORMAL ASPECTS OF MOC

The process of managing change incorporates both formal and informal elements. The formal element is needed to ensure that all changes have been properly identified and controlled, and to provide proper records should the change be audited or challenged in court. Because a formal MOC program is often legally required, and because the design and organization of such systems is relatively simple, most of the literature to do with MOC tends to concentrate in the development of such systems, often featuring the use of logic and arrow diagrams. These diagrams show how a proposed change wends its way through the process safety system. At each stage, there are various Yes/No questions to be answered. The proposed change must successfully address these questions present before moving on to the next step.

However, the MOC process includes important informal aspects. People will inevitably solicit opinions and thoughts from their colleagues before they commit their ideas to the formal system. Because discussions at this time are relatively open and unstructured, people will probably be more willing to think freely, and thus to come up with fresh ideas.

This informal process is going to take place, regardless of whether "the system" acknowledges it or not. Before anyone commits their ideas to paper, they will almost certainly choose to run it "up the flagpole" with their colleagues and coworkers. They do so because it is a rare individual indeed who has sufficient confidence to publicly propose a change without first checking it out on an informal basis with people that he or she knows and trusts. If it turns out that the idea is impractical or silly, not much time will have been wasted. Probably the worst that happens to the Initiator is that he or she will be subject to some reasonably good-natured kidding from those closest to him.

The informal review will sometimes quickly show that the suggested change is wrong or impractical because some simple fact or item had been overlooked by the person proposing the change. Having such problems identified by colleagues can prevent considerable embarrassment. This is why informal reviews of this type are sometimes referred to as a "red-face checks" or "giggle tests." If management decides to reject a proposed change they also must pass a "red-face test." Employees must be sure that the rejection of the idea was based on rational grounds, and that management was not just interested in saving money, or in avoiding extra work.

One informal aspect of MOC that is rarely discussed openly, yet that almost always exists—and that can be very important—is lobbying. If someone suggests an idea, he is placing some of his professional reputation and pride on the line. As a result, if a person really believes in the idea, he or she will lobby for it. Consequently, those people who are the most persuasive, or who occupy a position of authority, are more likely to have their ideas implemented than are people with less forceful personalities or who are of a lower rank. For example, it is a fact of life that an idea proposed by the Facility Manager will develop greater momentum and wider acceptance than one put forward by a newly hired pipe fitter—regardless of which idea was the better of the two. Similarly, the field supervisor who has 20 years of experience and has a strong personality will usually find that he has less trouble getting what he wants than a junior chemist working in a corporate office located a 1,000 miles from the facility. These biases may be unfair, but they are a fact of life. The ideal MOC system will provide checks and balances to ensure that all ideas are evaluated as rationally and as fairly as possible, regardless of who proposes them. Nevertheless, no system can ever be completely impartial and rational.

Another informal aspect of the MOC process is that of group rivalries. Many ideas for change will generate partisan support, and they could generate opposition from other groups. For example, if one shift of operators suggests a change in the way that facility should run, the other shifts may try to find fault with that idea simply because it did not come from them. Similarly, when outside groups, particularly those from corporate headquarters or from independent consulting companies, become involved in the discussions, there is a good chance that their input will generate resentment among the facility personnel.

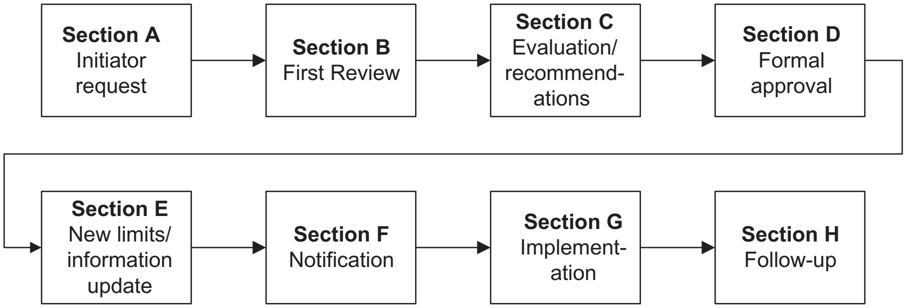


FIGURE 10.3

Eight-step process.

THE MOC PROCESS

The MOC process will generally be a team activity. Various departments and managers will have to approve the change, and the input from technical and operations specialists is always needed. Naturally, having a larger number of people involved in the MOC process will increase the amount of time that the change analysis takes, and it will also increase the possibility of disagreements and arguments between team members. Nevertheless, these problems are usually worth accepting in return for the benefits gained.

A problem that all MOC systems face is balancing the need for thoroughness with the problems of too much bureaucracy. The system has to be thorough and detailed, otherwise potentially hazardous changes will slip through. On the other hand, if the system becomes too cumbersome and slow, people will avoid using it. The MOC system should provide management with a regular overview as to progress, showing how many changes are in the system, and where any delays may be.

An eight-step approach to managing change shown in Figure 10.3 considers both the formal and informal aspects of change management. The first three steps—Sections A and B—are mostly informal. People are free to contribute ideas and recommendations without feeling that are any constraints on what they say. Sections C−H are more formal and structured.

SECTION A—INITIATOR REQUEST

The first step in making a change is to initiate the MOC process. It is very important to ensure that the problem identified cannot be addressed simply by ensuring that existing programs or systems are being properly followed.

Given that the proposed change will be taking the facility into new operating regions outside current safe operating limits, it is vital that people be encouraged to think creatively about the implications of the proposed change. When thinking creatively, people will often jump to conclusions that initially do not seem to make sense yet turn out on further reflection to provide fresh insights. Often the way in which this is done is intuitive; the persons concerned cannot explain how they came up with a particular idea, except that "it just feels right." This is why it is important not to be too critical during the early stages of the MOC process—people need space in which to think. This type of thinking is most likely to occur during informal discussions.

INITIATOR

The change process starts when someone identifies a problem that needs to be corrected, or when they find an opportunity to improve the facility's safety or operability. This person is referred to here as the *Initiator*. In the Initiator's opinion, the problem or the opportunity that has been identified cannot be handled simply by executing existing programs or policies more effectively. He or she believes that a system change is required—hence it will be necessary to implement the MOC system.

Usually the Initiator will be a manager, a supervisor, or an engineer. However, the MOC system should be open to everyone—all employees and contract workers should feel free to propose changes that they believe will make the facility safer, cleaner, and more profitable. Initiator initiative is the most important step in the whole process; if no one takes the initiative to suggest change, then no improvements will ever be made. The ultimate success of the MOC system depends on the enterprise and drive of the Initiator. There is little value in having a high-quality change review process if it is never used, or if it is used merely to evaluate management's instructions. Hence senior employees such as managers, technical experts, and experienced supervisors need to be willing to listen to the ideas of those who do not have their knowledge and seniority. An employee's lack of experience does not mean that he or she cannot come up with useful insights and suggestions. Indeed, lack of experience may even be an advantage at this stage of the MOC process.

The motives for someone to suggest a change include the following.

Personal recognition

People usually propose change in order to gain recognition from their colleagues and their company; they want to be separated from the pack. They also hope to be directly rewarded with money and promotions because they showed initiative.

Company loyalty

Most employees want to work for companies that are successful. They hope that their proposed change will contribute toward this success.

Safety

The Initiator may be working in a situation that, in his opinion, represents a significant safety problem, either to himself or to his work group. If he highlights the situation, but does not receive a response, then, by initiating a formal change, he is forcing management to take action. Once a request for change has been submitted to "the system" some response from management is required.

Whatever the reason for suggesting a change, the Initiator is stating implicitly that he or she cares enough about the facility operation to want to make it better. Because the initiative taken by the Initiator is so important, the MOC system must be administered so that he or she is always kept informed as to the status of his or her suggestion—particularly if it is rejected. If other employees see that the Initiator is fully involved in the discussions that take place once the proposal for change has been submitted, they are more likely to participate by making their own suggestions for change. On the other hand, if there is a perception that "the bosses" are making all the decisions and that the employees' input is being disregarded then participation and involvement will decline.

The Initiator should be involved in the subsequent decision-making processes, particularly the detailed analysis of the change even if he or she is not really qualified for that type of work. In particular, if the proposed change is rejected, it is very important to explain to the Initiator why the decision was made.

SPONSOR

All changes require someone to push them through the system; regardless of the inherent merits of the proposed change, it is unlikely that it will move forward as an inevitable consequence of its intrinsic merits—someone must make it happen. This person is referred to here at the *Sponsor*. It is the responsibility of this person to make sure that the proposed change does not get lost in the system and to check that it does not drift into some bureaucratic limbo. The Sponsor must engender a constant feeling of urgency, enthusiasm, and excitement about the proposed change.

Frequently the Sponsor and the Initiator are the same person. However, there may be logistical problems with asking the Initiator to be the Sponsor. For example, if the Initiator works on the night shift or has to take sick leave then someone else should Sponsor the proposed change. If the Initiator does not have much influence within the organization, then having a Sponsor with more seniority and authority may help push the change through the system.

REQUEST PROCESS

The Initiator's action is Section A of the eight-step process, as shown below in Figure 10.4, which is based on Figure 10.3.

The Initiator is not responsible for generating solutions. Just as a PHA team is charged with finding hazards, not with correcting them, so the Initiator's role is merely to identify problems or opportunities. The responsibility for finding solutions lies with others.

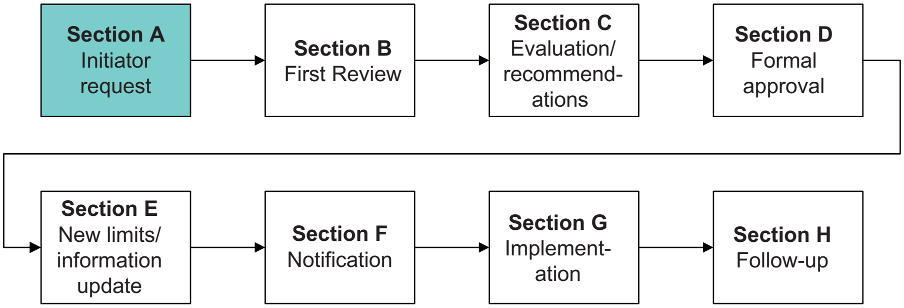


FIGURE 10.4

Section A—Initiator request.

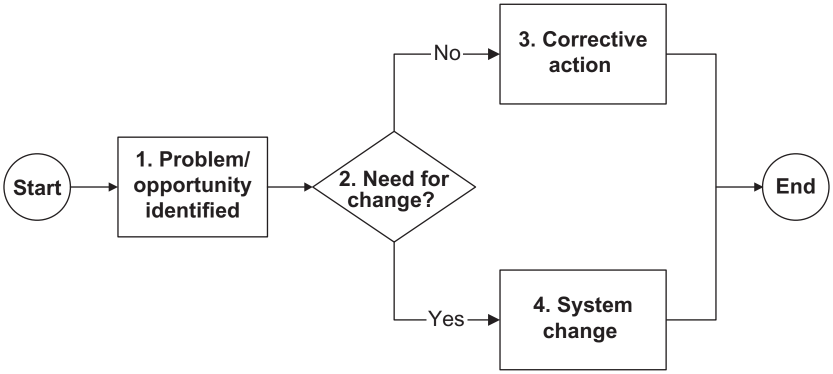


FIGURE 10.5

The change process.

Of course, in many situations, the Initiator *will* have a proposed solution in mind; he or she should then be encouraged to share that idea with the MOC team. However, the Initiator must understand that there may be better ways of solving the problem. Indeed, as will be discussed later in this book, it will often be the case that the Initiator will not be the best person to find a solution. He or she may lack "helicoptic vision," i.e., the ability to rise up above a problem and look around it for more holistic solutions. Moreover, by immediately putting forward a specific recommendation, the Initiator may stifle the suggestions of others.

The Initiator's request can be analyzed using the process shown in Figure 10.5.

Step 1—problem/opportunity identified

The MOC process is started by the Initiator in response to a problem that requires correction or as an opportunity for improvement.

Using Example 2 in Chapter 1 an operator (Carlos Hernandez) may note that production has had to be curtailed on a number of occasions due to high level of RM-12 in Tank, T-101.

Step 2—need for change

When someone requests that a change to the system be made, it is important to make sure that the problem or opportunity cannot be better addressed simply by making sure that existing management systems are used properly. It is tempting to call for a system change without making sure that the current equipment or organization cannot be remediated or improved using current management processes.

Step 3—corrective action

If the analysis of the change request shows that the problem or opportunity can be addressed by using existing systems more efficiently (or maybe with just a few minor modifications), then the appropriate corrective action should be taken. Only if corrective action is not possible should a system change be made.

Step 4—system change

If it is agreed that a system change is needed, then management may decide to conduct a root cause analysis of the problem or opportunity under consideration. Otherwise, there is a danger that the final solution will focus on the symptoms rather than the real cause of the problem. Hence the problem may recur.

In the example, analysis may demonstrate that the frequent occurrence of a high level in T-101 may have nothing to do with the operation of the tank itself. Other causes include the unsteady operation in either Units 100 or 200 that create fluctuations of the flow of RM-12 into or out of T-101. In turn, these problems could have other causes. For example, fluctuations in the flow through Unit 200 may be traced to problems with the steam supply system. Eventually, the analysis will identify a root cause, and may also show that resolving one of these other issues would be far more effective than changing T-101 instrumentation.

One additional benefit of root cause analysis is that once the fundamental problem has been identified and addressed many other problems will be eliminated with just one action. It may be found that the high-level problem in T-101 was just one of the problems that will be solved. In particular, the root cause analysis may identify common cause effects. These are problems that affect many systems, and that, if successfully addressed, can eliminate many problems at once.

MOC FORM—SECTION A

The first step in the formal MOC process is to complete the first part of the MOC form. An example of such a form is shown in Table 10.2, which is based on the first standard example. Some administrative detail, such as the request number that is usually found in forms such as this, has been omitted from Table 10.2 in order to save space.

Name of the Sponsor/Initiator(s)/date

The first line on the form shows the Initiator's name and the date on which the change was proposed. Sometimes the proposal will come from a team of people. The Sponsor's name is also provided. In this example, the Sponsor and the Initiator are the same person: Carlos Hernandez.

Description of problem and its consequences

The person(s) requesting the change must clearly define the nature of the problem to be solved, or the opportunity for improved performance that has been identified. This part of the form should not be used for describing any proposed change—it is only for outlining the problem or opportunity and explaining why, in the opinion of the Initiator and Sponsor, action must be taken.

Proposed change

Having defined the problem to be solved, the Initiator can then describe what he or she would like to do to address the situation. Once the change process has been initiated, it is quite possible that other, more effective, solutions will be generated.

Table 10.2 Section A—Initiator Request

Section A—Request for Change			
Name of Initiator(s): Carlos Hernandez		Date: 2015-06-01	
Name of Sponsor: Carlos Hernandez			
Description of the problem			
Tank T-101 provides surge capacity for the intermediate chemical RM-12. Due to problems with the Transfer Pumps, P-101A/B, T-101 has been filled to its maximum capacity four times during the last 6 months. Each incident forced a temporary shutdown of Unit 100. Each shutdown resulted in lost production worth approximately $25,000 in revenues. A high level in T-101 also creates the potential for a spill of RM-12, thereby creating a serious environmental problem were it to enter the drainage system.			
No way of improving the situation using the current organization and equipment or instrument has been identified.			
Proposed change			
A connection should be installed between Tank T-101 and the adjacent Tank T-102 so that excess inventory of chemical RM-12 can be stored in T-102 while P-101 is being repaired.			
Justification			
Safety. None. A spill of RM-12 does not have significant safety consequences.			
Environmental. Possibility of a spill, causing RM-12 to enter the drainage system, leading to a reportable incident.			
Operations. Lost production worth $200,000 per year.			
Maintenance. A facility shutdown increases the maintenance work load, particularly when the facility is being restarted.			
Public Relations. None			
Emergency Change	~~Y~~/N	Temporary Change	~~Y~~/N
Previous actions taken			
A reorganization, in which operators from Unit 200 took responsibility for the level in T-101 was attempted. However, the situation did not improve because the tank is located too far from their normal work areas so the Unit 200 operators were not able to check tank levels frequently enough.			

In the example, the Initiator is proposing that another tank, T-102, be used to store excess inventory of RM-12 while P-101 is being repaired. Other potential solutions include:

- Automate the operation of LIC-101 and the block valve.
- Make P-101 more reliable by implementing a preventive maintenance program for it.
- Install an on-line spare to P-101.
- Increase T-101 capacity.
- Streamline the shutdown and restart procedures for Unit 100 so that it is less sensitive to problems with T-101.
- Upgrade the control systems in Units 100 and 200 to provide for a more steady operation and hence fewer swings in the inventory of RM-12.

Table 10.3 Section B—First Review

Section B—First Review			
Name of reviewer	Bobby Smith	Date	2015-06-06
Discussion	Approximately 3 years ago, a serious near-miss occurred during an unplanned shutdown of Unit 100. <details here>. This proposed change would reduce the change of this happening again.		
Suggested modifications	Another solution may be to install a spare pump in parallel with P-101, rather than using T-102 as a spare tank.		

Justification

The Initiator should provide a justification as to why he or she thinks that a change should be made. Initially, this justification may be quite qualitative and general, but it will provide everyone involved with a sense as to the scope of the problem that is being addressed. Factors to consider include the following:

- Safety
- Environmental
- Increased production
- Increased productivity/efficiency
- Reduced energy consumption
- Reduced maintenance costs
- Reduced spare parts inventory
- Public relations
- Impact on other facilities in the area.

Emergency change/temporary change

The response in Table 10.3 shows that the proposed change is neither emergency nor temporary. The flags for these items are therefore set to "No."

Previous actions taken

Many facility problems have a long history; therefore, the current proposal may just be one in a series of attempts to solve this particular problem. If the Initiator is familiar with the historical background of the change scenario, he or she should provide that background at this point. In particular, if previous solutions to similar problems were attempted, and they failed, a description as to what happened should be provided. This is one area where the First Reviewer, as described in the next section, can be particularly helpful because he is likely to have a lot of facility experience, and will know all the war stories.

SECTION B—FIRST REVIEW

Following the initiation of the MOC process, the next step, as shown in Figure 10.6, is to carry out the First Review, which can be relatively informal and unstructured as compared with the Detailed Evaluation (Section C) that follows.

The First Review will be carried out by a team that provides a quick, commonsense reality check on the proposed change. The team is made up of experienced personnel who can quickly analyze the feasibility of the change.

Regardless of how the MOC system is organized, it should be recognized that the First Review process will happen anyway, and so it should be incorporated into the MOC system. No one wants to look foolish for proposing an idea that can be easily shot down, and very few people have the self-confidence to formally propose a system change without having other people "kick the tires."

In the case of the standard example an operator (Carlos Hernandez) may propose a change to the T-101 level control system in order to reduce the chance of the tank overflowing. What he may not know is that changes to the operation of Unit 200 have already been made (while he was on vacation) so that the overall operation is now much more stable. Consequently, the chance of occurrence of a high level in T-101 is now much reduced, and there is no longer any need to make changes to the operation of T-101. The First Reviewers will tell the Initiator of this change, and he can drop the idea right away before it goes any further.

If the Initiator has a proposed solution for the change being discussed (although this is neither necessary nor even desirable) the reviewers may also be able to come up with alternative solutions to those provided by the Initiator. Because they usually have a lot of experience of the facility's history they may recall, for example, that a similar change was proposed some years previously. That experience will help identify any potential problems with the proposed change and may suggest whether it will be effective at solving the problem it is intended to solve. Therefore, rather than installing brand-new instrumentation on T-101, the reviewers may note that a similar problem

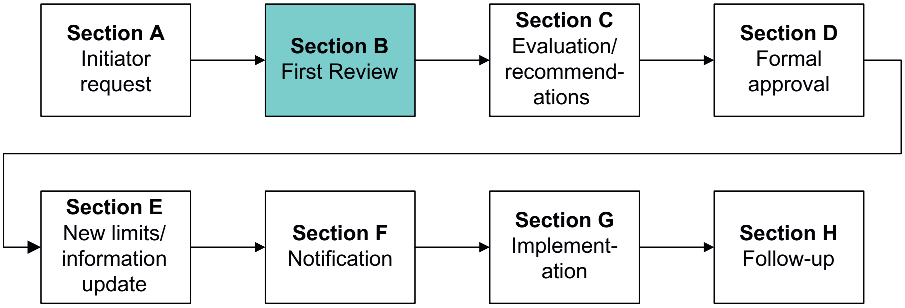


FIGURE 10.6

Section B—First Review.

with another tank was solved by making an operational change to the upstream operation. The same solution could be applied in this case, providing an elegant and cost-effective solution.

IN-KIND/NOT-IN-KIND CHANGE

If the Initiator should decide to push forward with the proposed change, it is necessary to determine whether the change is In-Kind or Not-In-Kind. The review team can help with this decision. If they decide that the change is In-Kind, then they can go ahead and take the necessary action without further review or analysis, and the formal MOC process is never initiated.

The In-Kind/Not-In-Kind decision is critically important. If a supposed In-Kind change turns out to be Not-In-Kind after all, then a serious accident may occur. Yet often there are few control mechanisms at this point in the MOC process. (The opposite scenario is less of a concern. If the change is incorrectly determined to be Not-In-Kind, but later turns out to be In-Kind, then the only loss is that some time has been wasted on unnecessary evaluation.)

Because of the criticality of this decision, the supervisors and lead operators need to be thoroughly trained on deciding whether a change should be In-Kind/Not-In-Kind, particularly since the choice of In-Kind change offers a tempting way of bypassing the whole MOC process.

SELECTING THE FIRST REVIEWERS

The people who perform the First Review are usually very knowledgeable and experienced in the operation of the facility where they work. Hence, they possess a good deal of influence within the organization due to their years of service, their knowledge of the facility, and their personal reputation. They are known and trusted. Consequently, a change that they endorse will acquire authority and momentum. The opposite also applies: if they are opposed to a change, they probably have sufficient influence to make sure that it never happens or that it is stalled indefinitely.

Moreover, their knowledge is not just technical; many reviewers, having had many years of service at the facility in question, and will so possess a thorough knowledge of the company's culture and organization. Hence, they will understand the political and organizational implications of the proposed change and will discern what changes and programs will be accepted in the current business, financial, and political environment.

There are, however, potential pitfalls to the high level of experience of the reviewers. One of these is that, if a review team opposes the proposed change, the Initiator may give up on his or her idea too quickly—particularly if the idea appears to be a little "off the wall."

A second potential pitfall is that, because most reviewers will have worked at the facility for many years, their experience can actually be a limitation to fresh thinking because they may not be able to think outside the boundaries of what they have seen and what they know. In particular, they may declare that they are opposed to an idea because something similar was attempted some years previously and "it didn't work then, so it won't work now." They may fail to recognize that the idea may be worth a second try, or that conditions have changed since the first time, or that the new idea is actually different from the previous one. In other words, the reviewers may not be good at "thinking the unthinkable"—they may be less adept at coming up with new ideas than people with less experience of that particular facility. After all, as has already been stressed, a change moves the facility into an area that it has never been before. Therefore, by definition, a reviewer cannot have direct experience of what the facility operation will look like following the change. Consequently his or her experience has in-built limitations.

A third potential pitfall is that the high level of experience possessed by the reviewers may serve as a drag on innovation, especially that of younger people who do not have the self-confidence to go against those with much more experience than they. The experienced reviewers may have become somewhat skeptical or cynical about the organization for which they work, and may therefore discourage Initiators from suggesting new ideas. They may be inclined to statements such as, "Everyone knows that we will never get funding for solving problems such as this," or, "The way things are around here, it will take a year and a day to get people to agree to this change." This response can be rather deflating to someone who is young and eager, but once more demonstrates the need for persistence and patience in the MOC process.

Moreover, it is important to keep a sense of perspective. Many good ideas in all parts of a company's business are rejected, or die stillborn. The company does not founder as a result, nor is the safety of the operation violated. Moreover, if someone finds that his or her idea has been "unfairly" rejected during the informal review process yet still feels strongly that it should go forward, then this first refusal will be treated as being no more than an interim rebuff ("there are no obstacles—only opportunities"). He or she will continue to lobby for what they want and believe in; if necessary, they will resubmit a rejected proposal in a different form, or work it through different channels. A good Initiator does more than really propose an idea—he or she actively champions it.

MOC FORM—SECTION B

Once the First Review is complete, the second part of the MOC form can be completed. An example, based on the T-101 illustration, is shown in Table 10.3. (In practice, Sections A and B will often be completed at the same time.)

Name/date

The name of the reviewer is needed for the same reason as the name of the Initiator is needed—it provides an essential part of the overall record as well as a description as to the authority and knowledge of that person with regard to the proposed change.

Discussion

Just as the Initiator had to provide an estimate as to the likely safety and health impact of the proposed change, so the First Reviewers should provide their own evaluation. They can often contribute their knowledge and experience to provide justification for the proposed change.

Suggested modifications

The First Reviewers should have an opportunity to add their own opinions about the suggested change. If they can think of a better way of implementing the change, it can be entered into this section of the form. In this example, it is suggested that a spare pump be installed rather than using T-102 to store excess RM-12.

SECTION C—DETAILED EVALUATION

Up to this point, the change process has involved only a few people, and has been relatively informal. However, if the Initiator and the First Reviewer(s) believe that the proposed change should be pursued, they are at the point where the change will have to be submitted for system-wide approval. The proposed change will be evaluated by a team of people representing different disciplines and specialties. The MOC process is now at the Detailed Evaluation step, as shown in Figure 10.7 (which is based on Figure 10.3).

A representative detailed evaluation process is shown in Figure 10.8.

REVIEW PROCESS

Figure 10.8 starts with the Initiator (at the left of the diagram) entering a proposed change into the MOC system (Sections A and B). The MOC Coordinator then creates a list of persons to carry out the review and in what order. Generally, there will be three types of person involved in the review.

Information only

Some people see the workflow documentation for information only. These people are not expected to comment on the proposed change, but they do need to know what is going on.

Approval

Some of the persons in the workflow process will approve (or reject) the proposed change based on their technical expertise. The workflow needs to be designed such that, if someone does reject a proposed change, the system "knows" that the rejection took place, and others are informed.

Modify the document

The third group of people who are in the workflow process consists of those who add value to the process, or change the documents associated with the proposed change before they move on to the next persons.

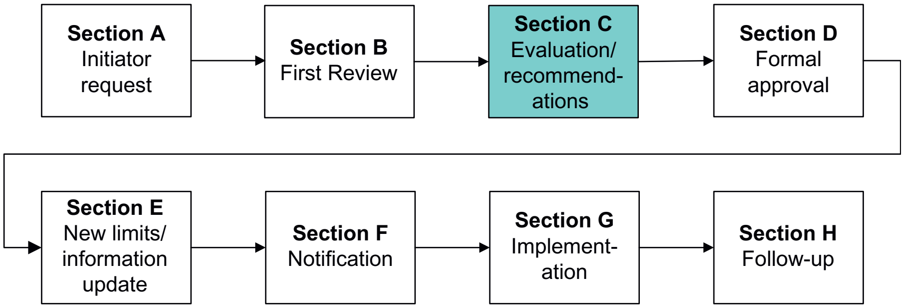


FIGURE 10.7

Section C—Detailed evaluation.

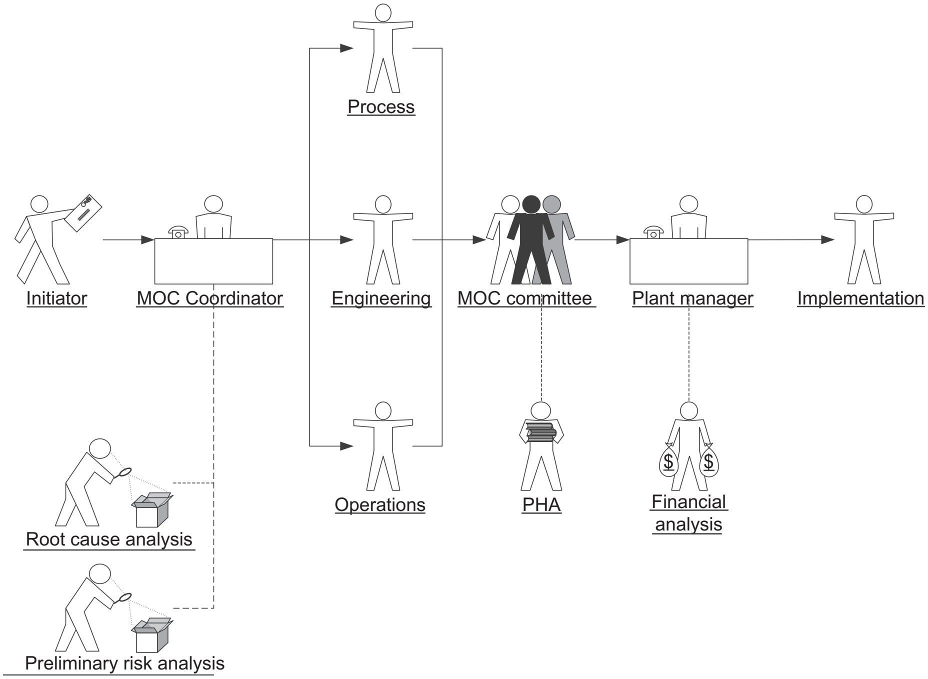


FIGURE 10.8

Workflow process.

The MOC Coordinator will also:

- Prepare a formal number and title for the proposed change.
- Find pertinent documents that the reviewers are likely to need. Such documents can include P&IDs, MSDS, and instrument logic diagrams.
- Decide on the review team. Generally, there will be a core team, supplemented by other experts, depending on the nature of the proposed change.
- Decide on details of the review process, particularly the deadlines that the reviewers have to meet.

The MOC Coordinator may suggest that a root cause analysis be carried out. Root cause analyses often come up with unexpected causes of problems. Hence, they can provide valuable insights for those considering what recommendations to make.

It will not normally be necessary to conduct a root cause analysis at the depth usually carried out for the investigation of actual incidents. However, the MOC Coordinator, the Initiator and others who are involved can consider whether the problem (or opportunity) identified has to do with major categories, such as:

- Equipment
- Instrumentation

- Operating Procedures
- Training.

At this stage in the MOC process, it is useful for the Coordinator to conduct a high-level hazards review, and to develop a preliminary risk ranking for the proposed change.

MOC COORDINATOR

Figure 10.8 shows that the MOC Coordinator (who may also be the facility's PSM Coordinator) plays a vital role in the change review process. He or she is responsible for:

- Selecting the members of the review team
- Making sure that technical information is available to all the reviewers
- Keeping the Initiator and Sponsor informed as to progress
- Summarizing the results of the evaluation for senior management
- Making sure that the evaluation process stays on schedule.

The MOC Coordinator may participate in the evaluation of the proposed change, but this is not his or her principal role. Rather, he must make sure that the evaluation of the change is managed properly. Since this means that he or she must retain some degree of independence, it is not reasonable for the MOC Coordinator to be either the Initiator or the Sponsor.

The MOC Coordinator is responsible for defining and enforcing the schedule for the implementation of the change. This responsibility may require coordination with other departments or functions. For example, if the change requires that the facility be shut down, and a full turnaround is scheduled for the near-term, the change review should be complete before that turnaround so that the work required by the change can be incorporated into the overall turnaround program.

REVIEW TEAM

The core of the review team is likely to consist of representatives from process engineering, operations, maintenance, and project management. Other departments that may be involved include safety, environmental, the laboratory, and vendors.

Process manager

The Process Manager (or his designee) is responsible for making sure that the proposed change does not put the process itself in an unsafe state. He or she will provide the current safe limits for temperature, pressure, level, and composition, and will check that the proposed change does not go outside these limits. If it does, the process manager will be heavily involved in setting new limits and creating new safeguards. He or she will probably manage the PHA, as needed.

Engineering manager

The Engineering Manager ensures that the proposed change meets the appropriate engineering codes and standards. The regulations to be followed will most likely come from OSHA, BSEE, or the EPA (along with their State counterparts).

- OSHA (Occupational Safety and Health Administration)
- BSEE (Bureau of Safety and Environmental Enforcement)
- EPA (Environmental Protection Agency).

The engineering standards will usually come from voluntary bodies such as ASME, API, ISA, and NFPA.

- ASME (American Society of Mechanical Engineers)
- API (American Petroleum Institute)
- ISA (Instrument Society of America)
- NFPA (National Fire Protection Association).

He or she will usually also be responsible for updating much of the engineering documentation.

Operations manager

The Operations Manager will have to operate the facility after the change is made. He will be closely involved in the PHA, and will supervise the Operational Readiness/Prestartup Safety Review.

The operations manager will also ensure that updated operating procedures are written, and that the operators are trained in those procedures.

BUILDERS

Although the MOC Coordinator is responsible for putting together the review team, in many cases he or she may not know all the people who could contribute to the analysis of the change. In such situations, the MOC Coordinator can appoint Team Builders, each of whom creates his or her own team.

For example, the Operations Manager may be asked to review a new way of carrying out an activity. He may decide that he would like the opinion of a particular operator who has extensive experience of the area that is being changed, but who is not on the original list of reviewers. Assuming that the Operations Manager is the Builder of the "Operations Review Team," he can add this operator to the list of reviewers.

One of the decisions that each Builder has to make for his team concerns the sequence of reviews. The Operations Manager may decide that it is best if the Operations Superintendent reviews the proposed change ahead of the Production Engineer.

In general, however, it is usually best if the proposed change can be distributed to everyone at one time, so that they can work in parallel. This not only reduces the amount of time needed for the review; it also encourages the reviewers to interact with one another, either in person or by e-mail, or in an electronic chat room.

PROJECT TEAM

Once the core management team has signed off on the proposed change, the MOC flows to a project team whose task is to decide on what actual change is most appropriate. The project team can use a root cause analysis to help them determine the best solution to the problem that has been identified.

SOFTWARE

MOC requires the use of specialist software. There is too much complexity and communication in even the simplest system to be managed using a paper-based system. The following guidance has been provided with regard to the design and selection of suitable MOC software:

- Develop a flow sequence for the documentation to do with the change
- Identify roadblocks
- Easy to use. As is stressed throughout this book, the MOC system should be available to all personnel on the facility. This means that people who rarely think about MOC must be able to use the software
- Built around a robust database system that allows for large amounts of information to be used by many people at the same time
- Badger mails to those who are on the critical path and who are behind schedule
- Issue reports to management as to what changes are in the system, and which ones are behind schedule
- Interface with the management systems used for the other elements of PSM.

REVIEWERS

The reviewers are those people selected by the MOC Coordinator and by the Builders to evaluate the proposed change and to come up with recommendations. The reviewers have three principal tasks.

1. Confirm the problem

The reviewers have to satisfy themselves that there is indeed a problem that requires solving and that it cannot be addressed simply by implementing existing work procedures more effectively or more completely.

2. Problem analysis

Having satisfied themselves that there is a need for a system change, the reviewers should analyze all aspects of the proposed change to make sure that it is thoroughly understood. They may choose to carry out a root cause analysis.

3. Identify possible solutions

Finally, the reviewers should, wherever possible, put forward recommendations as to how the change should be implemented. As has already been discussed, the first proposed solution may be neither the best nor the most elegant. During the Detailed Review process people should be encouraged to brainstorm, and to come up with as many ideas as possible, even if some of the ideas seem strange or unusual. The other reviewers and the formal MOC committee will evaluate all the proposals later and choose the one that seems to be the most effective and suitable.

QUALIFICATIONS

The members of the review team should provide the capabilities described in the following sections (no single person will be good in all areas; the review remains a team effort).

Experience

Very few problems are truly original—most have been observed before, at least in a similar form. Therefore, it is likely that experienced reviewers will be able to analyze the proposed change by analogy, i.e., they will compare it with similar problems that they have seen in the past. From such comparisons they may be able to develop useful insights as to how the problem should be addressed.

Although experience is an invaluable part of the analysis of change, it is important to realize that it has limitations. A change that requires the use of the MOC system is, by definition, taking the operation into new areas—it is moving the operation beyond the current Safe Operating Limits. Therefore, as has been discussed with regard to the input from the First Reviewer, no one can actually have knowledge and experience of the new conditions.

The potential problems associated with the input of highly experienced reviewers can be compounded by the fact that they will often possess a good deal of authority—both formal and informal (just as with the First Reviewer). Hence, they may tend to suppress creative thinking with statements such as "I've been here 20 years, and that's never been a problem before" (with the implication that it will not be a problem now). Or, "I've been here 20 years, and you're the fourth person to try to fix this problem" (with the implication that this attempt will also fail). The Initiator and the Sponsor must persevere in order to overcome such objections. Changes need champions.

Technical knowledge

The review team members should possess the appropriate technical knowledge in areas such as chemistry, instrument engineering, materials of construction, and equipment reliability. In the case of the standard example, technical reviewers could include the following personnel:

- A chemist or environmental engineer who can determine the impact of a spill of RM-12
- An instrument engineer who can evaluate the effectiveness of different types of level instrument
- A mechanical expert who can come up with ways of making P-100 more reliable.

Feasibility

Team members should understand the organizational issues related to the proposed change. Some changes—particularly those to do with safety—have to be made, regardless of organizational circumstances. But the justification for most changes is not totally compelling; therefore, organizational factors have to be considered.

Economic feasibility must always be considered. All companies go through cycles of funds availability. There are times when companies are willing to spend, and times when they are not. Therefore, assuming that the proposed change is not a "must-do," it should be submitted when funds are available.

Regulations are another factor. There is usually a political and/or public relations aspect to regulatory compliance. For example, a facility which has had a series of spills and is in trouble with an environmental agency is more likely to support changes that reduce potential environmental problems than one that has faced no problems in this area.

"Out-of-the-Box" thinking

Ideally everyone on the team should be adept at "Out-of-the-Box" thinking. However, this is unlikely to be the case. Therefore, at least one of the reviewers should be good at "thinking the unthinkable." Since the proposed change will—by definition—be taking the facility operation into areas that have not been experienced before. There needs to be at least one person on the Review Team who is thinking through the implications of this insight, and who has the self-confidence to put forward ideas that may be unusual or different.

Even if some team members have trouble with this way of thinking, they must learn to be tolerant with "off-the-wall" ideas generated by their colleagues. They must recognize that such ideas will occasionally generate fresh insights and innovative solutions to chronic problems.

RECOMMENDATIONS

The outcome of the detailed evaluation process is a specific recommendation (or set of recommendations). It is important to clearly distinguish between problem definition and solution development, in the same way as a hazards analysis needs to distinguish between findings and recommendations. Statements such as "We propose to increase the reactor temperature, so we need to install a high temperature alarm" should be broken down into:

- "We propose to increase reactor temperature outside the current safe limit."
- "Additional precautions are needed—one possible solution is to install a high temperature alarm."

When the logic is laid out clearly, as shown above, it becomes clear that the problem may have multiple solutions.

MOC FORM—SECTION C

Once the Detailed Review is complete and the recommendation(s) generated, the MOC Coordinator should collect all of the comments and ideas that have been generated, and summarize and analyze them as shown in Table 10.4.

SECTION D—FORMAL APPROVAL

Before a change can be implemented, it must be formally approved and accepted by the facility management (Figure 10.9). This approval is necessary to meet the requirements of the process safety regulations. The approval also serves as a formal record should there ever be an incident in which the change is implicated as a possible cause.

MOC COMMITTEE

Most facilities will use an MOC committee for the formal approval step. This committee evaluates the proposed change on behalf of the company's management, and, assuming that it agrees with what has been proposed, it selects one of the recommendations. The committee will consist not only of technical reviewers, such as were used in the Detailed Evaluation step, but also representatives from other departments, such as legal and human resources.

Table 10.4 Section C—Detailed Evaluation

Section C—Detailed Evaluation			
MOC Coordinator	Jane Chen	Date	2010-06-16
Review teams			
Operations	Corporate	Human Resources	
Rich Jones Unit 100 Supervisor Susan King Area Superintendent	Richard Gonzalez Project Manager Mike Chu Instrument Engineer . . .	Joe Smith HR Manager	
Process	Engineering		
Fred Thomas Unit 100 Engineer June James Instrument Engineer	Stan Chu Engineering Manager		
Discussion			
It was agreed that a system change is needed. In addition to the ideas already put forward, the following options were considered:			
Add high-level interlock to T-101. Modify operation of Unit 200. Put T-102 into service to store RM-12.			
Recommendations			
It is proposed that a high-level interlock be installed on T-101.			

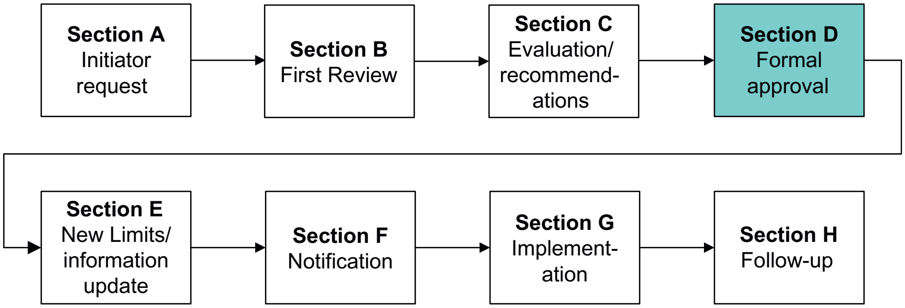

Section A Initiator request
Section B First Review
Section C Evaluation/ recommend-ations
Section D Formal approval
Section E New Limits/ information update
Section F Notification
Section G Implement-ation
Section H Follow-up

FIGURE 10.9

Section D—Formal approval.

Each of the committee members should sign off on the change once they are satisfied that it is safe and workable (Section D of the MOC form). When a committee member signs the change form, he or she is stating that a management system for controlling change has been implemented, and that it was properly followed. It is not likely that the committee members will have sufficient knowledge of the process to comment on the details of the change itself. If they do possess this knowledge, they will probably be reviewers in the detailed evaluation step.

If the proposed change is not safety-critical, it is likely that most of the committee's questions will be to do with the financial return on the proposed change.

Operations

The operations department will almost always have to review and comment on the proposed change because they are the ones who will have to operate the facility once the change has been implemented. Also, it is likely that they are the ones who will be responsible for writing new or updated operating procedures and for training the operators in the new way of running the facility.

Maintenance

Managers from the maintenance department are usually involved in reviewing proposed changes because they are likely to be involved with making the change itself, and then for maintaining the new system, once it is up and running. Also, they are usually responsible for integrating the changed into the facility's Asset Integrity program.

Technical

Personnel in the Technical Department are responsible for checking that the new process is safe and fundamentally workable. In the case of the Standard Example, they will comment on the use of the second tank, T-102, to store RM-12. They may predict that there is a serious risk of mixing two incompatible chemicals and that a violent and dangerous reaction could ensue. Hence, they will decide that the option of using T-102 should not be pursued.

Engineering/construction

If the facility has its own engineering department, its personnel will evaluate the technical and engineering integrity of the proposed change. The Engineering Manager will also ensure that the proposed change is legal and that it does not violate any safety, environmental or other regulations that could lead to problems later on. He or she must confirm that the proposed change also meets the appropriate engineering standards, as discussed above.

PROCESS HAZARDS ANALYSIS

One of the most important decisions that the MOC committee has to make is whether or not to require that a PHA be carried out. Such an analysis will generally be performed when critical variables are to be modified, or if the change involves input from many disciplines and departments, then a PHA may help in the identification of accident scenarios that result from potential interdepartmental misunderstandings, or if unanticipated consequences of the change could lead to a serious accident, then a PHA should be carried out.

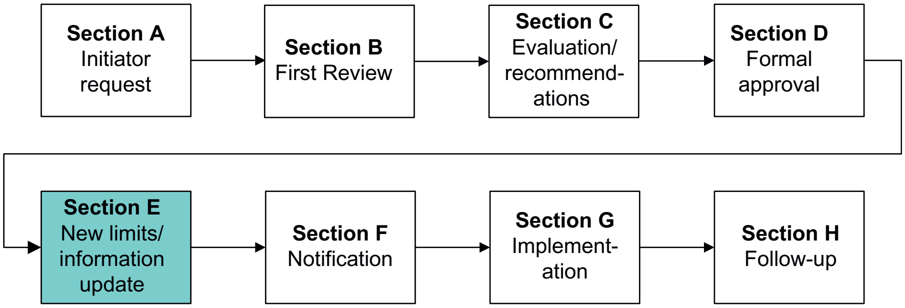


FIGURE 10.10

Section E—New limits.

VARIANCE PROCEDURES

To this point, it has been assumed that the MOC procedure is followed properly, and that the change is implemented (or not) according to the procedures prescribed by management. However, there are times when management may choose to take a variance, i.e., to go ahead and make a change, even though the complete MOC process was not followed.

In principle, there should never be a need to take variances. Yet the reality is that a large part of a manager's job consists simply of deciding when it is safe and proper to override established procedures. If it were possible to follow management procedures all the time, managers would have little to do.

If a manager does decide to take a variance, his decision should always be reviewed by at least one other person. This person may identify a problem that the manager overlooked. Only in a true emergency can one person assume the lone responsibility for a change.

An example of a typical variance would be the case where a facility is installing a new piece of equipment, such as a pump. The company standards may call for the pump to be located at a certain minimum distance away from other equipment. However, due to real estate limitations, this spacing constraint cannot be met. In this situation, the manager may permit a variance to be taken (the pump can be located close to other equipment)—but may then require that additional gas detectors be installed in the area so that a leak at the new location is picked up right away.

SECTION E—NEW LIMITS/PROCESS SAFETY UPDATE

Once the change has been approved, new Safe Operating Limits need to be defined (Figure 10.10) and engineering documentation be updated.

Also, all related elements of process safety (Tables 1.1 and 1.2), such as operating procedures, P&IDs, training, and asset integrity, must be updated. All these items fall under the area of Process Safety Information. It is vital that all process safety information be updated before the change is actually made; otherwise, there is a good chance that these administrative issues will be deferred indefinitely.

SECTION F—NOTIFICATION

All persons who are affected by the new values must be informed. They must also be trained in what to do if the new limits are exceeded.

The notification process is distinct from training; it concerns those people who have some peripheral involvement with the consequences of the change, but who are not directly affected by it. In the case of the Standard Example, the operators and instrument technicians will need to be trained regarding the operation of Tank T-101 if the instrumentation associated with it is modified. However, the administrative personnel and people at corporate headquarters need only be notified (Figure 10.11).

Those being notified should be told of the proposed change date, along with a brief overview of what is being done, why it is being done, and what the anticipated impact on the process might be. If the facility has an MOC software system, the MOC Coordinator can set up various e-mail lists, and notify people using those.

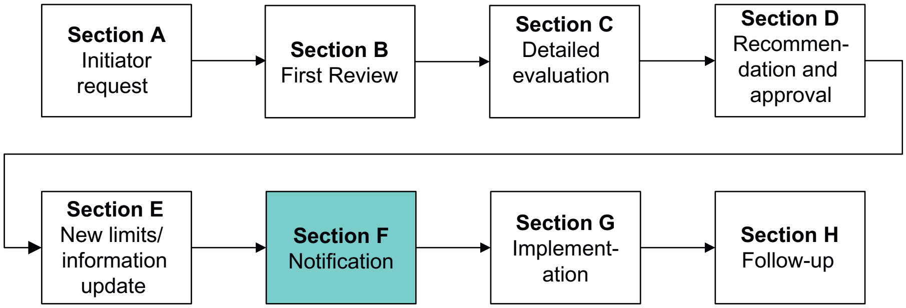


FIGURE 10.11

Section F—Notification.

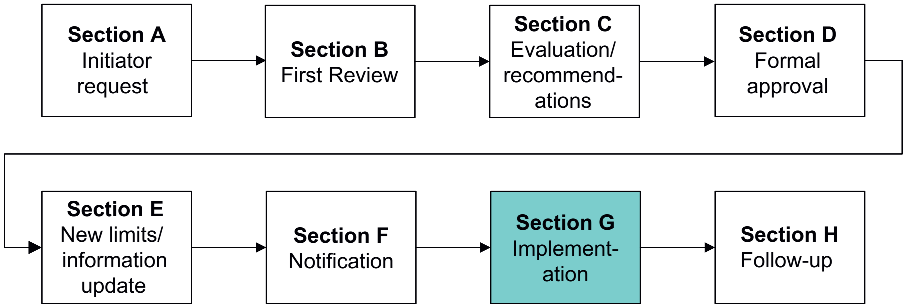


FIGURE 10.12

Section G—Implementation.

SECTION G—IMPLEMENTATION

Finally, the change can be implemented, as shown in Figure 10.12.

Before it is implemented, the proposed change may require approval from various people, depending on its nature. However, three approval signatures are critical, and should always be present.

The first is that of Process Manager. He or she is saying that the proposed change has been reviewed for its process impact and that the new conditions are acceptable (maybe after some modifications have been made). The second critical signature is that of the Engineering Manager. His signature states that the proposed change conforms to all engineering standards and codes, and that the change is properly incorporated into the overall facility project management system. Finally, the Operations Manager must sign off on the proposed change. His signature states that he has accepted the change, that it has been implemented correctly (probably using an Operational Readiness or Prestartup Safety Review). He is also stating that operating procedures have been updated and that the necessary training has been carried out.

SECTION H—FOLLOW-UP

Once the change has been implemented, there should be a follow-up to make sure that the change was implemented properly (Figure 10.13). Reminders to do with the various action items assigned to various individuals are often handled by an automated e-mail system—sometimes referred to as badger mail.

In general, the following three steps provide a good framework for the follow-up process:

1. Ensure that the change management procedure such as the eight-step process outlined above was followed.
2. Ensure that all the other elements of process safety were properly evaluated and that there were no unexpected side effects.
3. Ensure that the change itself was implemented properly, and that the operators have an understanding of the new operating limits and what to do if those limits are exceeded.

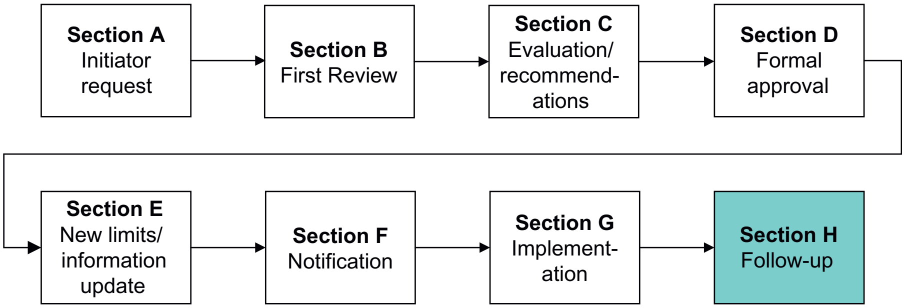


FIGURE 10.13

Section H—Follow-up.

Some of the documents that have to be checked and possibly updated after a change has been made include the following:

- P&IDs, including equipment lists and line lists
- Instrument loops, including alarm settings and interlock logic
- Operating procedures
- Operator training records
- Preventive maintenance procedures
- Isolation valve list
- Electrical one-line diagrams
- Blind lists
- Inventory levels
- Relief valve information.

Finally, the follow-up should also check that the change has actually achieved the desired results, i.e., that the goal of improved safety or operability was attained.

CHAPTER

INCIDENT INVESTIGATION AND ROOT CAUSE ANALYSIS

11

CHAPTER OUTLINE

INTRODUCTION

The thorough investigation and analysis of incidents (both actual events and near misses), along with the appropriate follow-up, provides one of the most effective means of improving the safety and reliability of process facilities. Other risk management programs, such as hazards analysis and management of change (MOC), are directed toward anticipating problems so that corrective actions can be taken before an event occurs. Yet, in spite of their undoubted value, these predictive techniques do have the following limitations:

- The analyses are, of necessity, theoretical and speculative; there can be no assurance that all plausible events have actually been identified. Indeed, it is likely that important failure mechanisms will be overlooked.

Process Risk and Reliability Management. DOI: http://dx.doi.org/10.1016/B978-0-12-801653-4.00011-4

- It is difficult to predict the true level of risk associated with each identified event because estimated values of both consequence and likelihood are usually very approximate. In particular, predictions as to what might happen are invariably colored by the personal experiences of the persons carrying out the analysis.
- Most serious events have multiple causes, some of which appear to be totally implausible or even weird ahead of time (which is why such accidents so often seem to come out of the blue). Even the best qualified hazards analysis team will have trouble identifying such multiple contingency events.
- It is very difficult to predict and quantify human error—yet most major events involve such error. Actual incidents, on the other hand, provide hard information as to how things can go wrong, thus helping to cut through wishful thinking, prejudice, ignorance, and misunderstandings. The root cause analysis that follows an incident investigation will help identify weaknesses and limitations in a facility's management system, thereby reducing the chance of recurrence of similar incidents.

Another reason for emphasizing the importance of incident investigation in the process industries is that process safety management (PSM) systems—of which Incident Investigation and Analysis constitutes one element—have been in place in many cases for more than 20 years. Many of these facilities have made good progress in meeting regulatory requirements. However, the fact that such systems can "survive an audit" and are working well on paper does not mean that they are as effective at actually improving safety as they might be. Incident investigations help identify how the elements of PSM really are functioning and can provide management with insights as to how the systems can be improved.

There is a good deal of publicly available information concerning incidents that can be of value to all facilities and plants. The public dissemination of accident and incident histories will help all companies improve their safety. For legal reasons, it may be necessary to change some of the information to protect individuals and to keep sensitive industrial information secret, but changing the information in this way is not likely to change the value of the lessons learned.

When a company develops an open attitude toward incident reporting, it may notice an increase in the number of recorded incidents. This does not mean that more incidents are actually taking place—it simply means that fewer mishaps are being swept under the rug and that people are reporting events more freely.

MANAGEMENT LEVEL

The ultimate purpose of an incident investigation is to determine how the facility or company's management systems failed. Therefore, when conducting an investigation it is important to understand what level of management is being considered. The following four levels can be considered:

1. Line supervision
2. Facility management
3. Executive management
4. Industry regulations and standards.

The level of root cause analysis that is typically carried out for each of these levels is discussed below based on an example of a seal failure of Pump P-101A in Example 2 in Chapter 1.

LINE SUPERVISION

Line supervisors and superintendents are often called upon to conduct a quick “root cause” analysis immediately following an event. Using the example of the pump seal failure, the line managers will be faced with questions such as:

- Was this failure unique, or is it part of a larger problem to do with pump seals? Therefore, should we immediately shut down other pumps that use this type of seal, even if that decision leads to lost production?
- Do we need to implement any Immediate Temporary Controls to minimize any problems that could occur from other seal failures? For example, are new fire control systems needed?
- Is there a need to replace the contract company that is running the preventive maintenance program (or to change the preventive maintenance program itself)?

At this level, the root cause analysis needs to address the supervisors’ primary responsibilities, which are to make sure that the immediate situation is brought safely under control, and to make short-term changes that prevent the immediate recurrence of this or similar events.

Line supervisors are not much concerned with the design or structure of their company’s management systems. However, the company culture will affect their decisions, particularly if there is a perceived conflict between production and safety.

FACILITY MANAGEMENT

A facility manager has direct control over a large operating unit such as a refinery or an offshore platform. With respect to root cause analysis, this manager probably has a time horizon of 3–6 months and has a substantial discretionary budget. By and large, he or she does not create management systems, but he is responsible for their implementation. Therefore, recommendations that call for better implementation of systems will often be his responsibility, but this manager is unlikely to have the authority or funds to make substantial changes to those systems.

With respect to the seal failure example, he or she should be able to improve maintenance procedures and training (and hire extra people to do so, if necessary). However, the facility manager is probably not able to make structural changes to the company’s enterprise software systems that are used for equipment purchase because he or she can affect culture only at the local level.

EXECUTIVE MANAGEMENT

A company’s senior managers have the most discretion with respect to the ability to change management systems—and to fund those changes. Their time horizon is likely to be months or years. Managers at this level are likely to be most concerned about cultural and people issues. For example, if the pump seal failure identifies problems with the enterprise software that the company is using, senior managers may be concerned that use of the same software team that installed the software to implement an upgrade may lead to a recurrence of problems because the root cause difficulty was not the software itself, but the team that installed and ran it. In other words, executives are concerned not just about management systems, but also about the people who implement and operate those systems.

INDUSTRY REGULATIONS AND STANDARDS

Every company operates within an industrial community that creates and administers rules and regulations, and that also creates consensus standards written by organizations such as API, ASME, and IEEE. The lessons learned from industrial events—particularly large accidents—help that community improve those regulations and standards.

Regulators and professional societies take a long time to introduce new standards—usually many years. However, their work can be extremely effective and can create widespread cultural change. For example, the Piper Alpha disaster (1988) made a large contribution to two distinct regulatory approaches to offshore safety (the Safety Case regime in Europe and API Recommended Practice 75 in the Gulf of Mexico). Both approaches have proven to be successful in changing fundamental practices and cultures.

INCIDENT INVESTIGATION AND ANALYSIS PHILOSOPHY

Publications in the field of incident investigation and analysis often promote a particular methodology with the implicit claim that their approach is better than the methods promulgated by other organizations. Such publications are often commercial in their approach, thus tending to create a concern in the mind of the reader as to the objectivity of the materials that are presented.

This chapter does not advocate or promote any particular methodology. Each analytical technique has its strengths and weaknesses—an effective investigation will use a judicious mix of approaches as circumstances dictate. Indeed, it is suggested here that an effective incident investigation and analysis requires much more than the mere application of a particular investigation technique. Equally important—maybe more so—is the ability on the part of the investigators to inculcate an atmosphere of trust and confidence with everyone with whom they work—not only those involved in the incident itself, but also the managers who will be charged with taking appropriate corrective actions. Moreover, a good investigator will have the experience and analytical skills to develop insights that let senior management understand what basic changes need to be made.

Therefore, rather than stress the use of just one particular analytical method this chapter suggests that a successful investigation should be conducted through use of the six strategies and techniques listed below and also in Figure 11.1.

- Establish trust, and thereby encourage candid discourse from those involved in the event and also from the managers responsible for follow-up
- Listen to what people actually say, base all findings on verifiable facts, and be thorough in all phases of the investigation
- Establish a clear cause and effect chart—backed up with solid evidence—integrated into a timeline
- Use technical experts to assist with understanding specialized issues

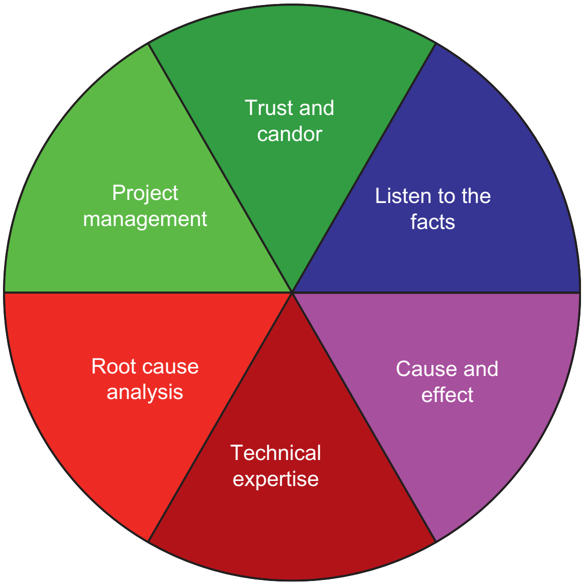


FIGURE 11.1

Elements of successful incident investigation and analysis.

- Develop an understanding of root causes and systemic issues at different management levels
- Manage an incident investigation and analysis as a project with a schedule, budget, and predefined deliverables.

TRUST AND CANDOR

The most important feature of a successful investigation is the establishment of trust between the investigators—who are *not* interrogators—and the persons involved in the incident itself. In one instance, a technician whose actions had contributed to the occurrence of an injury event approached his boss 24 hours after the interviews had been concluded; he voluntarily reported that a valve that for which he was responsible should have been open at the time of the incident was actually closed. Without that information it is unlikely that the investigating team would have ever have fully understood what happened. The technician was not the only person who was candid. His boss, who had 25 years of experience with the equipment involved, took the initiative to successfully work out the complex sequence of events that led to the incident, even though the upshot was to make his own company and he himself look more accountable for the event. The integrity and candor displayed by these two persons showed that the investigation process had gone well.

It is also important to establish trust with the managers of the facility where the incident occurred. This can be done by ensuring that the investigation team keeps management and other directly affected parties fully informed at each stage in the investigation process. Thus the project becomes “our investigation,” not “their investigation.”

LISTEN TO THE FACTS

Many incident investigators are intelligent, highly experienced, and are not lacking in self-confidence. Although these attributes are valuable, they can get in the way of simply listening to the facts. For example, during one investigation, the team members noted that a piece of equipment was damaged. By assuming that the damage occurred immediately prior to the event, a plausible explanation as to what happened was developed. Unfortunately, for the credibility of the team members who had jumped to the (incorrect) conclusion as to what had happened, a manager who had arrived at the site a few hours after the incident noted that the equipment had not been damaged at that time; therefore, the damage must have occurred when the affected equipment item was being removed at an earlier time for inspection and repair. This inconvenient fact overturned the investigators' elegant and satisfying analysis.

An investigator must always be thorough—particularly when he or she thinks that the investigation is complete, and no more fact finding work is needed. For example, on one investigation the equipment involved in the event was moved from its location in the field to the vendor's yard. The lead investigator felt that there was really no point in going to the site of the incident because there would be nothing to be learned. Nevertheless, he did visit the site. On doing so he uncovered new information that led to a basic reassessment as to how serious the event could have been.

TECHNICAL EXPERTISE

One engineering company once used the slogan "There's no substitute for knowing what you're doing." In many investigations, it is found that a real expert is needed in order to establish the technical details as to what happened. As already noted in the example provided above, a senior manager who had 25 years of experience to do with the equipment involved took it upon himself to determine what happened. Without his insight, knowledge, and experience, the investigation team would have taken much longer to determine what happened—indeed they might never have done so.

The root cause was shown to be the lack of proper MOC. Many years prior to the incident, a block valve had been placed into the system; this valve had the effect of allowing one part of a supposedly depressurized system to retain pressure. In order to demonstrate the dangers associated with having this valve in the system, the lead investigators visited a factory where brand new units are made and found that the valve in question is never installed in the factory, moreover, the factory superintendent gave it as his opinion that the installation of such a valve was an unacceptable practice.

ROOT CAUSE ANALYSIS

Once the facts have been established and an understanding of the event has been established, a root cause analysis can be carried out in order to apply lessons learned to a broader set of circumstances. There are four types of root cause analysis:

- Argument by analogy (story telling)
- Barrier analysis

- Categorization
- Systems analysis.

Each of these approaches can be of value—to purposely exclude any of them, particularly for commercial reasons, is short sighted.

Difficulties with "root cause"

Because the term "root cause" is inherently abstract and, because it means different things to different people, it is difficult to come up with an agreed-upon definition, as described in the following quotation (Nelms, 2007):

> An 800 person forum comprised of Root Cause Analysis (RCA) practitioners from all over the world tried to define "Root Cause Analysis." They could not agree on an answer... It means different things to different industries—even different things within the same industries. It is even difficult to find consistency within the same companies, or even sites within a company.

One of the reasons for this difficulty is that it is not possible to find the true, fundamental cause of an event. Every event has one or more causes. These causes are themselves events which have their own causes and so on. The chain can regress infinitely, thus creating what has been referred to as the "Root Cause Myth" (Gano, 2007). It is possible to find root causes, but not "the" root cause.

A further difficulty with the term "root cause" is that different people have different perceptions as to what causes events. For example, if a pump seal fails, one investigator may note that the wrong type of seal was installed. Therefore, her root cause trail will examine the company's purchasing and procurement procedures. At the conclusion of the investigation, she may define the root cause of the failure as "Limitations in the enterprise resource software."

Another investigator may find that the maintenance technician who installed the seal had not been provided with accurate procedures and had never received training for the installation of this type of seal. Therefore, his root cause trail will scrutinize the process for writing procedures and for making sure that people are properly trained in the use of those procedures. His definition for the root cause of the failure may be "Failure to write adequate maintenance procedures and to properly train maintenance technicians."

A third investigator may note that the process liquid in the pump is different from the original design. He or she may then develop a root cause trail to do with materials failure caused by the liquid change, resulting in a root cause, "MOC system provides inadequate guidance regarding material integrity checks."

Each of these investigators is essentially following a "Why Tree" approach to root cause analysis. Given that there is an indeterminate number of potential chains, no incident investigation team—no matter how well qualified its members may be—can identify every one of those chains.

The existence of an indeterminate number of root causes may help explain some of the frustration that is occasionally expressed with standardized incident analysis procedures and software. In spite of their structured approach, these systems are fundamentally subjective. For example, one technique helps the investigation team list many of the possible causes that led to an event. Some of these causes are then identified as "causal factors" which are then developed into root causes. Yet the determination as to which causes are causal factors will necessarily depend on the training and experience of the persons making that selection. The decision is inherently subjective. Nelms describes this difficulty:

> The problem with Root Cause Analysis is that it has become whatever people want it to be. If you only want to see problems in your "Management Systems," that's all you will see. If you only want to understand the physical mechanisms of problems that is all you will see.

A further potential difficulty with regard to root cause analysis is the danger of drawing general conclusions from inadequate sample sizes. For example, an investigation into a pump seal failure may find that the maintenance procedures for installing that seal were very difficult to follow. The investigator must be very careful, however, about developing a general recommendation such as "Maintenance procedures at the facility require a major upgrade." It could be that all the maintenance procedures are of high quality with the exception of this one.

Yet, in spite of all the difficulties outlined above a working definition for the term "root cause" is needed. The Center for Chemical Process Safety (CCPS, 2003) provides the following definition for the term root cause.

> A fundamental, underlying, system-related reason why an incident occurred that identifies a correctable failure(s) in management systems. There is typically more than one root cause for every process safety incident.

The above definition highlights some of the difficulties with defining the term "root cause" that have already been discussed. For example, the definition assumes that "fundamental" causes exist—yet every analysis has to be stopped at some point. Hence no investigation can identify the true "fundamental cause."

A key word in the above definition is "correctable." Managers at all levels need the root cause analysis to provide them with practical guidance—something that will help them correct their problems, and thereby improve their culture. The need for defining root causes that can help lead to solutions is demonstrated in the following paraphrased definition, adapted from Mark Paradies,

> A root cause of an incident is the most basic cause that can reasonably be identified and that management can change.

Senior management may wonder if there is a root cause behind all of the "root causes" that have already been generated. For example, with regard to the failed pump seal, they may wonder if there is a single deficiency that can help them understand why they have problems with enterprise software, maintenance procedures, and the MOC system. In other words, they may ask "Is there something in our culture that explains all these different system failures?" A good investigator will help management answer that question.

Ockham's Razor

The principle of Ockham's Razor is attributed to William of Ockham (c. 1285–c. 1349), an English Franciscan friar. He is credited with the concept of Ockham's razor, which states that, "simpler explanations are, other things being equal, generally better than more complex ones."

With regard to Incident Investigation, this principle means that simpler explanations should be preferred to those that are more complex, unless the facts indicate otherwise.

PROJECT MANAGEMENT

One of the difficulties associated with many investigations is that they tend to suffer from "scope creep." They grow and grow and grow with root causes being piled upon root causes, without any clear idea as to when the end point has been reached. As one manager once sarcastically observed "The team seems to be trying to solve world poverty." It must be understood by all the team members that an investigation is a project, just like any other project. As such it needs a budget, a schedule, a clear scope of work, and a contingency plan for when things go awry.

A common problem to watch for concerns the preparation and publication of the final report. Once the investigation is complete, and management has been verbally briefed as to its findings, the investigators' bosses will want them to get on with their "real work." But the final report must be written; it is an essential component of any successful investigation.

ATTORNEY–CLIENT PRIVILEGE

Some investigations are likely to be used in subsequent law suits. This means that management may decide to place the work under attorney–client privilege. This topic is discussed in Chapter 20.

BLAME AND FAULT FINDING

Those conducting the investigation must understand that it is not their goal to find fault with those involved in the event under investigation. The reason for conducting the investigation is to understand how management systems failed, and then to take actions to prevent the recurrence of such failures—not to find culprits. (If it is believed that someone is explicitly at fault, then that investigation should be pursued independently of the normal analysis as to what went wrong.)

There are two reasons for focusing on the system, rather than the individual. The first is simple justice and fairness. If the persons involved in an event were provided with equipment and systems that were not effective, then it is not their fault when something goes awry. Second, it is very difficult to change a person—not least because the behavior of an individual will vary from day to day. Moreover, different individuals will be assigned to cover the same task, and those individuals will differ from one another. Equipment and systems can, however, be adapted to address the investigation's findings because they are not subject to the whims and vagaries of mere mortals.

For example, if an operator opens a wrong valve, the investigation should consider human factor issues (such as the potential for confusion between two valves that look alike), whether the operator had had sufficient training, or whether he or she was required to carry out too many tasks in a short period of time. The investigation in this case focuses on systemic issues, not on the operator himself.

There are, however, five situations where it is legitimate to blame individuals and to discipline them. These situations are:

1. Sabotage and other malicious acts
2. Deliberately not following a well-communicated procedure

3. Dereliction of duty (e.g., a shift worker leaving the facility during his tour)
4. Working while under the influence of drugs or alcohol
5. Lying to investigators.

Other situations may also require some disciplinary action. If an operator fails to follow procedures, he or she may justify a reprimand. (Although he or she should always be allowed to tell their side of the story, he may say that the procedures were confusing or difficult to follow. In such cases, management should probably give the operator the benefit of the doubt.)

In the follow-up to many events, it is found that the persons involved were not properly qualified or lacked sufficient field experience. In such cases, the assignment of blame can be tricky. For example, on one facility the flow of gas through a fired heater was stopped due to an instrument failure. The lead operator took corrective actions based on his observation of faulty readings from the DCS (distributed control system) panel in the control room. In fact, he had misjudged what was taking place. Consequently, some heater tubes were burned through. Given that the heater was very close to the control room, management not unreasonably asked if the operator could simply have stood up, walked over the heater, and physically checked it out. In cases such as these, it is probably fair to say that management has some responsibility (for failing to install a low flow interlock on the heater) and that the operator has some responsibility for not conducting a field check.

MANAGEMENT TRUST

Trust must also be developed between the managers of the facility where the incident occurred and the investigation team. The reality is that the investigation is going to tell management that their baby is ugly—that their systems failed. Furthermore, individual managers will probably be shown to be at fault (say for not conducting an MOC review). It is possible that those managers will take umbrage and become defensive.

Yet trust between managers and the investigation team is crucial, not least because it is the managers who will have to handle the findings and recommendations by committing scare time, money, and people to the follow-up effort.

EARLY REPORTING OF BAD NEWS

No one likes to be the bearer of bad news. Nevertheless, it is the responsibility of the incident investigation team to inform management as quickly as possible about their insights regarding the incident, particularly if the news is bad or if it is possible that the incident could repeat. The team should then continue to issue interim follow-up reports.

MANAGEMENT PRESSURE

An underlying cause of some accidents is management pressure to maximize production or to get a facility started up as soon as possible. This pressure leads to the possibility of safety or environmental performance being compromised. As one worker put it, “Production trumps safety.”

Although it is easy to criticize such management pressure, it is more realistic to recognize that there has to be a balance between production and safety. After all, the safest plant is one that is not running at all. Just making the decision to operate is increasing risk. Managers do not want to operate unsafely; what they do is to balance economic and safety pressures. For example, whenever a manager is asked to give permission for a safety system to be bypassed so that maintenance can work on it while the facility continues to operate the manager is facing this tradeoff. That is what he gets paid for.

SAFETY AS A CAUSE OF INCIDENTS

Sometimes one of the causes of an incident is that someone was trying to improve safety or environmental performance, and, in doing so, created a greater risk. For example, on one offshore platform, a maintenance technician was replacing stair treads (a routine task) in order to ensure that no one slipped when walking on the stairs. During the course of his work, the technician fell through a gap in the stairs and later died of his injuries. In another case, a technician was preparing to stop a very small leak that was creating a near-trivial environmental problem. As he was setting up the task, a drain valve fell out and he was seriously injured. Offshore, it was found that launching lifeboats during evacuation drills was hazardous. Indeed, in one such drill a man died. The decision was made not to actually launch the lifeboats.

Events such as these point out the need to evaluate the safety consequences of all activities—even those that are intended to increase safety.

COMMUNICATIONS

An effective incident investigation and analysis program generally contains two major components: technical and human. The technical side of the investigation is what most publications in this area focus on, particularly with regard to root cause analysis. However, what does not always receive the same degree of attention is the human aspect of incident investigation work. An effective investigator understands how people think and behave. Consequently, he or she must be able to communicate with a wide range of people, particularly those listed below.

TECHNICIANS

Most incidents involve front-line technicians (operators and maintenance workers), some of whom may have been injured or emotionally shaken. These people will often be feeling defensive and upset. They may also be feeling guilty if any of their colleagues were injured or died.

Technicians often may not understand what caused the incident, but they worry that they will be blamed anyway. An effective investigator encourages these front-line technicians to be open and candid—primarily by simply shutting up and letting then them talk. Unfortunately, many investigators—who often possess years of experience—are much too quick to interrupt the technician's narrative flow with questions, war stories, or snap judgments at to what happened. An investigator should also make it clear to the technicians that the goal of the investigation is to find out what happened—not to apportion blame or to demonstrate how smart the investigator is.

MID-LEVEL MANAGERS

Most investigations find that changes are needed at the facility's mid-level management systems. Examples of such changes include an increased emphasis on equipment inspection, upgraded operating procedures, and beefed-up training for the technicians. The implementation of such changes requires that the facility managers commit scarce resources that they would prefer to spend on achieving other goals. An effective investigator will empathize with these mid-level managers and will understand the demands that are being placed on the organization by the investigation and its follow-up.

SENIOR MANAGERS

Many investigators find that technicians are candid and open, and mid-level managers are generally willing to honestly address the need for improvements to the facility's systems. What these investigators sometimes find, however, is that senior managers are resistant to the findings and implications of an investigation. These findings may indicate that systemic changes to the company's management systems are required; the senior managers in charge of such systems can become quite defensive—they don't like being told that their baby is ugly. Hence an effective investigator will know how to communicate with these senior managers, and how to get their buy-in—not least because they are the ones who provide the funding needed to implement the investigation's recommendations.

An additional concern regarding the involvement of senior managers is that they are usually strong personalities; they may try to take over the investigation and direct it to meet their own opinions, goals, and agendas. A strong investigator is able to resist these blandishments.

DEFINITIONS

Words and phrases such as "incident," "accident," and "near miss" tend to be used quite loosely in general conversation. They also tend to have different connotations in English, American, and Canadian usage. However, in the context of formal incident investigation and analysis such words need to be tightly defined. The definitions used for these terms in this chapter are provided below.

INCIDENT

> An incident is an event that has either caused harm or loss, or that has the potential to cause harm or loss, and that could have been prevented or reduced in severity through use of the company's management systems or by improvements to those systems.

The key to the above definition of the term "incident" requires that it be preventable through use of the facility's normal management systems—thus excluding bizarre external events such as an airplane crashing into the facility. However, many external events, such as earthquakes or severe weather, can be anticipated and should therefore be considered in the design and operation of the facility and in the development of the emergency response program.

Some incidents are outside the control of local management, and so require attention at a higher level. For example, most large corporations have a procurement policy that is used throughout the whole company. If an incident investigation at one site shows that problems with procurement were a contributing factor then the corrective action will probably have to be addressed at the corporate level.

The definition of the word "incident" covers not just safety and environmental harm but also economic loss. Most of the literature to do with incident investigation and analysis focuses on safety-related events. But there is no reason why the techniques developed to investigate and understand such events could not also be used to address lost production, reduced efficiency, and unexpected equipment failure.

ACCIDENT

The word "accident" should not be used during the incident investigation process because the word implies surprise and lack of controllability. There is nothing anyone can do about accidents. The whole point of an incident investigation and analysis program is that all aspects of an operation *are* under control of management. Only unpredictable external events such as an airplane crash alluded to above are true accidents.

NEAR MISS/HIT

The term "near miss"—which may better be called "near hit"—describes an incident that did not result in an actual loss but that had the potential to do so. For example, if an object is dropped from a crane but no one is hurt then the incident is a near miss. In terms of fault tree analysis, a near miss is an event in which one or more of the inputs to an AND gate was negative.

The following are examples of near misses:

- Process conditions go outside safe operating limits, but there are no direct consequences
- An emergency shutdown system is unnecessarily activated
- A safeguard such as a relief valve or fire suppression system is called upon to operate
- A hazardous chemical is released—but does not affect workers in the area.

Near misses, particularly those that could have had high consequences, should be investigated thoroughly because they are strong indicator of system failures. They are a free lesson learned.

POTENTIAL INCIDENT

A potential incident creates the possibility of an event, but nothing actually happens. The key difference between a near miss and a potential incident is that, with a near miss, an event did take place but the consequences were minor. With a potential incident, nothing happened at all. For example, if a worker drops a wrench from an upper deck and it hits the floor three stories below but no one is hurt then a near miss has taken place. If the same worker holds the same wrench such that, were he to drop it, it would fall, then he has created a potential incident.

Potential incidents can be classified as either unsafe acts or unsafe conditions. The worker who holds the wrench such that it may fall has committed an unsafe act. If he fails to secure the area immediately below him with barricade tape, then an unsafe condition has been created. A lot of behavioral safety work is to do with the identification of potential incidents.

Failures to employ authorized management systems properly can also be considered as being potential incidents. For example, if a maintenance manager authorizes a change to a piece of equipment without following his facility's MOC procedure, then the decision has created a potential incident.

HIGH POTENTIAL INCIDENT

A high potential incident (HPI) is a potential incident which would have led to major loss. For example, if a toxic gas leaks from a flange into the atmosphere but no one is present, then an HPI has occurred. No one was present, but the potential for a fatality existed.

In general, if a system has had to use its last safeguard, then the incident is probably high potential. For example, if the pressure in a vessel rises above the safe limit (see below) but the safety instrumentation systems bring the pressure back under control, then a potential incident has occurred. However, if the instrumentation does not work, and the high pressure has to be taken care of by the vessel's pressure safety relief valve, then the last line of defense has been used and the incident can be considered to be high potential.

INCIDENT INVESTIGATION STEPS

The process of investigating and analyzing incidents can be divided into the six steps shown in Figure 11.2.

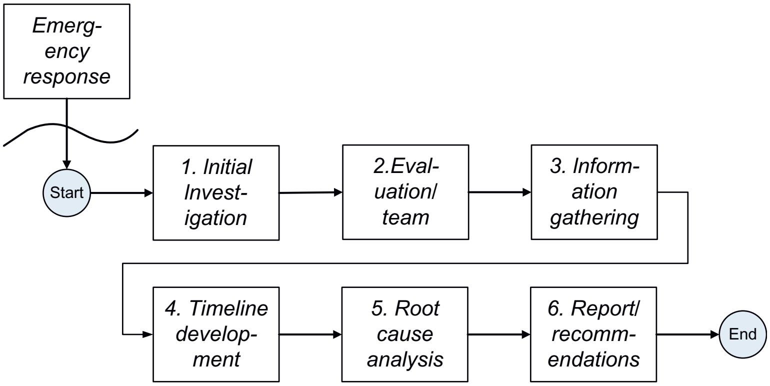


FIGURE 11.2

Incident investigation/analysis steps.

STEP 1—INITIAL INVESTIGATION

The initial investigation, which can start as soon as in the emergency response is completed, is carried out by what is sometimes referred to as the “Go Team.” Speed is of the essence at this stage of the investigation. The Go Team provides management with quick feedback as to what happened and what immediate corrective actions may need to be taken at other sites or facilities that share the same technology. The team collects information as soon possible, particularly information that may change quickly such as that do with process conditions. The team should not to disturb evidence, except as needed to ensure the continued safety of the facility. One of the team’s most important tasks is to interview participants and witnesses as soon as possible. People’s memories quickly fade, and they start to adjust their memories based on what they think should have happened or on what other people tell them. It is vital that these people be asked to tell their story as soon as possible.

During the initial investigation, the team will start to develop the document and information management systems that will be needed for the remainder of the project.

STEP 2—EVALUATION AND TEAM FORMATION

Following the initial investigation, management will evaluate the seriousness of the incident and assess the potential it provides for lessons learned. Management must also decide as to how detailed the investigation should be. This means that a method for evaluating the seriousness of events—particularly near misses and potential incidents—has to be selected.

Based on their incident evaluation, management will put together the formal incident investigation team (which will usually have a similar composition to that of the Go Team) as illustrated in Figure 11.3.

At the top of Figure 11.3 are the sponsor and the incident owner. The sponsor is an executive, usually with line authority over the persons involved in the incident. He or she will authorize the terms of reference for the investigation and fund the work. The incident owner will typically be the line manager over the facility where the incident occurs. The owner may not spend a lot of time working with the team, but he or she provides direction, ensures that the terms of reference are being followed and is the recipient of the final report. Figure 11.3 shows that the owner has delegated the task of managing the information to do with the incident to the PSM coordinator, who uses the incident register to document the progress of the investigation and to manage the subsequent follow-up.

A major incident investigation can have as many as three investigative teams, each corresponding to the stages of the investigation and analysis. The composition of the teams will depend on a variety of issues such as the seriousness of the event, the likelihood of litigation, and the technical aspects of the incident. It is likely that the three teams will have many members in common, but it is useful to make the distinctions shown in Figure 11.3 so that the team members have a clear idea as to their role at each stage in the process. (For example, the analysis team may have a member whose only role is to help the team understand the incident investigation methodology that has been selected and to run the applicable software.)

As an incident investigation proceeds, the teams will be required to brief management as to its findings on a regular basis. The frequency and level of detail of the briefings will naturally depend on the severity of the event. Figure 11.3 outlines a representative reporting procedure. The Go

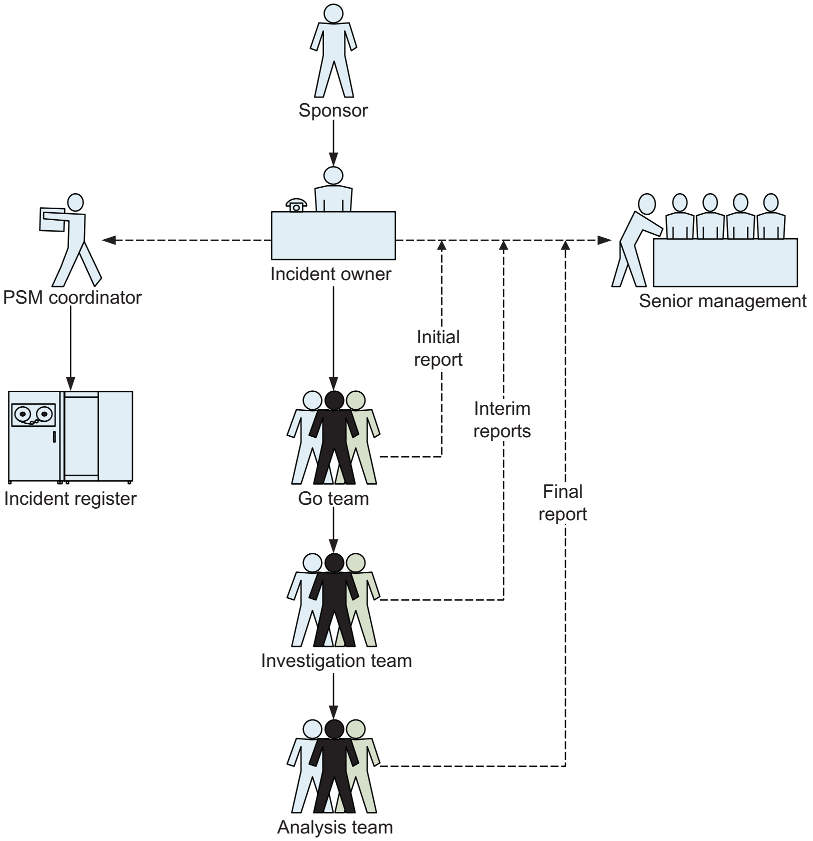


FIGURE 11.3

Incident investigation team structure.

Team issues its first report which summarizes the major issues to do with the incident. The formal investigation team issues one or more interim reports as it progresses with its work. Lastly, the analysis team delivers the final report, containing both the root cause analysis, the findings, and suggested action items.

STEP 3—INFORMATION GATHERING

After the team has been assembled and the terms of reference generated, the first step in the formal investigation process itself is to collect information about what happened. The information will generally come from interviews, documents, instrument records, and field observations. At this stage of the investigation, it is especially important not to jump to conclusions but to let the facts speak for themselves. The focus must be on gathering data—mostly from interviews, site inspections, and the examination of instrument records.

STEP 4—TIMELINE DEVELOPMENT

Once the information gathering step is more or less complete, the investigation team can develop a timeline that outlines the sequence of events. As the timeline is developed, it will become clear that certain information items are either missing or not detailed enough, so the team will go back to Step 3.

STEP 5—ROOT CAUSE ANALYSIS

Individual incidents are usually indicative of a broader range of management or system problems. Simply correcting the actions and events that led to the particular incident that is being investigated represents an opportunity missed—what is needed is a process for identifying underlying or root causes so that a broader range of future incidents can be avoided. Root cause analysis can start at this stage in the investigation.

STEP 6—REPORT AND RECOMMENDATIONS

The final step in an investigation is to issue a report to all affected parties and then to take the appropriate corrective actions to prevent recurrence of similar events. Typically the report will summarize the event itself, the root causes that were identified, and recommendations as to how the findings may be addressed. Follow-up of the recommendations is the responsibility of the facility management, particularly the sponsor—not the investigation team.

STEP 1. INITIAL INVESTIGATION

The first of the six steps shown in Figure 11.2—Initial Investigation—is highlighted in Figure 11.4.

THE “GO TEAM”

Once the emergency responders have completed their work, the incident investigation team can move in. As noted in the previous chapter, some facilities create what is called a “Go Team” to conduct these first investigations. This team is put together very quickly after the occurrence of the

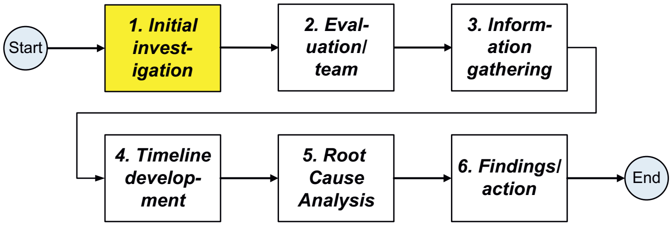

Start
1. Initial invest- igation
2. Eval- uation/ team
3. Inform- ation gathering
4. Timeline develop- ment
5. Root Cause Analysis
6. Findings/ action
End

FIGURE 11.4

Step 1—Initial investigation.

event in order to ensure that the investigation is conducted properly from the moment that the emergency responders have left the site. One of the team's most important responsibilities is to ensure that perishable or sensitive data is properly secured and retained. The team members should carry out their work as quickly as possible before evidence and memories are lost or changed. Paper documents should be photocopied and electronic records should be saved to a backup device. The team may also be charged with making the first communications to regulatory agencies.

Immediate actions

The following actions should be carried out immediately by the Go Team.

- Barricade the affected area in order to minimize the chance of additional injuries and to prevent the chance of evidence contamination or removal. Sometimes, physical data are destroyed simply because people walk through the area or while they are cleaning up the site. These cleanup activities should be stopped unless the current situation poses a significant safety or environmental hazard
- Secure related areas such as the control room, so that only authorized persons are allowed to enter
- Establish the chain of custody process
- Tag each valve, instrument, or equipment item once it has been examined
- Record the position of each valve
- If the event involved an explosion, find and tag all pieces of shrapnel and record their location
- Collect samples of process fluids from affected items of equipment
- Leave all switches, knobs, push buttons, and controllers in their current position (assuming that is safe to do so)
- Record the instrument settings (proportional, integral, and derivative)
- Check the status of panel (hard-wired) alarms
- Collect all alarm printouts
- Take pictures or videos of all relevant valves, instrument panels, alarm/annunciator panels, vehicles, and damaged equipment or piping. Pictures can be supplemented with hand-drawn sketches. Date stamp all pictures, videos, and sketches
- Develop a witness location plot showing the location of the witnesses at the time of the event
- Obtain and store securely documents such as log books, lab reports, and daily instructions
- Check log books and similar documents to make sure that their contents were not changed following the incident
- Obtain copies of standing orders and procedures in use or applicable to the situation when the incident occurred
- Record information from the facility's computerized maintenance management system (CMMS)
- Collect copies of relevant job safety analyses (JSAs), hazards analyses, and other safety evaluations.

Team preparation

Many incidents take place in harsh or remote locations. Potential team members should be sure that they are prepared for such conditions and that they have any specially needed training to do with topics such as cold weather driving or offshore survival.

Equipment that the team may need at the site includes:

- Barrier tape
- Water resistant storage boxes of various sizes
- Evidence bags
- Tags with strong wire ties
- Camera and accessories
- A portable document scanner
- Office supplies such as paper, pens, highlighters, and sticky notes
- "Attorney Work Product Privileged & Confidential, Do Not Disclose, Mark On, or Copy" stamp and stamp pad
- Clipboards
- Permanent Markers
- White Board Markers
- Labeling Tape
- A flashlight
- A magnifying glass
- Two-way radios
- An inspection mirror with flexible/retractable arm
- A compass
- Duct tape
- A computer to store records and pictures
- A sound level meter
- A light meter
- A thermometer.

DRUG AND ALCOHOL TESTING

If it appears that the event may have involved someone working under the influence of drugs or alcohol, then that person should be tested immediately by an independent laboratory. Given the sensitivity of this topic it is important that the company has a clear policy in place ahead of time, and that the policy is applied equitably to all employees and contract workers.

INCIDENT REPORT FORM

The incident will have to be reported using the facility's incident report form such as that shown in Table 11.1. (The space for written information provided in Table 12.1 has been compressed here in order to fit into a book format.) Generally, the information on this form will go directly into an incident tracking database or incident register.

The sections of Table 11.1 are discussed below.

Incident number

The incident number is a unique identifier that will be used for all investigation and analysis work to do with this incident. Generally, the number will be assigned by the incident investigation software and will never be changed or reused.

Table 11.1 First Report Template

First Report of Incident			
Incident Number		Title	
Location, Date, and Time of Event		Duration of Event	
Date and Time of Report		How Observed	
Person(s) Reporting		Preliminary Risk Ranking	
Incident Type	Fire	Unsafe condition	
	Explosion	Noncompliance	
	Gas release	Public complaint	
	Personal injury	Other	
	Near miss		
Incident Flags	Regulatory report	Other facility impact	
	Local government report		
First Description of Event			
Immediate Corrective Actions Taken			
Witnesses			
Contractor Involvement			
Detailed Location			
Consequences			
Emergency Response			
Security Issues			
System Alert			
Incident Owner/Department			
Notes			
Attachments			

Title

The title of the event should be explicit enough to provide a description as to the nature of the event and to avoid confusion with other reported incidents. At the same time, the title should not be too lengthy or wordy.

Location, date, and time of event

This box is self-explanatory.

Duration of event

Most events happen instantaneously, but some occur over a longer period of time. For example, one company found that they had an environmental violation that had been going on for many years.

Date and time of report

This box is self-explanatory (it is always important to distinguish between the date of the incident and the date of the report).

How observed

Generally, an incident makes itself known in the form of a leak or fire or emergency alarm. However, some incidents are passive, i.e., they are unsafe conditions that are corrected before anything goes wrong. On one facility, for example, it was noted that the relief valves in a critical area had been blocked in. One of the key questions for the investigators was how this very serious event had been identified and corrected, and for how long the relief valves had been blocked in without anyone noticing.

Person(s) reporting

The name(s) of the person writing the first description of the event should be recorded, along with his or her contact information.

Preliminary ranking

The evaluation and risk ranking of events is discussed in the next chapter. The first report can provide a first estimate as to the seriousness (or potential seriousness) of the incident.

Incident type

The initial report should indicate the primary type of the incident: safety, environmental, or economic (most serious events will include at least two of these categories).

Incident flags

Once an incident occurs, it is likely that various regulatory agencies will have to be notified promptly. Large chemical plants and refineries often have someone dedicated to this task full time, 24 hours per day. It is also important to inform the local community and media as to what happened as soon as possible. Therefore, a set of flags or check boxes that identify the organizations to be contacted is needed.

First description of event

The first description of the event is important because it captures information from witnesses before they have had an opportunity to analyze or edit (either consciously or unconsciously) what they observed.

Many first event descriptions are badly written, with many grammatical errors and spelling mistakes. Such errors do not matter at this stage of the investigation; what is important is to capture the immediate knowledge as to what happened.

Immediate corrective actions taken

In order to secure the facility and to ensure that the incident is not allowed to get worse, the persons present at the scene (and the emergency responders) have had to take immediate corrective actions such as draining tanks, shutting down equipment, and removing equipment that is restricting access. All such actions should be recorded in the first report because they may affect the subsequent analysis.

Witnesses

The names of any witnesses, along with their contact information, should be recorded as soon as possible.

Contractor involvement

Many events involve contractors and subcontractors. The companies involved, and their reporting structures, should be identified. The investigators will need information to do with the contract companies and contract workers in areas such as:

- Qualification records
- The contract and purchase order
- Specs and bid package
- Copies of all correspondence, warnings, letters, and minutes
- Medical reports
- Site orientation procedure
- Attendance records
- Insurance certificate
- Safety audits and meetings
- Permits
- Training records.

Detailed location

It is often important to describe the location of the event in as much detail as possible. For example, if a flange adjacent to a block valve leaks, it is necessary to state whether it was the upstream or downstream flange that leaked.

Consequences

The initial report will not include a formal or detailed consequence analysis. However, those writing the report should include as much information as they can about the consequences of the event, including details to do with personnel injuries, environmental releases, and economic loss.

Emergency response

If the incident required an emergency response (even if the response was limited to mobilization of the fire brigade), details as to how that response affected the consequences of the incident should be included.

Security issues

If the incident points to any immediate security issues, such as unauthorized entry into the facility, immediate corrective action should be taken. Also, the appropriate law enforcement agencies should be contacted.

System alert

Sometimes, the investigation team will identify a problem that could cause a similar event to occur at one or more of the company's other locations. In such circumstances, a safety alert should be issued to those locations and possibly to similar facilities owned by other companies. Some companies have a special newsletter system that can be used to issue bulletins to all departments and persons who may need to know about the event quickly.

Even better than issuing bulletins is for members of the investigation team to visit other sites and to make sure that the deficient conditions have been corrected and to explain to the personnel at those sites what the first conclusions are.

Incident owner/department

This section of the report will state which department is responsible for the equipment involved in the event. The manager of that department will probably be the incident owner.

Notes and attachments

Space in the report form should be provided for discursive notes that will amplify the checked sections. Attachments to the initial report can include the following:

- Sketches
- Photographs
- Engineering documents
- Medical reports
- Vehicle information
- Regulatory compliance reports (including the date and time of notification).

FIRST MANAGEMENT REPORT

In addition to completing the template shown in Table 11.1, it is important to send management an overview of what happened as soon as possible. They do not need to know all the details, but they do need a summary as to what happened. Naturally, not all levels of management need to know about every minor event. Table 11.2 provides the basis of a checklist that can be used to decide what gets reported to what level of management.

Table 11.2 Representative Reporting Levels

Level	Examples	Line Management	Senior Management	Corporate Management
1 Minor	Trace odor detected Employee falls but is not injured	Yes	No	No
2 Moderate	Check valve fails to close ESD activated Pressure safety valve (PSV) lifts Unignited fuel spill Management of change process not followed	Yes	No	No
3 Serious	Employee injured Emergency shutdown device (ESD) fails to respond PSV does not work on demand Fire suppression system fails Unignited gas release Relief valve blocked in without authorization Recordable environmental release	Yes	Yes	No
4 Very Serious	Major environmental release Serious injury or fatality	Yes	Yes	Yes

STEP 2. EVALUATION AND TEAM FORMATION

The second of the six steps in the investigation is to create the investigation and analysis team, as shown in Figure 11.5.

EVALUATION

Major incidents that involve injuries, large releases of chemicals, or serious production loss will always be thoroughly investigated. However, the great majority of incidents are either relatively minor or they are near misses. Yet investigation of these minor incidents can reveal as many insights as can that of major events. For example, on one facility a weld failed leading to a release of flammable gas. No one was hurt, but follow-up showed that many other welds in the same area were likely to fail for the same reason. It turned out that the wrong welding materials were being used due to a “cut and paste” error in the procurement process. Consequently, this minor event led to a major evaluation of the whole procurement procedure.

Otto von Bismarck once defined politics as being “the art of the possible.” His comment can be applied to virtually all human endeavors, including the follow-up to incidents on process facilities. Ideally, every incident would be investigated in depth, but the reality is that even the largest

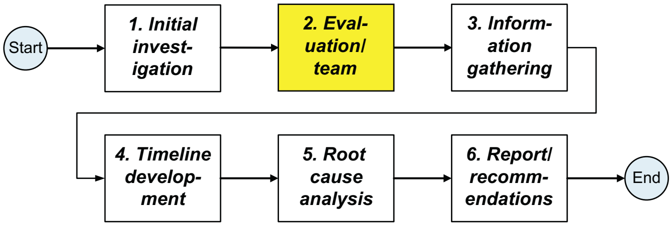

Start
1. Initial invest-igation
2. Eval-uation/ team
3. Inform-ation gathering
4. Timeline develop-ment
5. Root cause analysis
6. Report/ recomm-endations
End

FIGURE 11.5

Step 2—Team creation.

organizations have limited funds and personnel resources. Therefore, given the large number of minor and near miss events that occur on even the best run facilities, some type of assessment or screening process is required to determine which of them should be examined in detail.

TEAM FORMATION

Once the incident has been evaluated, and a level of effort that is needed for the investigation and analysis has been determined, the next step is to form the investigation and analysis teams and to provide them with their terms of reference.

The size and composition of the team will usually depend on the seriousness of the incident and the potential for lessons learned. As shown in Figure 11.3, the composition of the team will also change as the investigation and analysis process progresses. Large complex investigations may involve the use of three distinct teams: the initial "Go Team," the formal investigation team, and the analysis team. Needless to say, no member of the team should have been involved in the event itself, nor should the team include managers or supervisors who have line responsibility over the area affected.

The facility must put its best people on the investigation team. This work is not for neophytes. Management must ensure that the team members have sufficient time in which to carry out their work.

OUTSIDE INVESTIGATORS

An early decision that management must make is whether or not to bring in outside investigators or whether to handle the investigation and analysis using only internal resources. The use of outsiders on the team brings the following advantages:

- Outside team members will have high credibility because they will be perceived as being independent of internal management (credibility is basically a *perception* issue—in point of fact, an internal team member may be just as objective as a person from outside).
- An outside team can include experts on incident investigation and analysis. It is unlikely that persons working for the facility will possess such a level of expertise.
- Outsiders will probably be better at keeping information confidential and at working with attorneys. Indeed, if litigation is anticipated, then an outside team should always be used.

- Outsiders are likely to be assigned to work on the investigation full time, whereas internal investigators will be under constant pressure to get on with their "real work."
- Because they are not involved in internal management, outsiders are more willing to offer findings and recommendations that tread on toes.

In spite of the benefits of using outsiders, minor events that are perceived to offer little in the way of insights will usually be handled by an internal team, if only to keep costs down.

CORPORATE SUPPORT

The role of corporate support for the investigation must be considered. If the event is serious, corporate is going to be involved anyway. They will often provide the necessary infrastructure such as the incident register software.

TEAM MEMBERS

A list of team members is provided in Figure 11.3. In practice, one person may cover two or more of the roles, but that person must differentiate between them.

Sponsor

A senior executive will serve as sponsor of the overall investigation. He or she will usually have line authority over the incident owner.

Incident owner

The incident owner will usually be the line manager or supervisor responsible for the area in which the event occurred. The level of management of this person will depend on the severity of the incident.

He or she should not be involved in the investigation itself, but he or she must be made aware of general progress and must receive all pertinent reports and information as soon as possible. In some regards, the incident owner is more like a customer than an active team member.

Possibly the most important contribution that the incident owner can make to the investigation and analysis process is to create an atmosphere of seeking means of long-term improvement, rather than looking to blame someone or trying to find a quick fix.

Facility manager

The incident owner usually reports to the facility manager (who may be referred to as the plant manager or as the offshore installation manager depending on the location of the event and the industry that is affected). He or she will ensure that the site is safe before the investigation team enters the property or facility.

The facility manager will usually require that he or she be kept up to date regarding any significant findings to do with the incident, particularly as he is likely to have to fund the report's recommendations, and will be expected to report any major findings and conclusions to senior management.

As with the incident owner, the facility manager should not be an active team member because the investigation may show that he or she has responsibility for some of the events covered.

Lead investigator

Each investigation will have a leader who should be trained in the investigation process. He or she will work with the sponsor and the owner to develop the investigation's terms of reference and then to conduct the investigation.

The lead investigator will usually serve as the project manager for the investigation process—so he or she will also need the skills to manage the schedule, budget, and final report. The leader must also exert control over the flow of information; many incidents are sensitive—it is important that people be informed on a "need to know" basis—at least until the final report is issued.

The lead investigator's detailed responsibilities include the following:

- Select the team members
- Lead the investigation activities
- Assign responsibilities and actions to the team members
- Ensure that team members are properly briefed and trained
- Coordinate the transfer of the investigation from the "Go To" team to the formal investigation team
- Provide liaison with outside organizations, including the company's corporate office, regulatory agencies, and the public
- Set up the necessary logistics, including a team office and a secure location for collected evidence
- Obtain a budget for the investigation and manage expenditures
- Determine the scope of work with senior management, including the expectations for interim and final reports
- Coordinate with legal representatives, if required
- Acquire outside resources, such as subject matter experts (SMEs), as required
- Manage the collection and secure storage of incident information
- Write the final report
- Present the report to senior management.

One of the lead's most important tasks will be to recognize when outside expertise should be called in. An oft-repeated proverb in business circles is that "people don't know what they don't know." A good team lead, on the other hand, "*does* know what he doesn't know." He or she will have little hesitation in calling on outside help as needed.

Administrator

All but the smallest investigations should be supported by an administrator. He or she will provide logistical support for the team, schedule interviews with facility personnel, and manage the secure retention of documentation and other records.

Area supervisor

The area supervisor is often a critical team member due to his knowledge of people and technology. However, if it appears that his actions or nonactions may have contributed toward the event, it is probably best if his role is limited to that of a witness and an information provider. One option may be to use a supervisor who was not on duty at the time of the event, but who knows the facility well.

HSE representative

The team may include someone who is very knowledgeable about health, safety, and environmental (HSE) issues—particularly the rules and regulations that affect the facility's operations.

PSM coordinator

Many events imply that the facility's PSM systems have failed. Therefore, the PSM coordinator will probably be involved, either as a team member or as an information provider.

Employee representative

It is important to have an employee representative, where possible. If the facility is unionized it is likely that the union will want to be represented on the team, particularly if it is possible that one of their members may be disciplined.

Process/facilities engineer

If the event is process related, the team will need a process or facilities engineer to interpret what was going on inside the process itself.

Maintenance technicians

Many events involve the failure of equipment. Therefore, the statements of the maintenance technicians, supplemented by the maintenance records, can be critical in determining what happened.

Subject matter experts

SMEs may be required to provide their knowledge and experience in areas such as:

- Corrosion and materials selection
- Equipment inspectors
- Environmental compliance
- Fire protection.

Contractors/vendors

Many incidents involve the use of equipment and/or specialized services from contractors and vendors. In such cases, it makes sense to have a representative from those companies on the team.

Emergency response specialists

The persons who handled the initial response are not likely to be part of the investigation team, but they can provide valuable information as to what they observed when they arrived on the scene. They can also tell the team what evidence may have been moved or changed during the immediate response phase of the event.

Attorneys

It is unlikely that an attorney will actually be on the team. However, he or she may be closely involved in the on-going investigation, particularly if attorney/client privilege has been invoked.

CHARTER/TERMS OF REFERENCE

All incident investigations should receive a charter or terms of reference from the incident sponsor. The charter should consider the following issues:

- Objective of the investigation
- Identification of the key team members, particularly the incident owner and the lead investigator
- Physical scope of the investigation
- The type of investigation methodology to be used
- Level of priority for the investigation, with a proposed timeline for delivery of the final report
- An initial estimate as to the level of effort, time required, and cost of the investigation and analysis
- Identification of the key deliverables expected from the investigation and analysis, including interim reports
- The depth of root cause analysis required, and the extent to which such analysis should consider other units and facilities in addition to the one on which the event occurred
- The development of findings and/or recommendations based on the root cause analyses.

TEAM MEMBER QUALIFICATIONS

This section describes some of the attributes of an effective investigation team member.

Objectivity

Oscar Wilde's comment "A truth ceases to be a truth as soon as two people perceive it" was presented in Chapter 1. His comment very much applies to the process of investigating incidents. Facts are never truly objective; each person has their own perception of what they perceive to be the same reality. For example, when asked what happened in the case of the example, one person may say "The pump seal failed," another may state "Hydrocarbon vapors were released to the atmosphere." Both persons are correct but their statements reflect their different views of reality. Therefore, it is very difficult to develop a truly general incident analysis whose conclusions are independent of the profiles of the persons conducting that analysis.

Nevertheless, the team members must always strive to be objective. Their honesty and integrity should never be questioned. Those investigating the incident must never consciously allow their personal biases or feelings to affect their work. This is why it is generally a good idea to recruit team members from outside the immediate organization. In particular, any potential team member who has an obvious bias—such as being directly involved in the incident being investigated—must recuse himself from the investigation.

Common sense

Wilde's insight regarding objectivity suggests that there is no such entity as "common sense"—no two people have a truly common view of the world so they cannot share a "common sense."

This is because everyone—there are no exceptions—is prejudiced, i.e., everyone prejudges an issue depending on education, place of origin, experiences at work, and political/religious beliefs. This means that there can never be one single, universally agreed-upon explanation as to the root cause of events.

One indication that a person may have too limited a view of reality is that they descend too often into a story telling mode. There is nothing inherently wrong with the use of stories because they can provide insights through argument by analogy. Indeed, as discussed in Chapter 18, stories are an excellent means of communication. But too many stories become merely "war stories" that are used by the speaker merely to show off his or her knowledge, not to advance the state of understanding of the incident.

Jumping to conclusions

A second form of objectivity related to the war stories issue concerns the need to avoid jumping to conclusions based on previous experiences. For example, a chemical plant experienced a serious noninjury incident. All of the instruments at that facility were provided by a single vendor. After the event one of the operators was heard to say that "Everyone knows that instruments from that vendor are no good." In point of fact, the instruments performed well—the operator's prejudice probably came from bad experiences with that vendor's products at other facilities.

In another situation, a facility changed a process such that pure oxygen was injected into a process stream that contained small amounts of hydrocarbon (the bulk of the process materials consisted of high-pressure steam, inorganic solids, and inorganic liquids). About a year later, the facility suffered a devastating explosion. It was immediately "obvious" that the oxygen had somehow collected in sufficient quantity to generate the explosion. After all, virtually all explosions involve the ignition of a mixture of hydrocarbons and oxygen.

But the "obvious" result was wrong. It turned out that the explosion was caused by high-pressure steam entering vessels rated for low pressure. The event had nothing to do with the oxygen at all.

Haughtiness and empathy

One personal challenge facing many investigators is the need to maintain a balanced approach. It is self-evident that if a facility has experienced a serious event, then the management systems failed, and probably various individuals failed to do what they should have done. In such situations, it becomes very easy for an investigator to feel that he or she is somehow superior to the organization and the people who work there. This feeling of sanctimonious superiority is often exacerbated by the fact that the investigators are highly experienced and may therefore be quick to adopt an "I would never have done that" attitude. One "cure" for this problem is for the investigators to think about their own organizations or companies and to consider how bad they would look were they to be investigated by an outside organization.

One example of haughtiness concerns the tendency toward "everyone's an expert"—or at least they think they are. It is all too common for people who are not part of the investigation team, and who have not troubled themselves to learn all the facts to do with an event, to jump in with an instant analysis in order to show how expert they are. In fact, such persons all too often merely make themselves look foolish. Being an instant (yet ignorant) expert is perfectly acceptable when criticizing the manager of the local sports team, but must be avoided in incident investigation.

Most important—particularly with injury or fatality events—the investigator must never lose sight of the fact that these incidents involve real people, with real families and real friends. Incident investigation and analysis is not an intellectual exercise in which different investigators try to score points of one another or in which they show off their expertise. Incidents are about real people suffering from pain, grief, guilt, disability, and anxiety.

Understand incident investigation methodology

There is no single agreed-upon approach to conducting incident investigations. Nevertheless, there are a number of widely used methods and software tools. Generally, the team will agree to use one of these tools; everyone should be familiar with the technology being used and at least one team member should be an expert in the use of that technology.

You do know what you don't know

As discussed above, incident investigators cannot possibly understand all the details and intricacies of the systems that they are investigating. This means that they must be very aware of their personal limitations, and be very willing to reach outside for expert help as soon as it is needed.

Understand process systems

Each team member should have a good, general understanding of process technology and terminology. That is not to say that he or she should be an expert in the process being investigated—such a requirement is neither feasible nor desirable. However, the investigator should understand the basic principles of process operations such as how pumps work, what relief valves do, and how modern instrumentation systems operate. The investigator should also understand basic chemical processing vocabulary, including words such as blowdown, distillation, and exothermic reaction.

Anyone investigating an incident in the process industries should have a good grasp of the elements of PSM, and how they interact with one another.

Logical thinking/painstaking

An effective team member thinks logically. He takes that events *as reported* and deduces what is most likely to have happened. He or she should not be swayed by what should have happened, what happened elsewhere, or what other people think happened.

A good investigator is painstaking and takes nothing for granted. He or she checks all facts and statements, and works particularly hard at identifying and resolving inconsistencies, ideally by having at least two different types of evidence that address one single issue.

STEP 3. INFORMATION GATHERING

Once the team has been assembled, chartered, and given its terms of reference, the first step in the investigation proper is to collect pertinent information and data (Figure 11.6).

Information will generally come from one or more of the following six sources:

- Initial written statements
- Interviews
- Documentation
- Field information

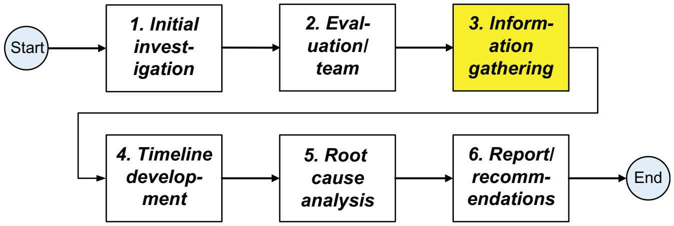


FIGURE 11.6

Step 3—Information gathering.

- Instrument records
- Testing/lab analysis.

Ideally, each information item should be cross-checked by more than one information source. For example, if an operator states that a certain control valve was open prior to the occurrence of the incident, his statement can be checked by reviewing the DCS record. Similarly, if an instrument shows that the process was running at very high temperatures, a lab analysis of the process fluids may confirm that conditions were indeed abnormal.

Not all information is direct and verifiable; some of it has to be inferred. For example, if liquid flowed from one vessel to another, it can be inferred that the valve in the line connecting those two vessels was open at some point in time. It is important, however, to use caution with inferred information. All experienced investigators will have run across situations where everyone knows that a certain fact "must be true," otherwise, there is no explanation for the event. Yet later investigation shows that the inference was not true after all, and that a different explanation was needed. Other attempts to develop inferred data—say through the use of analogy from previous events or general industry experience—should be recognized for what they are: attempts to create a cause−effect chain without really knowing what happened.

Unfortunately, there will never be enough information to be totally sure as to what happened. This is particularly true if one or more of the persons involved in the event were killed. Obviously, they cannot provide testimony this side of the grave. Other instances of missing information include:

- Equipment that is returned to a safe condition, so it cannot be known for sure what its status was prior to the event (this is often an issue when considering the performance of check valves)
- People lose memory to do with events very quickly (around 50% per day)
- People remember incorrect facts (or they pick up on what other people told them) and then they fixate on those incorrect facts.

Because peoples' memories are so short and unreliable, some investigators ask the key witnesses to the event to write down on a blank sheet of paper what they observed. This should be done as soon as possible following the incident.

INTERVIEWS

The first source of information comes from interviews with those involved in the event and with those who witnessed it. The purpose of an interview is to obtain information which can be used in preparation of the sequence of events and in determining the root causes. The quality of interviews is critical to the success of the incident investigation because only people can provide the narrative thread that links together the information from the other sources of information. Where possible, it is useful to have two interviewers. One can ask questions, the other can write down the answers, and provide a second perspective as to how the interview went.

The persons being interviewed generally fall into one of three categories:

- Those directly involved in the event
- Those who witnessed the event or its immediate aftermath
- Those who have relevant background knowledge such as workers on a previous shift, safety professionals, and management.

An interview is not an interrogation. Investigators should convey the sense of a cooperative, informal meeting. Only if illegal acts are suspected should the interview be treated as an interrogation—with control being passed on to law enforcement officials.

Evidence gathered through personal interviews is both insightful and fragile. People's ability to recollect facts accurately declines exponentially. A rule of thumb is that people typically forget 50−80% of the details of an event within 24 hours. They are also likely to have their mind swayed by other people as time progresses. Therefore, witnesses should be located and interviewed as soon as possible.

It is important to create a comfortable atmosphere in which interviewees are not rushed to recall their observations. Interviewees should be told that they are a part of the investigation effort and that their input will be used to prevent future events and not to assign blame. Before and after questioning, interviewees should be notified that follow-up interviews are a normal part of the investigation process and that further interviews do not mean that their initial statement is suspect. In addition, they should be encouraged to contact the Investigation Team whenever they can provide additional information or have any concerns.

Before the interview starts, it must be made clear to the interviewee that the purpose of the investigation is simply to establish the facts associated with incident under investigation. It is not the intent of the interview to establish root causes or to conduct any other type of analysis.

In general, the interviewer should use open rather than closed questions. An open question solicits a discursive reply, whereas a closed question generates yes/no answers. Closed questions are more likely to make the interviewee feel defensive because a "no" response may make him or her feel that they were at fault. On the other hand, an open question can open up unexpected and fruitful lines of thought. Therefore, it is much better to ask "What happened next?" rather than "Did you check the valve position?" Indeed, it is best to avoid use of the word "you" altogether. A question such as "Why did you do that?" is quite likely to arouse a defensive response.

The interviewer should also avoid leading questions. For example, it is better to ask a person what they could smell rather than ask them if they could smell H_2S.

INTERVIEW GUIDELINES

The following general guidelines should help ensure a successful interview.

- Interview witnesses as soon as possible and definitely before they talk to each other or to others not involved in the incident. Once witnesses talk to others, their memories as to what happened may be changed. For example, if an operator recalls that a certain block valve was closed, but his colleagues say that it was open, he may decide that he was wrong, and change his statement. He is being perfectly honest—but his second statement could be incorrect.

- At the start of the interview make it clear to the interviewee that the purpose of the meeting is to find facts, not fault, and that any information shared will be kept confidential wherever possible.
- Always try to establish a rapport with the interviewee. This is not an interrogation but a conversation to establish facts surrounding the incident. A relaxed person will have an easier time remembering what they experienced or observed and they will recall more information.
  - Smile and greet the person as they or you come into the room
  - As appropriate, spend some time at the beginning with simple tasks like getting the spelling of their name correct, asking for their title or position
  - Ask how long they have worked for their company or at the site
  - Ask how long they have been in their current position.
- Describe how the interview is to be structured.
- Treat the interviewee with respect and ask him or her general questions about himself or herself.
- Give equal treatment to all the persons being interviewed.
- Carefully record names, correct spellings, dates, times, and technical descriptions.
- Provide the interviewee with some personal details about the investigator in order to establish his or her credibility and trustworthiness.
- Interview a witness at the site of the event, where possible. Then he or she can walk through the sequence of events and point to any equipment that was involved in the event.
- Allow as much time as is needed. Do not rush the interviewee while he or she is describing the event or answering questions. If the person being interviewed is hesitant about his or her reply, a follow-up question such as “Tell me more about that” can help extract the necessary information.
- Ask for definitions of terms or abbreviations that may create confusion.
- Define potentially ambiguous words such as “tubing” and avoid acronyms.
- Use simple, nontechnical language.
- Ensure that information recorded is correct by feeding back what the person said. Statements such as “This is what I heard you say. Am I correct?” should be used.
- Ask “What did you do, see, hear, feel, smell, and taste?”
- Ask “Is there anything else that you think we should know to perform our investigation?”
- Ask if there is anyone else to talk to about what happened.
- Recognize that everyone—including the interviewer—has prejudices and biases. Do not direct the questioning toward so as to support a preconceived hypothesis.
- Do not make promises that may not be honored, particularly an offer to keep information confidential; such information may have to be revealed later in the investigation.
- Keep notes in a timeline format. Doing so provides a logical sequence of steps that provide a basis for the analysis step. Also, having a timeline will indicate any issues that may been overlooked in the previous questions.
- Do not interview people in groups (unless time is pressing or the people involved will not be available again). Inevitably one or two members of the group will dominate the interview

process, thus preventing less forceful group members from contributing what could be vital information. Moreover, the leaders of the group could cause other people to change their memories of what happened.

- Find out if the evidence on the site was affected during the response to the incident. Emergency response personnel should be asked if they moved any equipment.
- If resources permit, use two interviewers. Doing so makes it less likely that a key question will be overlooked. Also, one of the interviewers will be able to concentrate on taking notes during the interview while the other can concentrate on the interview process itself.
- Challenge leading answers. The statement "The temperature gauge read zero" is an observation. But saying "The temperature gauge failed" is an expression of opinion.
- Questions to do with feelings should be avoided. Answers to questions such as "How did you feel when the fire started?" are necessarily subjective and can never be confirmed with external evidence.
- Ignore attempts to blame others or to make a confession.
- Recognize that information is always "filtered" by a person's experience and can be influenced by emotions such as fear and embarrassment. Details of unpleasant experiences are frequently blanked from a person's memory.
- Recognize that people don't always remember things in chronological order.
- Note whether an interviewee displays any apparent mental or physical distress or unusual behavior; it may have a bearing on the interview results.
- Encourage the interviewee to make sketches.
- Be cautious about overly enthusiastic interviewees. By wanting to be highly cooperative, such persons may fail to recognize that they are not limiting their discourse to a mere statement of the facts, but that they are coloring their observations and describing what they thought they saw rather than what they actually saw.
- If the incident is serious and could lead to litigation, it may be necessary to ask interviewees sign their statements.

REGULATORY/LEGAL INTERVIEWS

It is critical that employees know how to conduct themselves during a regulatory or legal investigation. The following guidelines should be considered:

- Do not tell employees what to say or not to say before the investigation starts
- Keep detailed notes as to what the regulator is doing and saying, and keep a log of which documents he or she has examined
- Instruct employees not to give documents to the investigator—if asked for such documents, the employee should refer the request to his or her superior
- Refresh the employees' memories regarding the training and certifications that they have received
- Ensure that employees know of their rights to representation (from the union where applicable)
- Tell employees not to argue with the investigator, particularly when the investigator is wrong (A polite disagreement may be acceptable, as long as it is not presented in an emotional manner.)

- Ensure that employees are aware that all documents should be put away—if an inspector sees a document lying on a desk, say, then he or she can include it in the inspection record. However, if the document is not open to view, the inspector has to formally request that he or she be provided with it.

It is especially important that employees know not to blurt out damaging information without being asked for it. For example, during one investigation, the representative from the agency noted that a handrail was missing, and that an employee could fall from a platform to grade. (The missing handrail had nothing to do with the incident being investigated.) In response to the investigator's comment, the area supervisor said words to the effect. "Oh yes! We knew about that missing railing, but we just hadn't gotten around to fixing it." Such a statement could lead to a willful citation from the inspector because the company deliberately chose to let an unsafe condition exist.

WITNESS INTERVIEWS

Interviews with witnesses should generally be divided into three parts. First, the interviewee tells the interviewer what happened in his own words—without interruptions. The interviewer starts with an open-ended question such as "Please tell me what happened." He or she will use verbal and nonverbal reinforcement to encourage the interviewee to continue talking. The interviewer should not ask questions at this point; apparent inconsistencies can be sorted out later.

Then the viewer asks questions to verify and clarify what was said. Where possible, statements should be verified with reference information such as "Was the visibility better or worse than it is now?" The following is a list of potential clarification questions:

- What were the process operating conditions?
- Were there any unusual operations that took place before the incident?
- What were the weather conditions?
- What was the work plan for the day?
- Did that plan include any unusual job tasks?
- What other work was in progress?
- Were there any preexisting restrictions/issues?
- Who was in the unit?
- Where were these people located in the unit?
- What were you doing?
- What unusual conditions did you smell, hear, see, feel, or taste?
- What alarms do you recall?
- What equipment was damaged?
- What did you observe others doing around you?
- What was your immediate response to the incident?
- Were there any constraints on your ability to act (physical, procedural, training)?
- What involvement did you have with people from outside your department?
- What did you do after the event?
- What did you see other people doing?
- Who was directing these activities?
- What, if anything, slowed your activities down?

- When were things back to normal?
- Looking back, what would you have done differently?

Finally, the interviewer then asks supplementary questions such as:

- Is there anything else that you think we should know to perform our investigation?
- Is there anyone else that you think we should talk to about what happened?
- What do you believe to be the cause of the event?
- What data is available to support your belief?

At the conclusion of each witness interview, the interviewer should add the new information to the draft timeline, thus providing an early indication as to areas where information may be missing, or where confirmation is required.

INTERVIEWER ATTRIBUTES

In addition to the general team member attributes that have already been described, the ideal interviewer will be strong in the following areas.

Rapport and trust

An interviewer has to be able to work effectively with many types of people at all levels in the organization. Many of these people may be feeling emotional, fearful, and guilty. The interviewer has to be forceful enough to extract the needed information, while recognizing the feelings of those being interviewed.

The lead investigator (and the other team members also) need to be particularly sensitive the implicit authority associated with their position. Those being investigated will often be nervous about what the investigators find out, and what the consequences of those findings may be.

On one investigation, for example, two members of an investigation team were looking for the lead operator who had been in the control room at the time of the event. The facility—an offshore platform—consisted of two bridge-connected platforms. The investigation team members went to the control room on the first platform, only to be told by the board operator that the lead operator was on the other platform having his lunch. As the team members departed, they heard the operator call through to the other platform advising his colleague that an investigation team was on its way. His remarks also included the phrase "They said something about handcuffs." Of course, his remark was jocular, but it did illustrate the need for investigators to be sensitive to the implicit power that he or she may possess.

Interviewers should not ask inappropriate questions because those being interviewed may feel obliged to answer against their will. On one investigation, for example, one of the investigators was taking pictures of the equipment that had been involved in the event. He then participated in an interview with a person who had been injured in that same event. Although a picture of the man's injury may have helped illustrate the consequences of this event, the investigator realized that—were he to ask for permission to take the picture—the injured man may have felt obliged to agree, even though he did not want to. Fortunately, the investigators had the good sense not to raise the topic with the injured man.

Technical skills

The interviewer must have a good understanding of operations terminology, engineering documentation, processes, equipment, and modern instrumentation systems. He or she must also be able to learn the basics of new technology very quickly because it is likely that the investigation will be in an area that the interviewer does not fully understand (this can actually be an advantage, since the interviewer will be less likely to jump to conclusions).

Critical factors recognition

The interviewer must always be open minded and must assess information objectively. Nevertheless, a good interviewer will be able to recognize the critical factors in an operation and to identify which issues need more thorough investigation. He or she will be experienced in plant operations so that they can understand "the ways things really are around here," and can pick up on some of the unspoken communication that takes place. Following an incident, people may be reluctant to be completely candid. This is not to say that they are intentionally lying, but they may hold back on information. The leader should be able to read some of the unspoken signals so that he can direct his or her investigation in the correct direction.

Objective

It is human nature for an interviewer to give more credence to a statement from someone who is open and friendly rather than another person who is more defensive and/or hostile. This can be a trap. In particular, the friendliness or otherwise of the interviewee should not influence the need to check his or her statements against other sources of information, such as written audit findings.

Effective note taking

Note taking is difficult, particularly if there is only one interviewer. The note taker has to focus on the interview itself, making sure that all pertinent questions are being asked, capture the statements made by the interviewee, and write up the notes as soon as possible so that they make sense later. It is much better if one interviewer can lead the discussion and a second can concentrate on taking the notes.

As soon as possible, the interviewer should write up the notes. No one's notes are ever perfect or complete, and the interviewer will also lose about 50% of his memory as to what was said within 24 hours of the interview.

Management interviews

If senior management has to be interviewed, the interviewer will have to adjust his style. For one thing, he is likely to be provided with less time than is the case with other interviewees. However, the biggest danger is that the interview will be turned around and the manager will demand to know what the interview believes to be the findings and recommendations. Moreover, the manager may well attempt to force is his own conclusions on the investigator, often through the use of war stories.

DOCUMENTATION

Documents that are typically called upon by the incident investigation team fall into the following groups:

- Engineering information
- Operating information

- Process safety information
- Vendor data.

ENGINEERING INFORMATION

For most events, it will be necessary to ground the investigation in engineering documentation, particularly the following:

- Block diagrams
- Process flow diagrams
- Piping and instrument diagrams (P&IDs)
- Electrical one-line diagrams
- Layout drawings
- Material Safety Data Sheets (MSDSs).

OPERATING INFORMATION

Engineering information will be supplemented by operating information that records the day-to-day events taking place at the facility.

Instrument records

All instrument records to do with process conditions should be printed and stored. The records are likely to include pressures, flows, and alarm logs.

Log books, maintenance records, and JSAs

Log books and maintenance records will contain information as to what tasks were carried out prior to the incident. If the incident was associated with a nonstandard operation or maintenance task, it is also likely that a JSA will have been prepared.

Hazards analysis reports

The team should review all hazards analyses that were carried out prior to the event and that could have a bearing on what happened. If it turns out that a hazards analysis team had, in fact, forecast the event that occurred, then a strong recommendation regarding the follow-up process is likely to be generated.

MOC records

The root cause of many events is that the system was changed such that it moved outside its safe operating limits. Therefore, the MOC records should also be examined to see if the incident could have been avoided had the MOC system been better implemented.

Operating manuals/procedures

Most incidents involve either an operating or maintenance technician carrying out a task incorrectly. Therefore, the investigation team will usually need to check that manuals or procedures exist, and that they are accurate and usable.

Incident investigations and audits

The investigation team should review previous investigations to see if the current situation possesses any resemblances to what has occurred in the past. For the same reason, the team should review recent process safety audits in order to identify any findings that may apply to the current investigation.

VENDOR DATA

Vendor data in the form of specification sheets, maintenance manuals, operating instructions, and drawings often provides an important source of information for the investigating team.

FIELD INFORMATION

Physical evidence is probably the most noncontroversial information available. It is also subject to rapid change or obliteration; therefore, it should be recorded and protected as soon as possible. Sketching and mapping the position of debris, equipment, tools, and injured persons should be initiated by the "Go Team" and expanded on by the formal investigation team as needed.

DAMAGE ASSESSMENT

If the team is called upon to survey the physical damage following an explosion or large fire, they can use the techniques of *layer analysis* and *pattern analysis*. In layer analysis, the manner in which items are laid over one another provides an indication as to the sequence of events. In pattern analysis, information on items such as the following provides guidance as to what happened and where it happened.

Soot deposits, melt patterns, metal sag patterns, residue build-up, fracture patterns, and unusual marks can help develop an overall damage pattern, as can observations as to which sides of buildings and equipment items were most impacted.

The distance and direction of fragment parts from the site of the event can provide helpful information.

It is useful to determine which gaskets/rupture discs were blown and which were not.

PHOTOGRAPHS AND DVDs

With the widespread availability of low cost, high quality digital cameras, photographs are now an integral part of any investigation and the subsequent reports. Photographs need to be recorded and logged in the same manner as any other type of evidence. Each photograph should be dated, include a description as to what it is, and the name of the photographer (a camera that incorporates a date-stamp time capability should be used).

The following guidelines should be considered:

- Establish a progression of overall, mid-range, and close-up views of the incident scene
- Take pictures from all angles and perspectives. In the picture description, make it clear as to whether the picture was taken before or after any cleanup
- Photograph from eye level, where possible, in order to gain the most normal view

- Photograph the most fragile areas first
- Include a scale and color reference in the picture, where possible.

There are, however, potential problems with the use of photographs including the following:

- Pictures taken with a digital camera can easily be altered using readily available software. Such alterations may not be malicious, but they could inadvertently degrade the value of the evidence. For this reason, consideration should be given to taking pictures with a film camera. The original photographs can then be referred to if there is a disagreement as to the meaning of the picture.
- Many process-related near misses are not visual. If the pressure in a vessel rises to the point where high-pressure interlocks are activated, there is nothing to see and nothing to photograph. Yet such an event could be potentially far more serious than an event which is much more graphic—say a missing handrail.
- Farrell (2008) notes that photographs that show blood or serious injuries should be black and white as courts will not allow evidence to be presented that could inflame a jury.
- DVD/video cameras are sometimes used during interviews. However, their presence is probably likely to inhibit candid discussion. DVDs can be used to record the sequence of events in the field during the investigation process.

CLOSED CIRCUIT TELEVISION

Companies are making increased use of closed circuit television (CCTV) to enhance security. Such systems can sometimes provide invaluable information as to how a process-related incident occurred.

INSTRUMENT RECORDS

Instrument records are authoritative because they are objective and quantitative. Facilities that use SCADA (Supervisory Control and Data Acquisition) or DCS will generally have a large amount of instrument data that can be readily accessed.

TESTING/LAB ANALYSIS

Tests can be carried out by laboratories on failed metal parts, oil samples, and body fluids. All samples and collected evidence should be documented with:

- The name of the person collecting the sample
- Date and time sample taken
- Exact location/source of sample.

Testing often provides authoritative information that resolves misunderstandings. However, testing can be both expensive and time-consuming.

STEP 4. TIMELINE DEVELOPMENT

Once the facts of the incident have been established as shown in the previous chapter, the next step in the investigation is to develop a timeline or story line (Figure 11.7). A feedback loop from

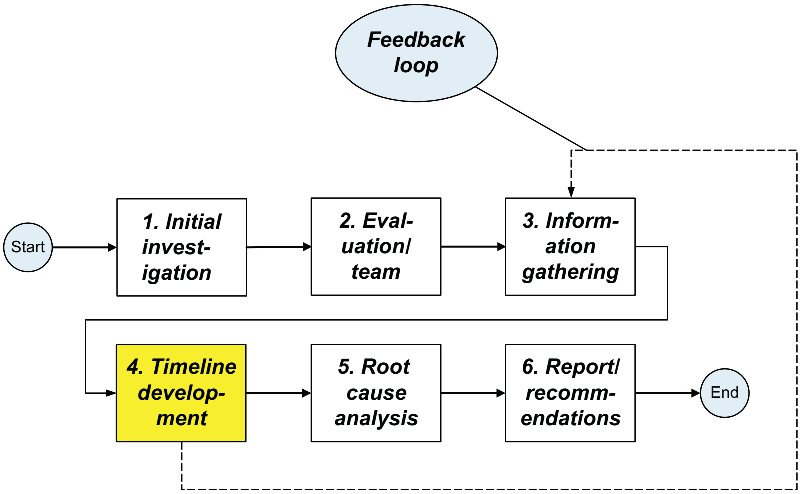


FIGURE 11.7

Step 4—Timeline development.

Step 4 to Step 3 is shown. This line is present because the development of the incident timeline will almost invariably identify a need to collect more information, to verify some of the data that has already been gathered, and to learn more about the facility's management systems.

TIMELINE STEPS

A timeline is made up of a sequence of events arranged in chronological sequence, thus providing a clear picture of causes and their effects. Timelines generally comprise three major sections.

Section 1—Events prior to the incident

Most of the investigation work and analysis will be conducted on the events and conditional or environmental factors that occurred prior to the incident itself.

Section 2—The incident

The second step in the timeline is the occurrence of the event or of a near miss situation. Most incidents occur more or less instantaneously, or over a very short period of time. However, some incidents may last for a much longer time. One company, for example, identified an incident in which it had been in noncompliance with an environmental regulation for a period of many years.

Section 3—Postincident response

Postincident response may affect impact of the event. For example, a well-trained emergency response team can remove injured persons from the area and get them to hospital quickly, thus reducing the ultimate severity of the injuries sustained. Similarly, a well-trained operator will know how to shut down other units in the facility in a safe and controlled manner, thus avoiding a follow-on fire or chemical release.

TIMELINE CONSTRUCTION

Descriptions of the events in the timeline (Figure 11.8) are shown in the rectangles. An event usually represents an action, such as "operator opens valve," or a sudden change in operating circumstances, such as "gasket failed." Conditional events are shown in the ovals below the event. They represent environmental or background conditions that allow the sequence to move forward. For example, if the event is "operator opens valve," then conditions may be that (i) "an operating procedure existed" and (ii) "the operator was not trained in this task."

The flow of time in Figure 11.8 is from left to right. The gaps between the events should be more or less to scale, i.e., distances on the chart are roughly proportional to the amount of time taken. The dashed lines show gaps in time, such as from one day to another, when no significant events took place.

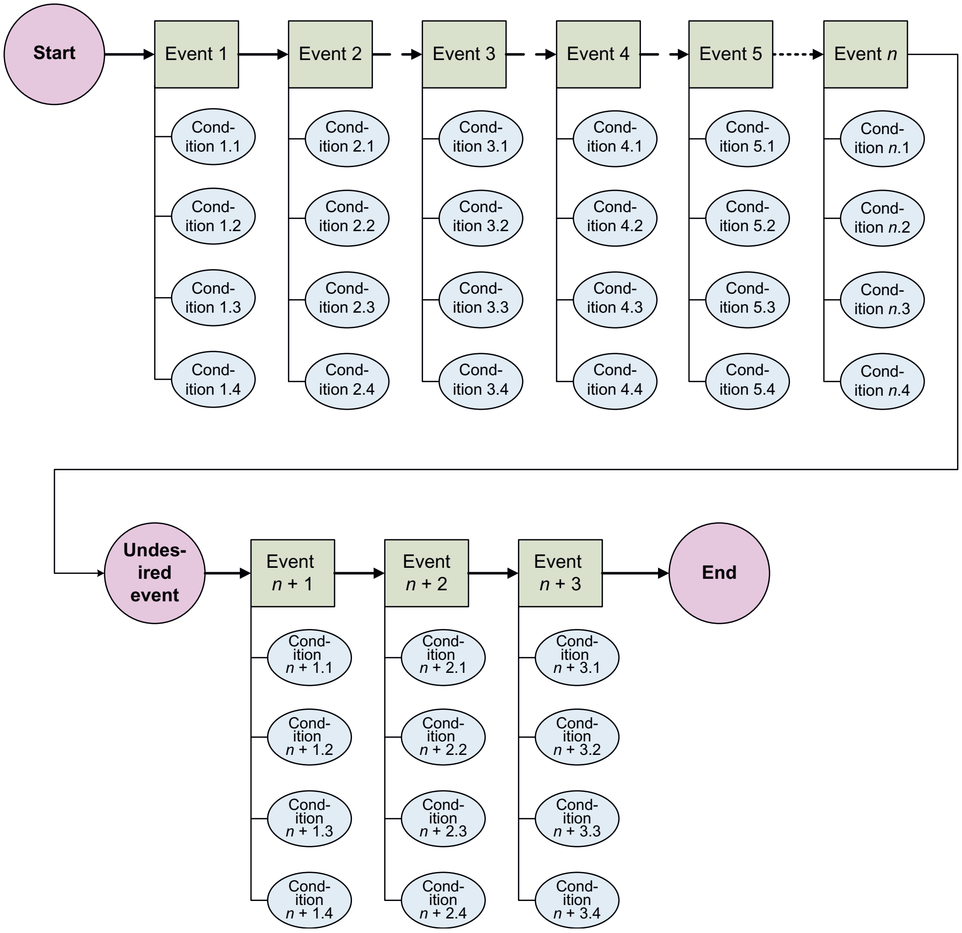


FIGURE 11.8

Simple timeline.

CONDITIONS

The conditions associated with the events in Figure 11.8 can be organized to follow a standard pattern. The first condition can be that an item exists, or that the event was necessary. The second condition is that the equipment design or management system is modern and up to date. Subsequent conditions describe undesired circumstances or deviations from normal operation. For example, if Event 4 in Figure 11.8 is "Truck Arrives at Tank," then the conditions could be:

- Truck exists
- Truck is of modern design
- Truck driver has entered this facility before.

The first item—Truck exists—may sound a little strange. After all, this analysis step is to do with the arrival of the truck at the tank, so the existence of that truck may be taken as a given. However, there may be other ways of delivering the chemical—by pipeline, for example—that could completely eliminate the risk associated with the truck movements. By creating this condition, the investigation team opens up the possibility of generating findings that lead to the possibility of a fundamental redesign of the system. Even if a truck is needed because no other method of delivery is plausible, it may be that the current schedule of one delivery every month could be cut to say one delivery every 3 months by making changes to the downstream process, thus reducing the risk associated with this operation by a factor of 3.

The second item—Truck is of modern design—is used when the equipment or the management systems are not new and/or of up-to-date design. By pursuing this line of thought, the investigation team can determine if the equipment on the truck is itself a contributing factor to the incident. For example, modern trucks may have greater capacity (thus reducing the number of trips that need to be made), or they may have more instrumentation on board to warn the driver and operator of potential problems.

The third item—Truck driver has entered this facility before—creates a possible line of further investigation and root cause analysis to do with the adequacy of the training provided to the drivers.

The next step, following the arrival of the truck, is Event 5: "Area checked with portable hydrocarbon detector." For this step, the corresponding conditions could be:

- Detector is effective for this type of hydrocarbon.
- Detector is of modern design.
- Operator has calibrated the detector.
- Operator knows how to use the detector.

MULTIPLE TIMELINES

Figure 11.8 shows just one timeline. It is possible to have two or more timelines, as shown in Figure 11.9. With regard to the standard example, the first timeline could be to do with the reverse flow of hydrocarbons into the tank, the second to do with truck movements and chemical unloading on the day of the incident. The two lines converge as shown prior to the occurrence of Event 2: "Truck Arrives at the Facility." In other words, the work to do with repairing the Lower Explosive Limit Alarm (LEL) and the reverse flow into the tank occurred during the same time period, and were independent of one another, but were completed before the truck arrived to load the tank with fresh chemical.

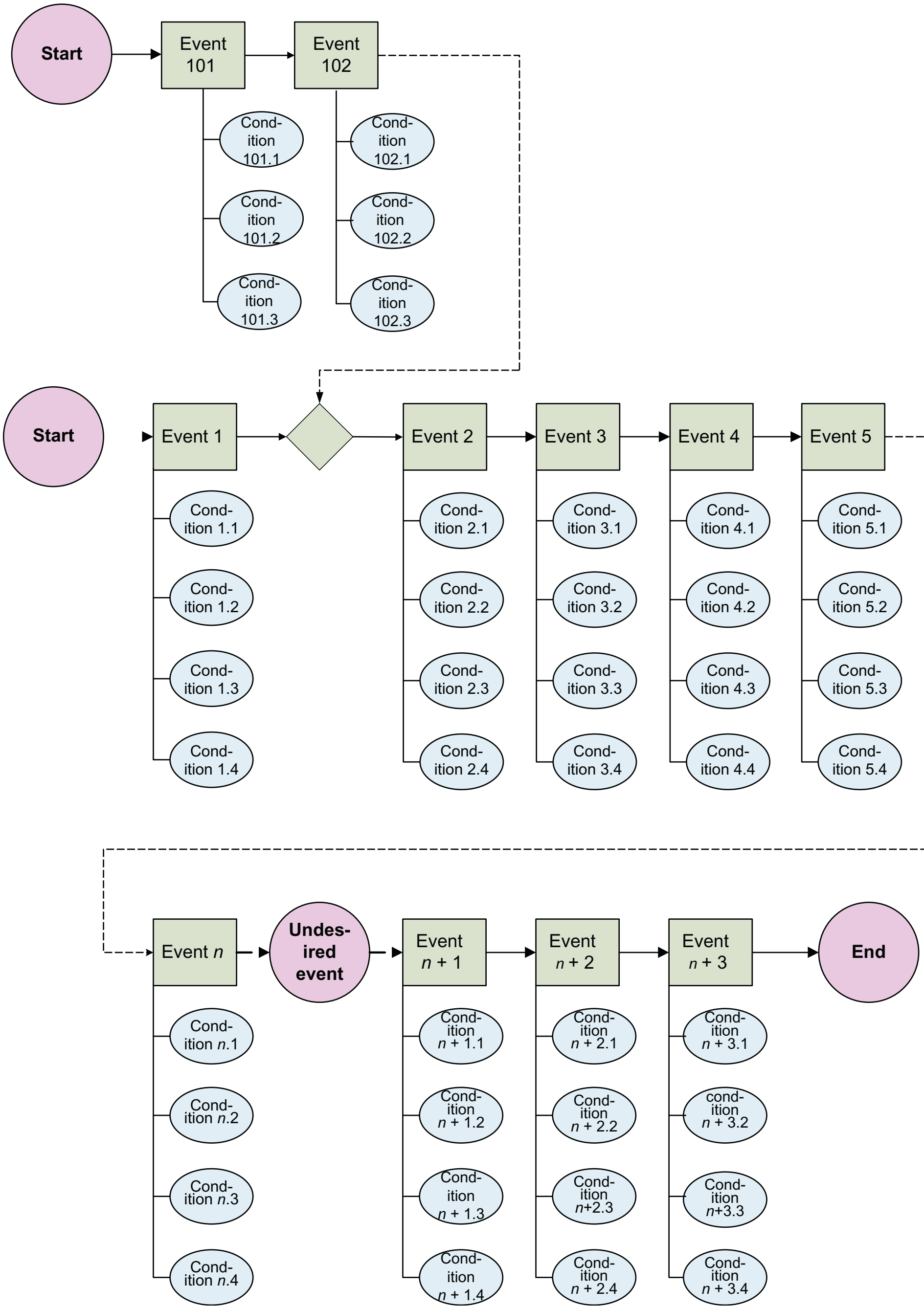


FIGURE 11.9

Multiple timelines.

TIMELINE TABLE

Sketches such as those shown in Figures 11.8 and 11.9 do not provide enough space for detailed information. Therefore, it is generally preferable to structure the timeline in the form of a table. Tables 11.3–11.5 provide an example of a partially completed sequence of events for the standard example.

Table 11.3 Sequence of Events Example—1

Date	**2/1/08**	**2/15/08**	**2/15/08**	**2/15/08**
Time	1000	0800	0815	0820
	1	2	3	4
Event	LEL adjacent to tank repaired after false alarm	Truck arrives at facility	JSA issued	Truck drives to tank
Conditional Events	LEL installed LEL about 5 years old	Truck used for chemical Truck about 10 years old		LEL installed LEL about 5 years old
Information Sources	Maintenance records	Front gate logbook Interview with truck driver Interview with technician #2	JSA database	Interview with technician #2
Discussion	3 false alarms in the previous month		Operator statement—time approximate	Required by JSA

Table 11.4 Sequence of Events Example—2

Date	**2/15/08**	**2/15/08**	**2/15/08**	**2/15/08**
Time	0830	0835	0840	0841
	5	6	7	8
Event	Area checked with portable hydrocarbon detector	Truck connected to tank, unloading starts	LEL alarms	Explosion at tank
Conditional Events	Truck exists Truck is of modern design Truck driver has not entered this facility before			
Information Sources				
Discussion				

Table 11.5 Sequence of Events Example—3

Date	**2/15/08**	**2/15/08**	**2/15/08**	**2/15/08**
Time	0842	0842	0840	1000–1200
	9	10	11	12
Event	Facility emergency announced	Inside operator starts shutdown	Injured workers rescued	Tank drained and secured
Conditional Events				
Information Sources				
Discussion				

The columns in these tables correspond to the events shown in a timeline. The rows provide:

- A more detailed title for the event
- Conditional events or environmental factors associated with that event
- A description of where the information came from
- General background discussion.

For each event, and for the associated conditions, the sources of information are provided. There is also a row in the table for background discussion.

BACKGROUND INFORMATION

As discussed in the previous chapter, development of the timeline is likely to generate a need for additional information. The most immediate need will be to fill in gaps in the narrative: items that were simply overlooked during the information gathering phase. However, as the timeline continues to be developed the analysts will see indications that point to systemic problems that are outside the immediate scope of the incident. For example, if an early indication is that the truck driver may have not followed the instructions in the JSA, the investigators may need more information to allow them to look more deeply in the JSA system. (In effect, they are starting the root cause analysis.) Therefore, the investigators may request more information regarding the JSA system, including records showing that the persons involved in the event have been trained in that system.

STEP 5. ROOT CAUSE ANALYSIS

Harry Hopkins—dubbed by Churchill as “Lord Root of the Matter”—was a key advisor to Franklin Roosevelt during the Second World War. For much of that time he was seriously ill and could work no more than a few hours a day; hence he had to focus on what was important and to ignore the dross. His success in achieving this focus led to Winston Churchill calling Hopkins “Lord Root of the Matter.” This ability to identify the core issues—what are often referred to as root causes—is the topic of this chapter and is the fifth step in the investigation and analysis process, as shown in Figure 11.10.

The value of root cause analysis is that conclusions are reached that may address a much broader range of issues than those immediately to do with the event being investigated. For example, the initial evaluation of the reverse flow problem in the standard example finds that the check valve failed. Further examination identifies a root cause that all check valves purchased from the manufacturer of that particular valve are unreliable and need to be replaced. This conclusion may, in turn, suggest weaknesses to do with the company's overall procurement system.

Use of the terms "root cause" suggests that there are one or more single underlying, objective, immutable causes for a wide range of observed events. Such a suggestion is, however, somewhat misleading; all events have one or more causes, each of these causes are themselves events which have one or more causes, and so on; the chain stretches backward indefinitely. Yet the concept of root cause remains fundamental to incident analysis. What is needed is a practical definition for the term "root cause" that allows management to understand and address the basic issues that they face while still remaining in the realm of practicality. It is important to provide a sensible framework in which underlying causes can be identified without having to spend an inordinate amount of time and money on the analysis itself, and without coming up with findings that are very difficult to implement.

One problem to watch for during root cause analysis is that of fixation. Fixation can be a serious problem when conducting a root cause analysis because people tend to view potential hazards in light of their own experiences and opinions. During discussions people tend to take up a particular point of view, and then obstinately defend it, even when they are proven to be wrong. They develop pride of ownership in their opinions. In other words, people tend to pick on one or two events, or perceived causes of events, and will not change their mind from that point forward. In the literal sense of the word, they are *prejudiced*, because they prejudge events and the causes of events.

LEVELS OF ROOT CAUSE

One of the difficulties associated with root cause analysis lies in determining the level at which to stop. After all, if the causes of an incident are pursued for long enough the team will eventually be discussing the philosophical, moral, and theological issues to do with human nature. This is obviously absurd; a sensible stopping point is required.

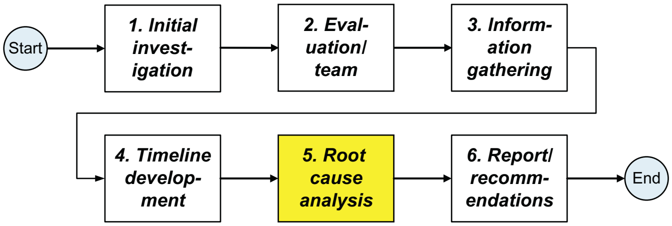

Start
1. Initial invest-igation
2. Eval-uation/ team
3. Inform-ation gathering
4. Timeline develop-ment
5. Root cause analysis
6. Report/ recomm-endations
End

FIGURE 11.10

Step 5—Root cause analysis.

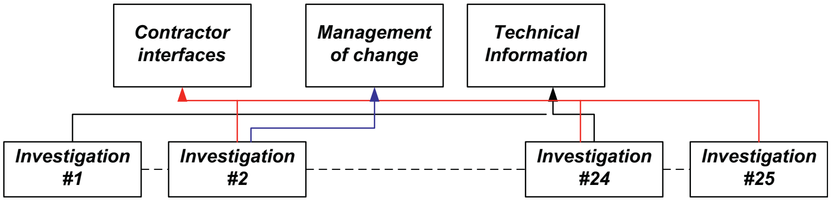


FIGURE 11.11

Levels of root cause.

Single incidents

Care has to be taken when developing root causes from the analysis of just one single incident. For example, a particular investigation may note that a cause of an event being examined was that the operating procedure was not correct. However, the team is not justified, based on this one incident, in saying that a root cause is "problems with operating procedures." However, if the same facility conducts say 24 more investigations, and operating procedures are never found to be a factor then it can be reasonably concluded that any broad conclusion about difficulties with operating procedures is wrong. It appears as if just one procedure was at fault, not the whole operating procedure library.

Similarly, in the standard example the check valve failed to close when reverse flow occurred. If this incident turns out to be a single instance of check valve failure, then a radical overhaul of the maintenance and purchasing procedures to do with check valves is hardly justified. The root cause for the reverse flow problem lies elsewhere.

Failure to understand the limitations to do with the establishment of root causes from just one incident is a reason that so many incident investigations seem to go on indefinitely. For example, if management accepts that a single check valve failure had, as its root cause, problems with the facility's purchasing procedures, then they may choose to examine other business systems and management programs. There can be no end to the extent of the analysis when such a philosophy is followed. For this reason, the use of strict project management techniques can be very helpful in "containing" the investigation.

Multiple incidents

Only when a facility has conducted a large number of incident analyses is it legitimate to talk about true root causes. In one facility, it became apparent, after 25 investigations of incidents (including near misses) that the following three issues kept bubbling up.

- Difficulties to do with communications at the operating company/contractor/subcontractor interfaces
- Failure to recognize that some apparently routine operations and maintenance work was, in fact, creating changes that should have been analyzed through the MOC system
- Lack of understanding of availability of technical information.

Figure 11.11 illustrates the above observation. Investigation #2, for example, showed that problems existed with contractor interfaces and MOC. Investigation #24, on the other hand, identified difficulties to do with contractor interfaces and the availability of technical information.

The same results were listed in the matrix shown in Table 11.6.

Table 11.6 Generic Root Causes

Incident	Contractor Interfaces	Management of Change	Technical Information
1			X
2	X	X	
...			
...			
...			
24	X		X
25	X		

TYPES OF ROOT CAUSE ANALYSIS

No single methodology for determining root cause has been adopted as a standard throughout the process industries. One reason for this lack of standardization is that different incident analysis consulting companies, some of which are marketing proprietary techniques and software, have different approaches and are in competition with one another. Many of the techniques that are available, however, can be classified into one of the following groups:

- Argument by analogy: story telling
- Barrier analysis
- Categorization
- System synthesis.

The progression shown in the above list is from more subjective to more objective.

Of the four approaches, systems synthesis is the most thorough and is likely to lead to the most creativity because it will open up "things that we haven't yet thought of." However, each of these approaches has value. If used together they can assist one another. For example, the analogy drawn from a story could help establish a new category, or it may provide ideas for new inputs to a fault tree.

ARGUMENT BY ANALOGY: STORY TELLING

Many people use stories to develop root causes by analogy. They examine incidents that have occurred elsewhere and develop lessons that can be used in the current situation. Indeed, many companies encourage the dissemination of incident stories in order to create a lessons learned culture, and some professional organizations publish information to do with incidents that can be used by other companies. For example, the journal *Chemical Engineering Progress* routinely publishes descriptions of actual events.

But the use of stories and analogies to create root causes does have significant limitations, including the following:

- False extrapolation
- Linearity
- Different world views.

False extrapolation

Root cause analysis through the use of analogy tends to focus on the development of solutions and corrective actions rather than determining what actually happened. Analogies are useful and can help generate insights, but they do not provide a rigorous, fact-based assessment as to the cause of the current incident.

For example, an engineer may recall that a facility where he once worked found that pumps supplied by company ABC were unreliable and hard to maintain. From this experience, he develops war stories—which may be considerably exaggerated—as to how he and his colleagues kept the place running in spite of the miserable performance of ABC's pumps. If the same engineer then moves to another plant that uses pumps provided by ABC, he will instinctively blame that company for any problems that arise, fairly or not. Yet it could be that a factual analysis shows that the problems are due to other causes, and the instruments are working well.

People sometimes unfairly extrapolate from a small number of bad experiences. For example, if a particular supervisor has had two or three bad readings from the production lab, he may be inclined to generalize with a statement such as "You can never trust the results from our lab" even though such an opinion really cannot be justified objectively.

In spite of its limitations, storytelling can lead to quick and effective problem solving. On one occasion, for example, a chemical processing company burned through the tubes of a fired heater thus creating substantial economic loss. When told of this event an experienced investigator immediately said "Oh, that's the empty kettle on the hot stove scenario." If an empty kettle is put on the stove, its bottom will burn through. Similarly, if the flow of gas or liquid through the tubes is halted, then the outlet temperature will go down, so the control systems will call for more heat. Yet there is no means of removing the heat, so the temperature of the firebox goes up, and eventually the tubes fail. In this case the expert identified the core problem within just a few seconds. He also developed an appropriate recommendation, which was to put a low flow interlock on the tube side of the heater.

Linearity

Most stories are linear with little or no branching. They proceed in the line, "first this happened, then that happened, then something else happened." Yet all but the simplest incidents involve contingency and complex relationships, which is why systems techniques, such as fault tree analysis, are likely to yield much more insightful findings.

World views

Each story teller has his or her own world view. This means that what is obvious to one person may not be at all obvious to another. In the case of the standard example, different people will tell the story as to what happened, thus reaching different conclusions such as the following:

- Maintenance should be checking our critical valves more often.
- Outside truck drivers really need to have more training.
- We need more money to upgrade our instrumentation.
- We don't even need to use that chemical.

None of these statements are inherently right or wrong—they merely represent the point of view and the manner of thinking of the persons speaking.

SAFEGUARDS

Safeguards—sometimes referred to as Levels or Layers of Protection (LOPA)—can be structured as shown in Figure 11.12. (The LOPA technique is discussed in Chapter 15.)

MANAGEMENT ACTION

Once the root cause analysis is complete, management will have to decide on the action to be taken. Three types of response can be considered (Wilson, 2013). Problems and corrective actions are given in Table 11.7.

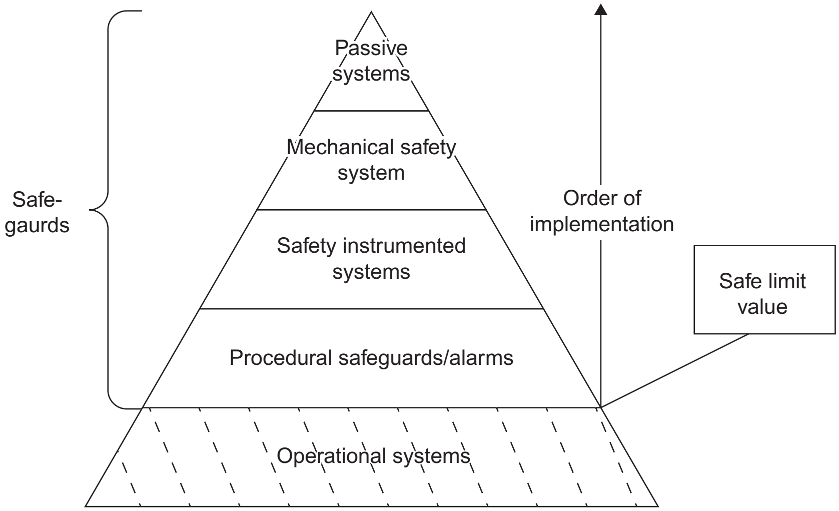


FIGURE 11.12

Levels of protection.

Table 11.7 Problem Types and Corrective Action

Problem	Corrective Action
Individual: Ordinary mistake; adequately covered by fully understood existing rules; limited harm	**Individual:** Resolve to follow rules and mentor others
Supervision: Willful individual or group violation of existing rule	**Supervision:** Apply existing rules to other people or associates
Management: Missing or inadequate policy, rule, or procedure	**Management:** Generate new rules, with a specified accountability

CATEGORIZATION

One of the fundamental discussions to do with incident analysis concerns the use of predefined categories for root causes, or whether a more open-ended, less structured approach is more appropriate. If no further guidance is provided, most plant personnel will instinctively develop root cause categories, such as the following:

- Difficulties with procedures and training
- Inadequate maintenance
- Excessive turnover.

Having created such categories, all events and subsequent analyses are organized so as to fall into that system.
The use of a categorization approach has the following advantages:

- Investigators can be provided with a tool that they can use with a relatively small amount of training.
- Large organizations can train everyone on one system, thus providing consistency across all of their analyses.
- Comparisons between multiple analyses can be made, thus allowing for the generation of more in-depth root cause generation.

Root cause categories are often placed into three groups:

- Equipment failure
- Human error
- Process systems failure.

Another organization uses a "Root Cause Map" which has the following categories and subcategories in its tree-like structure.

- Primary difficulty
- Problem category
- Cause category
- Cause type
- Specific cause
- Root cause type
- Root cause.

Equipment failure

Many incidents start with the failure of a piece of equipment. Equipment failure categories include:

- Failure of a check valve to hold
- Corrosion
- Erosion
- Electrical circuit failure
- Failure due to vibration.

Human error as a root cause

Virtually all incidents involve some sort of human error. Either a person initiated a train of events or failed to respond correctly as events started to go awry. Indeed, it is almost certain that some type of human error will be involved in incidents because usually the operator being, in Trevor Kletz' phrase, "the last man on the bus" had an opportunity to stop the chain of events. If he or she fails to do so, this does not mean that he is to blame—after all there were probably many other mistakes made by supervisors, managers, engineers, and designers.

Yet there is little value in trying to understand why *individuals* make mistakes. Each person has his or her own unique characteristics. Therefore, even a particular person can be made error-proof there is no reason to believe that his or her colleagues will not make errors. Moreover, any one person will perform differently at different times depending on a host of factors such as his or her level of fatigue, personal issues at home, and the amount of work they have to carry out at any one time.

Human error can be reduced through the use of human factors engineering and of behavior-based safety programs. Yet root cause analysis work is much more likely to yield benefits by focusing on equipment and management systems. This was understood by a vice president in a large energy company. His company's safety record was not good, so he decided to implement a rigorous incident investigation and analysis system. His (paraphrased) statement was "I'm tired of reading reports that say, *The cause of the accident was human error—recommendation: improve procedures and training*. We've got to do better than that—we've got to find out what's really going on."

Process systems failure

It was noted in Chapter 1 that major incidents tend to be rooted in *process* safety rather than *occupational* safety deficiencies. Therefore, one way of looking for root causes using a categorization approach is to create a checklist based on the elements of process safety as listed in Chapter 1.

SYSTEM ANALYSIS

The fourth type of root cause analysis discussed at the start of this chapter is Systems Analysis. Two methods are described here to illustrate this approach: Why Tree Analysis and Fault Tree Analysis.

Because both methods rely on the cause and effect principle, it is useful to ensure that the links between causes and effects are properly understood. This can be done by asking the following questions when creating a cause/effect relationship. These questions are:

- What concrete, measurable proof is there that the cause exists?
- Is there proof that the postulated cause could lead to the effect?
- What proof exists that the cause actually did lead to the effect?
- What other causes are needed, along with the postulated cause, for the effect to occur?
- Could a completely different set of causes lead to the effect?

WHY TREES

The Why Tree process is used by a single individual or a small team for the analysis of simple, straightforward incidents. The basic idea of the technique is that the analyst asks the question

Table 11.8 The Why Tree Process

Incident Description:
(1) Why did the incident happen?
(2) Why did (1) happen?
(3) Why did (2) happen?
(4) Why did (3) happen?
(5) Why did (4) happen?
and so on...

"Why did this happen?" about five times. By the time that he or she reaches the fifth level, it is likely that a root cause event will have been identified. It is not critical that the investigator ask the "why" question exactly five times; he or she may reach as satisfactory result after asking a smaller number of questions, or it may be found that a few more questions are needed before a useful insight is obtained.

The Why Tree process is shown in Table 11.8.

The simplicity and ease of application of the Why Tree approach makes its use very appealing. However, the technique does have two serious limitations: the single chain of events and the possibility of following a wrong chain.

Single chain of events

The Why Tree process uses a simple straight chain. No branching is allowed (i.e., there are no AND or OR gates such as are found in a fault tree). This lack of branching is also a feature of the story telling technique discussed earlier in this chapter. Yet, in practice, most events will have at least two causes. This restriction to a single causal string is a major limitation of the Why Tree process.

Wrong chain

The second difficulty with the Why Tree technique is that it becomes derailed if one of the answers provided is wrong and/or if a critical factor is overlooked or (incorrectly) considered to be unimportant. This concern links to the single chain problem. If the analyst follows the wrong chain, then the results become worthless.

FAULT TREE ANALYSIS

The second systems technique discussed in this chapter is Fault Tree Analysis, which is a technique that applies strict cause and effect logic to any system. The technique is described in detail in Chapter 15. When applied to incident analysis, a fault tree will have the structure shown in Figure 11.13.

The Top Event is an undesired outcome such as "Tank Overflows" or "Vapors Ignite." Below the Top Event is an AND gate with two inputs: "Action Taken" and "Conditions."

"Action Taken" means that someone did something (or failed to do something). Examples of "action taken" would be:

- Operator opened valve
- Manager did not initiate the MOC process
- Truck drives by
- Maintenance technician used wrong part.

"Conditions" are background or environmental factors that allow the event to happen given that the action has been taken. Conditions are also referred to as causal factors (Paradies, 2008). Examples of conditions are:

- Air present
- Tank exists
- Operating manual not available.

Whereas an action generally takes place over a short period of time, conditions can exist for much longer. For example, the action "operator opened valve" is essentially instantaneous, whereas the condition "valve existed" may have been present for many years before the operator took his action. Other conditions, such as the presence of oxygen in the atmosphere, are permanent (in fault tree parlance events of this type are referred to as "House Events").

Both the "Action Taken" event and the "Conditions Exist" event can be developed further. However, Figure 11.14 shows "Action Taken" as being a Base Event (a base event is identified

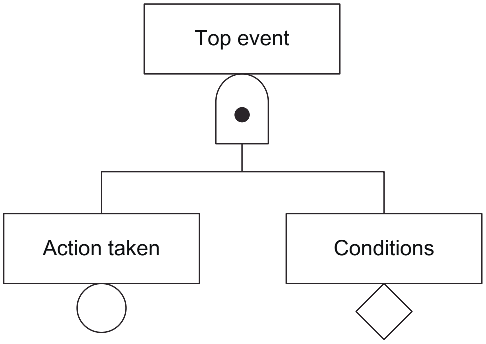


FIGURE 11.13

Incident analysis fault tree—1.

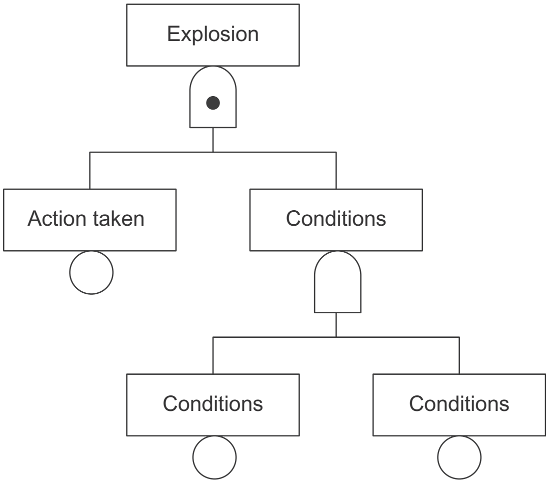


FIGURE 11.14

Incident analysis fault tree—2.

with the circle symbol). A base event is a stopping point in the tree development. Human actions are often considered to be base events because there is often little value to finding out why someone made a mistake. Humans are humans, and, as such are very difficult to analyze in the same manner as equipment failure. (A behavior-based safety program may help improve the general performance of human beings.)

"Conditions," on the other hand, will usually be developed further as part of the root cause analysis. Hence the "conditions" gate in Figure 11.13 is a diamond, which means that it is an Intermediate Event. The "conditions" gate is expanded through another AND gate as shown in Figure 11.14. Entering the new AND gate will be other conditions representing deeper levels of root cause. This process of developing conditions can be pursued for many levels.

The fault tree for the standard example is shown in Figure 11.15, which is developed from Figure 11.14.

Figure 11.15 shows that the explosion at the tank was initiated by the truck driving by. Conditional factors were that the truck was a source of ignition, the tank existed, hydrocarbon vapors were present around the tank and air was present.

Laying out the logic of the incident in this manner generates creative thinking. For example, the condition that the truck is a source of ignition may lead to an eventual recommendation to brining in the chemical in a new manner, say by use of a pipeline.

The new conditional events can be expanded further. For example, "Vapors Present" depends on the backflow into the tank and the fact that a direct vent pipe exists. The expanded tree is shown in Figure 11.16.

The use of the barrier analysis technique was discussed earlier in this chapter. Barriers or safeguards can be added to a fault tree. In the case of the standard example, backflow of hydrocarbons to the tank requires failure of both the pump and the check valve (the safeguard). The addition of the safeguards is illustrated in Figure 11.17.

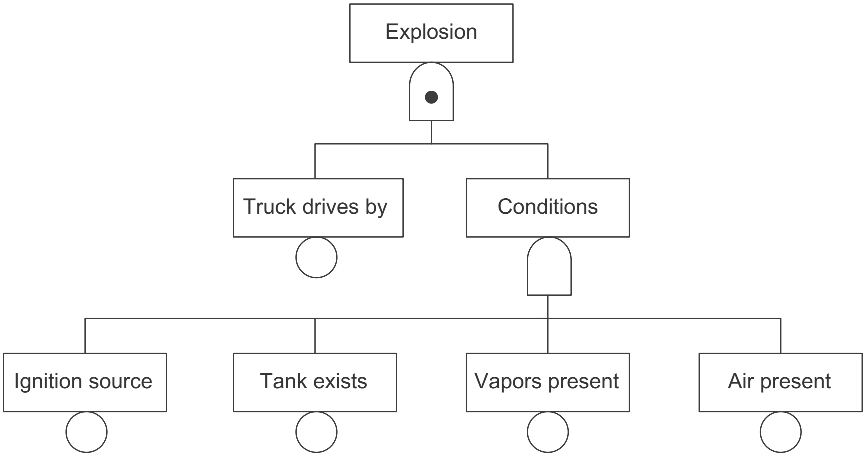


FIGURE 11.15

Incident analysis fault tree—3.

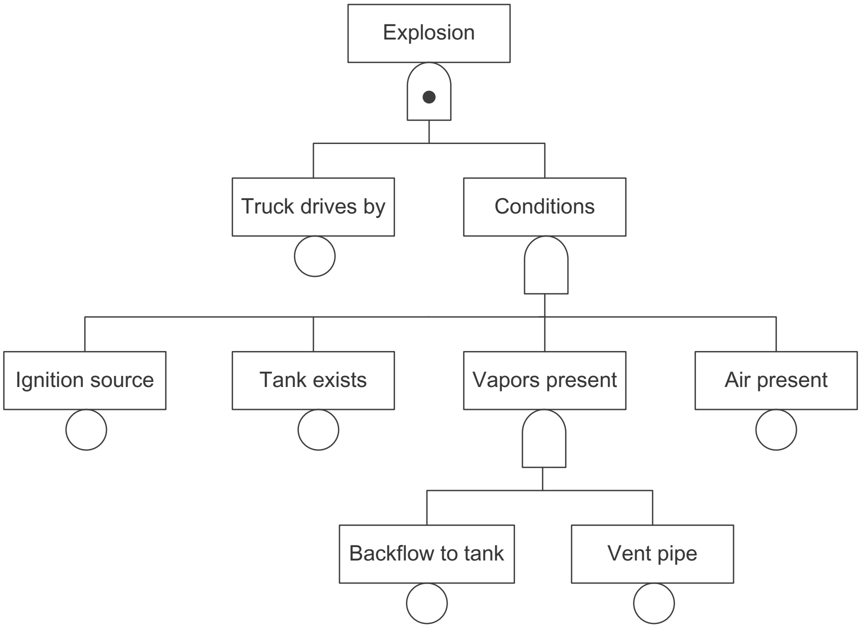


FIGURE 11.16

Incident analysis fault tree—4.

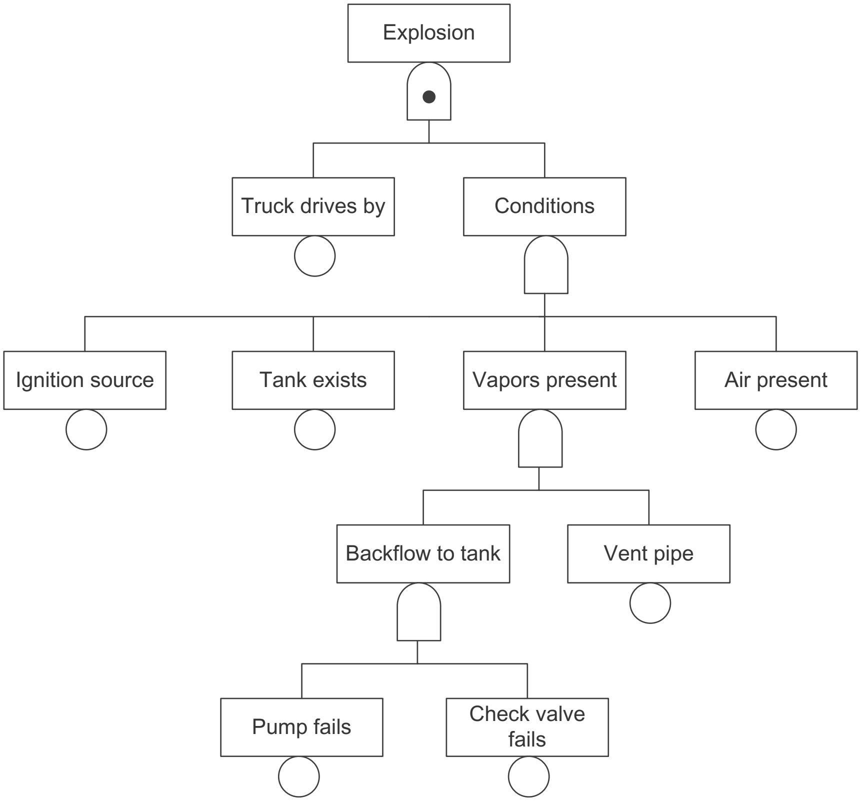


FIGURE 11.17

Incident analysis fault tree—5.

LINKAGE OF FAULT TREES TO THE TIMELINE

Almost all incident analysis techniques involve creation of a timeline, as described in the previous chapter. Yet a limitation of the fault tree method is that it is static—essentially it creates a snapshot of a system at a single point in time. This limitation in the fault tree method can be overcome by creating a mini tree for each step in the timeline, as shown in Figure 11.18.

COMMON CAUSE EVENTS

In conventional fault tree analysis, one of the biggest benefits of the technique is that it highlights common cause events, i.e., those events that occur in two or more places on the tree and thus bypass safeguards. A common example would be electrical power failure. Loss of power could cause equipment to fail and could also lead to failure of some of the backup systems.

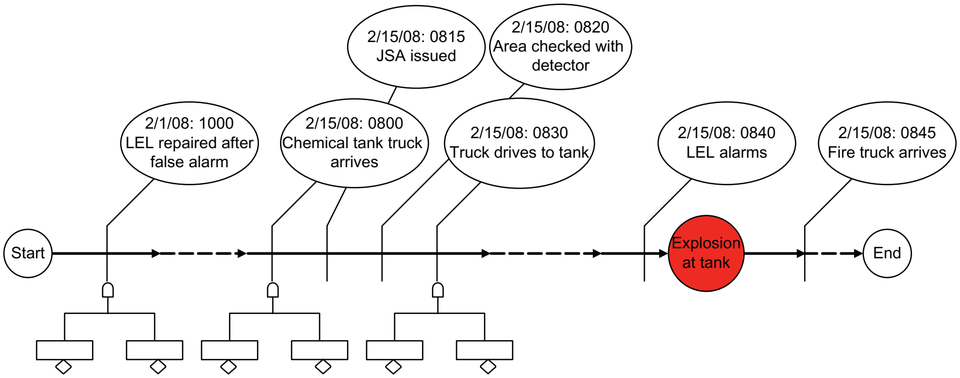


FIGURE 11.18

Timeline and fault trees.

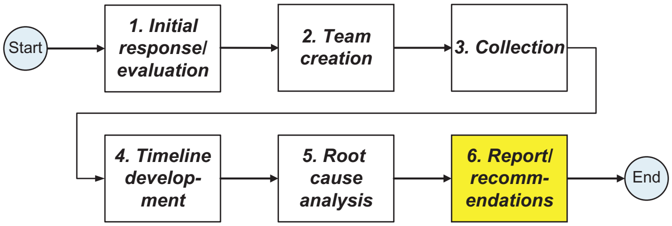


FIGURE 11.19

Step 6—Report the results.

Common cause analysis can also be very useful in incident analyses. If it is found that one factor keeps recurring, then a common cause has been identified. Its elimination is probably likely to have a powerful effect on reducing risk.

STEP 6. REPORT AND RECOMMENDATIONS

Once the investigation is complete, the team will close out the project by writing a report and issuing findings and/or recommendations (Figure 11.19). The writing of the final report is not something that most investigators like doing; they are skilled at investigating, not writing. Yet the importance of writing a good report cannot be overemphasized; not only does the report summarize the investigation itself, it also forces the team members to agree on their observations and conclusions.

General discussion and guidance to do with professional writing in general is provided in Chapter 16. Additional issues to do with the writing of an Incident Investigation report are discussed here.

In general, a consulting report should address the following three questions:

1. What's the problem?
2. What's the solution?
3. What's the cost?

In the context of incident investigation, these questions can be restructured as

1. What caused the incident and what was its impact?
2. What corrective actions need to be taken?
3. What's the cost (time, money, people) of implementing those corrective actions?

The Terms of Reference for the investigation should state clearly whether the investigation team is to issue *findings* or *recommendations*. Findings explain what happened, and what the root causes of the event were. Recommendations provide management with specific guidance as to what to do to prevent the recurrence of this event, and others like it.

The recipients of the report should always have a general sense of what it is likely to say before its formal publication, particularly if the recommendations are surprising, controversial, or expensive. In general, it is important to keep communicating with management as the investigation progresses. In particular, if it appears as if a strong or controversial recommendation is going to be made, the client management must be given as much notice as possible. That way the chance of their buy-in is greatest.

LEVELS OF RECOMMENDATION

Recommendations can be generated at four levels:

- Short term
- Intermediate
- Long range
- Industry wide.

Short-term recommendations

Sometimes, the incident team will uncover a situation that requires immediate corrective action at other facilities. (When you're in a hole, stop digging.)

In one case the team determined that an injury accident had been caused, in part, by a block valve being left in the closed position when it should have been open. The company had many other similar facilities. Therefore, two members of the investigation team toured those sites to ensure that the equivalent valve at those sites was open and tagged. Also, each site crew was briefed as to what had happened. Finally, on the following day, the safety manager issued a company-wide bulletin in which all managers were told of what had happened, and what immediate corrective actions to take.

Intermediate recommendations

The intermediate findings are those that would normally be addressed by the facility management, but that do not require a fundamental change of policy. The time frame for implementing recommendations at this level will typically be around 3 months.

In the case of the incident discussed in the previous section, management decided to:

- Conduct a detailed hazards analysis of the affected units to see if any other similar problems were present
- Ensure that contract workers were provided with improved procedures, and that they were trained in the implementation of those procedures
- Remove the offending valves altogether, rather than trust to the tagout system for keeping them open.

Long-term recommendations

Finally, the report should help senior managers understand how their systems failed, and whether they are addressing the correct goals. In the case of the above example, one of the root causes was determined to be failure of communications at the owner/contractor/subcontractor interfaces. Since similar communication problems had been observed on other incidents, senior management decided to thoroughly evaluate and update the whole contractor management system.

Further examination of a range of incidents may lead to even more sweeping conclusions, such as a corporate-level decision to introduce a new information management system or to relocate a facility to a different state or nation.

Industry guidance

Some events are sufficiently serious as to justify making recommendations throughout the industry; for example, an incident involving a highly hazardous catalyst could lead to a recommendation that new technology—one which uses a much less hazardous catalyst—is needed. A well-known example of an industry-wide recommendation occurred following release of the Baker report to do with the explosion at a Texas City refinery (Baker, 2007). The persons who died were all working in temporary trailers. Within a very short period of time, most other refineries had removed trailers that were within their battery limits.

REPORT STRUCTURE

Table 11.9 provides a representative Table of Contents for the team's report.

Executive summary

The Executive Summary is the most important part of the report because, in the words of the proverb, "You don't get a second chance to make a first impression," and that first impression is made by the first page of the report.

In the space of a single page, the event is described, the analysis discussed, and the recommendations explained. The following would often be included in the executive summary:

- What happened?
- What could have happened—how bad could it have been?
- What was the cause?
- What actions should be taken?
- Immediately
- Within the next 3–6 months

Table 11.9 Representative Table of Contents of the Final Report

Executive summary
Terms of reference
Reason for selection
Sequence of events
Consequences
Root causes
Other hazards
Recommendations
Attachments
  A—Regulations and standards
  B—Root cause analysis
  C—Organization chart
  D—Review of similar events
  E—Investigation team
  F—Review of modern designs
  G—Index to pictures and documents
  H—Detailed timeline

- Long term
- Recognition.

What happened?

In a few words, the executive summary should explain what happened. It should be possible to explain the highlights of the event in no more than two or three sentences.

What could have happened?

If the event was a near miss, or a minor injury, it is important to identify how bad it could have been—without being alarmist. For example, if a falling object struck a technician on the shoulder, then it is reasonable to postulate that the event could have led to a fatality had the object hit him on the head.

What was the cause?

In two or three sentences, the executive summary should highlight both the immediate and the root causes of the event. In the case of the falling object, the immediate cause may be a failed crane winch. A root cause may be the lack of an effective inspection program.

What actions should be taken?

The Executive Summary does not need to list all of the actions or recommendations that were generated. However, it should identify those proposed actions that require significant change to management systems and/or that are expensive.

Recognition

The executive summary should also include acknowledgements (as long as they are sincere). A statement such as the following at the bottom of the page will make a good impression.

> The team members wish to acknowledge the high degree of cooperation that was provided by all parties at all stages in this investigation and analysis. In particular, the team recognizes the invaluable support that was provided by the expert staff at companies ABC and XYZ.

This type of comment should not be *pro* forma, nor should it be a mere general statement of goodwill—it should reflect what actually took place.

For example, during one investigation it became clear that an inexperienced technician who was injured showed (arguably) poor judgment in the decision he made immediately prior to the event occurring. However, the senior technicians and supervisors who were interviewed all stated that they would have carried out the same action. Their candor and honesty led to recognition in the executive summary.

Terms of reference

The report should provide the investigation's Terms of Reference or Charter.

Reason for selection

If the incident was a near miss or of low consequence, the report should probably explain why it was investigated in depth. The consequence matrix (Chapter 1) may be placed in this section of the report, with a discussion as to where this particular incident fits into that matrix.

Sequence of events

The report should contain an overview of the major sequence of events, with details being provided in an attachment to the report.

Consequences

The consequences of the event should be described; they will generally fall into one or more of the following categories:

- Personal Injury Information
- Environmental Impact
- Cost Impact
- Loss of Production
- Loss of Inventory
- Repair Costs
- Emergency Response Costs
- Litigation Costs
- Medical Costs
- Insurance Coverage
- Workers' Compensation.

Root causes

A summary of the root causes and the process that was used for identifying them should be provided, along with a working definition of the term "root cause."

Other hazards

The team should note any other hazards that they uncovered but that were not directly related to the incident that they were covering. However, it is important not to report too extensively on such findings because they are out of scope and because the team is not likely to know all the pertinent facts.

Recommendations

All findings/recommendations should be listed in the section of the report.

The team should be careful about making recommendations that are too specific. For example, a recommendation to do with the standard example could be "Replace all check valves from vendor A with check valves from vendor B." However, the mechanical engineer at the facility may have additional information to do with check valves in this service such that the recommendation will not achieve the desired effect. It is better in such circumstances to generate a finding such as "The integrity of the check valves was determined to be unacceptable, and a new mechanical integrity policy regarding these check valves is required."

If a choice of recommendations is available, they can be evaluated through a simple risk analysis.

Attachments

Attachments can include pertinent supporting information collected in support of the investigation such as timelines, drawings, calculations, pictures, decision matrix, risk matrices, fault trees, fishbone diagrams, and cause and effect diagrams.

Attachment A—Regulations and standards

This attachment will identify any regulations or standards that apply to the incident.

Attachment B—Root cause analysis

The root cause analysis work is provided in this Attachment.

Attachment C—Organization chart

Many events involve multiple persons, often from different companies. An organization chart can be very useful and can help demonstrate the decision making process, the manner in which instructions were issued and how information was conveyed prior to the incident.

Attachment D—Review of similar events

The event should be compared with other, similar events that have occurred within the same company to see if any generic, root cause issues can be identified and with similar events that have taken place at other companies.

Attachment E—Investigation team

The members of the investigation team can be listed in this Attachment, along with their roles on the project.

Attachment F—Review of modern designs

If the incident occurred on an older piece of equipment or system, examination of new designs can sometimes provide insights as to what recommendations should be made. The same examination may also identify problems with unauthorized MOC.

Attachment G—Index to pictures and documents

The report itself will use only a tiny fraction of the pictures and documents that were referred to during the investigation. An index should be provided that lists all of the items that were made available to the team.

Attachment H—Detailed timeline

The final attachment is a printout of the detailed timeline, along with the associated tables. This Attachment is shown last because it may require that the formatting of the report has to switch from portrait to landscape.

ISSUING THE REPORT

The mechanics of issuing the report can be divided into the following steps:

- Writing the report
- Presenting the report
- Follow-up
- Legal issues.

Writing the report

Most teams find it best to assign the report writing to one individual. He or she will collect information and opinions from the team members, issue a preliminary report (to the team only), and make updates and corrections.

However, even if one person is responsible for writing the report, it is important to understand that the report should represent the conclusions and opinions of all the team members, each of whom will therefore need to review the draft before it is finalized.

Once the final draft of the report is released, the management of the facility where the event took place will generally review what is written and possibly ask for changes to be made, particularly if they feel that the team's conclusions are based on incorrect information. However, management must not ask the team members to modify their judgment or opinions. The team must maintain its integrity.

Presenting the report

It is unlikely that the report will be read in depth by more than a few people. Generally, communication to do with the event will be *via* meetings with key information being shown in overheads.

These meetings should be short and will essentially summarize the report's Executive Summary. A typical set of overheads will have five slides with the following topics:

- A statement as to what happened
- The consequences (actual and potential)
- Lessons learned
- Recommendations.

All employees and other personnel who were involved in the incident should be informed as to what happened and what actions are being taken (unless restricted from doing so by legal). Injured employees should have a copy of the report delivered to them by management. Details of the incident and follow-up can also be provided to all employees through the facility newsletter or web site.

Follow-up and recommendations tracking

Finally, no investigation is worth doing unless facility management follows up on the recommendations that were made. However, the responsibility for proper follow-up is rarely the responsibility of the investigation team (although the team may be able to offer advice as to what the next steps should be).

There needs to be a process in place for tracking incident recommendations to completion. All of the incident recommendations need to be kept in a centralized database of incident register. Key information to maintain for each recommendation includes:

- Incident number
- Date of incident
- Description of recommendation
- Recommendation owner
- Status (open, complete)
- Date of last update
- Actions taken.

The First Report Template can form the basis for the incident register. However, additional space should be provided for information to do with the formal investigation, the investigation team's report, and the findings and recommendations. Not only is the incident register used to record information to do with the event itself, it can also serve as a tool for managing the results of the subsequent analyses.

Legal issues

Many incidents result in significant loss, which, in turn, means that legal action may result. Examples of such action include:

- Injured employees or contractors suing for damages
- Facility management attempting to recover costs from equipment suppliers
- Regulatory agencies filing charges for failure to comply with a rule or standard.

The potential for litigation means that all those involved an incident investigation and analysis need to be sensitive to the legal implications of their work—particularly with respect to the secure retention of notes and other records, and the potential need to work within attorney/client privilege.

INFORMATION SECURITY AND CHAIN OF CUSTODY

Security and custody of evidence are necessary to prevent its alteration or loss and to establish the accuracy and validity of all evidence collected. One of the first tasks of the "Go Team" is to create a chain of custody process.

Table 11.10 provides an outline of a representative Chain of Custody form. It is in five sections:

- Information to do with the initial submittal
- Description and location of the items submitted
- Records of transfers of items to other persons
- Disposal of the items at the conclusion of the investigation
- Supplemental information.

RECORD RETENTION

Records of all types, including hand written notes, should be retained until the final report is issued. At that time, the team members may be instructed by their legal advisors to discard their notes and preliminary reports. However, the final report will generally be retained for a number of years, depending on regulatory requirements and company policy. The team should be provided with guidance as to whether they are to retain notes and other interim documents. Some government agencies in the United States have a clear policy that only the final report is to be retained; all other notes and electronic records are to be destroyed.

The investigation team should be provided with a room or other secure location to which access is limited to team members. Evidence should be carefully labeled and stored in the secure location.

REMOVING EVIDENCE

Before removing any evidence, always establish a protocol for transporting, analyzing, and testing physical evidence using the chain of custody described above.

Following the initial inspection of the scene investigators may need to remove items of physical evidence such as damaged piping to be sent to a lab for testing. To ensure the integrity of evidence for later examination, the extraction of parts must be controlled and methodical. The removal process may involve simply picking up components or pieces of damaged equipment, removing bolts and fittings, cutting through major structures, or recovering evidence from beneath piles of debris. Before evidence is removed from the scene, its location should be documented using position maps and photos. All items that are being moved must be carefully packaged and clearly tagged. In particular, items that have been damaged should be packaged carefully to preserve surface detail.

If evidence is to be transported to another location, not in the direct control of an investigation team member, a chain of custody form should be completed.

FILE SYSTEMS

Each facility should set up a standard file structure on the company network that is accessible to all authorized persons, and that is consistent across different investigations. The structure shown in Table 11.11 can be used as a go by.

Table 11.10 Sample Chain of Custody Form

Section A—Initial Submittal					
Name and Title of Submitter:				Date Submitted:	
Company:					
Address:					
Telephone number:		Mobile number:		E-mail address:	
Section B—Description and Location of Items Submitted					
Sampling Site:				Site Address:	
Collected By:		Date Collected:		Company:	
Description of each item, including number of containers, identification number(s), and a physical description					
Submitter Comments:					
Section C—Transfers[a]					
Relinquished By (Submitter)	Organization	Date/Time	Received By	Organization	Date/Time
1.					
2.					
...					
Section D—Disposal					
Disposition Site:			Method of Disposition		
Performed By:			Date:		
Witnessed By:			Date:		
Section E—Supplemental Information					

[a] *The person receiving an item during a transfer should sign a statement on the following lines:*
I certify that I received the above item which was removed from (the event location), and owned by (company name). I further certify that said item shall remain in my immediate possession at all times during transport to the above shipping location.

Table 11.11 Representative File Structure

- Terms of reference
- Scope of work
- Policies
- Procedures
- Incident register
- Images
- Notes
  - Interviews
  - Procedures
  - Written records
- Report
  - Drafts
  - Final
- Standards/Regulations
  - API
  - ASME
  - Company
  - OSHA
- Technology
- Administration
- Correspondence
- Travel
- Working Folders
  - Person A
  - Person B
  - ...

INCIDENT/RISK REGISTER

For each identified hazard, a full description of its nature, consequences, and likelihood is provided. The register contains a section for follow-up, as shown in Table 11.12.

The follow-up section describes how the identified hazard was handled, and when the associated recommendation was completed. On a large project, it is necessary to have one person who is assigned the task of making sure that all findings are closed out properly before the new facility is started up. In addition to managing the risk register itself, the person in charge of follow-up generally is assigned the broader responsibility of filing all of the hazards analysis reports. Questions that have to be answered in this context include:

- How are the hazards analysis records to be managed?
- How are the recommendations and action items to be managed?
- How are the recommendations to be communicated?
- What media are to be used for storing the hazards analysis records?
- How and when are they to be purged?
- Who has access to the hazards analysis records?
- Who can modify the hazards analysis records?

One potential problem to do with the management of the incident register is determining who has access to the information about the incident. On the one hand, it is important that all company employees can read the reported information so that they can pick up lessons learned. On the other hand, the register will probably contain sensitive material that should be kept confidential, as should personal details to do with injuries and any suggestion of fault finding.

Information that can be available to anyone with access to the company intranet includes:

- Facts about the incident itself
- Follow-up actions that others can take
- The final report (depending on the sensitivity of the information).

Table 11.12 Sample Incident Register

Finding		Notes
Finding Number		
Node		
Date of Finding		
Hazard		
Source		
Consequences		
Safety		
Environmental		
Health		
Economic		
Likelihood		
Risk Rank		
Follow-Up		
Assigned to		
Company		
Department		
Recommendation		
Status		
Resolution		
Date Approved		
Approved by		

Other information, such as the following, should be accessible only to the investigation team:

- Interim reports
- Details of the investigation notes (particularly interviews)
- Pictures.

FEEDBACK

Once the investigation is complete, the team leaders and the managers who receive the report should provide their feedback. A representative feedback form is shown in Table 11.13.

INCIDENT DATABASES

It can be useful to compare a facility's incident records with national averages and to learn from the experiences of others. The following organizations provide information on nationwide and worldwide incidents.

Table 11.13 Feedback Form

	Needs Improvement	Satisfactory	Excellent
Was the investigation completed in a timely manner?			
Was the investigation of sufficient depth?			
Was the scope of work correct?			
Were the Terms of Reference clear?			
Was a project plan developed?			
Did the report provide a clear insight as to what occurred?			
Did the report provide suggestions for immediate corrective actions?			
Did the report provide a satisfactory root cause analysis?			
How were internal communications during the investigation?			
How effective were communications with those involved in the incident?			
How effective were communications with outside parties, such as equipment manufacturers?			
Was the final report of good quality?			
Was the final presentation to management effective?			
Was the project plan followed?			
How was the professionalism and effectiveness of the investigators?			
Will the findings of this report assist you and other managers in preventing similar events in the future?			
What were your overall impressions of this investigation?			

NATIONAL RESPONSE CENTER

The National Response Center (NRC) is the single contact point for reporting all environmental incidents in the United States. There is a standard series of questions that have to be answered in the report, including material name, date, and time when the incident occurred, and the cause of the spill or release. The NRC database spans the period from 1982 to 2001; it contains about 23,000−35,000 entries for each year.

ACCIDENTAL RELEASE INFORMATION PROGRAM (ARIP) DATABASE

The ARIP database was developed by the Environmental Protection Agency (EPA) to determine the causes of accidental chemical releases, to identify the steps that could be taken by industrial facilities to prevent these releases, and to outline industrial prevention practices.

Releases are first reported by facilities to the NRC—described in the previous section. The EPA then enters this information into its Emergency Response Notification System (ERNS) database. EPA reviews these release reports and decides which reports should be included in the ARIP database using the criteria shown below.

- The release must be from a fixed facility
- The release must result in a death or an injury
- The quantity released must involve at least 1,000 pounds of a hazardous substance, as defined by Section 102 of the Comprehensive Environmental Response, Compensation and Liability Act
- The release must be one in a trend of frequent releases from the same facility (>3 releases within a 12-month period)
- The release must involve a chemical listed by the EPA as an extremely hazardous substance (EHS) under Section 302 of the Superfund Amendments and Reauthorization Act of 1986 (SARA).

CENSUS OF FATAL OCCUPATIONAL INJURIES (CFOI)

The Bureau of Labor Statistics (BLS) of the United States Department of Labor annually reports the number of workplace injuries, illnesses, and fatalities ever since the year 1972. Starting in 1992, BLS began collecting additional information on the major injuries in the form of worker and incident characteristics. At that time, BLS also initiated a separate CFOI to review events more effectively than had been possible in the previous survey. The CFOI database can be used to do statistical analysis for fatalities by Standard Industrial Classification (SIC) Codes. The CFOI fatality data is presented in several different categories as shown below:

- Fatalities by event or exposure
- Fatalities by occupation and major event or exposure
- Fatalities by industry
- Fatalities by selected worker characteristics
- Fatalities by state and event or exposure.

Data for the CFOI are compiled from various federal, state, and local administrative sources, including death certificates, workers' compensation reports and claims, reports to various regulatory agencies, medical examiner reports, police reports, and news reports. Source documents are matched so that each fatality is counted only once. To ensure that a fatality occurred while at work, all information is verified from two or more independent source documents or from a source document and a follow-up questionnaire. Approximately 30 data elements are collected, coded, and tabulated, including information about the worker, the fatal incident, and the machinery or equipment involved. This database does not give any descriptions of the accidents (types or causes).

MAJOR ACCIDENT REPORTING SYSTEM (MARS)

In the year 1984, the Directive to the European Commission established an industrial accident notification scheme, the MARS, operated and maintained by the Major Accident Hazards Bureau of the Commission's Joint Research Center in Ispra, Italy. The objective is to use this information as a basis from which to draw lessons learned for preventing major accidents and mitigating their consequences.

MARSH AND McLENNAN REVIEWS

The company Marsh and McLennan has been publishing annual reviews for major worldwide accidents in the Hydrocarbon and Chemical Industries since 1977. Each review lists the largest 100 accidents in the last 30-year period. For each accident, the report provides a brief description of the location, type of facility, dollar loss, and possible causes.

ANNUAL LOSS PREVENTION SYMPOSIA

This annual symposium (which started in 1967) is organized by Loss Prevention Committee within AIChE's Safety and Health Division. The objective of the annual symposium is to help industry (refineries, chemical industry, and allied industries) to improve their safety performance by providing a forum for people in academia, industry, and the government to exchange ideas. Each symposium has five sessions covering various topics of loss prevention, such as reactive chemicals, static electricity, fires and explosions, storage of flammable and combustible materials, automation, management, and case histories. A case histories session is included.

PROCESS SAFETY BEACON

The *Process Safety Beacon* is a regular news bulletin issued by the American Institute of Chemical Engineers in their *Chemical Engineering Progress* magazine. The *Beacon* reports on actual events show how they occurred and highlight lessons learned.

GOVERNMENT AGENCIES

Many government agencies such as the Mine Safety & Health Authority (MSHA) publish information on their websites describing events that have occurred in the industries that they cover.

CHAPTER

EMERGENCY MANAGEMENT

12

CHAPTER OUTLINE

Some of the detailed information, such as fire water systems and Personal Protective Equipment that were in the first edition of this book have been moved to the new book, *Design and Operation of Process Facilities.*

INTRODUCTION

The focus of this book is on helping companies meet their safety, environmental, and operational goals. Yet, no matter how well designed and operated a facility may be there are times when an emergency occurs and an immediate response is required. This chapter discusses the topics of emergency management and of emergency response systems in the context of a risk and reliability management program.

Emergency response falls under the broader rubric of Abnormal Situation Management (ASM), in which a variable moves from the safe range, through the area of troubleshooting, and on to a true emergency as illustrated in Figure 12.1.

Process Risk and Reliability Management. DOI: http://dx.doi.org/10.1016/B978-0-12-801653-4.00012-6

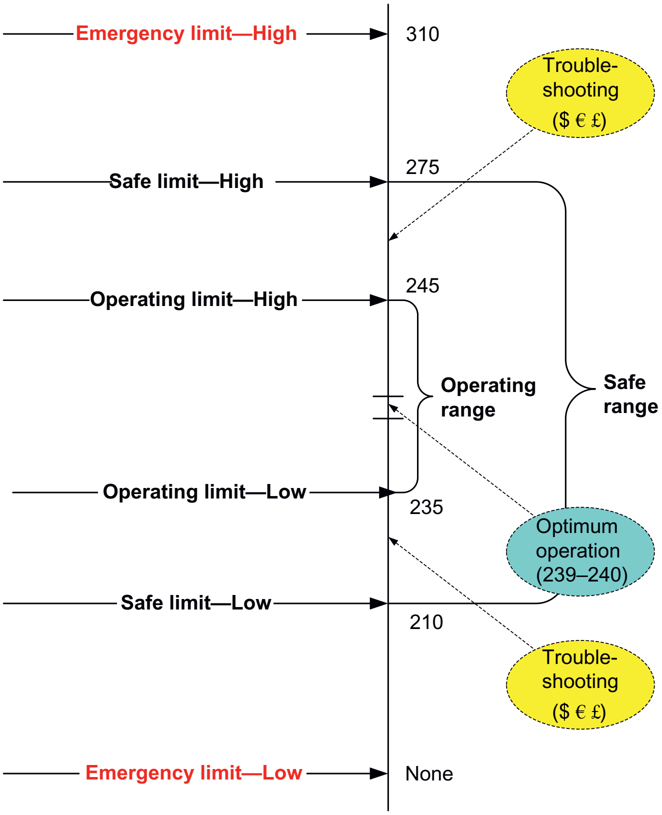


FIGURE 12.1

Operating, safe, and emergency limits.

Once a process variable moves outside its normal operating range it enters the region of "trouble" (245–275 in the upper range in Figure 12.1). When a facility is in its normal operating range the system is controlled by its instrumentation; the operator usually does not have a lot to do except keep an eye on things. It is when things start to go awry, i.e., when the system runs into trouble that the skills of the experienced operators and maintenance technicians are called upon. As the system moves out of the trouble range (275 in the example), the system becomes increasingly unsafe until eventually an emergency is declared (310 in the upper range of the example; there is no lower emergency limit in this case).

ABNORMAL SITUATION MANAGEMENT

ASM has been defined as "undesired plant disturbances or incidents with which the control system is not able to cope, requiring a human to intervene to supplement the actions of the control system" and “The objective of ASM is to bring the process back to normal before safety-shutdown systems or other safety-protection systems are engaged” (Carpenter, 2013). The consortium has identified three items as being particularly important:

1. Better shift handover communication
2. Better alarm flood management
3. Better situation awareness through the use of overview displays using qualitative gauges

They have identified “Top 10 Failure Modes across all Incidents.” Of these the top three are:

1. Hazard analysis and communication
2. Establish effective first-line leadership roles to direct personnel, enforce organizational policies, and achieve business objectives
3. Establish an effective and comprehensive program to continuously improve the impact of people, equipment, and materials on plant productivity and reliability.

Although the above topics are worthy to be emulated, they are very general in nature and provide little practical guidance to the managers who are actually running a facility.

HUMAN RESPONSE

Emergency response always involves people. Therefore, it is important to understand how people respond during an emergency and how they should be trained, especially as the manner in which they behave during an emergency is likely to be quite different from their normal behavior.

HUMAN ERROR RATE

When a situation is out of control and people are scared or panicky, their error rate is likely to be in the 10%—20% range, or higher. This means that, if an untrained person is asked to carry out five actions and a success rate of 80% for each action is assumed, then the probability of overall success is 0.8^5 or 33%. In other words, that person will most likely fail to execute the tasks properly. Instruments and mechanical equipment items, on the other hand, are not subject to emotional pressures, which is why it is usually best to rely on them during an emergency.

The high error rate that most people exhibit during an emergency can be reduced by making sure that good emergency procedures are in place and by conducting as many drills as possible so that operating personnel have experience of what a real emergency may look like.

FIXATION

During an emergency, people are often overloaded with urgent information. Consequently, they may tend to “fixate” on just one or two items, even if these items are only a minor part of the overall story. The situation will further deteriorate, if it turns out that an instrument signal on which the operator was fixated was wrong. Then, he or she will take actions that will exacerbate the situation. (Fixation on an incorrect signal was a factor in the accident at the Three-Mile Island nuclear power plant.)

HEROISM AND BUDDY LOYALTY

In many plants, there is a general rule that anyone who is not part of the emergency response team (ERT) should always move away from an emergency situation, not toward it. In practice, people sometimes feel compelled to take "heroic" action—thus violating this rule. One reason they do so is to protect or save a colleague who has been hurt. Such loyalty can lead to inappropriate action. For example, if someone is knocked down by fumes his buddy may go into the situation to rescue him without wearing the proper breathing gear. As a result there could be two people overcome by the fumes. The buddy should summon help as quickly as possible but not put himself in danger.

> A situation such as this occurred on a refinery. A supervisor had been over the isomerization unit for a few years, so he knew that unit very well indeed. However, some months prior to the incident he had been transferred to another department within that refinery.
>
> One morning he was walking past the isomerization unit on a routine task to collect environmental information. Suddenly, without any type of warning, a pump on the unit blew a seal and a large cloud of butane vapor was emitted. A fired heater was located nearby. If the butane cloud had lit off, a catastrophic explosion and fire would have occurred.
>
> The supervisor was faced with an immediate decision: (1) Should he run up to the pump, shut it down, and block it in and start the spare pump? Or (2) Should he move quickly to the control room, report the situation, and have them take the appropriate, formal action?
>
> In this case, the supervisor chose the first route, i.e., he decided to run to the pump and bring it to a safe condition and keep the facility running with the spare pump. Yet this was probably the wrong decision. After all, if the leak had lit off while he was taking those actions he would most likely have been killed or grievously injured.
>
> It is important to stress that the above comment is not a criticism of the person involved. After all, no one knows what they will do in an emergency. But the situation does stress the importance of going through drills and simulations so as to maximize the probabilities that correct actions will be taken.

TROUBLESHOOTING

Troubleshooting has been defined as "the search for the hidden cause or causes that leads to inadequate performance." A troubleshooting response is appropriate when there is no anticipated danger to personnel and when there is little chance of any significant equipment damage; usually the main concerns are about product quality, production rates, productivity, and equipment repair costs. Examples of "trouble" include:

- Product quality problems
- Erratic machinery performance
- Preparation for extreme weather conditions such as hurricanes or ice storms
- Minor environmental problems
- Reduced yields of raw materials and/or increased energy consumption

One of the most important decisions that an operator has to make when an abnormal operation occurs is to determine whether or not the situation with which he is faced represents "trouble" or an "emergency." This decision often has to be made quickly and under considerable pressure. For this reason, knowledge of safe limits for all critical parameters (Figure 12.1) is vital.

If the operator were to handle an emergency as if it were only an operational problem the consequences could, of course, be very serious. However, the opposite situation can be almost as bad. If he erroneously decides that trouble is an emergency not only will his subsequent actions lead to unnecessary production and productivity losses, but they may actually create an emergency. For example, tripping a motor-operated valve to its closed position in response to a misdiagnosis of an emergency can cause hydraulic and thermal shocks in other parts of the process that might cause an upstream flange to spread, leading to a release of toxic or flammable chemicals.

LEVELS OF EMERGENCY

An emergency response can be divided into three phases:

1. The system is at or near the emergency limits, but the operators and supervisors believe that they are able to return the plant to normal conditions using normal operating procedures and techniques. It is critical that they understand the exact nature of the problem if they are to be successful in this. Many accidents would have been less severe had the operators not tried to "fight" the situation, but simply shut down the facility in an orderly manner. (On the other hand, a full facility shutdown is not always the best response to an incipient emergency because doing so increases the number of actions that the operator has to perform, and can stress many equipment items. The advantage of keeping the unit running is that the operators can concentrate on correcting the emergency situation. They do not have to simultaneously cope with bringing down all the other equipment in a safe manner. Moreover, the avoidance of a full shutdown means that the unit can be brought back online relatively quickly with minimal production loss).
2. The second phase of an emergency occurs when the safety instrumented system and other high reliability, automated devices (including relief valves) take over. At this point in time the role of the operator is simply to secure the unit as it shuts down.
3. In the third phase of an emergency, the situation is out of control. There may be a large fire or chemical release to contend with. The full emergency response system is needed to minimize injuries, environmental damage, and loss of equipment.

Figure 12.2 provides more detail about what to do with the third phase. It shows the ways in which emergencies can be initiated, along with the appropriate levels of response.

CAUSE OF EMERGENCY

At the top of Figure 12.2 are the possible causes of an emergency: either an internal event such as the failure of a pump seal leading to a major fire, or an external event such as a lightning strike or an explosion at an adjacent facility. These initiating events can be identified, listed, and analyzed when conducting hazards analyses and preparing a risk management plan. Factors to be considered when identifying potential accident scenarios include the location of a release, its magnitude, wind direction, and the number of people who may be in the area at the time of the release.

It can be useful to model some of the scenarios, particularly the release of hazardous chemicals so that, if the accident actually does occur, the emergency responders will have some idea as to the size of the incident with which they may be expected to cope. Some companies even have online

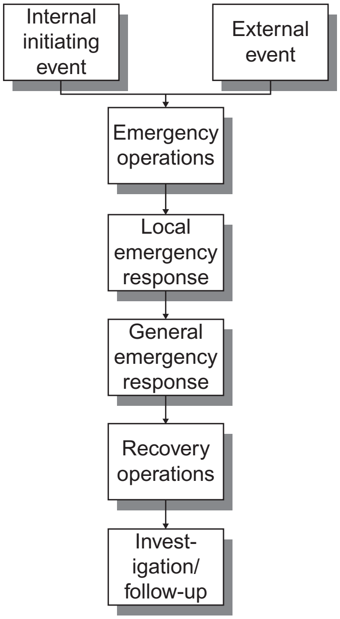


FIGURE 12.2

Levels of emergency.

models that are available in real time. Then, if there is a release of that chemical, the response team can provide the modelers with current information so that a real-time prediction as to the magnitude of the incident can be developed.

It is important to identify any chemicals that require special treatment during the course of an emergency. For example, the use of water on some chemicals may cause them to ignite. Chemicals such as these will need their own special means of response.

A complicating factor is that most emergencies do not occur in isolation. Usually, there is a whole host of events going on at once. For example, the immediate emergency may be hydrocarbon overflowing from a tank. However, the cause of the overflow may have been the loss of electrical power to the site. That loss of power may also have compromised the firefighting capability of the ERT, or it may have led to a degradation of the internal communications channels. Moreover, if the spilled liquid were to ignite, the subsequent fire could burn through a critical utility header. Environmental events, such as earthquakes, are particularly prone to creating multiple, simultaneous emergency situations. For example, the earthquake that causes lines and vessels to rupture may also break the fire water header, thus placing the ERT in a less than enviable position.

EMERGENCY OPERATIONS

The first level of response can be termed “emergency operations.” A line operator or maintenance technician notices that an emergency situation is developing and quickly responds to bring the system to a safe condition. For example, if a pump seal fails and flammable hydrocarbon liquids are being sprayed into the air, the operator will usually shut down and block in the pump, hose down the area, get the spare pump started, and call in maintenance to repair the failed seal. The emergency condition has been identified and corrected within just a few minutes.

If immediate operating response is not sufficient, the operator can shut down sections of the unit so that the affected equipment can be repaired. Procedures to do with emergency operations and shutdown tell the operator how to do this without causing any further damage and without jeopardizing other units. Once more, the facility remains in operation.

As a general rule, sources of heat such as fired heaters and steam reboilers should be shut down as an emergency develops. Cooling systems should continue to operate because they remove heat from the system. Utilities, such as the steam and air supplies, should remain in operation in order to retain control of the equipment that is still in operation.

If there is a major accident, an accurate head count will determine if anyone needs rescuing. Therefore, the facility managers must always know how many people are on the site at any one time. For larger facilities, they should also know roughly where those people are within the facility. If key-swipe cards are used, barriers can be placed between major operating sections so that a person's location is always roughly known. The persons responsible for running the unit should always know how many people are on the site at any one time. For larger facilities, they should also know roughly where those people are within the facility.

LOCAL EMERGENCY RESPONSE

If an operator or maintenance technician recognizes that the situation is out of control and cannot be addressed through emergency operations, he or she can declare an emergency. With regard to the leaking pump seal the operator may not be able to get near the pump due to fumes in the area or because he feels that doing so would put him in danger. Therefore, he calls in the facility's own ERT. The personnel on this team will be trained in the handling of emergencies, and they will be issued with the appropriate equipment and protective clothing.

GENERAL EMERGENCY RESPONSE

If the situation becomes too large for the ERT to handle then they can call for help from outside organizations, including the local fire department, ambulance services, and other facilities in the area. The emergency plan must take into account the fact that these people are not familiar with the particular process where the emergency has occurred. Where possible, these outside agencies should have the opportunity of training with the plant ERT.

In large industrial centers, such as the Texas Gulf Coast, the various plants coordinate their emergency response efforts in a mutual support system. So, if a facility has a fire and needs additional firefighting trucks, they will be supplied by neighboring units. If the incident is bad enough, there will be a ripple effect of emergency equipment moving toward the affected site from dozens of miles.

It is important that the press and the public be informed of what is going on at the site, particularly if anyone is in any danger. Facility management should take the initiative when communicating with the public, and they should be open and as forthright as possible (given that there will be a good deal of uncertainty in the early stages of the response to an emergency). Telephone lines and other links for public communication must be available, and they must have sufficient capacity that they do not become jammed with unnecessary calls.

RECOVERY OPERATIONS

As soon as the site is secure, and there is no danger to anyone, recovery of equipment and chemicals can start. At this time, the plant may contain many unexpected hazards, such as the danger of being struck by falling equipment that has had its foundations weakened by fire. Or there may be pockets of spilled chemicals in unexpected places. Some equipment may be contaminated with hazardous chemicals, and may need to be specially treated before it can be returned to service, or before the operators or maintenance personnel can use it.

INVESTIGATION AND FOLLOW-UP

If the incident is serious, an investigation as to its cause will start as soon as everyone is out of danger. It is particularly important to find out what happened if there are reasons to believe that it could happen again, maybe at another site.

EMERGENCY PLANNING

Once the nature of potential emergencies has been identified and analyzed, an emergency plan is needed.

ORGANIZATION AND PERSONNEL

Each facility should have a special organizational structure for emergency response. There should be a single Incident Commander, who is in complete charge of the facility during the course of the emergency, and who directs an ERT; everyone else on the unit, including the normal management, report to the commander. The normal chain of command is bypassed until the emergency is over. The Incident Commander does not have to be a senior manager. The management skills required to run the plant on a day-to-day basis differ from those needed during an emergency. Therefore, line management may choose to assign this responsibility to someone else, probably a shift supervisor or a unit superintendent. An emergency command headquarters should be set up with communications equipment and bunker gear for the ERT members.

The Emergency Plan must identify all the equipments that the emergency responders have and the equipments that they need to do their work properly. A map showing the location of fire hydrants, hose reels, safety showers, and other emergency equipment is needed.

EMERGENCY RESPONSE MANUAL

Table 12.1 provides an example of a Table of Contents for an Emergency Response Manual.

Table 12.1 Emergency Response Manual: Representative Table of Contents

- Introduction
- Emergency Operations
- Initiating an Alarm
- Response to Alarm in Other Areas
  - Use of Fire Monitors
  - Use of Fire Extinguishers
- Evacuation Procedures
- Adverse Weather Conditions
- High Water/Floods
- Command Headquarters
- Equipment and Clothing
- Equipment Failure
- Line Break
- Hose Break
- Excessive Flaring
- Loss of Utilities
  - Loss of Cooling Water
  - Loss of Steam
  - Loss of Control Central
  - Loss of Instrument Air
  - Loss of Plant Air
  - Loss of Nitrogen
- External Coordination
- Other Facilities in the Area
- Equipment Suppliers
- Fire Department
- Police Department
- Regulatory Agencies
- Emergency Shutdown
- When to Shutdown
- Sequence of Actions
- Responsibility for Emergency Shutdown
- Post-Emergency
  - Cleanup following a Spill
  - Decontamination
- Reference Material
- Alarm Codes
- Area Responsibilities
- Description of the Fire Water Header
- Telephone List
- Fire/Police/Ambulance Coordination
- Mutual Aid List
- Emergency Organization
- Emergency Control Center
- Emergency Drills
- System Test and Maintenance
- Terrorist/Security Threats

EMERGENCY PROCEDURES

Emergency procedures differ from normal operating and troubleshooting procedures in the following ways:

- They should be short and to the point. Ideally, the emergency procedures should be memorized—there is no time for reading books or manuals during an emergency.
- They should not require complex decision making.
- Because there is an almost infinitely wide range of accidents that might occur, the emergency procedures have to be flexible. Yet, because time is of the essence, the procedures also need to be rigid, short, and precise. In practice, a procedure will be written to address a general problem, such as a hydrocarbon fire. The operators and emergency responders then need to be trained to use that procedure as the basis of their specific response.

Most facilities have three types of emergency procedures:

1. Emergency *Operating* Procedures that describe how to run the plant when an emergency situation has been declared (say on another unit).
2. Emergency *Shutdown* (ESD) Procedures that describe how to conduct a crash shutdown, usually as the consequence of a fire or explosion.
3. Emergency *Response* Procedures that describe a site-wide response to an emergency that is affecting more than one unit.

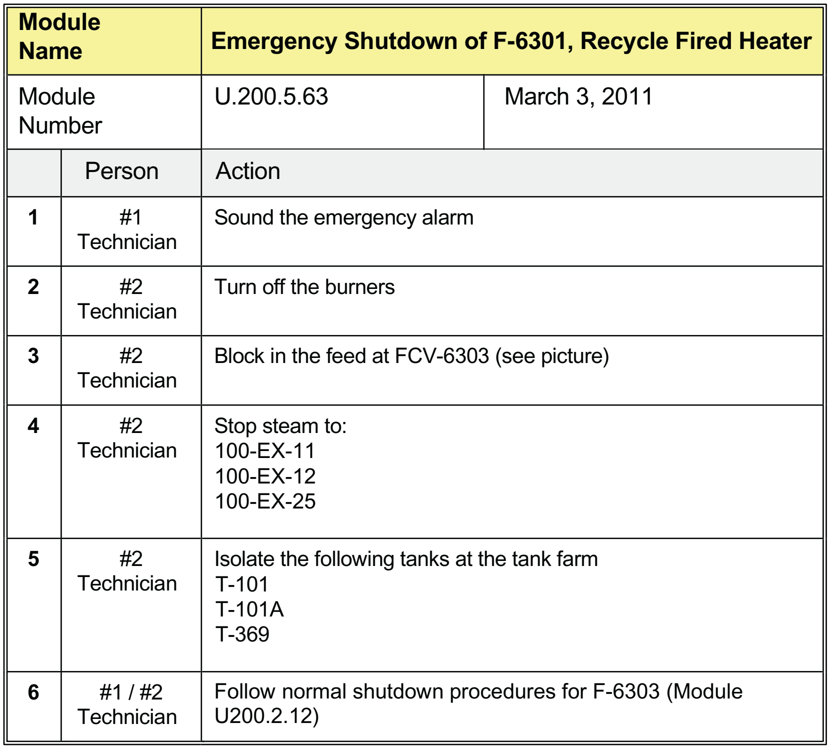
When writing emergency procedures it is important to make sure that they focus on bringing the facility to a safe state, at which time management and the operators can decide on the next step. It is tempting to turn an emergency procedure into an "Emergency Response and Restart" procedure. The danger with such an approach is that the operators may be tempted to restart before the facility has been secured, and before everyone understands what caused the ESD in the first place.

Emergency operating procedures can be written in the same manner as normal operating procedures. Figure 12.3 is an example of an emergency procedure module. It uses the same format as shown for normal operating procedures. However, the "Response/Discussion" column has been eliminated because action must be immediate and unambiguous.

EMERGENCY RESPONSE TRAINING

Although emergency procedures have to be written, they differ from normal procedures in one major respect: they are not likely to be used at the time of the event that they cover because, as already pointed out, technicians are not likely to have time to read a manual during an emergency. With regard to normal operations, if an operator is starting a pump, say, and has some concerns as to what to do, he can stop the operation, go to the manual, and find out what he is meant to do before taking further action. In an emergency, the operators and emergency responders must know what to do right away. In other words, they need to be trained in the use of the manual, and to drill as wide a variety of scenarios as possible.

Another reason for the importance of training for emergencies is that, during an emergency, operators are going to behave on instinct, and to make snap decisions. For example, on one facility



Module Name		**Emergency Shutdown of F-6301, Recycle Fired Heater**	
Module Number		U.200.5.63	March 3, 2011
	Person	Action	
1	#1 Technician	Sound the emergency alarm	
2	#2 Technician	Turn off the burners	
3	#2 Technician	Block in the feed at FCV-6303 (see picture)	
4	#2 Technician	Stop steam to: 100-EX-11 100-EX-12 100-EX-25	
5	#2 Technician	Isolate the following tanks at the tank farm T-101 T-101A T-369	
6	#1 / #2 Technician	Follow normal shutdown procedures for F-6303 (Module U200.2.12)	

FIGURE 12.3

Emergency response module.

a pump seal started leaking a flammable hydrocarbon. A supervisor from another unit was walking by. He instantly decided to walk quickly up to the pump, shut it down, and block it. He then reported his actions to the control room (which was close by). They started the spare pump, and returned the plant to normal operations within a few minutes. The supervisor's quick response prevented a potentially catastrophic fire from starting. Nevertheless, he probably made the wrong decision. If the pump had caught fire while he was near it, he could have been killed or seriously injured. Probably his best response would have been to report to the control room that a pump was leaking, and have the unit operators shut down the pump in an orderly manner. The essential point was that he had not been trained in how to handle this situation so he made a snap decision. It would have been much better if that facility had trained everyone on what to do in the event of an unexpected pump seal leak, and then held some drills on the topic.

COMMUNICATIONS

Coordination of the numerous activities involved in controlling a large fire requires a reliable means of communication. This is best accomplished with a dedicated emergency radio channel that provides rapid communication. Messengers should also be available to maintain communications should the radio system go down.

It is also necessary to develop a plan for communicating with the public and outside agencies, as discussed by Wilson (1992).

EMERGENCY SHUTDOWN

If a facility does suffer from a loss of containment due to a large leak from a valve, the rupture of a vessel or pipe, or the overflow of a tank, then an ESD sequence should be initiated. An ESD may also be initiated if the process has deviated outside its safe range and it is not being brought back to a safe condition in a timely manner.

The response to emergency situations is often controlled by the Safety Instrumentation System and its associated Safety Integrity Levels (SILs).

ESD HIERARCHY

An ESD is generally a hierarchical system that can perform a range of shutdowns from local to global depending on the extent of the emergency encountered.

Table 12.2 provides an example of the level of shutdown that can be followed, depending on the severity of the emergency. For each level it is assumed that the actions of the level before it has taken place.

A printer should record all the actions taken during an emergency, including:

- The sequence of events both before and following a trip
- All the operator actions, systems alarms, system input, and output status
- Color prints of graphic screens.

SHUTDOWN ZONES

The philosophy for determining the number and extent of shutdown zones should include an evaluation of the maximum permissible inventory of various fluids in any one zone. This will be an output from a risk assessment. The defined quantities are likely to be different for onshore and offshore facilities. The following should be considered for the analysis:

- Areas containing significant flammable gaseous inventory
- Areas containing significant toxic gaseous inventory
- Equipment items containing significant hydrocarbon inventory.

For vessels containing large inventories of liquid hydrocarbon or liquids above their autoignition temperatures (AIT), emergency isolation facilities should be provided. An emergency isolation valve should be provided on a vessel or column liquid outlet when inventories of flammable materials exceed values such as those shown in Table 12.3.

More stringent inventory limits may apply offshore.

Table 12.2 ESD Hierarchy

Level	Typical Causes	Suggested Actions to be Taken
1 Unit shutdown	• Deviation outside safe limits that cannot be brought under control • Automatic shutdown	• Production shutdown • Localized equipment shutdown • Shutdown of packaged equipment • Depressurization/blowdown (with a 1 minute delay timer to allow for operator override) However: • Where possible, other units will be kept running • Utility systems may be kept running
2 Process shutdown	• Loss of a utility such as instrument air, hydraulic pressure, electrical power • Hi-hi level in a flare knockout drum or scrubber	• Shutdown all process equipment • Shutdown all chemical injection • Offshore: shut subsea production valves
3 Emergency shutdown	• Manual ESD • Automatic ESD • Fire or explosion • Confirmed toxic gas detection in a nonhazardous area	• Close all ESD valves • Open all blowdown valves • Shut down all electrical equipment apart from life-support systems • Start fire water pumps, emergency generators • A read-only communications link should exist between the ESD and plant control systems to allow the display of alarm and status information to the operator However: • Continue power generation but switch from fuel gas to diesel until the diesel day tanks are empty
4 Facility abandonment (offshore)	Can be initiated manually from the Central Control Room or from selected, strategically located manual stations such as the helideck or lifeboat stations Only authorized personnel should initiate this action	• Total shutdown However, the following will remain operational: • Emergency lights • Navigational lights (offshore) • Public address and alarm systems • Diesel fire water pumps

SYSTEM RESET

Once the emergency is over, and assuming that the facility is fit for operation, a restart sequence has to be initiated. Generally, this means that all individual field inputs will have to be reset before the overall field reset can be applied.

Table 12.3 Vessel Content Limits (Typical)

Vessel Content	Inventory at Normal Liquid Level
LPG	>4 tonnes
Hydrocarbons above AIT	>5 tonnes
General hydrocarbons	>30 tonnes

FIRE AND GAS DETECTION

The best response to an emergency is to know about it as soon as possible, which means that instruments for detecting fire and/or gas releases should be provided in all sections of the facility. The signals will go to a central fire and gas detection system, which will call for the appropriate response to the alarm (either from the operators or the automatic instrumentation). Responses can include:

- Providing warning to the operators so that can start manual firefighting immediately.
- Providing an alarm to workers in specific areas so that they can evacuate those areas.
- Starting fixed fire suppression systems and special systems such as CO_2 deluge.
- Shutting down Heating, Ventilating and Air Conditioning System (HVAC) and electrical systems.
- Starting fire water pumps in standby mode.
- Initiating a partial or facility-wide shutdown.

A fire or gas alarm will be communicated through audible alarms, usually supplemented by a public address system. In high noise areas (80 dBA and greater) visible strobes can also be provided.

FIRE DETECTION

Fire detection systems used in the process industries are listed in Table 12.4, along with a summary of the advantages and disadvantages of each.

FIRE EYES/FLAME DETECTORS

A fire eye or flame detector detects the radiation from a flame. It requires line-of-sight capability—there must be no blockages between the instrument and the potential fire locations. A fire eye's field of vision usually covers a larger area than that of a heat detector, but it will not detect a smoldering fire as quickly as some smoke detectors. Flame detectors are not affected by air flow characteristics. They are suitable for inside or outside use, but they must be shielded from external sources of ultraviolet or infrared radiation such as welding arcs, lightning, or radiating black bodies such as hot engines or manifolds. Ideally, the fire detection system should have more than one fire eye detecting a fire so that false alarms can be weeded out. Flame detectors can be installed inside the enclosures of all engine-driven equipment; including turbine-driven generators, compressors, and emergency and essential generators.

Table 12.4 Fire Detection Systems

Type	Advantages	Disadvantages	Applications
Fire eye (ultraviolet)	High speed High sensitivity Moderate cost	Potential for false alarms Blinded by thick smoke	Outdoors or indoors
Fire eye (infrared)	High speed Moderate sensitivity Easy to test manually Moderate cost	Affected by temperature Subject to false alarms from the many other sources of IR radiation	Outdoors or indoors
Smoke detectors (ionization)	Detects smoldering fires Low cost	Easily contaminated Affected by the weather	Indoor use
Smoke detectors (photoelectric)	Detects smoldering fires Low cost	Easily contaminated	Indoor use
Thermal/heat detectors	Reliable Low cost	Slow Affected by the wind	Indoor use
Rate of heat rise detectors	Self-adjust for temperature and ambient conditions Rapid detection of growing fire	Affected by the wind	Indoor use
Fusible links	Does not need electricity High reliability Low cost	Very slow Heat must impinge	Outdoors or indoors
Low oxygen detectors	Warn of accidental release of inert gas	Do not warn of fire directly	Indoors—especially in confined spaces
Combustible gas detectors	Warning occurs before the fire starts	Require more than one instrument to confirm a release	Outdoors or indoors. Can be portable
Manual call points	Does not rely on instrumentation	Likely to be slow False alarms possible	Outdoors and at key locations indoors

Older types of fire eye detector, which worked in the ultraviolet range, sometimes had difficulty distinguishing between the fire radiation and other sources of radiation, such as that from a lightning bolt. Modern detectors, many of which use infrared, generally do not suffer from this defect.

SMOKE DETECTORS

Smoke detectors are particularly useful in those situations where the fire is likely to generate a substantial amount of smoke before temperature changes are sufficient to actuate a heat detection system and before a fire eye will detect a flame. Smoke detectors use a photoelectric beam between a receiving element and light source. If smoke obscures the beam an alarm is sounded. There are also refraction-type models that measure the light changes that occur within the instrument when smoke particles enter it.

Area smoke detectors are generally installed in buildings and accommodation areas. Where this is not practical—say in the galley area—other types of fire detector should be used. Actuation of a single smoke detector will initiate a fire alarm. If additional detectors sound an alarm, the equipment in the area of the fire and HVAC systems will be shut down.

HEAT DETECTORS

Heat detecting devices fall into two categories: those that respond when the detection element reaches a predetermined temperature (fixed-temperature types) and those that respond to an increase in temperature at a rate greater than some predetermined value (rate-of-rise types). The two types can be combined into a single instrument. They are generally installed when the use of smoke detectors is not practical, or as a backup to smoke detectors. They are used in the following locations:

- Engine-driven equipment enclosures
- Living spaces
- Maintenance workshops and laboratories
- Machinery and pump rooms
- Electrical rooms.

Actuation of a single thermal fire detector can be considered a confirmed fire condition, resulting in actuation of appropriate shutdown and fire protection actions.

FUSIBLE LINKS

Fusible links are made of low melting point materials designed to vent pneumatic systems as the fire melts the link. The depressurization can open fire deluge valves. Fusible links are very reliable, but they do require that the fire be well under way before they work, whereas other detectors, such as fire eyes, act more quickly. Depressurization of a fusible loop is considered to be a confirmed detection of a fire, and will automatically initiate appropriate shutdowns and activate fire protection equipment.

LOW OXYGEN DETECTORS

Areas that could be flooded with nitrogen, carbon dioxide, or halon-like materials should have oxygen detectors installed. Their use is particularly important in electrical switch gear rooms because inert gases are used to suppress fires. It is vital to know if the inert gas is accidentally leaking into the confined space.

COMBUSTIBLE GAS DETECTORS

Combustible gas detectors are generally installed in buildings and in the intakes to the HVAC air ducts. They can also be installed in outdoor areas that could have hydrocarbon vapor present, particularly remote areas such as truck unloading stations that may not have personnel present all the time. They should always be installed in living quarters, high-value computer facilities, and offices that store vital records.

They will typically have two levels of alarm: 20% LFL and 60% lower flammable limit (LFL). If multiple detectors are installed in a single location then a voting system can be installed. For example, if just one 20% alarm sounds then all hot work must stop but other work can continue as normal. If three 20% alarms or one 60% alarm sounds, then an emergency response is called for.

Special types of detector will warn of the presence of hydrogen, carbon monoxide, or hydrogen sulfide.

MANUAL CALL POINTS

Sometimes an emergency will be detected by a person rather than by the instrumentation. In such situations, manually activated call points (MACs) are used to declare an emergency and to activate the emergency response system. MACs are generally located at entrances to buildings and at strategic positions throughout process units, including escape routes. Each call point should be accessible from at least two different locations.

The typical MAC is of the open contact “Break Glass” type, suitable for Division 1 locations. MACs should be covered with a guard to prevent inadvertent alarm activation. Alternatively, the MAC can be actuated by a pulling action (to prevent spurious trips caused by someone pushing the button by mistake). The emergency response system should tell the operators and ERT which MAC was activated.

TOXIC GAS RELEASES

If someone is working outdoors and they are exposed to a toxic gas, it is generally a good idea to get indoors. As a rule of thumb the concentration of toxic gas inside a building is around a tenth of the concentration outside. In principle, were the gas release continue for a long time, the concentration of the gas in the building would eventually increase to the level outside. However, most gas releases do not go on for a long time. After the initial puff release, the amount of gas reduces, either because the inventory is exhausted or because the affected unit is isolated by the operator or by the safety instrumentation.

ESCAPE ROUTES

The following guidance regarding the design and use of escape routes, particularly offshore, should be considered.

- The main escape route will normally be around the outside of the facility, and should be as straight and level as possible; on large platforms, there will be parallel routes at different elevations.
- The escape routes should direct personnel to the primary temporary refuge (TR), with alternate routes to the lifeboat embarkation points.
- Escape routes should be clearly marked. Usually this is done through the use of yellow paint on the deck, with arrows pointing in the direction of the TR.

- The escape routes should be well illuminated at night.
- The escape routes should also be provided with plenty of signs at eye level. These signs should be designed and installed so that they can be seen when visibility is impaired. They also must be illuminated so that they are visible at night (and the lights should be provided with power from an uninterruptable power supply).
- Any tripping hazards, such as steps from one section of deck to another, must be clearly marked.

FIREFIGHTING

The most effective way to extinguish a hydrocarbon fire is to stop feeding fuel to it. This is often done with isolation valves that are located at the perimeter of the facility. These valves either stop the flow of fuel to the fire, as with remotely operated fire-safe valves in pump suction lines, or they direct the inventory of hydrocarbon to a safe location, as with emergency depressuring valves. The valves must be able to withstand the largest plausible fire radiation (this is often done by placing the valves behind an earthen wall or bund). If operators need to reach these valves during an emergency they should be provided with protected access and egress routes.

SINGLE FIRE CONCEPT

The fire water system and the firefighting equipment are generally designed to handle just one major fire at a time. In other words, the design capacity of major firefighting facilities is determined by the largest single fire contingency (this is analogous to the single event scenario concept used in relief valve design). Some firefighting systems are sized to handle less significant contingencies. For instance, foam concentrate requirements are usually determined by a tank fire rather than by the worst contingency, which may be a fire in the process area.

DELUGE SYSTEMS

Deluge systems are used to extinguish fires, and to dissolve, disperse, or cool flammable liquids and gases so as to minimize gas expansion and/or liquid boil off. Deluge water also cools structures to prevent deformation or collapse due to heat and can help additional leakage from flanges or connections, as well as a vessel rupture. In general, nonfireproofed vessels with liquid holdup of 3,500 liters or more should be provided with water cooling. Remote locations where a fire does not pose a significant risk to people or equipment may be an exception.

FIRE ZONES

For all but the smallest facilities fire zones are used. They ensure that firefighting systems are used only in those areas that actually have a problem. Offshore platforms, e.g., are typically divided into about seven zones.

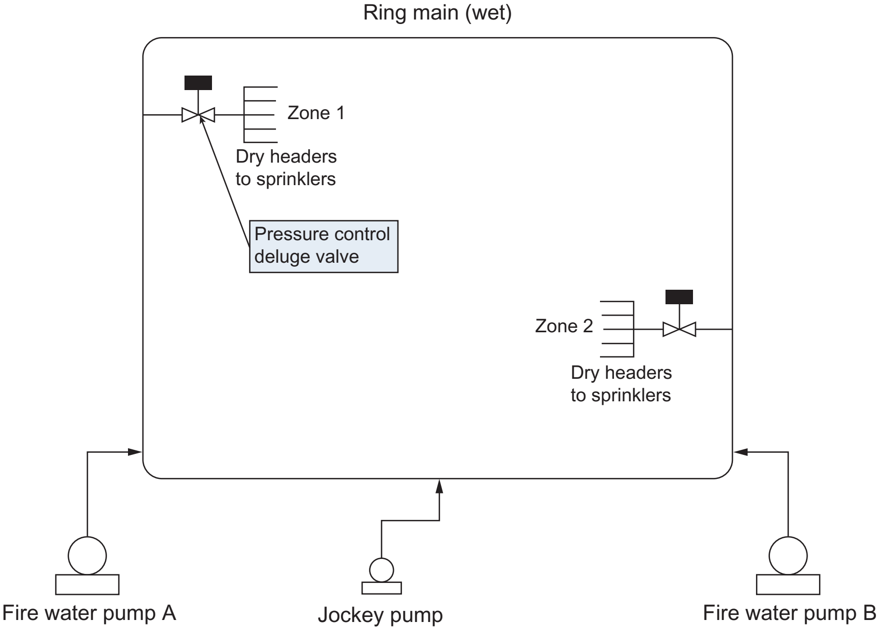

Ring main (wet)
Zone 1
Dry headers to sprinklers
Pressure control deluge valve
Zone 2
Dry headers to sprinklers
Fire water pump A
Jockey pump
Fire water pump B

FIGURE 12.4

Fire protection system.

Figure 12.4 shows the use of fire zones. A ring main goes around the entire facility. It is filled with water whose pressure is maintained with a jockey pump. Connected to the ring main are multiple zones. The fire water headers in each zone are normally dry. In this example, there are two fire water pumps, each of which has sufficient capacity on its own to handle the design fire case. These pumps are placed in different locations at the facility so that, if one is destroyed, the other will provide a full flow of fire water. It is common for them to have different power supplies—in particular, one of them will be driven by a stand-alone diesel motor that operates independently of the facility's utility systems.

If a fire occurs in one of the zones a fusible link will fail, causing the pressure control deluge valve (PCDV) to open and the main fire water pumps to start. Water will flow out of the sprinkler heads in that zone only. The PCDV can also be tripped manually.

Once the fire has been brought under control the system is reset. If seawater is used as deluge water, then it is important to flush the zone headers and deluge nozzles with freshwater, otherwise corrosion products will build up.

CHAPTER

13 AUDITS AND ASSESSMENTS

CHAPTER OUTLINE

INTRODUCTION

This chapter describes the audit process that is a necessary part of any process risk management program. Discussion is also provided regarding assessments and reviews.

An audit has been defined as follows (CCPS, 2011):

> A systematic, independent review to verify conformance with established guidelines or standards. It employs a well-defined review process to ensure consistency, and to allow the auditor to reach defensible conclusions.

In other words, an audit compares "what is" with "what should be." A management program is measured against an external standard such as a regulation or corporate benchmark. It is fundamentally a pass/fail test. For example, paragraph 1910.119(a)(1) of the Occupational Safety and Health Administration (OSHA) Process Safety Standard states that:

> the employer shall complete a compilation of written process safety information. . .
>
> This information shall consist of at least the following:
>
> **(i)** Toxicity information
> **(ii)** Permissible exposure limits

Process Risk and Reliability Management. DOI: http://dx.doi.org/10.1016/B978-0-12-801653-4.00013-8

(iii) Physical data
(iv) Reactivity data
(v) Corrosivity data
(vi) Thermal and chemical stability data
(vii) Hazardous effects of inadvertent mixing of different materials that could foreseeably occur.

An auditor who is examining a facility's process safety information against the OSHA standard will check that the information specified is written down and made available to those who need it. If those requirements are met then the audit requirement has been met. If they do not then the auditor has identified a deficiency or gap. It then becomes someone else's responsibility to turn the findings into recommendations or action items. An auditor's job is to objectively uncover deviations from the standards—no more, no less. The auditor is interested primarily in the letter of the law. Therefore, with regard to the safety information example just provided it is not the auditor's job to assess the quality of the information or the manner in which it is communicated.

The findings of a formal audit can lead to major improvements in the design and implementation of management systems; the fear of looking bad or of penalties is a strong motivator. [Concern to do with penalties was in evidence in the early 1990s. Although the value of process safety management (PSM) principles had long been recognized, it took a regulation from OSHA to force companies to complete their process safety work.]

In addition to audits, company management may elect to have outsiders conduct a review or assessment. This type of evaluation is less formal. A reviewer provides an opinion as to the quality of the risk management program. In the case of the initial start-up procedures just discussed, a reviewer will provide an opinion as to whether or not those procedures will actually help ensure that the facility starts safely and according to plan. He or she will develop that opinion by asking questions to do with the level of detail, the writing style, and the clarity of the instructions. Based on the answers to those questions, he will provide an opinion as to the effectiveness of the initial start-up procedures. (The terms *Verification* and *Validation* are sometimes used to make the same distinction between audits and assessments. Verification is concerned with ensuring that a facility meets the letter of the law or regulation; validation determines whether it is meeting the spirit of the same law.) Hence it is quite possible for a facility to satisfy audit requirements but to receive a low review evaluation.

It is therefore important to maintain a clear distinction between the roles of an auditor and a reviewer. For example, an auditor may find that a facility has a set of operating procedures, as required by regulation. A reviewer, however, could state that, in his opinion, the procedures are not well effective and should be rewritten.

However, an auditor may report that many of the elements of the standard to do with operating procedures have not been completed and so the audit requirements have not been met. It is natural at this point for the facility management to ask the auditor to offer an opinion as to the causes of these failings. If the auditor does offer an opinion then he or she has moved into a reviewer role. An auditor's opinions and insights may be extremely valuable, but they are not a part of the formal auditing process.

In the same vein, much of the literature to do with auditing stresses the "team relationship" that should exist between the auditor and the personnel of the facility being audited. According to this view, both auditor and persons being audited work together to develop improved performance of excellence. This rather rosy picture belies the fact that a formal audit is a structured process in which a facility's performance is measured against some predefined standard. The auditor helps only by identifying gaps. How management elects to close those gaps is not the auditor's concern. Indeed, given that the identification of gaps or deficiencies may result in penalties being applied or careers being held back, it would be naïve to believe that the auditor and the facility management are always "on the same team." Audits inevitably are adversarial, at least to a degree. A reviewer, however, *is* on the same team as his or her client. He or she is not measuring performance against an external standard but trying to find ways of improving performance.

FORMAL AUDITS

Audits are a fundamental component of any management system. By comparing actual performance with written standards audits help pinpoint that bad news. The standards may be external, such as those promulgated by a government agency or an engineering society, or they may be internal, such as corporate standards. Regardless of their source, the standards must be written down and they must be accepted by the facility that is being audited as authoritative.

Table 13.1 shows the OSHA regulatory requirement for auditing process safety programs in the United States. It is the representative of all effective audit protocols in that it contains within itself the following elements:

- Compliance with a defined, external standard
- Auditor qualifications
- Reporting
- Response
- Documentation

The audit and its report will generally be directed toward the facility's line managers. They are the ones who provide information to the audit team and who will have the responsibility of addressing the audit's findings. Senior managers are not likely to read routine audit reports in depth. They rely on their line managers to accept or reject the findings and then to implement the subsequent recommendations. Instead, senior managers are more interested in understanding how the audit findings can help them improve overall management systems. They also want to know if any major liability or safety issues have been identified.

Table 13.1 OSHA PSM Standard for Audits

1. Employers shall certify that they have evaluated compliance with the provisions of this section at least every 3 years to verify that the procedures and practices developed under the standard are adequate and are being followed.
2. The compliance audit shall be conducted by at least one person knowledgeable in the process.
3. A report of the findings of the audit shall be developed.
4. The employer shall promptly determine and document an appropriate response to each of the findings of the compliance audit, and document that deficiencies have been corrected.
5. Employers shall retain the two most recent compliance audit reports.

A concern sometimes expressed about audits is that they create "smoking guns," i.e., they identify problems which, if not addressed, could create liability—particularly if a serious incident occurs and in which that deficiency was implicated. Although this is a legitimate concern, implicit in the decision to conduct an audit is the commitment to address any problems that are uncovered.

Although an audit may be triggered by an external event such as a law suit or a serious accident, most audits are internal and are conducted according to a preestablished audit cycle. Some of these voluntary audits are carried out as if they mock regulatory audits, i.e., the auditors behave as if they are regulators who are investigating an accident. Not only does this tactic help identify problems related to regulatory noncompliance, it may also reduce a company's exposure to penalties should there actually be an accident because it demonstrates the company's commitment to doing a good job. In addition, mock regulatory audits familiarize the plant personnel with what a real audit might be like should there ever actually be a major event.

REASONS FOR AUDITS

Some of the reasons for conducting an audit are discussed below.

Accident follow-up

The most serious type of audit is that which is carried out following an accident in which someone was badly hurt or killed, and/or in which there was a major environmental release. Although rare, such audits can be expected to be both serious and very adversarial. The persons being audited must realize that the auditors (regulators and opposing attorneys) are looking to find fault and to assign blame. Specifically, they are looking for evidence that will justify the prosecution of the facility's management, and/or that will provide the basis for large financial claims. This type of auditor has no interest at all in helping the facility management improve its performance.

Regulatory/standards compliance

The second most serious type of audit is that which is conducted by an agency such as OSHA or the U.S. Environmental Protection Agency to see if the pertinent laws and regulations are being followed. (Such audits are sometimes triggered by a complaint by an employee or a member of the public). Although there may not have been an actual accident prior to the audit, the audit findings could result in serious financial penalties and even criminal action. Once more, the auditor and the facility personnel are most definitely not on the same team. This means that those being audited must be careful about revealing out-of-scope problems.

Stakeholder outreach

Audits are sometimes carried out in order to demonstrate to outsiders that a facility is safe and operable. These stakeholders could include members of the public, potential purchasers of the property (as part of the due diligence process) and the news media.

Voluntary check

Facility management may decide to conduct a regulatory style, mock audit on their own initiative in order to identify any weak spots should a real audit ever occur. Such audits are often conducted by companies that believe that they are in good shape, but they want to be sure that nothing has been overlooked.

For example, the OSHA PSM regulation requires that operating procedures be validated annually. It is possible that the procedures at a particular facility are of very high quality but have not been formally checked within the last year. An internal regulatory audit will highlight problems of this nature.

Companies that conduct voluntary checks tend to fall into one of the following three categories:

1. *We are the best*. Some companies believe that they have an excellent operational integrity/PSM program, but they want the auditor to double check this belief.
2. *We want to improve a good program*. Other companies believe that they have a good program but recognize that it can be improved. They want the audit to provide them with guidance and suggestions as to how to go from good to best.
3. *We have nothing*. The third type of company is one who recognizes that their program is severely deficient, and that fundamental changes are required. The audit establishes a baseline and a starting point.

Mock audits may help reduce a company's exposure to penalties should there actually be an accident because it demonstrates the company's commitment to doing a good job. They also familiarize the plant personnel with what a real audit might be like should there ever actually be an accident.

Insurance and business security

Insurance companies sometimes conduct audits—generally for one of two reasons. First, they want to establish the correct premium payment. Second, the insurance company wants to help their client company operate more safely so that there is less chance that payments will have to be made, and that, if they are made, that they are of a smaller size.

AUDIT STANDARDS

The first step in the formal audit process is to decide on the standard that is to be used as the basis for the investigation. Typically, there are three types of standards: regulations, industry codes, and internal standards.

Regulations

Management's first priority must always be to make sure that they are in compliance with the law. In some ways, this type of audit is the easiest to carry out because the audit questions are predefined. All that the auditor need to do is take a regulatory statement or sentence, and invert it to create the audit question. For example, the OSHA PSM standard to do with hazards analysis contains the following requirement:

> (3) The process hazard analysis shall address... (v) Facility siting;

The matching audit question becomes:

> Did the process hazard analysis address facility siting?

Reporting requirements

Most regulators require that audits be conducted at a prescribed frequency—say once in every 2 years. However, they do not require that the results of the audits be sent in to the agency unless the regulator requests a copy of the audit report. (In this regard, the Safety and Environmental Management Systems (SEMS) audit requirements are unusual—companies operating offshore are required to send their audit reports regardless of whether the agency requested them to do so).

Industry standards

The auditor may be asked to check the facility's performance against industry consensus standards from organizations such as the American Petroleum Institute (API), the National Fire Protection Association (NFPA), and the American Society for Mechanical Engineers (ASME). Such standards represent an industry-wide consensus as to what constitutes safe and effective performance. They may not carry the full force of law, but they are authoritative, and are often cited in lawsuits.

Many companies have also committed to quality-control standards, such as ISO 9000 and ISO 14000. There is often considerable overlap between these programs and process safety systems.

Internal standards

Many companies find that industry standards are not detailed or specific enough to cover the particular circumstances to do with their particular operations and technology. For example, a company that manufactures a hazardous chemical that is used by very few other organizations may choose to write its own standards for handling that chemical. These internal standards can be used as the basis of an audit protocol.

AUDIT FREQUENCY

The frequency with which audits should be conducted is often driven by regulatory or standards requirements. If a company is able to set its own schedule, a risk-based approach such as that described by DeWitt (2005) can be used. Other factors to consider are the results of previous audits, the number and severity of incidents, and the number of changes to the process that have been made.

AUDIT PERSONNEL

An auditor must always be independent of the facility being reviewed and must always have complete freedom to observe and report on all aspects of the operation covered by the auditor's Scope of Work. His or her outside perspective not only ensures that there is no conflict of interest; it can also provide alternative points of view that can be helpful to the people working within the facility if he or she is asked to offer advice following the formal audit.

An auditor must always be a person of high integrity. There should be no doubt in anyone's mind that the audit is being conducted fairly, and against objective standards. There should be no suspicion that the audit is "wired" to give a desired result, or to protect certain individuals or departments.

Most auditors are paid by the facility being audited. Hence, in principle, they can be influenced by those who hired them. However, a good auditor knows that his or her professional reputation rides on his or her objectivity, integrity, and balance. Consequently, the auditor will report the facts, as he or she sees them, regardless of external influences. If toes get trodden on, then toes get trodden on. The auditor makes his or her living by maintaining professional independence and integrity.

Outside auditors

Outside auditors generally come from one of the following four groups:

1. A regulatory agency
2. Attorneys representing plaintiffs following an accident
3. An outside company that specializes in process safety work
4. A person from within the client company but based in another department

The use of outside companies should make the audit more objective. Outsiders are not likely to be familiar with the processes being audited, nor are they involved with the interpersonal relationships on the unit. For them, this project is only one of many, so they will not be hesitant about issuing critical findings. A second benefit of using an outsider is that he or she will bring a fresh perspective based on their knowledge of how other companies and facilities operate. In particular, he or she may identify hazardous situations that employees at a facility have learned to live with, but that would not be accepted as being safe elsewhere.

An outside auditor should not provide follow-up services to the audit. Such services represent a conflict of interest, with the exception of reviewer-type comments, as discussed above.

Internal auditors

Large companies sometimes appoint auditors from other departments or facilities within that company. These people act as if they are completely independent of the facility that they are auditing. In practice, achieving this independence can be difficult for four reasons:

1. The company as a whole may have some blind spots that are common to all of their facilities. Every company has its own culture, and it may be that internal auditors will not realize that such blind spots exist.
2. Internal auditors must rise above their own knowledge of company problems and internal personal relationships. Such knowledge may not be explicit, and may even be unconscious, but it is still a factor, and may affect the auditor's judgment.
3. Internal auditors do not see the facility with an outsider's eyes. Hence they may lack "helicoptic vision," i.e., the ability to rise above the minutiae of a problem to see the surrounding countryside. In other words, they can't see the forest for the trees.
4. Finally, it has to be recognized that internal auditors and those whom they are auditing ultimately work for the same bosses. Their chains of command may not join until high up in the organization, but they are joined. Consequently, there will always be concerns—whether justified or not—that the auditor is not truly independent. He or she knows that, sooner or later, it is possible that he may be working directly with or for the people being audited. In point of fact, most auditors would not actually let such matter affect their judgment. But auditing is not just about facts—it is also about the perception of those facts, as summed up in the Chinese proverb, "Do not tie your shoes in a melon patch; do not adjust your hat under a plum tree." So with auditing, there needs to be a *perception* of detachment and objectivity.

When a company is conducting a review rather than an audit, the appearance of independence is not so important. Nevertheless, it still makes sense to use an outsider to lead the review because he or she will bring fresh points of view and fresh insights to the way the facility is operated, which is one of the most important reasons for conducting the review in the first place.

Team composition

A short audit of a simple unit may be carried out by a single individual who is knowledgeable in the process. However, most process facilities are large and complex so a multiperson audit team is needed. The team should be led by an experienced auditor. He or she is not likely to possess detailed knowledge to do with the process that is being audited so support will be needed from specialists in area such as the following:

- Process engineering
- Electrical engineering
- Instrument engineering
- Maintenance/mechanical engineering
- Quality assurance
- Process safety/risk management

AUDITOR ATTRIBUTES

Audits are stressful for those being audited. No matter how good a plant's performance may be, there is every chance that the auditor is going to find something that indicates a problem; and most problems and deficiencies are eventually traced back to specific individuals. Therefore, the personal attributes and demeanor of the auditor are extremely important. Some of these attributes include the following:

- Interview skills
- Technical knowledge
- Writing skills
- Demeanor

Audit service providers

Some companies specialize in providing audits for their clients. These companies are sometimes referred to as Audit Service Providers or ASPs. They have the systems and people in place to conduct a professional audit. The standard reference for meeting ASP requirements is ISO/IEC 17021, *Conformity assessment—requirements for bodies providing audit and certification of management systems*. The following is from the abstract for that standard:

> ISO/IEC 17021:2011 contains principles and requirements for the competence, consistency and impartiality of the audit and certification of management systems of all types (e.g., quality management systems or environmental management systems) and for bodies providing these activities.

Certification of management systems is a third-party conformity assessment activity. Bodies performing this activity are therefore third-party conformity assessment bodies.

Another standard reference document is ISO 19011, *Guidelines for quality and/or environmental management systems*.

ASPs are generally required to develop and implement standards that address issues such as the following:

- Confidentiality of information
- Appointing audit teams with properly qualified leaders and auditors

- Finding and appointing Subject Matter Experts (SMEs) as needed
- Ensuring that the auditors' qualifications are kept up to date

Interview skills

A critically important skill for an auditor is interviewing. In particular, he or she needs to be someone who can ask open-ended questions and is a good listener. As discussed in Chapter 12 (Incident Investigation) the auditor should listen to what people actually say, focus on facts not opinions, and establish trust with the people they are talking to.

The auditor will have to work with a wide variety of people. He or she will be interviewing a full gamut of personalities and job descriptions, ranging from the facility manager to temporary workers who have no knowledge of the plant culture. This means that the auditor will have to be empathetic, i.e., he or she needs to understand where people are coming from, and what they can be expected to know. (Empathy is different from sympathy in that the auditor may relate to a person's concern but still retains his or her detachment and objectivity.)

In addition to listening to what people say, the auditor should also be able to read body language. Some workers may have trouble verbalizing what they want to convey—but their body language may indicate that the auditor should pursue a certain line of inquiry.

The auditor should keep good notes that document the results of interviews, document reviews, and equipment testing. These notes will be essential for communicating findings.

Technical knowledge

The auditor must possess good technical knowledge of the process industries. It is unlikely that the auditor will be an expert in the technology of the process being investigated. However, he or she should possess a good understanding as to how process plants work, and what items to look for. The auditor also needs to be familiar with regulatory requirements in the industry, and should have a good knowledge of the pertinent codes and standards.

A catch with using experienced people for formal audits is that they may be too sympathetic to the persons that they are auditing. Hence, they will want to try to help, not to evaluate; thus degrading their objectivity.

Writing skills

The final product of any audit is a written report. Therefore, the auditor should possess good writing skills. He or she must be able to quickly prepare a report that is complete, readable, accurate, and fluent. It is good to deliver the report quickly while everyone's mind is on the audit and has not moved on to the next set of activities.

Demeanor

Throughout the audit, the auditor must be pleasant and empathetic and conduct himself in a professional manner. The auditor should not make any negative comments during the audit process, but he or she should always express appreciation for the effort that the client is making to provide information and assistance.

Auditors need to be circumspect—they should not make off-the-cuff comments that could be misinterpreted and exaggerated by those listening, nor should they offer comments on matters that are not related to the audit itself. In other words, throughout the audit, the auditor must be friendly and empathetic without losing sight of the fact that he or she is an outsider who is not involved with local organizational or personal issues. The auditor should not make any negative or positive comments as to how the audit is going during the audit process, but he or she should always express appreciation for the effort that the client is making to provide information and assistance.

Occasionally the auditor will have to work with one or more persons who are openly antagonistic, uncooperative, and even hostile to the audit process, and to the auditor himself. In such situations, the auditor must not give up on digging out the necessary facts, while always maintaining a professional demeanor.

The auditor must be careful not to personalize his or her work. The identification of a deficiency does not symbolize success, nor is it a personal triumph. The auditor's job is to report facts as dispassionately as possible.

THE HOST COMPANY

It is often necessary to brief those people in the company that is being audited on how to work with the auditors. Items to be considered include:

- How to answer all questions fully and honestly, without volunteering information that does not pertain to the question being asked.
- The use of gifts. Inspectors from some government agencies, e.g., cannot accept even a cup of coffee.
- How to respond when deficiencies or problems are uncovered.
- The purpose of the opening meetings.
- Whether to allow the auditor independent access to people and records, or whether the auditor should always be accompanied by a staff counterpart, who will serve as a watchdog.
- When to refuse to answer questions on grounds of not having sufficient authority or knowledge to make a trustworthy reply.
- Knowledge of which records are open for inspection.
- Whether to take matching information. For example, if the auditor takes pictures, his or her escort must know whether to take a picture of their own at the same time so that there is independent verification of the auditor's findings.

Those being audited should always keep in mind the importance of the impressions that they make. An auditor will be impressed not only by a high-quality process safety or operational integrity program, but also by one that looks good, i.e., one where the documentation is neat and tidy, and it is easy for the auditor to find his or her way around the system.

First impressions

The facility management needs also to recognize that auditors are human; as such, they will always be impressed by a program that looks good. In particular, management should never forget that "you don't get a second chance to make a first impression."

For example, if a facility has written first-class operating procedures, it makes sense to publish them in high-quality binders, with lots of color pictures included with the text. The auditor who reads these procedures is likely to be impressed. This does not mean that appearance is everything—the procedures themselves must also be complete, accurate, and up to date. Nevertheless, their quality will appear much greater if they also look good.

Employees

Just as the auditor should conduct himself in a professional manner, so do all employees at the facility being audited should behave calmly and without emotion—regardless of how they really feel. This is particularly true if the audit is basically hostile in tone—presumably following a serious accident. In particular, employees should understand that it is their responsibility to answer questions truthfully, but to say no more than the question requires. Especially, they must learn not to volunteer information. Such information could be used against them or their company.

On occasion, the persons being audited may not know the answer to the questions posed by the auditor. They must state that they do not know an answer, or they do not have the required information. They should then assist the auditor with finding the information from someone else in the facility.

PLANNING THE AUDIT

Like any other management activity, an audit should be properly planned. In particular, as many as possible of the administrative details and information acquisition steps should be carried out before the audit team actually starts work. The plan should clearly define the objectives of the audit, the geographical and organizational scope of work, and the anticipated amount of time that will be needed.

Audits are generally organized around the following steps shown in Table 13.2

Goals

Before the audit starts, the facility management must decide what it intends to gain from the audit in addition to simply verifying that they are in conformance with a regulatory standard. For example, the auditors can be asked to measure compliance with additional standards such as ISO 9000. Also, the audit team needs to know whether the present audit is meant to evaluate compliance with the recommendations and findings of the previous audits.

Topics that can be raised while setting goals include the following:

- The business objectives of the facility
- Safety or environmental targets

Table 13.2 Audit Steps

1. Determine the goals of the audit.
2. Establish the audit standards to be followed.
3. Define the scope and budget.
4. Conduct the audit.
5. Issue a report.
6. Have a closeout meeting.
7. Follow-up.
8. Provide guidance as requested.

- Management philosophy and organization
- PSM objectives
- Regulations and standards

The parties involved need to determine if the audit report should focus just on findings that identify deficiencies, or whether it should comment on other issues that were identified as being worthy of attention. Also, it should be determined if positive findings, i.e., items that were considered to be exceptionally good, should be reported on.

Determine the audit standard

The next step in the audit process is to create a standard or protocol. With regard to risk management and PSM, the standard is generally provided by an external organization such as a regulator or corporate office.

Scope

The physical or geographical scope of the audit must be clearly defined. This is generally a two-step process. First the fraction or percentage of facilities to be audited needs to be determined. This number is sometimes provided by a regulatory agency. For example, the SEMS audit program requires that 15% of a company's facilities be checked, and that different types of facility should be included.

The next step is to clearly define the physical boundaries of the audit. Figure 13.1 is an example as to how this can be done. The shaded area is to be audited; the remainder is excluded—including the process links between Areas 100/200 and the remainder of the facility.

It is important to decide to what extent utility systems are to be included in the audit. Because they provide physical connections between units, utilities run everywhere. For example, systems

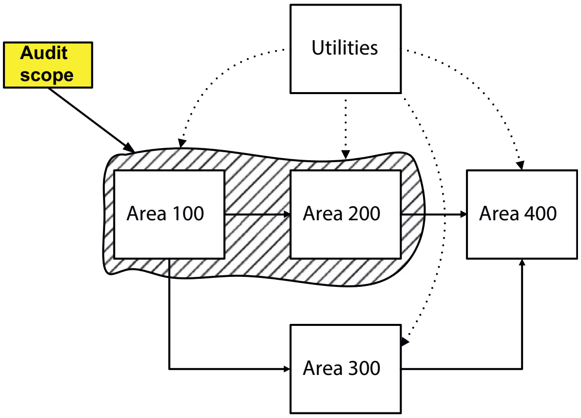


FIGURE 13.1

Geographical scope.

such as steam, cooling water, and instrument air are to be found in all parts of a facility. Therefore, if the auditor is analyzing just one section of a facility, he or she has to know exactly which utilities are included, and where the boundaries are to be drawn.

The problems associated with connectivity and utilities have provided the basis for much legal discussion with regard to process safety. After all, all plants are connected to the "outside world" in many ways, often through utility systems such as electric power and water sewers. The existence of these connections provides connectivity (in the legal sense) between the process and outside facilities. These issues need to be resolved before the audit starts.

The audit team also needs to establish whether stand-alone items such as skid-mounted units that are provided complete and ready-to-go by outside companies, are to be included in the scope.

Budget

The final part of the planning process is to develop a budget. Since process safety is an ongoing program, there really should be no need for special efforts before the audit starts. However, there will be some costs associated with the audit work. For example, one employee may be designated as the point contact for providing written information to the auditors. If the audit is known about ahead of time some of the facility's documentation may be reprinted and reorganized, but such activities should be minimal. If the auditor is hired from outside the facility there will be a direct out-of-pocket cost. Qualified auditors usually charge a high hourly rate because their skills are not widely found.

In addition to funding, quality personnel are needed. On the facility side, there will be some preaudit preparation. Typically, some of the necessary documentation will be collected and organized so that the auditor's time is not wasted. It may also be necessary to print fresh copies of pertinent documents. However, the major use of personnel time will be during the audit itself, when key personnel are interviewed and records are researched.

The biggest cost of most audits is the funding needed to carry out the recommendations that address the auditor's findings. However, as has already been noted, if a company commits to being audited, they have also committed to the investment required in the follow-up.

Schedule

Although most process safety audits are quite short (typically just a few days) it is still important to prepare a formal schedule. Not only does a schedule minimize problems such as two auditors wishing to speak to the same person at the same time, it also is a courtesy to the host company. Most people are very busy, and they do not want to waste time waiting for an auditor to show up.

Generally, the order in which the elements of the risk management programs are audited is not important. Logistics often force a particular schedule to be implemented. For example, if the plant maintenance engineer is only available on a particular day, then that will be the time to review mechanical integrity with him. However, the order in which items are discussed may be directed by the results found to that point. For example, if a problem to do with the emergency procedures is found, the auditor may suspect that the same problem will occur with the operating procedures. Hence, he may choose to review both of these items at the same time.

Leaving these considerations aside, the auditor should start with those items that are likely to have general application throughout the entire facility. That way, if he finds a problem, his subsequent investigation will serve to confirm or deny that first impression. For most plants, therefore, the following three items provide a starting point:

1. Employee Participation because of its central importance to process safety
2. Piping and Instrument Diagrams (P&IDs) because they provide the informational base
3. Management of Change (MOC) because of its criticality in preventing uncontrolled change.

One-point contact

It is crucial that both the audit team and the facility each have a one-point contact. All communications such as requests for information and schedule adjustments should go through these persons.

Preaudit activities

Before the audit starts, the host company will probably spend some time preparing for their visitors (unless the audit is unannounced). This period of time can be used to make corrections to items that obviously require attention.

AUDIT FORMS

Audit forms will usually contain four major sections:

1. A question that refers back to the appropriate standard
2. A check box that provides space for the answer to the above question
3. Space for recording where the information came from
4. Space for discussion and comments

Usually, each question has one of four possible answers:

- Satisfactory: Meets requirements
- Unsatisfactory: Does not meet requirements
- Not audited
- Not applicable

Table 13.3 provides an example of an audit protocol design (the "Not Applicable" answer is omitted.)

The first square in the Protocol contains the number 3.9. This is the number of this particular question. Below it is the question itself, "Are inadvertent mixing scenarios anticipated?" This question matches the requirement that the employer must compile information to do with the "Hazardous effects of inadvertent mixing of different materials that could foreseeably occur."

The next two squares contain a Y/N representing a Yes or No response to the question. There is no "Partial" response; a "Partial Yes" is recorded as "No." There is, however, an NA space that stands for "Not Applicable." Not all plants have to meet all the requirements of the standard, so space must be provided for this.

The next two rows (Facility and Area) describe which areas the question is being applied. In order to reduce the amount of space used, this type of information could be put on a single cover page.

Table 13.3 Audit Protocol Design

3.9 Are inadvertent mixing scenarios anticipated?		Y	□
		N	□
		N/A	□
Facility			
Area			
Chemicals			
Persons interviewed	Name	Title	Date
Documents reviewed	Document title		Date
Notes			

The Chemicals row lists those chemicals that are present that could cause an accident if accidentally mixed.

The next row provides space for the names and titles of the people who were interviewed in order to obtain the information necessary to answer the audit question. Similarly, there is space for the names of the documents that were reviewed as part of this audit.

Finally, there is a Notes section. If more space is needed, observations can be recorded in separately, with the notes linked to the question number.

CONDUCTING THE AUDIT

An audit generally consists of a combination of interviews and review of documentation. Ideally the one verifies the other. For example, the auditor may ask an operator how he performs a certain task (the interview). Having been told, he will then ask for a written procedure that confirms this (documentation). Or the auditor may review a Material Safety Data Sheet (MSDS), and then ask the operator to verbally confirm that he understands the major safety issues to do with the chemical in question.

The auditor will have to be selective regarding the documents that he reads and the people who are chosen for interviews. There simply is not enough time to read and discuss everything. An experienced auditor will sense where the soft spots are and, based on the information received to that point, will use his or her experience to choose the follow-up questions. For example, if the operating procedures on the facility being audited are much shorter than the operating procedures on other similar facilities, he or she may choose to investigate this element with increased scrutiny. The shortness of the procedures may indicate that the facility has a deficiency in this area (or it may mean that they were very well written).

Formal audits must be objective and all findings must be based on observed, verifiable facts. Ideally, two auditors would reach the same conclusions when asked to analyze the same situation with regard to the same baseline standard. If the auditor does provide an opinion, it should be very clear that he or she is doing so.

Auditor preparation

The auditor needs a good general knowledge of processes in general in order to be able to conduct an effective audit. However, the auditor cannot initially have a detailed knowledge of the facility or of the process that is to be audited.

It is suggested that, at this stage in the audit process, the auditor should learn the details of the process and the facility that he or she is about to audit. This includes learning the client's organizational structure, the equipment being used, plant capacity, age of the facility and of the equipment, and the means used to bring materials into and out of the facility. This work must be done before the audit starts; otherwise, the auditor will waste a good deal of everybody's time while he gets up to speed.

Kick-off meeting

The audit will start with a kick-off meeting. The audit team and representatives from the client company will meet to discuss the way in which the audit is to be carried out. Basically they will discuss four items:

- The objectives of the audit—why it is being performed
- The mechanics of the audit, including issues such as schedules, budgets, and facilities to be covered
- The scope of the audit, including regulations to be covered
- The depth of the audit questions on technical issues

The kick-off meeting is not a one-time affair. Every time a new person from the facility is brought into in the audit, he or she should have their own kick-off meeting, that provides them with an explanation as to what is going on, and what is expected of them. In particular, it must be made clear to those people who have not been through an audit before that the aim is not to find fault with individuals but to identify limitations in the management systems.

During the kick-off meeting, background documentation, including items such as those listed below, can be made available.

- Permits
- Incident reports

- Logbooks and DCS records
- MSDS and other safety information
- An organization chart
- A plot plan, including information on population concentrations such as schools, hospitals, and prisons
- Process description
- Previous audits and inspections (including the action items that they generated)

Either at, or just before the kick-off meeting, the schedule for the audit should be developed. The creation of a schedule is particularly important if the audit is being carried out by a team.

Plant tour

The inspection will usually start with a plant tour, during which the auditor will obtain a general overview of the facility and its operations. During this tour, a management representative should accompany the inspector—particularly if the auditor is from a government agency or is representing a plaintiff. The auditor should inspect areas where which may normally be overlooked, such as platforms at the top of large columns or behind the control panels.

Information collection

Having determined the standards, information must be collected. This step consists of collecting and reading documents, interviewing operators and maintenance personnel, and conducting a plant tour. Wherever possible, auditors should try to cross-check information with information from a different source. For example, the auditor can check an operating procedure by asking an operator to demonstrate how a particular task is carried out in the field. Or he can check the MOC system by ensuring that a field change that is currently taking place was properly analyzed, and that it was marked up on the P&IDs.

Role of personnel

With regard to the role of people on a facility, an audit team should consider the following questions:

- Are people available?
- Are they present?
- Are they fit?
- Are they capable?
- Do they know what to do?
- Are they willing?
- Are they aware of what is going on around them?

Interviews

The interview is at the heart of most audits (interview skills were discussed earlier in this chapter). The auditor systematically works through a series of questions with one or more of the people who work at the site. Typically, the process follows these steps:

1. The auditor asks the interviewee to describe his work. This gives the auditor a sense of the boundaries for this particular interview.

2. The auditor then works through a questionnaire that corresponds to the pertinent standard. The OSHA standard with respect to emergency response, e.g., requires that "the emergency action plan shall include procedures for handling small releases." The auditor will ask to see the emergency action plan, and will ensure that it contains provision for handling small releases.
3. The auditor will then pursue the question in more detail, often using the other elements of the standard for guidance. So, using the above example of emergency response to small releases, the auditor will ask the interviewee for copies of the procedures to handle this scenario, evidence that the operators have been trained in it, documentation that contract workers know what to do in the event of a small release, and so on.
4. The auditor will then move on to the next question. He or she is always watching out for systemic problems. If one particular procedure is not in place, that may be an oversight. If, however, it is found that there is a general lack of emergency procedures, this indicates a more fundamental management problem. The auditor can also use the first answers as guidance for where to focus later on in the audit.

During the interview the auditor must take notes, otherwise he will not be able to verify his findings. The note-taking should be as discrete as possible, so that the interviewee is not distracted or worried.

In principle, voice recorders are an excellent way of capturing information during interviews. No matter how skillful the auditor may be at capturing statements in his notes, it is inevitable that he will miss some of the statements that are made. If the interview has been recorded, the auditor has an opportunity to go back and make sure that he captured all the information provided to him. In practice, however, recorders are rarely used because the person who is speaking may fear that any off-the-cuff comments could come back to haunt him. Consequently, the interviewees become very cautious to the point where they simply do not communicate the information that the auditor needs to do his job properly.

The auditor should use a mix of open and closed questions. An open question such as "How are contract workers trained?" invites a discursive response. A closed question such as "Are the contract workers trained?" invites a Yes/No response. Leading questions such as "Have you started training contract workers, yet?" should be avoided because of the bias that they introduce.

One problem that sometimes occurs with regard to interviews is that the interviewee's manager or supervisor may wish to be present during the conversation. It is up to the auditor to decide if this is acceptable (with a regulatory audit, legal requirements may come into play). The presence of a manager may inhibit the interviewee, and prevent him from describing the situation as it is, rather than as it should be. Moreover, the manager may attempt to direct the audit in ways that make him look favorable. This is particularly the case with issues to do with communication and training because of a possible gap between theory and reality. A manager may point out that written policies and programs are available for these topics, but he may be reluctant to have an auditor speak to an operator because the operator is completely unaware of these written policies.

On-site inspection

The auditor should verify information by field inspection wherever possible. For example, an operator may have a procedure for carrying out a task, but, when demonstrating what he actually does when working with the plant equipment, may demonstrate that his actions are not in conformance with the procedure.

Closeout meeting

At the conclusion of the audit, the audit team should have a closeout meeting with the host company. This meeting will provide an opportunity for the auditors to provide an overview of their results and to highlight any serious issues that may have been identified and that require immediate attention. The response of the facility personnel to these preliminary findings can be incorporated into the final audit report. If agreeable to both parties, it is possible to have debriefing meetings as the audit progresses (government regulators would probably not agree to this).

REPORT

Once the audit has been completed a report must be issued. An audit report should stress the reasons for conducting the audit, and should make explicit the standards against which the audit is being conducted. Discussion as to the organization and content of a representative professional report is given in Chapter 26. Specific comments to do with audit reporting are provided below.

Draft report

The auditor should prepare a draft report as quickly as possible. No matter how effective the auditor's note-taking may have been there will always be some observations and facts that were not properly written down. These should be captured before the auditor forgets them. It also gives the client an early opportunity to correct any factual errors in the report.

Where feasible, the report should be presented in a meeting, particularly if it contains difficult or sensitive findings. The auditor should expect to be questioned and challenged as to his conclusions, and it is best if he can do this face to face.

How the draft report is handled at this point will depend on the relationship between the auditor and the client. If the audit is truly formal, then the facility personnel will not be provided with a chance to review it (this is particularly true if the audit is by a regulatory agency, or is organized by opposition attorneys). However, if the audit is internal there should be no problem in having the facility personnel look over the findings before the final report is issued. They cannot change the overall tone of the report, nor do they have the authority to change any of the statements in it. Nonetheless, they may be able to point out factual errors or identify significant typographical problems that could lead to a misunderstanding.

Sometimes a client will wish to add information concerning action that was taken immediately following the audit, particularly if the auditor had identified a serious problem that was corrected right away. This type of information should not be included in the audit report itself, which is based on observations at a particular time.

It is important that the auditor has someone within his or her own company review the report before the client sees it. The purpose of this review is to catch any obvious, and potentially embarrassing, errors. Items to watch for include the following:

- Inconsistency between reported facts
- Inappropriate language
- Opinions masquerading as facts or observations
- Completeness, particularly with respect to the standard being used

Generalities

At all times, the auditor must be careful to distinguish between what was observed and what he deduced, and must avoid the trap of slipping into unconfirmed generalities. For example, he may have asked for copies of the inspection programs for three different pumps. On finding that there is no inspection program for these pumps, he could write, "There is no pump inspection program." Actually, the finding should read, "Inspection programs for pumps…were not available." He may then go on to say, "Based on the above finding, there is reason to believe that the pump inspection program is deficient." Similarly, if he or she notes on two occasions that the facility was carrying out temporary operations without having written procedures for them then the report should state, "Observed that two temporary operations were being carried out without written procedures." The report should not state, "Facility does not have a policy for writing temporary procedures, as evidenced the following two incidents." Even if someone tells the auditor that a policy for writing temporary operating procedures does not exist, the auditor should make it clear that he is reporting that statement. The only conclusion that the auditor can draw from that statement is that that person is not aware of the existence of such a policy, not that such a policy does not exist at all.

The above comments do not mean that there is no place for general conclusions and deductions, particularly in reviews as distinct from audits. However, such conclusions should be identified as such. In the above example, the auditor might write, "There appears to be no policy for writing operating procedures for temporary operations. This conclusion is based on the following observations…"

Report distribution

It is important to prepare a list of who receives the draft and final reports. A wide circulation will allow many people to understand what the audit found and to take corrective actions in their particular areas. But an audit report can create legal liability problems so the distribution list should also be screened by the company's legal department. Also, it needs to be recognized that the report could be embarrassing for some of the managers, so their concerns should be recognized.

It is important that the report not be screened too heavily by middle managers. In Chapter 12—Incident Investigation—it is pointed out that the causes of major incidents had often been identified before the event happened, but that critical information had been either diluted or buried (a *vignette* on this topic is provided in Chapter 2). One of the case studies discussed in Chapter 3 is to do with an explosion that occurred at a facility in Gramercy, Louisiana. After that event the facility manager made it clear that all safety and environmental audit reports should land directly on his desk. He did not want any of his middle managers screening the findings in any way.

Letter of certification

The audit should be certified by the auditor. A representative Letter of Certification is provided in Table 13.4 for use in PSM work.

Audit verification

This section provides a clear description of how the audit met the requirements of the standard or regulation against which the audit was being conducted. Table 13.5 provides an example. It lists the paragraphs associated with the auditing standard in the left-hand column (in this case taken from the

Table 13.4 Representative Letter of Certification

The attached audits meet the requirements of the OSHA PSM standard, 29 CFR 1910.119.

- The audits were conducted within the 3-year program required (paragraph o.1).
- One of the auditors (the process safety manager at the facility) was knowledgeable in the process (paragraph o.5).
- One of the auditors (from the auditing company) was knowledgeable in audit techniques (paragraph o.5).
- The audit included outside field work (paragraph o.7).
- Sample sizes were big enough (paragraph o.8).

Table 13.5 Sample Audit Verification

Requirement	Action Taken
1. Employers shall certify that they have evaluated compliance with the provisions of this section at least every 3 years to verify that the procedures and practices developed under the standard are adequate and are being followed.	This report includes a letter of certification. It also shows that the audit was conducted within the 3-year schedule required by the regulation.
2. The compliance audit shall be conducted by at least one person knowledgeable in the process.	This audit was conducted by ______, whose resume is included. It shows that he is knowledgeable in the process.
3. A report of the findings of the audit shall be developed.	This audit report contains a listing of the findings.
4. The employer shall promptly determine and document an appropriate response to each of the findings of the compliance audit, and document that deficiencies have been corrected.	A follow-up report will be prepared based on the findings of this audit. This report will develop recommendations that address each of the findings. Also, it will include a process for making sure that all recommendations are executed and closed out in a timely manner.
5. Employers shall retain the two most recent compliance audit reports.	The audit reports are retained as part of the overall process safety documentation.

OSHA regulation). The statements in the right-hand column show what was done to in this particular audit in order to comply with those requirements.

Positive findings

Before the audit starts it should be determined if the auditors are expected to identify any findings that indicate exceptionally good performance. Doing so can help ameliorate a report that comes over as being totally negative. Also the positive findings may provide a basis for setting best practices, particularly if the company being audited has multiple facilities.

Report retention

A policy regarding the retention of reports and audit notes should be established. It is possible that the company's attorneys will ask that the reports not be retained on the grounds that they may contain information that they would not wish to be discovered in the event of a litigation following an incident. However, given that audits should be part of a continuous improvement program, the facility managers should insist that the reports be kept for a substantial period of time, such as

7 years. At a minimum audit reports should be retained until the next round of the audit cycle because future auditors will want to judge how well the previous findings were implemented.

FINDINGS

All findings must have enough detail to implement and verify closure. Findings that are vague or that cannot ever be addressed should not be issued. As with hazards analysis a clear distinction between findings and recommendations is required. An audit team issues findings; it does not make recommendations.

FOLLOW-UP

The audit does not stop with the release of the auditor's report. Management is required to address the audit's findings—possibly with the assistance of the auditor—to correct specific deficiencies and, more broadly, to improve management systems. The purpose of an audit is to help management improve performance, not to find fault, or to establish blame (although it has to be recognized that one way of improving performance may be to change some of the managers). Facility management must treat the audit as being part of the continuous improvement program rather than a law enforcement activity.

The auditor may be asked by the client to use the findings to identify management problems that lie behind the issues that were reported on. To do this, the approach used in Chapter 11 for Incident Investigation can be followed. That is, the elements of process safety are used to structure the analysis of the management systems.

Audit findings can be incorporated into a facility's overall hazard management system. Items for the system can come from hazards analyses, incident investigations, and audits. The system will be designed such that managers can choose not to follow up on a finding. However, if they do so, they must clearly justify that decision.

Finally, as part of the follow-up, the company that was audited should tell the audit team how they felt about the exercise and the value of the findings that came out of it.

UNANNOUNCED AUDITS

Wherever a company may be with respect to the status of its risk management programs, it is important to be ready for an unannouced audit. There is no telling when an accident might happen, and, if the accident is bad enough, there will be audits from regulators and attorneys representing various plaintiffs. The fact that a facility is in the middle of developing its risk management program is not a valid excuse; an accident can happen at any time, therefore, an audit can take place any time.

The practical implications of this understanding are twofold. First, it means that all information to do with risk management must be properly organized and indexed so that it can be quickly located. Doing so will create a good impression with the auditor, and it will reduce the possibility of not being able to find the information that was asked for.

A second implication of being ready to meet an audit at all times is that it strongly encourages a top-down approach to developing a risk management program. Initially, there will be very little detail in the program. But, as it develops more detail will be added. The key is that, at all times, the program will be complete, and it will not be a collection of miscellaneous documents that may or may not be connected to one another in a coherent manner.

Additional advantages to having a top-down approach include the following:

- If the plant is audited, there is always a complete, coherent, integrated, and holistic program to show to the auditor. He or she will probably be impressed with the organization and control of all the risk management activities that this exemplifies.
- It helps sustain employee morale and enthusiasm. Risk management programs are hard work and can become debilitating for those involved in it; the completion of stages on a regular basis will help create a sense of progress.
- It will be relatively easy to identify those areas that need the greatest attention.

THE SEMS AUDIT RULE

The SEMS rule for offshore facilities in the United States was introduced in Chapter 2. Because this rule is the newest process safety standard in the United States and because the agency placed a very heavy initial emphasis on audits, it is useful to examine this standard in detail.

The SEMS audit requirements are shown in Table 13.6. The left column in the table quotes the rule; the second column provides some discussion and interpretation of that section of the rule. Additional guidance is provided in Table 13.7.

Table 13.6 SEMS Rule (Audits)

SEMS Rule	Discussion
12.1 General	
The operators [and contractors with Safety and Environmental Management Programs (SEMPs)] should establish and maintain an audit program and procedures for the periodic audit of the safety and environmental management program in order to determine if the program elements have been properly implemented and maintained and to provide information on the results of the audit to management.	The BOEMRE requirements are typical of any audit. Specific features of this program are discussed below.
The audit program and procedures should cover the following: a. The activities and areas to be considered in audits b. The frequency of audits c. The audit team	Activities and areas for the audit should be defined in the SEMS management document. It is important to give this topic sufficient consideration. It will include physical boundaries (e.g., whether subsea pipelines are included), and organizational issues such as the relationship with contractors. Much of the information will be stored at onshore facilities. However, the safety-critical information that onboard personnel may need—often in a hurry—should be identified. Information of this type should probably be available in hard copy format, since, during an emergency, it is more than likely that normal electronic data management system will not be functioning properly.

Table 13.6 SEMS Rule (Audits) *Continued*

SEMS Rule	Discussion
d. How audits will be conducted	Audits will usually be conducted by evaluating a mix of facility documents, interviews with key personnel, and field observations.
e. Audit reporting	Audit reporting covers not just the structure and content of the report itself but also a list of who is to receive a copy of the report, and how action items are to be followed up on.
Sufficient resources should be committed by management to the audit in order to meet its intended scope.	
12.2 Scope	
The scope of the audit should include the following:	
a. Determine if the management program elements of Sections 2–11 (of the SEMP program) are in place.	The audit plan should have a section for each of the elements.
b. Determine if the management program elements incorporate the required components.	This requirement is also part of the audit plan.
c. Testing system to evaluate the effectiveness of the management program. The system should include a review of records and documentation as discussed in Section 13, private interviews of various levels and disciplines of personnel, and facility inspections.	
d. Identify areas of potential improvement in the safety and environmental management program.	
12.3 Audit Coverage	
When selecting facilities to audit, consideration should be given to common features (e.g., field supervisors, regulatory districts, facility design, systems and equipment, office management) to obtain a cross section of practices for the facilities operated.	The standard calls for the audit to cover a broad range of information sources.
The testing system of the audit need not be applied to each facility; rather, interviews and inspections should be conducted at fields that differ significantly (e.g., oil vs. dry gas). This should include a number of facilities sufficient to evaluate management's commitment to items a, b, and c in 12.2.	Similarly, the audit should cover a range of facilities and technologies.
During each audit, at least 15% of the facilities operated, with a minimum of one facility, should be audited. The facilities included in the audit should not be the same as those included in the previous audit. When sufficient deficiencies are identified in the effectiveness of any safety and environmental management program elements, the test sample size shall be expanded for that program element.	The requirement for 15% coverage is substantial. This paragraph does not identify what constitutes "sufficient deficiencies."

Table 13.6 SEMS Rule (Audits) ***Continued***

SEMS Rule	Discussion
12.4 Audit Plan	
Prior to an audit, a written audit plan should be developed. The plan should be designed to be flexible in order to permit changes in emphasis based on information gathered during the audit, and to permit effective use of resources. The plan should include the following elements: a. Audit objectives and scope b. Audit criteria c. Identification of the audit team d. Identification of the facilities to be audited e. Identification of the program elements to be audited f. Procedures to be used in the audit g. Confidentiality requirements h. Report contents and format, expected date of issue, and distribution It should be recognized that the audit material collected during the audit will only be a sample of the information available. This will lead to a level of uncertainty which should be taken into account when planning the audit.	Many of the topics discussed in the bullet points have already been discussed in this section. The previous section—Audit Coverage—calls for a 15% coverage rate, which is quite high.
12.5 Audit Frequency	
The first audit should be accomplished within 2 years of initial implementation of the management program. The audit interval for the management program should not exceed 4 years.	The working assumption in this book is that BSEE will have the right to conduct an audit at any time following November 15, 2011. Presumably, however, they cannot require a company to have performed an internal audit until 2 years after that date.
12.6 Audit Team	
Audits can be conducted either by personnel from within the organization or by outsiders. At least one person on the audit team should be knowledgeable in the processes involved and other specialties as deemed necessary. Care should be exercised when selecting the audit team to ensure impartiality.	Although not a stated requirement, it is good if one person on the team is familiar with the auditing process itself.
12.7 Audit Report	
The audit team should prepare an audit report. The topics to be addressed in the audit report should be those determined in the audit plan. It should contain the audit findings. The audit report should be dated and signed by the audit team.	One of the challenges of process safety work is that the analyses and studies often result in a written report. But getting the report finished on time and of sufficiently high quality often turns out to be quite a challenge.

Table 13.6 SEMS Rule (Audits) *Continued*

SEMS Rule	Discussion
Audit-related information that may be in audit reports, includes, but is not limited to, the following: a. Identification of the facilities audited b. Identification of the program elements audited c. Summary of objectives and scope of the audit d. Criteria against which the audit was conducted e. Period covered by the audit and the date(s) the audit was conducted f. Identification of the audit team g. Statement of the confidential nature of the contents h. Distribution list for the audit report i. Summary of the audit process, including any obstacles encountered j. Audit findings and conclusions, such as whether the program element(s) is properly implemented and maintained	The bullet items in this list can form the basis for a Table of Contents of the audit report.
The findings and conclusions of the audit should be provided to the management personnel responsible for the SEMP. Management should establish a system to determine and document the appropriate response to the findings and to assure satisfactory resolution. The audit report should be retained at least until the completion of the next audit.	The audit report must show that there is a system for responding to findings. The system can be part of the facility's overall process for tracking and responding to identified hazards.

Table 13.7 § 250.1920 Auditing Requirements

BSEE Requirement	Discussion
a. You must have your SEMS program audited by either an independent third party or your designated and qualified personnel according to the requirements of this subpart and API RP 75, Section 12 (incorporated by reference as specified in § 250.198) within 2 years of the initial implementation of the SEMS program and at least once every 3 years thereafter. The audit must be a comprehensive audit of all 13 elements of your SEMS program to evaluate compliance with the requirements of this subpart and API RP 75 to identify areas in which safety and environmental performance needs to be improved.	The BOEMRE requirements are in alignment with those listed above, with the following differences. • The audit frequency has changed from once in 4 years to once in 3 years. • The audit includes 13 elements. The "General" requirements of SEMP must be covered.

Table 13.7 § 250.1920 Auditing Requirements *Continued*

BSEE Requirement	Discussion
b. Your audit plan and procedures must meet or exceed all of the recommendations included in API RP 75 Section 12 (incorporated by reference as specified in § 250.198) and include information on how you addressed those recommendations. You must specifically address the following items: 1. Section 12.1 General 2. Section 12.2 Scope 3. Section 12.3 Audit Coverage 4. Section 12.4 Audit Plan	
You must submit your written Audit Plan to BOEMRE at least 30 days before the audit. BOEMRE reserves the right to modify the list of facilities that you propose to audit.	One of the general features of SEMS is that companies are not required to submit a program or plan. They must simply have the program in place such that they are ready for an audit (or incident investigation). There are, however, a number of exceptions to this generalization—and this 30-day requirement is one of them.
5. Section 12.5 Audit Frequency, except your audit interval must not exceed 3 years after the 2-year time period for the first audit. 6. Section 12.6 Audit Team. The audit that you submit to BOEMRE must be conducted by either an independent third party or your designated and qualified personnel. The independent third party or your designated and qualified personnel must meet the requirements in § 250.1926.	As already noted, this requirement is over and above what RP 75 calls for.
c. You must require your auditor (independent third party or your designated and qualified personnel) to submit an audit report of the findings and conclusions of the audit to BOEMRE within 30 days of the audit completion date. The report must outline the results of the audit, including deficiencies identified.	This paragraph is self-explanatory. Once more, BOEMRE is adding a timetable requirement to the original SEMP standard.
d. You must provide the BOEMRE a copy of your plan for addressing the deficiencies identified in your audit within 30 days of completion of the audit. Your plan must address the following:	If the facility has an overall hazards tracking system then its workings should be included in the audit report.
1. A proposed schedule to correct the deficiencies identified in the audit. BOEMRE will notify you within 14 days of receipt of your plan if your proposed schedule is not acceptable.	1. The agency does not say what happens if they themselves fail to meet the 14-day requirement.
2. The person responsible for correcting each identified deficiency, including their job title.	2. Identification of responsible parties is an integral part of the Hazards Register.
e. BOEMRE may verify that you undertook the corrective actions and that these actions effectively address the audit findings.	How this requirement is to be met is not specified.

In addition to transforming RP 75 from a *recommended* practice to a legal requirement, BSEE has added supplemental material.

There are four sections to do with auditing and the follow-up to audits. Once more, the material is presented in tabular form with discussion and commentary provided in the second column of the table.

§ **250.1924 How will BSEE determine if my SEMS program is effective?**

BSEE Requirement	Discussion
a. BOEMRE or its authorized representative may evaluate or visit your facility to determine whether your SEMS program is in place, addresses all required elements, and is effective in protecting the safety and health of workers, the environment, and preventing incidents. BOEMRE or its authorized representative may evaluate your SEMS program, including documentation of contractors, independent third parties, your designated and qualified personnel, and audit reports, to assess your SEMS program. These evaluations or visits may be random or based upon the OCS lease operator's or contractor's performance.	This paragraph is self-explanatory: the agency has the legal right to evaluate the effectiveness and application of an SEMS program at any time of its own choosing.
b. For the evaluations, you must make the following available to BOEMRE upon request: 1. Your SEMS program 2. The qualifications of your independent third party or your designated and qualified personnel 3. The SEMS audits conducted of your program 4. Documents or information relevant to whether you have addressed and corrected the deficiencies of your audit 5. Other relevant documents or information	Once more, this paragraph is both self-explanatory and sweeping in its scope. When reviewing documents an auditor is likely to want to know four pieces of information: 1. The document type 2. Examples of the document 3. Where the documents are retained 4. The retention period
c. During the site visit BOEMRE may verify that: 1. Personnel are following your SEMS program. 2. You can explain and demonstrate the procedures and policies included in your SEMS program. 3. You can produce evidence to support the implementation of your SEMS program.	Although the SEMP/SEMS standard does not include an Employee Participation element in the way that OSHA's PSM standard does, this paragraph has something of the same effect.
d. Representatives from BOEMRE may observe or participate in your SEMS audit. You must notify the BOEMRE at least 30 days prior to conducting your audit as required in § 250.1920, so that BOEMRE may make arrangements to observe or participate in the audit.	At the time of writing, the practicalities of this requirement are not clear, since it would appear as if BOEMRE does not actually have enough personnel to meet the considerable requirements of this paragraph.

§ **250.1925 May BOEMRE direct me to conduct additional audits?**

BSEE Requirement	Discussion
a. If BOEMRE identifies safety or noncompliance concerns based on the results of our inspections and evaluations, or as a result of an event, BOEMRE may direct you to have an independent third-party audit of your SEMS program, in addition to the regular audit required by § 250.1920, or BOEMRE may conduct an audit.	This paragraph contains one of the many BOEMRE references to "independent third-party audits."
1. If BOEMRE directs you to have an independent third-party audit, (i) you are responsible for all of the costs associated with the audit, and (ii) the independent third-party audit must meet the requirements of § 250.1920 of this part and you must ensure that the independent third party submits the findings and conclusions of a BOEMRE-directed audit according to the requirements in § 250.1920 to BOEMRE within 30 days after the audit is completed. 2. If BOEMRE conducts the audit, BOEMRE will provide a report of the findings and conclusions within 30 days of the audit.	The 30 day requirements in both of these paragraphs is likely to be a challenge. Writing the audit report, having it checked, and then issued can take quite a lot of time.
b. Findings from these audits may result in enforcement actions as identified in § 250.1927.	
c. You must provide the BOEMRE a copy of your plan for addressing the deficiencies identified in the BOEMRE-directed audit within 30 days of completion of the audit as required in § 250.1920.	

§ **250.1926 What qualifications must an independent third party or my designated and qualified personnel meet?**

BSEE Requirement	Discussion
a. You must either choose an independent third party or your designated and qualified personnel to audit your SEMS program. You must take into account the following qualifications when selecting the third party or your designated and qualified personnel: 1. Previous education and experience with SEMS, or similar management-related programs 2. Technical capabilities of the individual or organization for the specific project 3. Ability to perform the independent third-party functions for the specific project considering current commitments 4. Previous experience with BOEMRE regulatory requirements and procedures	This requirement has changed under the proposed SEMS II extension to the rule.

§ 250.1926 What qualifications must an independent third party or my designated and qualified personnel meet? *Continued*	
BSEE Requirement	**Discussion**
5. Previous education and experience to comprehend and evaluate how the company's offshore activities, raw materials, production methods and equipment, products, byproducts, and business management systems may impact health and safety performance in the workplace. b. You must have procedures to avoid conflicts of interest related to the development of your SEMS program and the independent third-party auditor (I3P) and your designated and qualified personnel. c. BOEMRE may evaluate the qualifications of the independent third parties or your designated and qualified personnel. This may include an audit of documents and procedures or interviews. BOEMRE may disallow audits by a specific independent third party or your designated and qualified personnel if they do not meet the criteria of this section.	

SEMS II

The original SEMS rule was supplemented by additional requirements—informally known as SEMS II. Its guidance to do with auditing is discussed below.

AUDIT REQUIREMENTS

The same paragraph number system is used by the agency as for SEMS. Once more, the proposed rule is presented in a two-column table, with the first column quoting the rule and the second column providing some discussion.

§ 250.1920 What are the auditing requirements for my SEMS program?	
BSEE Requirement	**Discussion**
BOEMRE proposes to revise this section by removing the option for the operator to use designated and qualified operator personnel to perform an audit of the SEMS program. Use of an independent third party will provide for increased objectivity in regard to improving personnel safety and achieving environmental protection as compared to utilizing a designated and qualified person of the operator. Therefore, BOEMRE would require that audits of operators SEMS programs be conducted by independent third parties. Independent third parties would be required to meet the qualifications under § 250.1926.	This is a substantial, and probably unrealistic, requirement. Additional discussion is provided in the next section.

§ 250.1924 How will BSEE determine if my SEMS program is effective?

BSEE Requirement	Discussion
BOEMRE proposes to require the operator to conduct audits using only an independent third party. The proposed rule would revise this section to be consistent with that requirement by removing the option to allow the operator to use designated and qualified operator personnel to perform an audit of the SEMS program. The audit is the initial step to determine if an operator's SEMS program is effective. It will take time to ascertain the ultimate effectiveness of this regulatory requirement.	This is a repeat of the requirements provided in § 250.1920.

§ 250.1926 What qualifications must an I3P meet?

BSEE Requirement	Discussion
BOEMRE proposes to revise this section by removing the option for the operator to use designated and qualified operator personnel to perform an audit of the SEMS program. This section also would include new qualifications that the I3P must meet. The operator would be required to nominate an independent third party to audit its SEMS program. The independent third party must be capable of performing all tasks associated with an audit. The operator would be required to notify BOEMRE in writing of its nomination and to submit a request to BOEMRE for approval of the proposed third-party auditor at least 30 days prior to the next audit. The request must state the name and address of the nominated individual or organization. The request would have to include the following items: qualifications of the nominated individual or organization relating to education and previous experience with SEMS, or similar management-related programs; previous experience with BOEMRE regulatory requirements and procedures; and the educational background and previous experience that qualifies the proposed auditor to understand and evaluate how the operator's offshore activities, raw materials, production methods and equipment, products, byproducts, and business management systems may impact health and safety performance in the workplace. A request would also have to include a signed statement that the independent third party is not owned or controlled by, or otherwise affiliated with, the operator. An operator would also need to have procedures to avoid conflicts of interest related to the development of the operator's SEMS program and the I3P. The proposed rule would provide that if a third-party auditor was involved in developing and/or maintaining the SEMS program, then that person, organization, and/or its subsidiaries could not audit the SEMS program.	In practice, it is likely that the company's own auditors and audit systems will have to be incorporated into the I3P work, as discussed below. BSEE will not maintain a list of qualified auditors. Instead, an operating company will propose a person, who will then be either accepted or rejected by BOEMRE. The Center for Offshore Safety plays an important role in the assessment of potential I3Ps. BSEE may also employ its own I3Ps. The audit report would probably remain confidential. But the agency does state It is the intention of BOEMRE to share information with the public on aggregated results from SEMS audits.

§ 250.1926 What qualifications must an I3P meet? *Continued*

BSEE Requirement	Discussion
Under the proposed rule, after evaluating the third party's qualifications, BOEMRE could accept or not accept the operator's independent third-party nomination. If BOEMRE does not accept the nomination of an independent third party, then the operator must submit a new nomination before the audit may go forward. The audit report, once completed, must be submitted to BOEMRE and the operator. BOEMRE will notify the operator of whether or not the audit report is sufficient and acceptable. Under the proposal, the operator would be responsible for the costs of the audit.	

INDEPENDENT THIRD-PARTY AUDITORS

The I3P requirement could be onerous and very difficult to meet. The proposed SEMS II rule justifies the requirement with the following statement:

> The addition of a mandatory independent third party auditor brings necessary objectivity to identifying good practices and any deficiencies that may exist in an operator's SEMS program.

I3P QUALIFICATIONS

The qualifications for I3Ps are provided in Paragraph §250.1926 of the proposed SEMS II standard.

A fully qualified I3P is a rare bird. He or she will have to possess the following attributes:

- A thorough knowledge as to the development and workings of process safety systems, including the more abstract elements such as MOC
- Years of offshore experience
- The engineering training and skills necessary to interpret and understand a large number of engineering and technical standards from the API and other organizations
- Willingness to fly offshore and sleep in cramped quarters (something that cannot be taken for granted since many I3Ps will be at retirement age and so will not relish the offshore life any more)
- True independence from the companies he is auditing—yet it is more than likely that he will have worked closely with many of these companies over the years.

The supply of fully qualified I3Ps will not be nearly sufficient. A rough calculation shows why based on the following very rough assumptions.

- Number of platforms in the Gulf of Mexico: say 4,000
- Number of audits per year: say 1,000

- Length of each audit: say 6 weeks, including report writing and management discussions
- Number of auditors per team: say 4

The above assumptions would create a need for something like 500 I3Ps. This is not practical. Potential work-arounds include the following:

1. The audit team is made up mostly of company personnel. One or more I3Ps would join the team, and provide the independence that the agency is looking for
2. An I3P could be composed of different persons representing disciplines such as mechanical integrity, human factors, and labor relations

NATIONAL EMPHASIS PROGRAM

One of the consequences of the Texas City explosion that occurred in 2005 is that OSHA came under criticism for not conducting inspections of refineries thoroughly enough or frequently enough. In response to this criticism OSHA implemented a National Emphasis Program (NEP) for refineries. The program was later expanded to cover chemical plants.

The NEP audits were intense, generally involving large audit teams and sometimes lasting as long as 6 months.

The following four elements of process safety were identified as the leading causes of failing to meet the standard:

- Process Safety Information
- Process Hazards Analysis
- Mechanical Integrity
- MOC

REVIEWS AND EXPERT ASSESSMENTS

The discussion to do with auditing stressed the formal nature of the audit process and the need for objectivity. The auditor compares actual performance against a clearly defined, agreed-upon standard. He or she then provides a "Yes/No" result of the item under consideration. If the auditor moves beyond this restricted role he or she is acting as a consultant, not as an auditor.

In practice, most clients want both a mock formal audit (in order to make sure that they will "survive" a real audit from an agency) and an expert assessment or review, in which the auditor/reviewer provides a more subjective analysis of the client's process safety systems. During an assessment, the reviewer typically works as part of a team with the facility personnel. Even though he or she is looking for problems, he is not trying to find fault; any problems are identified as "recommendations" or "action items"—not "findings." There is no threat of penalties or retributive action based on his findings. This type of review is not adversarial; the reviewer and the plant personnel are on the same team. Moreover, the recommendations associated with a review can be considered against the reality of budgets, schedules, personnel availability, and turnaround schedules. Finally, a reviewer will often work with the facility being audited on developing solutions to the problems that have been identified.

An analogy can be drawn between financial audits and economic analysis. A financial audit checks that a company is conforming to the goals and standards set by external agencies such as the tax authorities and the company's own finance department. Economic analysis, which corresponds to measurement and metrics, seeks to understand issues such as the best pricing level for the company's product, labor rates, and how to finance the enterprise.

The distinction between audits and reviews was made clear at one facility at which the audit/review team delivered two physical reports. The first was a mock OSHA audit. When it came to the client's operator training program the audit noted that all regulatory requirements were being met fully—a training program was in place and was being implemented. However, an assessment provided by the same audit/review team stated that there were so many problems with the operator training program that the best strategy may be to start a brand new program.

An audit always results in a formal report. Such is not necessarily the case with regard to reviews. Moreover, the persons carrying out the review can come from the same organization as the facility being audited; there is no concern about conflict of interest. A reviewer will often work with the facility being audited to help develop solutions to the problems that have been identified. He or she may be able to bring experience and knowledge to assist the facility personnel in finding cost-effective solutions to the problems identified. The auditor may also make recommendations regarding the company's management structure. He or she may suggest that a root cause of many of the problem areas was that the organization was not set up correctly, and that alternative organizations may be more effective.

REVIEW ISSUES

Issues that a review will typically look for include the following:

- The effectiveness of management systems
- Workforce involvement
- Real-world usefulness
- "Learned to live with it" problems
- Lessons learned from other facilities

Management systems effectiveness

Operational integrity management is—at its root—a management process. It provides a framework whereby managers can develop, implement, and run systems that encourage all workers to operate safely. This being the case, the reviewer should evaluate the management systems by making sure that policies are in place, that the policies make sense, and that they are properly understood and followed by all workers.

The reviewer should check for the following:

- Policies are in place
- Those policies are appropriate and relevant
- The policies are properly understood and followed by all workers
- Ensure that individuals within the host organization have the right levels of responsibility, authority, and accountability

Workforce involvement

The topic of Workforce Involvement is difficult to measure and audit because it is concerned with the spirit rather than the letter of the program. Although it is quite simple to have employees fill out forms and questionnaires, it is much more difficult to determine if they are truly participating. Some questions that might help guide an audit in this area are listed below.

- Is there an overall policy or mission statement that is perceived as being real, and that is not just some form of management fad?
- Does the process safety program have clearly defined target and objectives—including dates when these will be met—and are the employees familiar with these targets and dates?
- Is upper management perceived as being committed to these objectives?
- How well is the overall strategy translated into detailed plans?
- Do the employees understand the program and the detailed plans?
- Are they committed to it?

Real-world usefulness

The reviewer will check the process safety and operational integrity systems to see if they are really adding value. For example, he may find out that the operating procedures are almost never used—even in situations where they should be. He or she should dig into this finding and try to learn why the procedures are not used.

"Learned to live with it" problems

Most people and facilities find that they eventually get used to certain problems, and, rather than trying to fix them, they learn to live with them or they have developed work-arounds. A good reviewer will identify these problems and point out that they need fixing. Many housekeeping issues fall into the "learned to live with it" category.

Lessons learned

The reviewer can examine events in other companies, and determine what lessons can be learned.

REVIEWER ATTRIBUTES

The personality and experience of the reviewer is of paramount importance to the quality of the review. To be effective in his or her analyses the reviewer has to have extensive plant experience. In addition to the personal attributes discussed under the role of auditor, the reviewer should possess considerable experience of process facilities similar to the one being audited. He or she should also have the strength of personality to be able to communicate opinions and suggestions to all levels of management within the host company. Ideally, the reviewer will also be able to generate creative solutions to previously intractable problems.

MANAGEMENT ELEMENTS ASSESSMENT

The previous sections of this chapter have looked at formal audits, lagging indicators, leading indicators, and expert reviews. An additional approach to quantifying risk management programs is through an assessment of management elements. This approach addresses some of the limitations to do with lagging and leading indicators discussed above.

Managers generally ask four questions regarding their risk management programs:

1. What is our current status?
2. Where are we most vulnerable?
3. How are we progressing?
4. How do we compare to others?

One approach is to have industry experts create a very large number of evaluation questions that cover all aspects of a facility's design, construction, operation, maintenance, and ongoing engineering. The questions are organized hierarchically around the 20 elements shown in Figure 13.2.

The topic of MOC has been highlighted in Figure 13.2 in order to illustrate the assessment concept discussed in this section. This topic is divided into 12 sections, as shown in Figure 13.3.

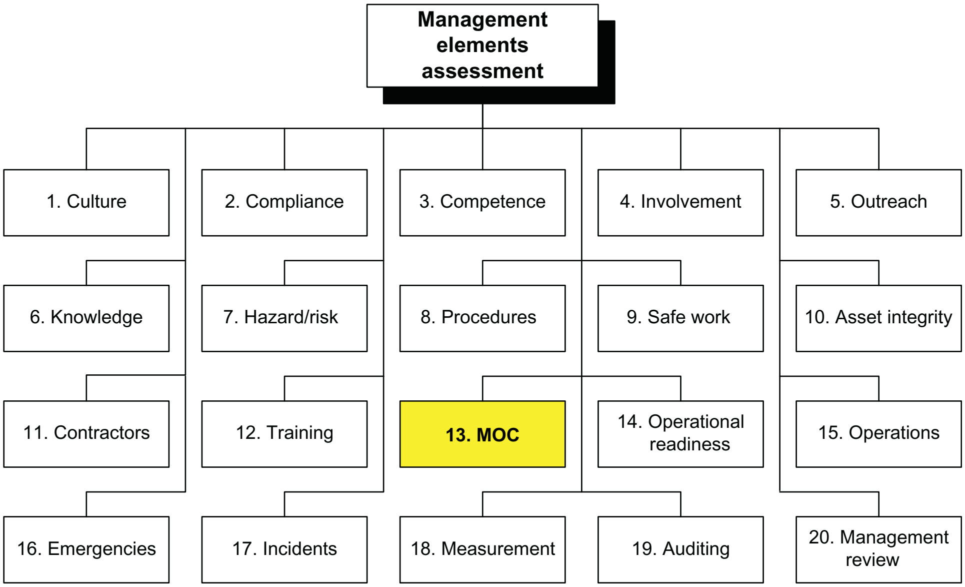


FIGURE 13.2

Assessment structure.

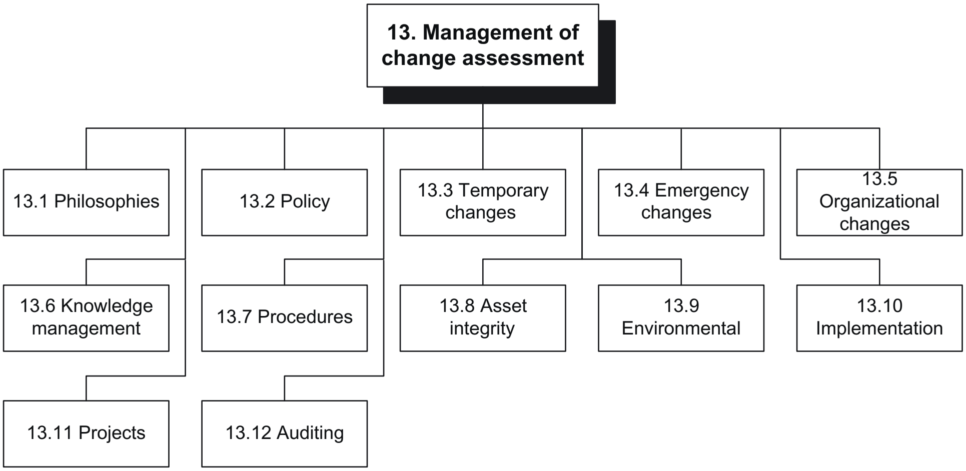


FIGURE 13.3

Operational readiness structure.

LEVEL 1: RISK MANAGEMENT

The top-level risk management structure of Figure 13.3 is shown below in Figure 13.4 in a spreadsheet format.

The table in Figure 13.4 has four columns. The first column lists the 20 CCPS management elements starting with “1. Process Safety Culture” and finishing with “20. Management Review.” The topic of MOC, which is the 13th of the elements, is used here to illustrate the spreadsheet process.

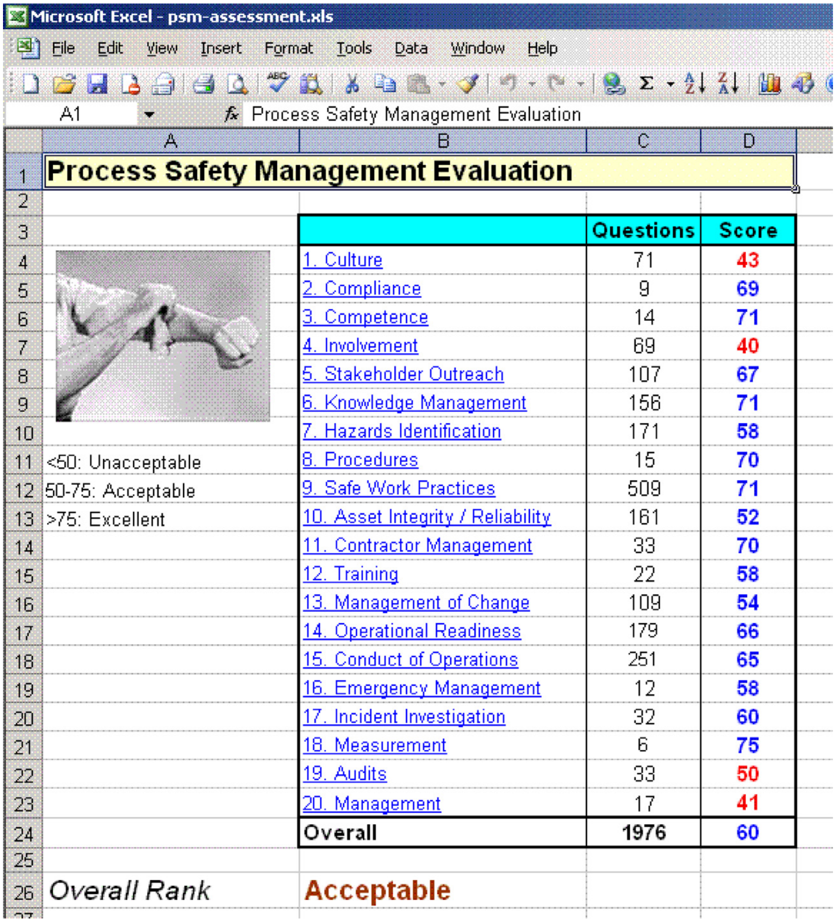
The second column shows the total number of questions to do with each topic. In the case of MOC there are 109 questions. The third column provides the overall score for each topic as a percentage or normalized total. In this example, MOC scores 54%. Each spreadsheet is given the same weight regardless of the number or nature of the questions within it.

The total number of questions is 1976 and the total score is 60%.

To the left of the spreadsheet the ranking system is explained. A score of <50 is “unacceptable.” Therefore, any values below 50 are shown in red. A score in the 50–75 range is “acceptable” and is shown in blue. A score of 75 or greater is “excellent” and is shown in green. Figure 14.4 shows four reds, fifteen blues, and one green. MOC has a score of 54, which is considered “acceptable.” The overall score is 61.

LEVEL 2: MANAGEMENT ELEMENT SPREADSHEET

The topic titles in Figure 13.4 are colored blue and are underlined. This means that each is hyperlinked to a daughter spreadsheet. Figure 13.5 shows the sheet for MOC. It contains 12 sheets, starting with “13.1 Philosophies” and “13.2 Policies,” and finishing with “13.12 Auditing.”


Microsoft Excel - psm-assessment.xls
File Edit View Insert Format Tools Data Window Help
A1
A B C D

Process Safety Management Evaluation

Process Safety Management Evaluation

	Questions	Score
1. Culture	71	43
2. Compliance	9	69
3. Competence	14	71
4. Involvement	69	40
5. Stakeholder Outreach	107	67
6. Knowledge Management	156	71
7. Hazards Identification	171	58
8. Procedures	15	70
9. Safe Work Practices	509	71
10. Asset Integrity / Reliability	161	52
11. Contractor Management	33	70
12. Training	22	58
13. Management of Change	109	54
14. Operational Readiness	179	66
15. Conduct of Operations	251	65
16. Emergency Management	12	58
17. Incident Investigation	32	60
18. Measurement	6	75
19. Audits	33	50
20. Management	17	41
Overall	**1976**	**60**

<50: Unacceptable
50-75: Acceptable
>75: Excellent

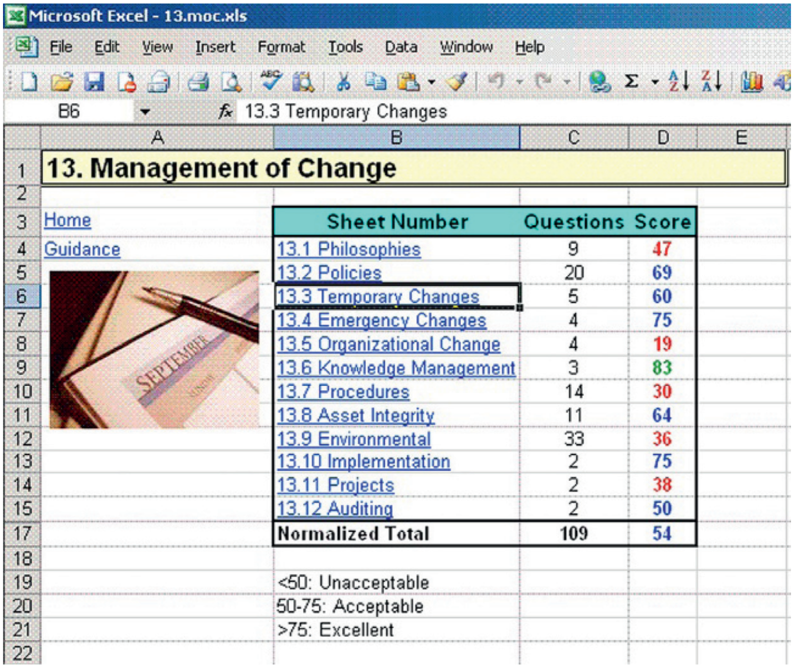
Overall Rank **Acceptable**

FIGURE 13.4

First-level spreadsheet.

The structure of Figure 13.5 is similar to that of Figure 13.4. The number of questions for each spreadsheet is shown, along with the normalized (percentage) score for each. Each topic is hyperlinked to another spreadsheet, one level down. Once more a color scheme showing the ranking for each sheet is used using the same three levels as in Figure 14.4. Of the 14 spreadsheets, 5 have a score of less than 50, which means that the result is “unacceptable”—so the score is shown in red. Six have a score in the 50–75 (“acceptable”) range. Hence they are shown in blue. Just one is above 75. It is “excellent,” and is shown in green.

The total score is 54% which is “acceptable.”



B6 13.3 Temporary Changes

13. Management of Change

Home

Guidance

Sheet Number	Questions	Score
13.1 Philosophies	9	47
13.2 Policies	20	69
13.3 Temporary Changes	5	60
13.4 Emergency Changes	4	75
13.5 Organizational Change	4	19
13.6 Knowledge Management	3	83
13.7 Procedures	14	30
13.8 Asset Integrity	11	64
13.9 Environmental	33	36
13.10 Implementation	2	75
13.11 Projects	2	38
13.12 Auditing	2	50
Normalized Total	**109**	**54**

<50: Unacceptable
50-75: Acceptable
>75: Excellent

FIGURE 13.5

Second-level spreadsheet—MOC.

LEVEL 3: DETAILED QUESTIONS

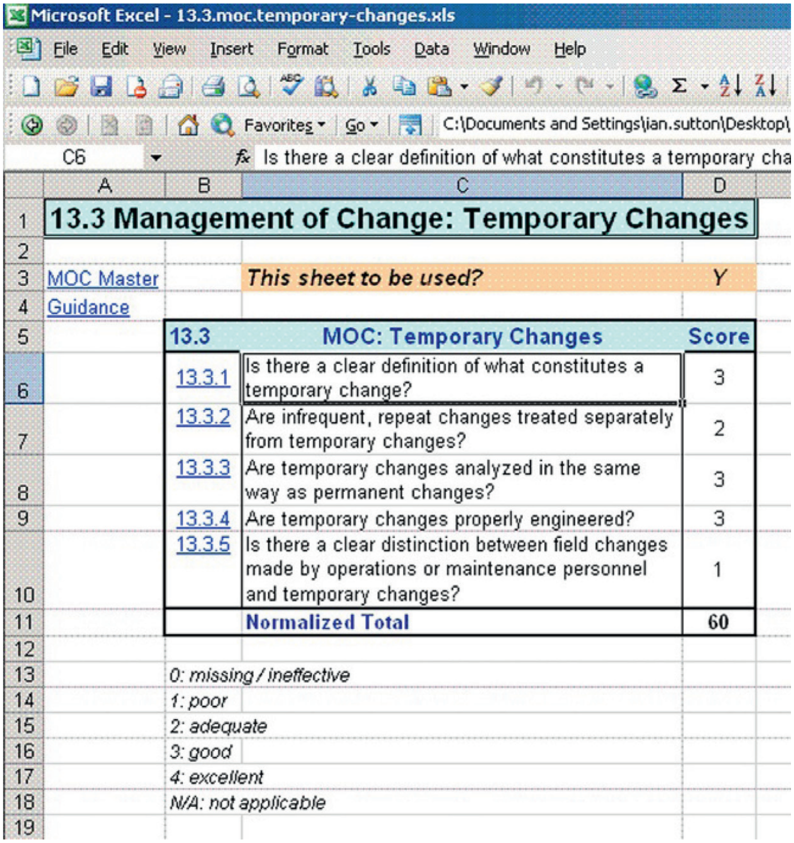
Each of the topics shown in Figure 13.6 has a set of detailed questions associated with it. Of the 12 sheets to do with MOC, Figure 13.7 provides an example for one of them: 13.3. Temporary Changes.

At the top of Figure 13.6 is the question "This sheet to be used?" The default condition is "Y." If any other entry is made then the results from this sheet are removed from the overall scoring system—both numerator and denominator.

Each sheet has a set of questions—generally about 5−15 per sheet. For "Management of Change: Temporary Changes" there are just five questions. The general philosophy is that a "yes" answer to a question is desirable. For example, question 13.3.1 asks, "Is there a clear definition of what constitutes a temporary change?" Clearly an answer of "yes" is desirable.

In order to provide a range for the response to a question, a scoring system is provided. The system used here is shown below:

0: missing/ineffective
1: poor
2: adequate
3: good
4: complete/excellent
N/A: not applicable


Microsoft Excel - 13.3.moc.temporary-changes.xls
File Edit View Insert Format Tools Data Window Help
Favorites Go C:\Documents and Settings\ian.sutton\Desktop\
C6
Is there a clear definition of what constitutes a temporary cha
A B C D

13.3 Management of Change: Temporary Changes

MOC Master

Guidance

This sheet to be used? *Y*

13.3	MOC: Temporary Changes	Score
13.3.1	Is there a clear definition of what constitutes a temporary change?	3
13.3.2	Are infrequent, repeat changes treated separately from temporary changes?	2
13.3.3	Are temporary changes analyzed in the same way as permanent changes?	3
13.3.4	Are temporary changes properly engineered?	3
13.3.5	Is there a clear distinction between field changes made by operations or maintenance personnel and temporary changes?	1
	Normalized Total	**60**

0: missing / ineffective
1: poor
2: adequate
3: good
4: excellent
N/A: not applicable

FIGURE 13.6

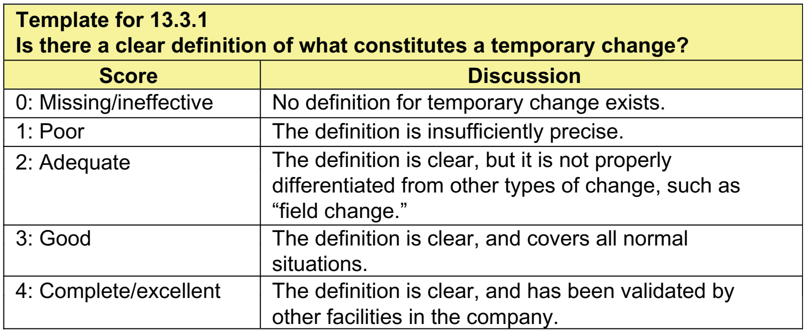
Third-level spreadsheet.

When a range of responses is possible, then an appropriate score is given. With regard to question 13.3.1, the reviewer may find that the facility does have a definition for temporary change, but that there are some areas of misunderstanding and potential confusion. Therefore, he provides a score of 3. If the question can generate only a “yes” or “no” response, then the score is either “0” or “4.” If an answer is not relevant to the current situation then “N/A” is entered; this removes that question from the calculation of both the numerator and denominator terms in the normalized total.

The individual scores are added together to give a normalized (percentage) total. Figure 13.6 shows that the overall score for “Management of Change: Temporary Changes” is 60%.

SCORING TEMPLATE

Figure 13.7 shows that each question number is hyperlinked. The link is to a scoring template that provides guidance to do with that particular question. Use of the template helps ensure high levels



Template for 13.3.1
Is there a clear definition of what constitutes a temporary change?

Score	Discussion
0: Missing/ineffective	No definition for temporary change exists.
1: Poor	The definition is insufficiently precise.
2: Adequate	The definition is clear, but it is not properly differentiated from other types of change, such as “field change.”
3: Good	The definition is clear, and covers all normal situations.
4: Complete/excellent	The definition is clear, and has been validated by other facilities in the company.

FIGURE 13.7

Scoring template for question 13.3.1.

of consistency between different reviewers and when the system is being applied to multiple facilities. Figure 13.7 shows a template for question 13.3.1, “Is there a clear definition of what constitutes a temporary change?”

GUIDANCE

At the top of Figure 13.6 is the word “Guidance.” This links to a document that provides background information and assistance to do with the topic in question—in this case Temporary Change. Figure 13.8 provides the Guidance that is available for the topic and also includes links to citations and other reference material.

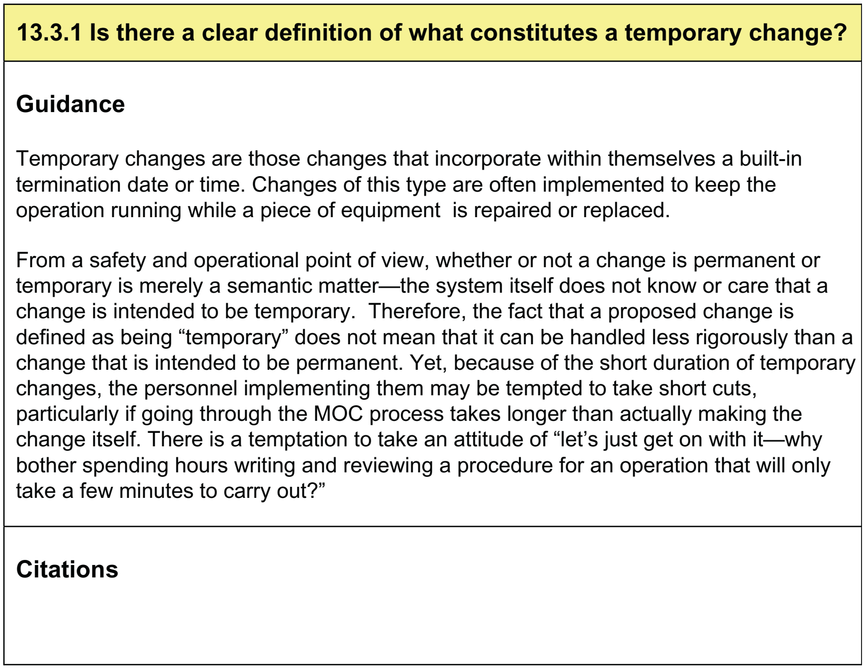
BENEFITS OF THE ELEMENTS ASSESSMENT APPROACH

The elements assessment approach has the following advantages over the more traditional lagging and leading indicator methods.

Independent of events

The assessment system does not rely on the occurrence of events or near misses. For example, even if there has not been an incident attributable to failure of the operational readiness system, potential problems to do with this element should be identified once the 14 spreadsheets have been completed.

By contrast, the lagging and leading indicator approaches can only identify underperforming management elements through the use of root cause analysis. As discussed in the previous chapter, such analyses are inherently subjective—different people and different techniques will come up with different answers as to why an event occurred.



13.3.1 Is there a clear definition of what constitutes a temporary change?

Guidance

Temporary changes are those changes that incorporate within themselves a built-in termination date or time. Changes of this type are often implemented to keep the operation running while a piece of equipment is repaired or replaced.

From a safety and operational point of view, whether or not a change is permanent or temporary is merely a semantic matter—the system itself does not know or care that a change is intended to be temporary. Therefore, the fact that a proposed change is defined as being "temporary" does not mean that it can be handled less rigorously than a change that is intended to be permanent. Yet, because of the short duration of temporary changes, the personnel implementing them may be tempted to take short cuts, particularly if going through the MOC process takes longer than actually making the change itself. There is a temptation to take an attitude of "let's just get on with it—why bother spending hours writing and reviewing a procedure for an operation that will only take a few minutes to carry out?"

Citations

FIGURE 13.8

Background for question 13.3.1

Handling abstraction

Lagging and leading indicators provide little guidance to do with some of the more abstract management elements such as process safety culture and management review. This difficulty is entirely overcome when a management assessment approach is used.

Smoothing of results

Through the use of literally thousands of questions, the results are smoothed out. Even if some of the questions are answered incorrectly, the overall results should be of high quality.

Objectivity

The results of the assessment are likely to be quite objective. In the system shown below, each question has a potential score ranging from 0 (missing or ineffective) to 4 (complete or excellent). It is unlikely that two assessors would come up with dramatically different responses to the questions.

Like any other management activity, an audit should be properly planned. In particular, as many as possible of the administrative details and information acquisition steps should be carried out before the audit team actually starts work. The plan should clearly define the objectives of the audit, the geographical and organizational scope of work, and the anticipated amount of time that will be needed.

CHAPTER

14 CONSEQUENCE ANALYSIS

CHAPTER OUTLINE

INTRODUCTION

In Chapter 1, it was shown that risk has four elements:

1. A hazard
2. The consequences of that hazard should it occur (safety, environmental, and economic)
3. The likelihood of occurrence of the hazard
4. Safeguards that reduce consequences and/or likelihood.

The relationship between the first of the above three terms is shown in Eq. (1.1), which is repeated as Eq. (14.1).

$$\text{Risk}_{\text{Hazard}} = \text{consequence} \times \text{predicted frequency} \tag{14.1}$$

The previous chapter discussed the first term in the risk equation: hazard identification. This chapter discusses the analysis of the consequence and frequency terms in Eq. (14.1).

The topics of consequence and likelihood analysis are fraught with issues that bring into question the accuracy and usefulness of the results because so many assumptions have to be made, and because the analysts' opinions (many of which are implicit) play such an important role. For example, many fires and toxic gas releases start with a leak from a piping system. Yet the size of the leak could vary from a pinhole to a partially failed gasket all the way to a complete guillotine break

Process Risk and Reliability Management. DOI: http://dx.doi.org/10.1016/B978-0-12-801653-4.00014-X

of the pipe. Clearly, the assumption made about leak size is going to strongly affect all discussions to do with the consequences and likelihood of that leak.

The subjectivity that is implicit in analysts' opinions is very difficult to recognize. For example, it is likely that anyone who has suffered from H_2S exposure would treat a release of that gas as being very significant, regardless of what the calculations say. Similarly, people will often give a higher probability of occurrence to events that have already occurred once than to events that have never occurred.

RANGE OF CONSEQUENCES

Most hazards have a wide range of consequences—ranging from minor to very serious. Some potential consequences to do with the operation of Tank T-100 in Example 1 are shown in Table 14.1.

The discussion to do with hazards analysis in the previous chapter noted that it is not possible to identify all possible hazards. Similarly with consequence analysis—there will always be consequences that the analysts fail to identify. Hence, the list in Table 14.1 can never be complete. Therefore, in each case, it would be appropriate to add a category "Other" for all of the consequences that exist but were not identified. Doing so acknowledges the limitations of human knowledge and imagination.

It is important to ensure that the consequence terms really are consequences and not just intermediate events. For example, Hazard #1.5 in Table 14.1—"Air ingress leading to formation of explosive mixture in V-101"—is not really a consequence; it is a step toward the final, undesired event. If air enters V-101, then an explosion may occur. However, if there is no source of ignition

Table 14.1 Hazards and Consequences

Hazards	Consequences
Tank T-100 is pumped dry	• Loss of production for a few moments • Loss of production for an extended period of time • Downstream pump cavitation leading to need for maintenance • Downstream pump cavitation leading to fire at the pump • Air ingress leading to formation of explosive mixture in V-101
Hazard: Tank T-100 overflows	• Environmental citation • Contamination of ground water • Fire leading to loss of tank
Hazard: P-101A seal fails	• Fire with possibility of serious injury or death • Lost production • Equipment damage
V-101 is overpressured	• Discharge to atmosphere through relief valve PSV-101 • Rupture of V-101
Liquid flows backward into T-100	• Runaway chemical reaction in T-100 • Cost of replacing contaminated RM-12

in V-101 nothing will happen; eventually the air in the vessel will be purged, and conditions will return to normal. Air in the vessel is a precursor to the ultimate consequence term: explosion in V-101. An event tree, such as that shown in Figure 14.1, shows the sequence of events that lead to the final consequence term.

Consequences generally fall into one of the following four categories: safety, health, environmental, and economic.

SAFETY

Many hazards have the potential to injure or kill workers at the facility. In the case of the hazard to do with overflowing storage tank T-100, a worker may be injured or killed by a fire that could result from the spill, or he/she could be overwhelmed by toxic fumes from the spilled RM-12.

Because safety consequences are potentially so serious, they are generally given the most attention during the analyses of hazards and their consequences. Indeed, safety is often the only topic looked at during a risk analysis. The assumption is that a safe operation will also be environmentally clean and economically efficient.

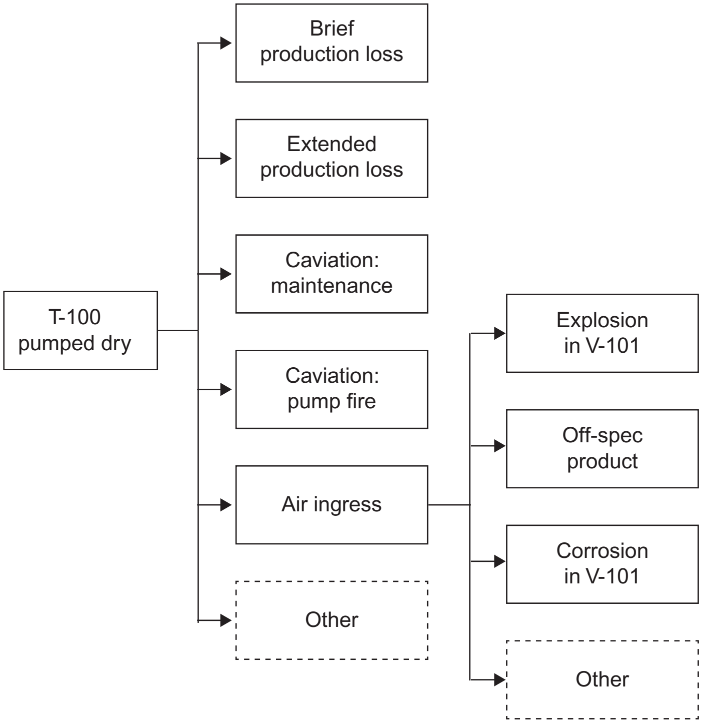


FIGURE 14.1

Consequence event tree.

HEALTH

Some hazards do not have an immediate safety effect but they can cause health problems over a long period of time. For example, offshore facilities will often use produced gas to drive turbines or in fired heaters. If the gas contains hydrogen sulfide (H_2S) then, during the burning of the gas, the H_2S will be converted to sulfur dioxide (SO_2). The concentration of SO_2 in the exhaust plume will be very low because it is extensively diluted with the other gases such as nitrogen and carbon dioxide. Hence, it does not pose a safety threat. However, over a long enough period of time, the SO_2 can have a health effect on those working on the platform.

ENVIRONMENTAL

Some hazards do not have a direct impact on human beings but they can cause harm to the environment. Using the high level in T-100 scenario once more, the spilled RM-12 could flow into an environmentally sensitive area such as a river or lake. Environmental consequences are often closely linked to regulatory violations.

ECONOMIC

Virtually all hazards have economic consequences in the form of lost production, reduced productivity, and increased repair costs. Overflow of T-100, for example, leads to the loss of valuable product and to the costs associated with equipment replacement and repair, particularly if the spilled material catches fire.

EFFECT OF A RELEASE

If a flammable gas or liquid is released to the atmosphere, the potential sequence of events is shown in Figure 14.2.

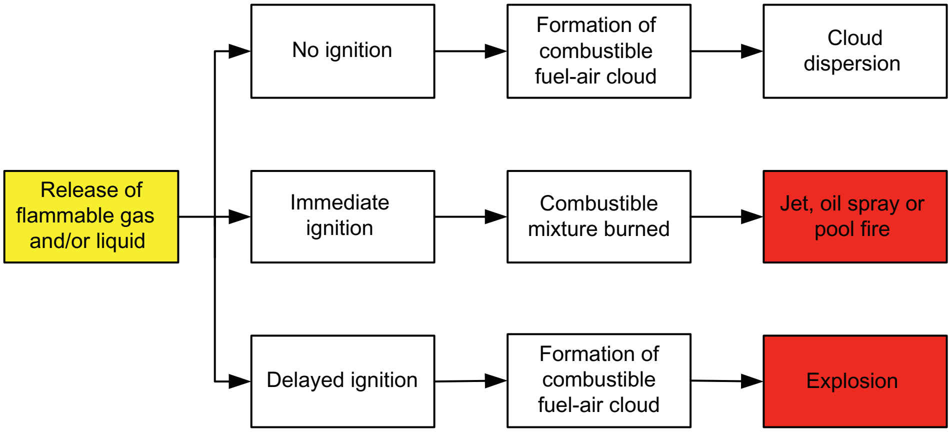

Release of flammable gas and/or liquid
No ignition
Formation of combustible fuel-air cloud
Cloud dispersion
Immediate ignition
Combustible mixture burned
Jet, oil spray or pool fire
Delayed ignition
Formation of combustible fuel-air cloud
Explosion

FIGURE 14.2

Effect of a release.

HOLE SIZE

Fires, explosions, and toxic gas releases all result from the release of hazardous materials through holes in equipment or piping. The holes can form gradually—say through corrosion—or they can be formed suddenly—say through vehicle impact. Clearly, the size of the resultant hole will have a profound effect on the magnitude of the event.

The worst case scenario is to assume a guillotine break of a large, high-pressure line. This does sometimes happen, for example, if cryogenic liquids enter a carbon steel flare header the line may shear right through as if someone cut it with a saw. A more probable scenario is the failure of a section of a gasket between two flange bolts. To further complicate matters, there will be a frequency/size relationship; small holes will develop more often than large ones. Formal safety analyses will generally consider a range of hole sizes and develop a model in which they are all considered. A frequency-based approach to hole size selection is provided by Stahl and Kenady (2011).

FIRES

Fires are often the most serious hazard faced by process facilities. Explosions can be more devastating and will often lead to greater overall losses but they occur less frequently than fires. Moreover, explosions are almost followed by fires in the area that was damaged.

Fire analysis quantifies the loads on structures, equipment, or personnel arising from fires or explosions. Heat fluxes and temperatures are predicted for structures and equipment exposed to fires. This information is used to determine the response of the structure and equipment to the fire, which in turn is used to determine and evaluate risk levels and to select prevention or mitigation measures.

Professional understanding to do with fires and explosions is still limited. For example, the initial report to do with the Buncefield explosion and fire that occurred in England, December 11, 2005, states that the authors "...cannot explain why an ignition of gasoline vapor with no obvious source of confinement led to such a devastating explosion". Similar observations are made by Allen (2011).

It is probably fair to say that similar comments to do with lack of understanding also apply to toxic gas releases.

FLAMMABLE RANGE

Fires require the presence of fuel and air (oxygen) along with a source of ignition. These criteria are sometimes referred to as the fire triangle. Flammable mixtures have upper and lower limits for the concentrations of the fuel in the vapor space. Below the lower flammable limit (LFL), there is insufficient flammable material for a fire to occur—the mixture is "too lean." Above the upper flammable limit (UFL), there is too much flammable material—the mixture is "too rich." The flammability limits vary according to the pressure and temperature of the mixture, and on the presence of inert components such as steam, carbon dioxide, or nitrogen.

For most flammable hydrocarbons, the LFL is around 2–5%. For gasoline vapors, the range is from a little over 1% to almost 8%. For simple alkanes, such as methane and ethane, the UFL value is in the 10–15% range. Some chemicals, such as hydrogen, ethylene oxide, and acetylene, have much higher values for UFL.

Increasing the oxygen content of the flammable mixture increases the flammable range, reduces the ignition energy, and increases the energy of combustion, resulting in much more damage from explosions.

IGNITION TEMPERATURE/ENERGY

Figure 14.3 can be used to illustrate ignition temperatures and flashpoints.

Before a flammable mixture can ignite its temperature must be at or above the flashpoint. If the temperature is below this point, then the vapor mixture will not burn, even if a source of ignition exists. The left line in Figure 14.3 is the flashpoint line.

Even if the material is above its flashpoint, the ignition source must be of sufficiently high temperature and must also contain sufficient energy to ignite the fuel. The minimum energy varies with type of gas and concentration; for hydrocarbon vapors it is low, for high flashpoint liquids, such as diesel and fuel oil, it is much higher—usually in the form of an existing fire.

If a flammable mixture is heated to a high enough temperature, it will spontaneously ignite; an ignition source such as a flame or spark is not needed. Spontaneous ignition occurs at the auto-ignition temperature (AIT), which is also shown in Figure 14.3. In general, the AIT will decrease as the molecular weight of the flammable material increases.

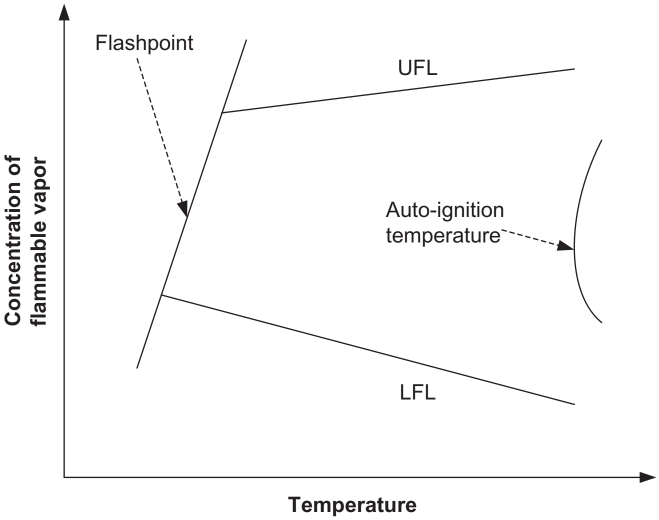


FIGURE 14.3

Flammability and ignition limits.

A well-known example of auto-ignition is the operation of a diesel engine. As the diesel vapor/air mixture is compressed, the temperature rises until it reaches the AIT, at which point the mixture spontaneously ignites. A gasoline engine, on the other hand, needs a spark from a spark plug to cause ignition.

Oil-soaked insulation can auto-ignite. The insulation holds the oil vapors near the heat source and prevents the oil trapped in the insulation from cooling. Furthermore, the heavy oils trapped in the insulation on very hot lines may be cracked to release lighter materials in the kerosene and diesel range, which are easier to ignite. When fed by dripping heavy oil, the oil-soaked insulation can smolder for extended periods.

Discussion to do with ignition issues is provided by Det Norske Veritas. Some of their conclusions are:

- Natural gas released in the open will not normally auto-ignite when contacting hot surfaces at temperatures below approximately 1000°C unless the gas remains in contact with the hot surface for a sufficiently long period of time.
- Hydrocarbon liquids will auto-ignite upon contact with hot surfaces above approximately 300°C.
- Rotating equipment or moving parts can cause ignition due to heat generated by friction or due to static electricity discharging to earth.
- Gas from pipes that rupture due to overpressurization or corrosion are unlikely to auto-ignite because the heat generated by the rupture is unlikely to be sufficient to cause ignition. In addition, the gas has insufficient time to mix with air to form a flammable mixture at time of rupture.
- Ruptures due to impacts (e.g., dropped objects, swinging loads) can cause significant sparking subsequently resulting in a relatively high ignition probability.
- Hot work (e.g., welding and grinding) will cause ignition of a flammable gas cloud.
- Lightning is a potential cause of both leak and ignition.
- Helicopters, boats, lifeboats, and crane engines are all sources of ignition.
- Attempts to disperse gas (e.g., by starting ventilation fans) have resulted in ignition.
- Faulty electrical equipment can cause ignition either through arcing or by the buildup of heat.

SPONTANEOUS COMBUSTION

There is an important difference between spontaneous combustion and auto-ignition: spontaneous combustion can start at ambient temperature when conditions are right. For example, vegetable oils, turpentine, and other pine tar derivatives used in paints oxidize very rapidly. If this process is allowed to occur in a protected space with air circulation, such as a pile of oily, paint-saturated rags in a corner, or clothes locker, enough heat can be generated to cause spontaneous combustion. Prompt and safe disposal of these materials is an important safeguard to avoid fires.

Petroleum products do not undergo spontaneous combustion. In general, they must be heated to 400°F or higher before oxidation occurs. Adsorbed hydrocarbons adsorbed on activated charcoal have been known to auto-ignite. This is most likely to occur when the petroleum product has a significant olefin content and has been on the carbon for a considerable amount of time. Given that activated carbon is fairly frequently used to remove small amounts of hydrocarbon from air to reduce hydrocarbon emissions or for odor control the hazard can be common. Potential mitigations include monitoring the temperature of a carbon filter and regeneration or disposal after a set period of time.

IGNITION SOURCES

Sources of ignition on process facilities include the following:

- Flames and hot surfaces
- Wiring (overhead and buried)
- Electrical equipment
- Low-voltage devices, radios, and telephones
- Stray currents
- Electrostatic charges
- Hot work
- Sparks from tools
- Smoking and matches
- Static electricity
- Lightning
- Exposed internal heating coils (e.g., those used in lube oil blending tanks)
- Radiant heat
- Pyrophorics such as iron sulfide (FeS).

Vacuum trucks

Due to turbulence and high velocity in the liquid being pumped, static charges are frequently generated during vacuum truck operations. To prevent charges from accumulating on an insulated section of hose, it is important to check the continuity of the hoses and to ensure all hoses are conductive from the truck to the equipment. This prevents a spark gap between the hose nozzle and the equipment.

Radiant heat

Radiant heat from items such as flares, fired heaters, and exhaust pipes can be a source of ignition. Radiant heat can also injure people directly, and can damage or destroy equipment.

Table 14.2 provides guidance as to representative values for the effects of radiant heat.

For most facilities, the most effective means of mitigating the effect of radiant heat is through the use of firewater, which can absorb around 9000 BTU/gallon.

Static electricity

Flowing liquids generate static charges as they move through pipes, pumps, valves, and especially as they pass through filters. Static charges can also be created by steaming, spraying, grit blasting, two phase flow, and solid flow.

When a container or tank is filled, a charge is generated in the fill pipe and container, and an opposite charge is generated in the liquid. When handling volatile liquids, it is important to maintain an electrical path between the pipe and container in order for these charges to recombine without the

Table 14.2 Radiant Heat Effects

Item	Intensity (Btu/h ft^2)
Solar radiation on a hot summer day	320
Continuous exposure (no evacuation required)	500
Immediate evacuation from area required	1,500
Damage to exposed skin within 1 minute	1,760
Damage to exposed skin within a few seconds	3,000
Plastic melts	4,000
Plant equipment damage	7,000
Full storage tanks	10,000
Cotton clothing ignites within a few seconds	12,800
Spontaneous ignition of wood	20,000

chance of producing a spark, particularly for refined products which tend to have a low conductivity (other materials such as crude oil and water soluble materials have a higher conductivity).

Other activities that generate static include mixing and splashing. If the turbulence is sufficient, charges will accumulate in separated droplets. Air blowing can also create static charges. When water droplets fall through liquid hydrocarbon, they will carry a charge, leaving the opposite charge on the hydrocarbon liquid. This mechanism can be created by air blowing that picks up water from the tank bottom and mixes it in the oil.

Static charges can be dissipated by several methods. The safest method is to control the generation rate so that static charges are dissipated as rapidly as they are generated by controlling fluid velocity in piping, splashing, mixing, and general agitation so that high levels of charge are not generated. Also, antistatic additives can be injected into refined oils, improving their conductivity and thus allowing the charges to dissipate as rapidly as they are formed.

Static problems can also be minimized by:

- Not bubbling air or vapors through liquids
- Not using jet or propeller blending
- Avoiding free falling or dropping of liquid through the surface of a stored liquid product
- Preventing droplets of water or other particulate matter from settling through the body of a liquid.

Bonding and grounding are helpful in keeping charges in balance on the tank shell, tank trucks, and piping. However, the charge that accumulates on the surface of liquids cannot be removed by bonding or grounding the container holding the liquid.

Lightning

Ignition of a tank by a direct strike is an obvious problem. However, nearby tanks can also be ignited even though they may not have been directly hit. As clouds build up and travel across land masses, they collect huge electrical charges of millions of volts. As these charged clouds pass over trees, houses, and industrial sites, they induce an opposite charge on these ground objects. When a charged cloud passes over a group of tanks in a tank farm, the charge is great enough to induce charges on all tanks. When the cloud discharges in the form of a lightning strike, a “bound” charge is left on the storage tanks surrounding the one that was struck. The bound charge on an external floating roof, for example, may have a 100,000-volt driving force to get to ground. The nearest path is the tank shell. So, without proper shunts, sparks can jump across the pantograph hanger joints or other joints, causing sparks and possible ignition in the vapor space between the floating roof and shell below the fabric seal. Four or five tanks, or more, can be ignited by the electrical discharge from one cloud.

Guidance to do with protection against lightning and charged clouds is provided in NFPA 780 and API 2003.

Pyrophorics/iron sulfide

Pyrophoric materials are self-igniting when exposed to air (oxygen). The most common pyrophoric in the process industries is iron sulfide, FeS (also known as pyrite). It forms as a scale in piping, vessels, tanks, and equipment when H_2S reacts with iron and moisture in a low oxygen environment according to the following equation:

$$Fe_2O_3\text{(iron oxide)} + 3H_2S \rightarrow 2FeS + 3H_2O + S\text{(sulfur)}$$

Because FeS has a very fine crystalline structure, it is pyrophoric, i.e., it spontaneously ignites on exposure to air. When a vessel or tank is opened for maintenance, the pyrophoric material can catch fire and then ignite flammable or combustible materials. Not only is the fire itself dangerous, particularly if residual hydrocarbons are still present before opening the equipment, but SO_2 that is generated from the combustion can be hazardous. The standard precaution against this event is to make sure that all combustible hydrocarbons are removed, that the equipment is thoroughly water washed before being opened and that everything is kept wet (API, 2001).

FLAMMABILITY HAZARD RANKING

Flammability can be ranked using the Flammability Hazard Ranking (NFPA, 2007) as shown in Table 14.3.

In general, materials with a flammability rating of 3 and 4 represent fire hazards that are relatively easily ignited. However, materials with flammability rating of 1 or 2 require preheating; generally, they are only capable of ignition as a result of flame impingement from an existing fire.

If a gas/air mixture is feeding a fire, the flame will not travel backwards as long as the velocity of the incoming gas mixture is greater than the velocity of a backwards traveling flame. If the gas velocity should fall too low, the flame could travel backwards into the process equipment. Flame arrestors are installed to prevent this phenomenon from taking place. A typical flashback velocity is 10 ft/s.

PASSIVE FIRE PROTECTION/FIREPROOFING

The best form of fire protection is passive, i.e., it is effective regardless of actions taken by individuals or active safety systems. Fire protection generally includes the following items:

- Sufficient separation between equipment items
- Fire protection barriers and walls to prevent the spread of fire
- The use of fire-rated insulating materials to protect the integrity of structural steel members, risers, vessels, and other safety critical items.

Table 14.3 Flammability Ranking

Ranking	Description	Example
0	Materials that will not burn	
1	Materials that must be preheated before ignition will occur, such as combustible liquids and solids and semisolids whose flashpoint exceeds 93.4°C, as well as most ordinary combustible materials	Triethylene glycol
2	Materials that must be moderately heated before ignition will occur; this includes combustible liquids and solids and semisolids that readily give off ignitable vapors	Diesel fuel, helifuel, lube oil, hydraulic oil, and hot oil
3	Flammable liquids and materials that can be easily ignited under almost all normal temperature conditions. (A flammable liquid is one that has a flashpoint below 100°F. A combustible liquid has a flashpoint at or above 100°F.)	Methanol
4	Flammable gases, pyrophoric liquids, and highly flammable liquids	Flammable gases and hydrogen

EXPLOSIONS

An explosion creates an overpressure that damages or destroys buildings and equipment (most deaths and injuries are caused by flying missiles and/or building collapse rather than by the overpressure itself). Explosions often occur very quickly after initial release of gas or liquid (flashing or forming mists) and are capable of causing significant damage to facility, sometimes where recovery is not possible. By comparison, major fire events that are not caused by an explosion do not usually cause extensive damage so quickly so there is chance of the event being controlled before structural impairment occurs.

Large explosions are capable of causing immediate critical damage, but it is also possible for relatively small explosions to result in critical escalation through damage to systems and equipment if design fails to take account of explosion hazards. The capacity of an explosion to deform structures on which equipment is supported, displace vessels and pipes through direct overpressure and drag loading, and produce serious missile hazard is what sets explosions apart from other hazards.

Some effects of explosions are:

- Direct impact on systems and deformation of structure, leading to widespread loss of containment integrity as pipe and vessel connections become overstressed.
- Impairment or loss of safety systems, including Emergency Shutdown (ESD) facilities, blowdown, and deluge systems in affected areas, and protective instrumentation. This could be from direct blast pressure, drag loads, or missile damage.
- Penetration or failure of blast barriers and firewalls, destroying protective area directly or allowing subsequent fire to enter protected areas. Damage could be from blast overpressure

exceeding strength of barrier, missile penetration, or failure of other structure leading to collapse of heavy equipment.
- Subsequent fire involving multiple release sites that may overwhelm fire hazard management measures, particularly if they have been damaged by the explosion (e.g., passive fire protection coating).

PHYSICAL EXPLOSIONS

Physical explosions arise from a sudden release of stored energy, such as failure of pressure vessel or high-voltage electrical discharge (or even the popping of a balloon). Examples include failure of a fitting on a high-pressure gas system or failure of pressure containment in high-pressure pipes and vessels that have been physically weakened by an external event, such as a fire. The key to a physical explosion is that no chemical reactions are involved.

VAPOR CLOUD EXPLOSIONS

Vapor cloud explosions are due to rapid combustion of flammable gas, mist, or small particles that generate pressure effects due to confinement; they can occur inside process equipment or pipes, buildings, and other contained areas. A vapor cloud explosion can be either a deflagration or a detonation (the distinction between deflagrations and detonations is important when deciding on whether or not to use a flame arrestor in pressure relief systems).

The severity of a vapor cloud explosion depends on the fuel type, with the order of reactivity being in the following order:

- Hydrogen
- Acetylene
- Ethylene
- Ethane
- Butane
- Propane
- Natural gas
- Methane.

Inert gases, such as N_2 or CO_2, reduce reactivity of the mixture if they are present in significant concentrations (at least 20% CO_2 in methane).

Maximum explosion pressure is normally observed at stoichiometric (for uniformly mixed volume) or slightly richer concentrations. Explosion forces are generally weaker as the mixtures move toward the LFL and UFL values.

DEFLAGRATIONS AND DETONATIONS

A *deflagration* occurs when a flame front propagates by transferring heat and mass to the unburned air—vapor mixture ahead of the front. The combustion wave travels at subsonic speeds to unburned gas immediately ahead of the flame front. Flame speeds range from 1 to 350 m/s; at low speeds there is little effect from the blast overpressure, at high speeds peak overpressures can be as high as 20 times the initial pressure. Most vapor cloud explosions fall into this category.

A *detonation* occurs when the flame velocity reaches supersonic speeds above 600 m/s and generally in the 2000-2500 m/s range. Peak overpressures can be 20−100 times the initial pressure, with typical values of 20 bar. Detonation can be initiated either by use of a high explosive charge or from a deflagration wave that accelerates due to congestion and confinement. Certain chemicals are more prone to create detonations than normal hydrocarbons. These include ethylene, acetylene, and hydrogen.

The United States Environmental Protection Agency (EPA) provides lookup tables and simple equations for some of the commoner chemicals to calculate the distance of the overpressure waves. These tables are generally conservative, i.e., they predict greater impact than would be likely to actually occur. Nevertheless, they do provide a useful starting point.

As an example of the EPA method, Eq. (14.2) shows the overpressure equation for propane.

$$D = 0.0081 \times (0.1 \times W \times (46,3333/4680))^{1/3} \tag{14.2}$$

where D is the distance in miles that a 1 psi overpressure wave (which has sufficient force to knock down nonreinforced buildings) can be expected to travel and W is the weight in pounds of propane involved (see the EPA reference for an explanation of the other terms). Therefore, for example, if the inventory of propane in a tank is 50,000 lb and 10% of it is involved in an explosion, the 1 psi overpressure wave would extend for 0.3 miles.

BLAST EFFECTS

The calculation of explosion effects is a complex topic involving many variables. Table 14.4 shows some overpressure values with typical effects.

BLEVEs

A BLEVE (Boiling Liquid Expanding Vapor Explosion) is a special type of explosion. It can occur if a tank or vessel containing a liquid is subject to external fire. The heat causes the liquid in the

Table 14.4 Effect of Overpressure

Overpressure (psi)	Damage
0.15−1.0	Glass failure
1.0	Person knocked down
0.4	Minor structural damage
2.0	Partial collapse of walls and roofs
3.0	Eardrum damage
3.0−4.0	Light buildings demolished; storage tanks ruptured
5.0−7.0	Complete destruction of domestic buildings; loaded rail cars overturned
10.0	Total destruction of buildings
15.0	Lung damage
35.0	Fatalities

tank or vessel to boil, thus raising the pressure. The heat also weakens the metal walls of the tank, particularly above the liquid surface. The combination of these two factors can lead to a sudden explosion of a tank or vessel which can produce blast and fragmentation and buoyant fireballs.

A special form of BLEVE may occur if a pressure vessel has little or no liquid in it, and the set pressure of the relief valve is much higher than the vessel's normal operating pressure. An external fire may then lead to vessel failure before the internal pressure rises high enough to cause the relief valve to open.

DUST EXPLOSIONS

Dust explosions can occur in equipment such as decokers, where small diameter particulate solids can form an explosive mixture.

TOXIC GAS RELEASES

Many facilities in the process industries produce, use, or store toxic materials that can, if accidentally released, lead to either short- or long-term health effects for both workers and members of the public.

The study of toxic gas behavior has two major components. The first is to determine concentrations of gas downwind of the release point. These concentrations will depend on a plethora of factors such as the density of the gas, the amount released, weather conditions, and the roughness of the ground surface. The second part of toxic gas modeling has to do with the effect of the gas on the human body. (Some gases, notably nitrogen, simply replace the oxygen needed to breathe. Therefore, although the presence of such gases can lead to fatalities, they are not, in and of themselves, toxic.)

Throughout this section, the term "ppm" is used. It stands for "parts per million" of gas in air measured by volume. So, if the concentration of the gas is 100 ppm, then 1 m^3 of air contains 0.0001 m^3 of the undiluted gas. This is a very small volume and can be very difficult to measure with accuracy.

GAS RELEASE MODELING

The modeling of a vapor cloud following a release requires the use of highly specialized mathematical models, most of which are based on the Gaussian model, which assumes that the released gas has a normal probability distribution. Generally, the output from one of these models has a cigar shape, such as that shown in Figure 14.4, which is an elevation view for the release of the toxic gas H_2S.

The following information can be gleaned from the model's output:

1. The release is at a height of 124 feet above grade.
2. Three profiles are shown: one for a concentration of 15 ppm, one for 10 ppm, and one for 5 ppm.

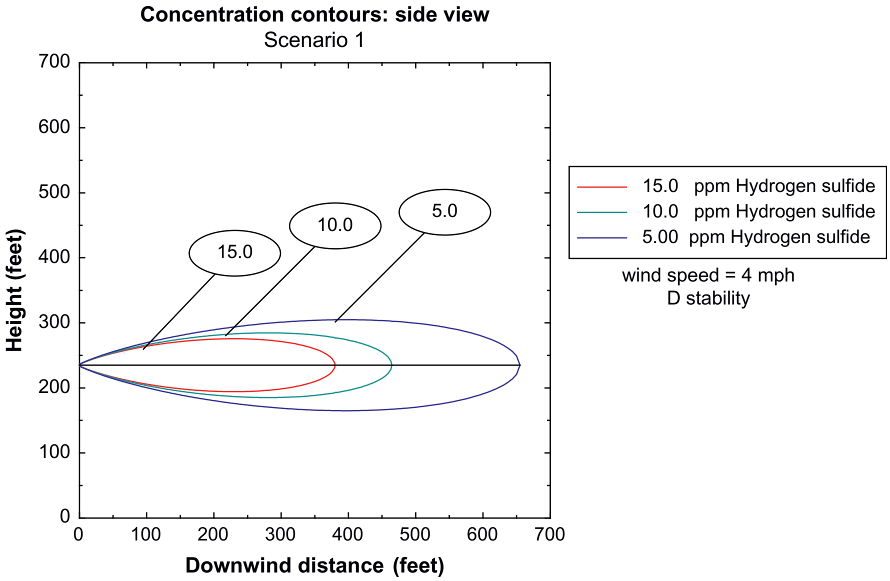


FIGURE 14.4

Gas plume—Elevation view.

Table 14.5 Air Stability Classes

Class	Description
A	Very unstable
B	Unstable
C	Slightly unstable
D	Neutral
E	Slightly stable
F	Stable

3. Using the 5 ppm profile as an example, the (blue) contour line represents the points at which the concentration of H_2S exactly equals 5 ppm. Concentrations rise toward the center of the plume and toward the point of release.

4. The furthest range of the 5 ppm plume is 650 feet.

5. The plume does not show any significant change in elevation (in spite of the fact that H_2S is "heavier than air," at these low concentrations it does not rise or fall much).

6. The wind speed is 4 miles per hour.

7. The air has stability "*D*."

In general, the higher the wind speed the more quickly the plume disperses because the air is more turbulent. Atmospheric stability is divided into six classes (Pasquill, 1961), given in Table 14.5.

Table 14.6 Air Stability Factors by Meteorological Conditions

Surface Windspeed		Daytime Solar Radiation			Night-time Cloud Cover	
m/s	mph	Strong	Moderate	Slight	>50%	<50%
<2	<5	A	A–B	B	E	F
2–3	5–7	A–B	B	C	E	F
3–5	7–11	B	B–C	C	D	E
5–6	11–13	C	C–D	D	D	D
>6	>13	C	D	D	D	D

Table 14.6 shows the factors used to determine the stability level.

Class D applies to heavily overcast skies at any windspeed day or night.

EFFECT OF TOXIC GASES

It is difficult to predict the effect of toxic gases on the human body with any degree of certainty. Obviously, people cannot be tested directly, so data is normally taken from tests with laboratory animals. Assumptions then have to be made as to how similar human response would be to that of the animals. Moreover, two people with very similar physiologies may react to a chemical quite differently. For example, the toxic gas H_2S has a strong odor at moderate concentrations. However, when the concentration rises above a certain point, human olfactory nerves are disabled and so the gas cannot be smelled. Thus H_2S famously has the property that "If you can smell it you're in trouble, if you can't smell it you're in real trouble." Unfortunately, the odor threshold varies significantly from person to person, hence the sense of smell cannot be used as a reliable gauge to do with the presence of toxic gases.

When information to do with the safety effects of toxic gases is not available, it is possible to take health exposure data and to extrapolate. Such an extrapolation may be very approximate, but it does provide some guidance for safety work.

Toxic chemicals can enter the human body in one of four ways:

- Inhalation
- Dermal (skin) absorption
- Ingestion
- Injection.

It is only the first two that are usually important in process safety work. The effects of exposure to a gas are affected by the following factors:

- Concentration of the material
- Duration of the exposure
- Health and sensitivity of the person(s) affected.

A term that is commonly used to predict the effect of a toxic chemical on the human body is the median lethal dose, LD_{50}. This is the dose required to kill half the members of a tested population.

Table 14.7 Example of Probit Values

k1	k2	*V*	ln *V*	*Y*
−15	3	100,000	11.51293	19.5
−15	3	1,000,000	13.81551	26.5
−15	3	10,000,000	16.1181	33.4

In all cases, there is a concentration−time relationship. The higher the concentration of the chemical, the less time can a person be exposed to it before they are affected. Haber's law describes a simple linear relationship between concentration and time, as shown in Eq. (14.3).

$$C = t \times a \tag{14.3}$$

where "*c*" is the exposure concentration, "*t*" is the exposure time, and "*a*" is a constant. In practice, the use of Haber's Law often leads to oversimplification. For example, it does not apply to hydrogen cyanide because that chemical is quickly broken down by the human metabolism.

The linearity implicit in Eq. (14.3) may not apply to any toxic gas. As concentrations increase, so permissible time exposure decreases logarithmically. In other words, the time that a person can be exposed to say 50 ppm of a chemical is less than half of the time that they can be exposed to 100 ppm.

PROBIT EQUATIONS

Modeling of releases is usually based on probit (probability estimate) equations, such as that shown in Eq. (14.4).

$$Y = k_1 + k_2 \ln V \tag{14.4}$$

where *Y* (the probit) is related to the percentage of the population affected by the release (or fire or other event), k_1 and k_2 are constants, and *V* is the magnitude of the effect (dose or thermal effect), which, in turn, depends on both the magnitude and duration of the event.

The probit equation shows that the percentage of the population affected by an event goes up by a disproportionately small amount as the magnitude of the event increases. For example, if the values shown in Table 14.7 are assigned to the terms in Eq. (14.4) it can be seen that, if the event increases in size by a factor of a 100, the factor affecting the percentage of people impacted by the event goes from 19.5% to 33.4%.

SHORT-TERM EXPOSURE LIMITS

Information to do with the effect of a chemical on human beings is provided in Material Safety Data Sheets (MSDSs) as discussed in Chapter 5. The EPA RMP Lookup Tables provide further guidance. Other sources of information include the following:

- ANSI (American National Standards Institute)
- API (American Petroleum Institute)
- ASME (American Society of Mechanical Engineers)

- Dangerous Properties of Industrial Materials, van Nostrand Reinhold
- Emergency Action Guides, Association of American Railroads
- NFPA (National Fire Protection Association)
- Handbook of Chemistry & Physics, CRC Press
- Hazardous Chemical Desk Reference, van Nostrand Reinhold
- Merck Index, Merck Company
- NIOSH/OSHA Pocket Guides to Chemical Hazards
- Chemical Engineers Handbook, McGraw-Hill.

When discussing exposure to toxic gases, the phrase "short term" is generally taken to be a time period of 60 minutes or less. Short-term limits are usually concerned with worker safety (although the Bhopal incident is a major exception to this generalization). It is generally assumed that exposure occurs through inhalation through the lungs (toxic materials can also be absorbed through the linings of the eyes, mouth, and throat).

Exposure limits are usually measured either in parts per million by volume or micrograms per cubic meter of air ($\mu g/m^3$). Concentrations can be converted from $\mu g/m^3$ to ppm by volume at 20°C by multiplying the value by (24.04/MW), where MW is the molecular weight of the gas.

Various short-term exposure limits values are in use. They include:

- ERPG—Emergency Response Planning Guidelines
- PEL—Permissible Exposure Limits
- TLV—Threshold Limit Value
- STEL—Short-Term Exposure Limit
- IDLH—Immediately Dangerous to Life and Health.

Regardless of which method is used, it is important to recognize that large differences exist between individuals regarding their response to exposure to toxic gases.

Emergency response planning guidelines

ERPGs are widely used. As defined by *The American Industrial Hygiene Association*, ERPGs (AIHA, 2009) provide estimates for concentration ranges "where a person may reasonably anticipate observing adverse effects as a consequence of exposure to the chemical in question."

Three ERPG values are provided for each of the substances that have been researched:

- ERPG-3: The maximum airborne concentration below which it is believed nearly all individuals could be exposed for up to 1 hour without experiencing or developing life-threatening health effects.
- ERPG-2: The maximum airborne concentration below which it is believed nearly all individuals could be exposed for up to 1 hour without experiencing or developing irreversible or other serious health effects or symptoms that could impair an individual's ability to take protective action.
- ERPG-1: The maximum airborne concentration below which it is believed nearly all individuals could be exposed for up to 1 hour without experiencing other than mild transient adverse health effects or perceiving a clearly defined objectionable odor.

ERPG values for some widely used chemicals are provided in Table 14.8.

Table 14.8 ERPG Values (ppm by volume)

		ERPG		
Chemical	**Formula**	**1**	**2**	**3**
Ammonia	NH_3	1000	200	25
1,3 Butadiene		5000	500	10
Chlorine	Cl_2	20	3	1
Ethylene oxide	C_2H_4O	500	50	N/A
Hydrogen chloride	HCl	100	20	3
Hydrogen fluoride	HF	50	20	5
Hydrogen sulfide	H_2S	100	30	0.1
Methanol	MeOH	5000	1000	200
Phosgene	$COCl_2$	1	0.2	N/A
Sulfur dioxide	SO_2	15	3	0.3
Vinyl acetate		500	75	5

Workers at process facilities are generally quite healthy and they know what to do and where to go in the event of an emergency. Hence, there is not usually a justification for using very conservative exposure limit values for short-term exposure to a toxic gas release. For this reason, the ERPG-2 value can be used for workers rather than the ERPG-3 level. ERPG-3 is more useful when considering members of the public, some of whom could be in ill health and others of whom could have trouble evacuating the affected area.

A key feature of all ERPG levels is that exposure is measured over a period of 1 hour. In practice, a worker who is exposed to one of these chemicals is not going to stay in the same place for an hour; he or she is going to move to a safe place (assuming that he is conscious and mobile).

Immediately dangerous to life and health

The IDLH concentration value (NIOSH, 2004) is defined as:

> The maximum concentration from which...one could escape in 30 minutes without experiencing any escape-impairing or irreversible health effects.

IDLH is intended to provide guidance for determining respiratory protection requirements in occupational environments; it is not necessarily suitable for emergency planning and risk assessment. However, IDLH information is often the only form of exposure information available. IDLH values are often found in MSDS and in standard references. Some practitioners use a value of IDLH/10 as a working number for defining acceptable risk.

Table 14.9 provides IDLH values for some of the more common toxic chemicals. (For reference, the ERPG-2 values are also shown; typically, they are much lower than the IDLH levels.)

Permissible exposure limits

The United States Occupational Safety & Health Administration (OSHA) sets PELs to protect workers against the health effects of exposure to hazardous substances. PELs are based on an 8-hour time weighted average (TWA) exposure.

Table 14.9 IDLH Values (ppm by volume)

Chemical	Formula	IDLH	ERPG-2
Carbon monoxide	CO	1200	350
Chlorine	Cl_2	10	3
Ethylene oxide	C_2H_4O	800	50
Hydrogen chloride	HCl	50	3
Hydrogen fluoride	HF	30	20
Hydrogen sulfide	H_2S	100	30
Methanol	CH_3OH	6000	1000
Phosgene	$COCl_2$	2	0.2
Sulfur dioxide	SO_2	100	3

Threshold limit values

TLVs are guidelines (not standards) prepared by the American Conference of Governmental Industrial Hygienists (ACGIH) to assist industrial hygienists in making decisions regarding safe levels of exposure to various hazards found in the workplace. TLV incorporates the PEL values already described. However, it also incorporates a short-term exposure limit and an absolute upper limit. A TLV reflects the level of exposure that the typical worker can experience without an unreasonable risk of disease or injury.

TLVs can be measured in one of three ways: TLV-TWA, TLV-STEL, and TLV-C (Ceiling). TLV-TWA represents the concentration to which a worker can be exposed for 8 hours per day, 40 hours per week without suffering adverse health effects. This is equivalent to the PEL-TWA, already described. No more than 4 excursions per day are permitted with at least 60 minutes between excursions and provided that the 8-hour TLV-TWA is not exceeded.

TLV-STEL represents the maximum concentration of the chemical to which the worker can be exposed for up to 15 continuous minutes without suffering from one or more of the following.

- Intolerable irritation
- Chronic or irreversible tissue damage
- Narcosis of sufficient degree to increase accident proneness (narcosis affects a person's judgment and can impair their ability to work safely). No more than four excursions per day are permitted with at least 60 minutes between excursions and provided that the 8-hour TLV-TWA is not exceeded.

TLC-C represents the concentration which should not be exceeded, even instantaneously. This is usually the one of most interest in safety work.

Short-term exposure limit

STEL is a U.K. term that sets the maximum concentration to which a person can be exposed for a 15-minute period.

Levels of concern (EPA)

The definition of Level of Concern (LOC) provided by the EPA (2007) and other federal agencies is as follows:

> The concentration of an Extremely Hazardous Substance in air above which there may be serious irreversible health effects or death as a result of a single exposure for a relatively short period of time.

Unlike ERPG and IDLH, the period of exposure is not defined.

Acutely toxic concentration/levels (New Jersey/Delaware)

For its Toxic Catastrophe Prevention Act (TCPA), New Jersey defined the Acutely Toxic Concentration as the lowest of:

- The IDLH value published by NIOSH (the National Institute for Occupational Safety and Health)
- LC_{10} (lowest concentration reported to be fatal to humans or animals)
- One-tenth of LC_{50} (medium lethal concentration).

The Acute Toxicity Concentration (ATC) as used by the State of Delaware is defined as being the lowest reported concentration of the substance that will cause death or permanent disability from an exposure of 1 hour. The order of preference for determining ATC is:

- ERPG-3 (where available)
- The Acutely Toxic Concentration (New Jersey)
- The EPA LOC.

Substance hazards index

With regard to hazards affecting the general public, a release of a toxic liquid is likely to be less dangerous than the equivalent release of toxic gas. Liquid spills can usually be contained, and even if they do escape outside the boundaries of the facility, measures can be taken to make sure that people do not come into contact with them. Gases, however, move quickly and are much more difficult to contain.

Recognizing this, some authorities (such as the states of Delaware and New Jersey) require that the Substance Hazards Index (SHI) for each chemical be developed for each hazardous chemical (assuming that sufficient data are available). This index incorporates terms for both toxicity and the ease with which the liquid can vaporize following a spill.

The following definition for SHI is used:

$$\mathrm{SHI} = \frac{\mathrm{EVP} \times 10^6}{760 \times \mathrm{ATC}}$$

EVP is the substance's vapor pressure in mmHg at 20°C; ATC (which has the same value as ERPG-3) is its acute toxicity concentration in ppm, defined as the lowest reported concentration based on recognized scientific test protocols that can cause death or permanent injury to humans after a single exposure of 1 hour or less. The constant 760 converts the vapor pressure from mmHg to atmospheres.

Although SHI is a simple way of determining the danger associated with a toxic gas, it does not cover all parameters, such as the density of the gas cloud once it is in the atmosphere. Nor is it useful in distinguishing between materials which are always present in the gas phase at all times.

LOCATION OF MONITORS

Guidance to do with the location of H_2S monitors on offshore facilities is provided by API RP 14C. Monitors are required when the atmospheric H_2S concentration could be >50 ppm or where the H_2S concentration in piping is >100 ppm.

Monitors for SO_2 are provided when atmospheric concentrations could be >2 ppm.

CHAPTER

15 FREQUENCY ANALYSIS

CHAPTER OUTLINE

INTRODUCTION

The quotations, "What gets measured gets done" and "You become what you measure" are well known. This means that if risk is to be properly understood and reduced to an acceptable level then quantification is needed.

The basic risk equation was provided in Chapter 1. It is repeated below as Eq. (15.1).

$$\text{Risk}_{\text{Hazard}} = \text{Consequence} \times \text{Predicted Frequency} \tag{15.1}$$

This chapter discusses how a value for the Predicted Frequency term can be obtained (the distinctions between frequency, predicted frequency, probability, and likelihood are explained in Chapter 1). Concepts covered include:

Process Risk and Reliability Management. DOI: http://dx.doi.org/10.1016/B978-0-12-801653-4.00015-1

- The Pareto Principle: identifying the important few and ignoring the unimportant many
- Fault trees
- Event trees
- Monte Carlo simulation
- Markov models
- Layers of Protection Analysis.

THE PARETO PRINCIPLE

In the late nineteenth century the Italian economist and misanthrope Vilfredo Pareto (1848–1923) famously noted that most of the wealth in a community was held by a small proportion of the population. From this insight he developed the 80/20 rule, or the Pareto Principle, which, in the case of community wealth, meant that about 20% of any population owns about 80% of the wealth.

His principle, which has no theoretical underpinning, is widely observed to be true in many fields of human activity (Juran, 1951). It is applied here to the topic of risk analysis in the process industries.

The Pareto Principle can be expressed mathematically as shown in Eq. (15.2).

$$\log n = c + (m \times \log x) \tag{15.2}$$

where n is the number of items whose value is greater than x, c and m are constants.

Examples of the principle's applications in an industrial context include:

- 80% of a company's sales come from 20% of its customers.
- 80% of a company's sales are made by 20% of the sales force.
- 20% of the workers are involved in 80% of the accidents.
- 20% of the equipment items cause 80% of the facility shutdowns.
- 20% of a company's products will account for 80% of the total product defects.
- 80% of weight loss during a diet is achieved with the first 20% of the effort.

In each of the above examples, an "important few" or the "vital few" have a great impact on the business, whereas the "unimportant many" are much less significant. Therefore, a safety manager should direct his or her program toward that minority of incident-creating workers. Spending time on the "unimportant many" is not likely to have much benefit.

One commonly held misconception to do with the Pareto Principle is that 80% of the problems can be resolved with 20% of the resources. In fact the Principle makes no statement at all as to how much effort is needed to address the contributing factors.

IMPORTANCE RANKING

The Pareto Principle expresses itself in an industrial context in the form of "importance ranking." In the second example (Chapter 1), the electrically driven pump, P-101B, has a probability of failure to start of 0.1, i.e., it will not start one times in ten. Management may decide that this failure rate is too high; they wish to reduce the rate to lower than 0.02, i.e., one time in 50.

Table 15.1 Analysis of Pump Failing to Start

Reason for Failure	Number of Incidents	% of Total	Cumulative %	Rank
Operator busy elsewhere	123	60.6	60.6	1
Electrical power not available	44	21.7	82.3	2
Motor fails	18	8.9	91.1	3
Operator starts the wrong pump	12	5.9	97.0	4
Start switch does not work	5	2.5	99.5	5
Discharge valve sticks closed	1	0.5	100.0	6
Totals	**203**	**100.0**		

A survey of facility records for this and similar pumps is made. The following reasons for a pump of this type failing to start immediately are identified:

- Operator busy elsewhere
- Electrical power not available
- Start switch does not work properly
- P-101B motor fails
- Discharge valve sticks closed
- Operator starts the wrong pump.

The number of occurrences of each of the six steps listed above is shown in Table 15.1 and Figure 15.1. The events are sorted by importance ranking.

The data in Table 15.1 show that the items “Operator busy elsewhere” and “Electrical power not available” contribute 82% of the overall failure rate. In terms of the Pareto Principle, these two items are the “important few,” with the others being the “unimportant many.” Therefore, to improve the system reliability, all efforts should be directed toward ensuring that the operator has sufficient time to start the spare pump. If this failure mode can be removed from the system, the system reliability will increase by 60%. If the second high ranked item, “Electrical Power Not Available” can also be eliminated, the system reliability will improve by more than 80% over the initial value. However, if management works on correcting one of the “unimportant many,” say the “Start switch does not work,” the overall failure rate moves from 0.1 to 0.098, a trivial improvement.

FAULT TREE ANALYSIS

Risk can be analyzed in one of two basic ways: inductively or deductively, that is either bottom-up or top-down. In a deductive analysis a system failure is postulated. The analyst then works backward to deduce what combinations of events could have occurred for the system failure to have taken place (a detective solving a crime is thinking deductively). Fault tree analysis (FTA), the topic discussed in this section, is deductive. An inductive analysis works in the other direction. A single failure, such as a pump stopping or a valve closing at the wrong time, is postulated. The

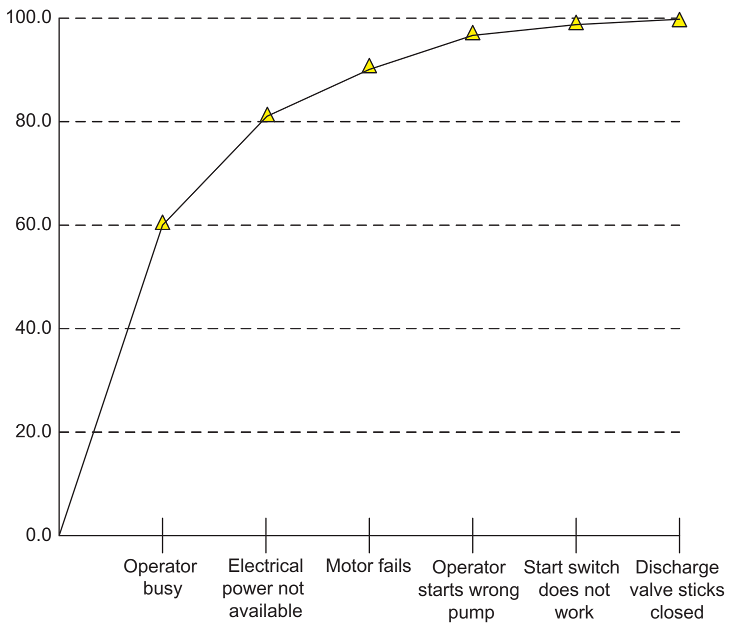


FIGURE 15.1

Cumulative failure rate.

inductive approach then determines what impact the item failure could have on the overall system performance. By contrast, event tree analysis (page 725). Both techniques provide a clear and intelligible way of determining the combination of events needed for an undesirable incident to occur. Their strict logic cuts through the "I think/You think" discussions that are the bane of so much risk analysis.

First used by the Bell Telephone Laboratories and the Boeing Corporation in the years 1962–64 to analyze potential problems with the Minuteman missile launch control system, FTA provides a clear and intelligible way of determining the combination of events needed for an undesirable incident to occur (Vesely, 1981). In particular, the graphical nature of the analysis can help managers, engineers, and operators better understand how their systems can fail. Moreover, it is often found that the rigor and logic of an FTA stimulates creative thinking, and allows experts to add their experience and opinions in a structured manner. So the fault tree method—in spite of the fact that it is based on logic and Boolean algebra—can help identify new hazards and previously unthought of failure mechanisms.

Once a fault tree has been developed, failure rate data for individual components in the system can be entered into the tree so that an estimate of the likelihood of the undesired event (the "Top Event") can be made. Frequently the quality of the failure rate data is poor; nevertheless, through use of the Pareto Principle or 80/20 rule discussed above, a quantified analysis still provides useful insights because it identifies which items in the system contribute the most to system failure. Moreover, once the model has been developed, and preliminary estimates as to failure rates have been made, case studies that examine changes to the process and the effects of additional safeguards can be carried out. Also, as improved data for equipment failure rates and repair times becomes available, the quality of the analysis will improve.

FTA has a reputation for being time-consuming and costly, and for requiring the services of highly specialized risk analysts. This reputation came about because most of the original FTA work was carried out in the aerospace and nuclear power industries. In both of those industries the consequences of an accident can be very severe so highly detailed analysis was required. This perception that FTA is extremely time-consuming may be one reason that the technique has not been more widely adopted by the other industries. (Another reason for the method's lack of general adoption may be that fault tree diagrams are not immediately intuitive; the managers who are the ultimate customers of the analysis require some training in how to understand the results.)

In fact, fault trees do not have to be large, nor does their development have to be excessively time-consuming. The simple example provided in this chapter shows how the rigorous logic and quantification provided by even a small, quickly executed fault tree can provide useful and unique insights into how a system can fail, and what can be done to reduce the associated risk. Moreover, sophisticated software is not needed for smaller FTAs. As the examples in this chapter demonstrate, simple trees can be drawn using basic graphics packages, and their quantification can be executed with spreadsheets, or even hand calculations.

Some of the technical terms used in fault tree and ETA are explained below. In this book, words such as "or," "and," and "if" are put in small capitals when referring to the elements of a fault tree. Doing so helps distinguish the use of those words when used in normal discursive text.

GATES

A fault tree is built up of gates and events. The principal types of gate are:

- OR Gates
- AND Gates

Although other types of gate are sometimes used, they can all be created from a combination of OR and AND Gates.

OR Gate

An OR Gate is a logic gate that gives a positive output if one or more of the inputs to the gate are positive. The symbol for an OR GATE is shown in Figure 15.2. Various labeling conventions are used in FTA. The system used in this book is to put a cross inside the OR Gate symbol. Other analysts use a plus sign to provide the same meaning.

An example of an OR Gate is the source of ignition for a fire hazard. For example, four possible sources of ignition may exist:

- A naked flame (say from a welding torch)
- A spark from electrical equipment
- A hot surface (such as the outside of a fired heater)
- Lightning.

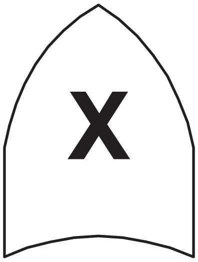


FIGURE 15.2

OR Gate.

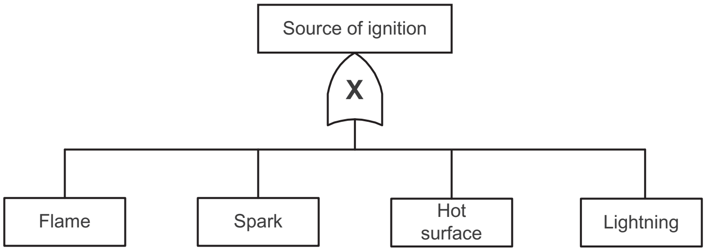


FIGURE 15.3

Example of the use of an OR Gate.

The OR GATE for these four items can be written in words as follows:

> IF a naked flame exists OR IF a spark exists OR IF a hot surface is present OR IF lightning is present, THEN a source of ignition exists.

Figure 15.3 shows the OR Gate that corresponds to the above logic.

There is no theoretical limit to the number of events that can enter an OR GATE. However, more than five inputs can be difficult for people to visualize and understand. In such circumstances, it generally makes sense to create two or more OR GATES; the output from each then enters a higher level OR Gate as illustrated in the transition from Figure 15.3 to Figure 15.4.

The logic and mathematics to do with the system analysis is not changed by dividing the gate into two; the division is made just to provide humans with a better understanding as to what is going on (Figure 15.5).

AND Gate

The second type of logical gate used in fault trees is the AND GATE, the symbol for which is shown in Figure 15.6. All inputs to an AND GATE need to be positive for the output to be positive.

AND GATES are frequently found in safety systems. One of the events entering the AND gates represents an item or equipment failure; the other input represents a safety system whose purpose is to protect the system against the consequences of that failure. For this reason, the more AND Gates that can be introduced into a Fault Tree, the more reliable and safer the system will be.

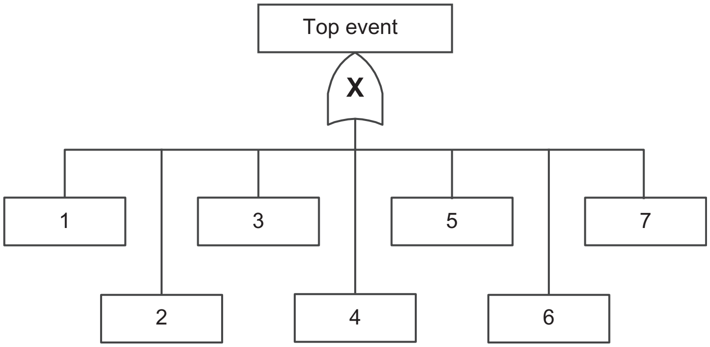


FIGURE 15.4

OR Gate with seven inputs.

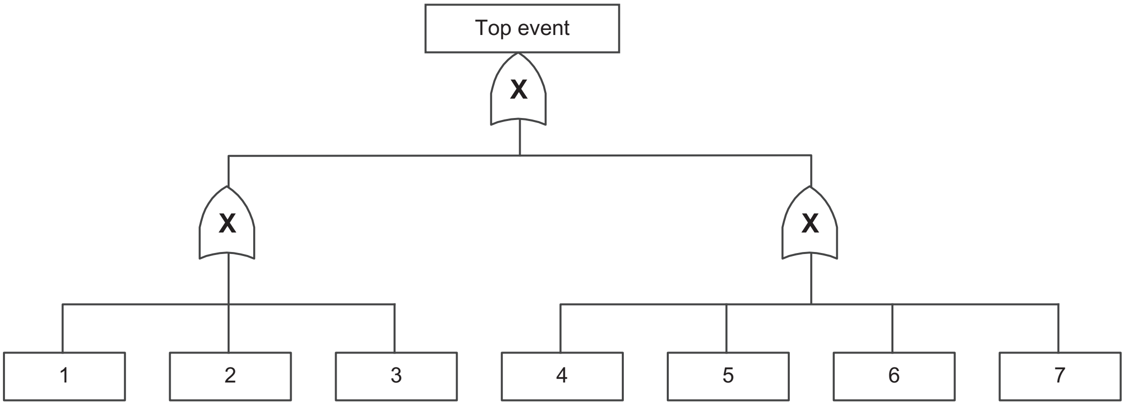


FIGURE 15.5

OR Gate divided into two.

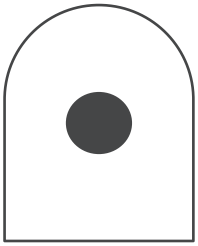


FIGURE 15.6

AND Gate.

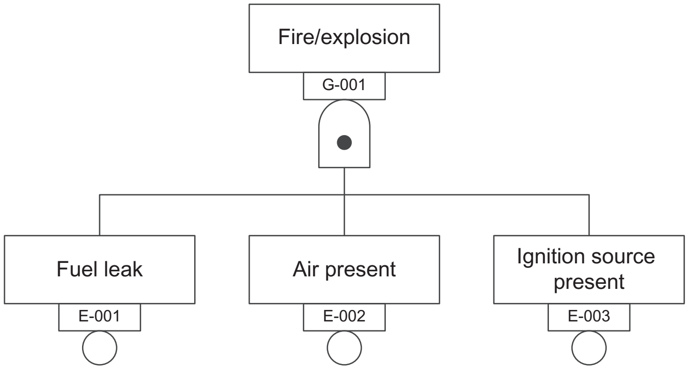


FIGURE 15.7

Fire triangle.

As with the OR Gate, there is no mathematical limit to the number of inputs to an AND Gate. However, it may also make sense to divide the gate into subgates so that the tree is easier for humans to understand.

The classic "fire triangle" can be visualized as an AND GATE. For a fire to exist three conditions must be met:

1. Fuel above its flash point must be present.
2. Oxygen (usually as a component of air) must be present.
3. An ignition source such as an open flame or hot surface must exist.

The above logic can be expressed as follows:

> IF fuel is present AND IF oxygen is present AND IF an ignition source exists, THEN a fire will occur.

The Fault Tree Gate corresponding to the above statement is shown in Figure 15.7.

The events and gates each have a Description and a Label associated with them. The Description is intended for use by persons reading the results of the analysis. It provides detail as to the purpose and function of that event or gate. The label is a unique identifier used by the fault tree software. Generally, the label will be composed of a letter and a number. The letter "G" indicates a gate; the letter "E" an event (any type).

It is important to give unique labels to each of the gates and events for the following reasons:

- Different events may have the same name. If the process contains two tanks, then the event "Tank Overflow" can occur in two places. However, each will have its own distinct label.
- Some events occur in more than one place on the tree. In the worked example, the event "Instrument Plugs"—E-004—occurs three times. This is a common cause effect. Common Cause events need to be identified properly before the Tree is quantified. How this can be done is discussed later in this chapter.

Figure 15.7 can be quantified, as shown in Figure 15.8.

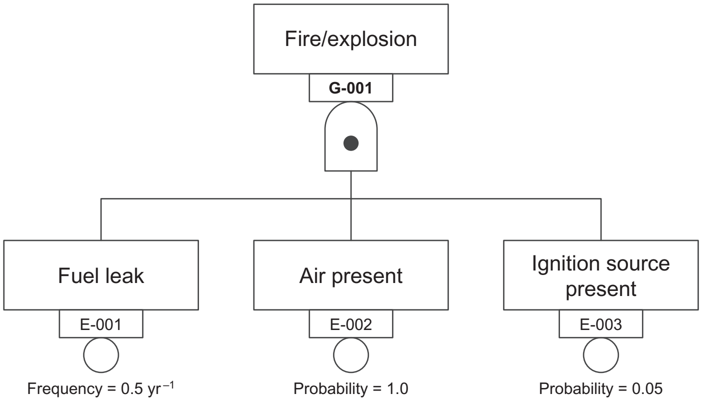


FIGURE 15.8

Quantified fire triangle.

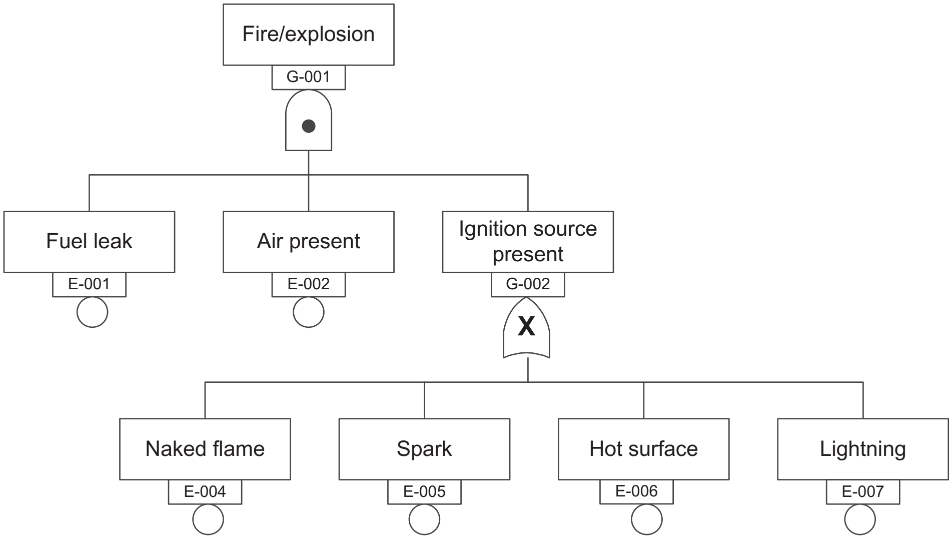


FIGURE 15.9

Expansion of the fire triangle.

Figure 15.8 shows that a fuel leak somewhere on the facility is expected to occur once every 2 years; air will always be present; the probability of an ignition source being present is one in 20. Hence the overall chance of a fire is one in 40 years.

Figure 15.8 can be further expanded as shown in Figure 15.9 by using an OR Gate to expand the "Ignition Source Present" term.

Some of the events that enter an AND Gate are conditional terms that have a probability of 1.0, i.e., they are certain to exist. For example, if the possibility of an outside fire is being considered, the probability that air will be present is 1.0, and therefore this term may be excluded from the tree on the grounds that it can be taken for granted. (On the other hand, by including it, fresh ideas for controlling the fire to do with excluding air may be generated.)

VOTING Gate

A VOTING Gate has at least three inputs; two or more of which need to be "positive" for the outcome to be "positive." For example, if the VOTING Gate has three inputs, where two of them must be "positive" for the output to be "positive" then a 2 out of 3 (2oo3) VOTING GATE has been created. The basic purpose of such a gate is to have a system that operates safely, but which allows for one of more inputs to be erroneous without leading to a system trip. VOTING GATES are often found in safety systems where spurious or nuisance trips are highly undesirable but the potential for major loss is high.

For example, in furnace operation it is important that there be a check for the continued presence of a flame at the burners. If the flame goes out but fuel continues to flow into the hot furnace, an explosive gas cloud may be created in the furnace. Were this cloud to ignite on, say, a hot surface in the firebox, the furnace could be destroyed by the resulting explosion. To prevent such an explosion from occurring, it is common to install a fire eye in the furnace. This is a device that detects the presence of a flame at the burners. If the fire eye does not see a flame it sends a signal that cuts off the flow of fuel. Since it is vital that this shutdown system works properly, a second fire eye is often installed. Then, if the first fire eye does not work for some reason, the second fire eye will detect the problem and shut down the system.

Fire eyes can generate false alarms. If the instrument has internal problems, or if there is smoke or dirt in the furnace, the fire eye may (incorrectly) determine that the flame(s) have gone out, leading to a spurious or nuisance system shutdown. In such situations, it is possible to enhance both safety and reliability by installing *three* fire eyes, and put their signals through a voting system, in which two of the three must detect a flame-out condition before the furnace is shut down.

The symbol for a 2oo3 VOTING Gate is shown in Figure 15.10. This example has three inputs, A, B, and C, two of which have to be positive for the output to be positive. The VOTING Gate symbol has the shape of an OR Gate, but a diagonal line is inserted across it, and the voting numbers put on

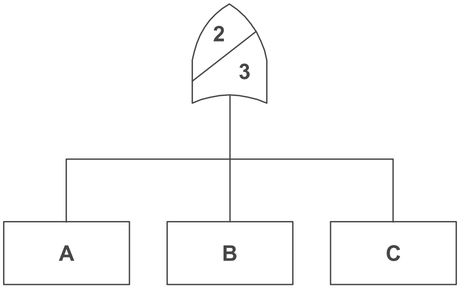


FIGURE 15.10

Voting Gate.

either side of the line. The numbers “2” and “3” shown in Figure 15.10 represent a 2oo3 Gate, i.e., two out of three inputs have to be positive for the output from the Gate to be positive.

As already noted, all gate types can eventually be broken down into a combination of AND and OR gates. For example, the voting gate shown in Figure 15.10 can be broken down to the structure shown in Figure 15.11.

EVENTS

The events in a fault tree are connected to one another with the gates that have just been described. There are three types of events:

1. The Top Event
2. Intermediate Events
3. Base (or Basic) Events.

Top Event

As already noted, the purpose of a fault tree is to determine how some undesired event is caused. This undesired event, which typically represents a system failure, is referred to as the TOP EVENT because it is at the top of the tree. Examples of Top Events include:

- Loss of containment from a storage tank
- High temperature in reactor
- Loss of production.

The Top Event should be defined as precisely as possible. In general, the answers to the following questions should be included in the definition of the Top Event:

- How much (quantity)?
- How long (duration)?
- What is the safety impact?

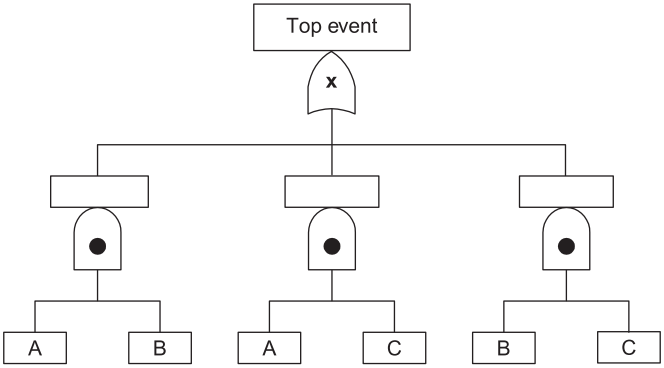


FIGURE 15.11

2oo3 VOTING Gate breakdown.

- What is the environmental impact?
- What is the production impact?
- What is the regulatory impact?

For example, the phrase “Loss of production” is not detailed enough to build a useful fault tree. Using the key phrases above, a better description for this Top Event would be:

> Loss of at least 200 tons of production of light oil. Safety, environmental and regulatory issues are not considered in this top event.

Figure 15.12 shows the Top Event for the standard example. It has a Gate label—G-001—because it will be developed further.

Intermediate Events

An Intermediate Event is an event that is one that has been designated for further development as the analysis progresses. For example, when developing the fault tree to do with the loss of production just discussed, an intermediate event could be: “Reactor shuts down.” It is likely that, as the tree is developed, this simple phrase will be expanded as various reasons for reactor shutdown are considered. The reasons for reactor shutdown could include loss of feed, loss of flow of heating medium, or instrument malfunction.

The symbol for an Intermediate Event is a diamond as shown in Figure 15.12, in which the Top Event is also an Intermediate Event because it is to be developed further.

As a tree develops, the Intermediate Events will be expanded into additional gates and events. Even though these Intermediate Events then disappear from the tree, the original label is retained, even though it is no longer used.

Base Events

Intermediate Events are expanded through OR and AND Gates until eventually they become Base (or Basic) Events, at which point development of that particular branch of the tree ceases. A Base Event is a stand-alone event that will not be developed further (at least at this stage of the analysis). Base Events, which are sometimes referred to as Primal Events (Lapp, 2005), must be independent

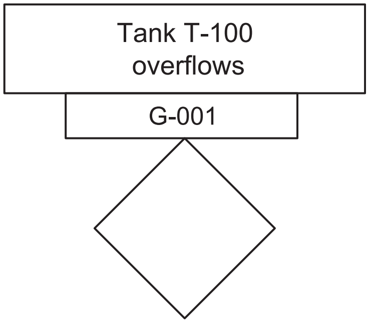


FIGURE 15.12

Top Event.

of one another. If the tree is to be quantified, each Base Event will have either a predicted failure rate or a probability value associated with it.

The symbol for a Base Event in a fault tree is a circle, as shown in Figure 15.13.

House Event

A House Event (Figure 15.14) is one that is present all the time. An example of such an event would be the presence of air when analyzing fire scenarios.

TOP-DOWN DEVELOPMENT OF A FAULT TREE

An FTA starts by defining the "undesirable" Top Event, then working out what other events are needed for the Top Event to be initiated, and how all the events interact with one another. Once the tree has been constructed, it can be quantified.

Fault trees are developed top-down, i.e., the analyst starts with a very simple big picture, then adds more and more detail in an orderly manner. The process for developing a fault tree can be divided into the following steps:

1. Define the Top Event
2. Build the Fault Tree
3. Identify the Cut Sets

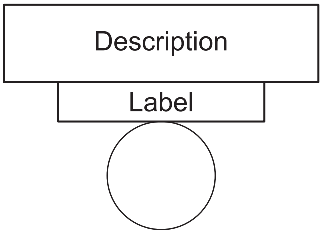


FIGURE 15.13

Base Event.

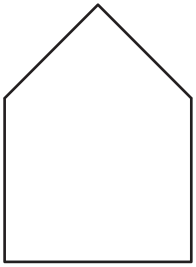


FIGURE 15.14

House Event.

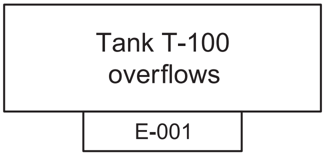


FIGURE 15.15

Top Event label.

4. Eliminate Repeat Sets
5. Eliminate Repeat Events in a Set
6. Eliminate Redundant Events
7. Quantify the Risk
8. Risk Rank the Base Events
9. Reduce Risk through use of the Pareto Principle.

The process listed above is described in more detail below, using the overflow of Tank, T-100, from the standard example to illustrate concepts as they are introduced.

1. Define the Top Event

The first step in the analysis is to define the Top Event. In the example, the Top Event is "Tank T-100 Overflows." A more detailed description for the Top Event is:

> Tank, T-100, overflows sufficient liquid such as to require an environmental report to be submitted to the regulatory agency.

The detailed description will be entered into the fault tree software database; the abbreviated description is used for the fault tree sketch.

The first building block in the Fault Tree can now be put in place, as shown in Figure 15.15. The label in Figure 15.12 has now become E-001.

2. Build the Tree

Having defined the Top Event, development of the tree can begin.

Figure 15.16 shows an OR Gate below the Top Event. Entering the OR Gate are two Intermediate Events. The first of these is "System Fault"—it covers all the equipment, instrument, and human failures that can cause the tank to overflow. The second input to the Top Event is "All Other Events." This phrase covers all those events that could cause the Top Event to occur, but which have not been identified. It is a truism that no hazards analysis can ever be complete; there will always be scenarios and hazards that were not identified, or not properly understood. Putting an "All Other Events" gate into the fault tree at this juncture serves as a reminder that no hazards analysis can ever be complete; and that predicted risk values are likely to be overly optimistic.

In Figure 15.16, E-001 has been renamed G-001—an event is now a gate.

The second stage in the development of the tree is shown in Figure 15.17. The Intermediate Event at G-002 has been expanded through an AND Gate as shown.

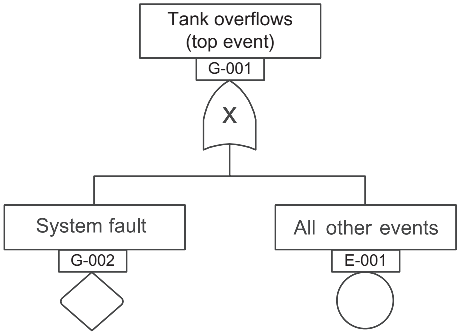


FIGURE 15.16

Top Event development.

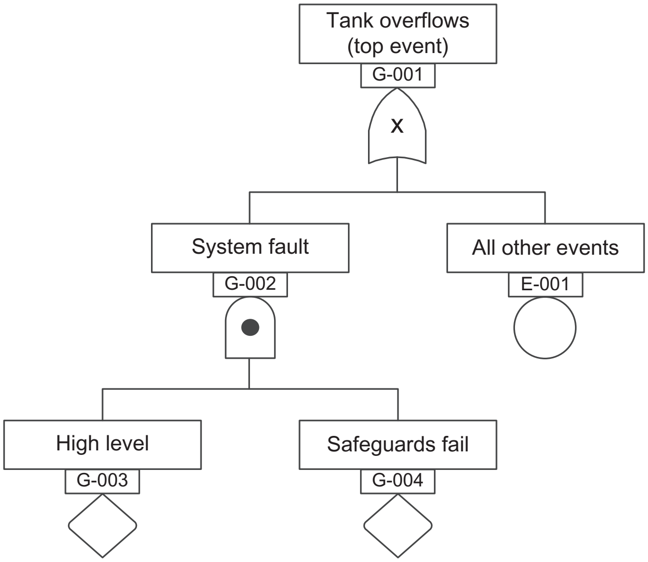


FIGURE 15.17

Second level of development.

The logic of Figure 15.17 is that high level in T-100 has various causes—these are collected in the Intermediate Event G-003. The system also has various safeguards to prevent high level—they enter the Intermediate Event G-004. G-003 and G-004 enter an AND Gate whose meaning is, “If we get high level, and if the safeguards fail, then the tank will overflow.”

The third level of development for this fault tree is shown in Figure 15.18.

The “High-Level” scenario divides through an OR Gate into two Intermediate Events: the pumps fail or the instruments fail. Two new Intermediate Events, G-005 and G-006, are thus created.

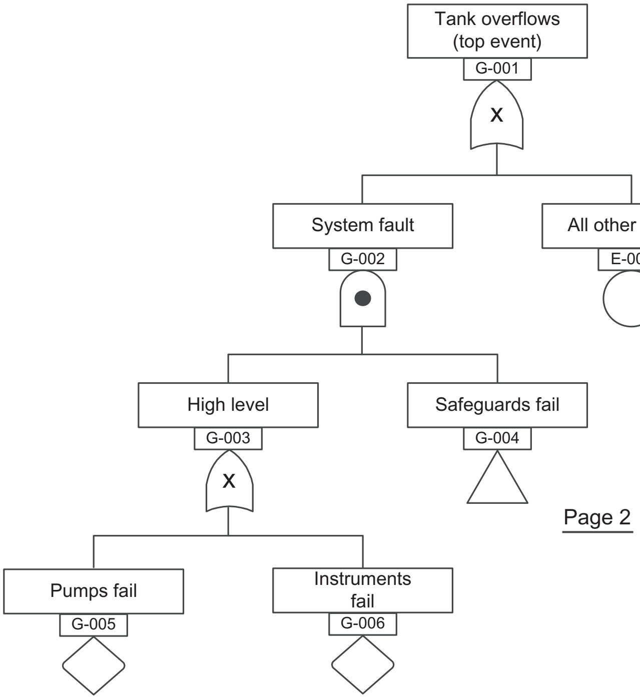


FIGURE 15.18

Third level of development 1.

The diamond beneath G-004—"Safeguards Fail"—has been replaced by a triangle with a reference to "page 2." This means that the logic for "Safeguards Fail" is developed on another sheet of paper as shown in Figure 15.19. The analysis and eventual quantification are not affected in any way by this division into two pages, which is done simply to make the tree of a manageable size for those who are printing and reading it.

The process of developing the Fault Tree in a top-down manner continues to the level is shown in Figures 15.20 and 15.21. Figure 15.20 focuses on the development of the "Event Occurs" scenario, whereas Figure 15.21 develops the "Safeguards Fail" scenario.

Inspection of Figures 15.20 and 15.21 leads to the following observations:

- Page 1 (Figure 15.20)—the System Failure—develops through a series of OR and AND Gates. The system can fail due to problems with the pumps or with the instruments. Eventually, this part of the Tree leads to the creation of six separate Base Events.
- Page 2 (Figure 15.21)—the Safeguards Fail—has only OR Gates. It generates a total of four Base Events. There is no redundancy within the safeguard system. *A priori* this lack of AND Gates may suggest that this is the area where improvements could be made, i.e., it may make sense to have additional safeguards.

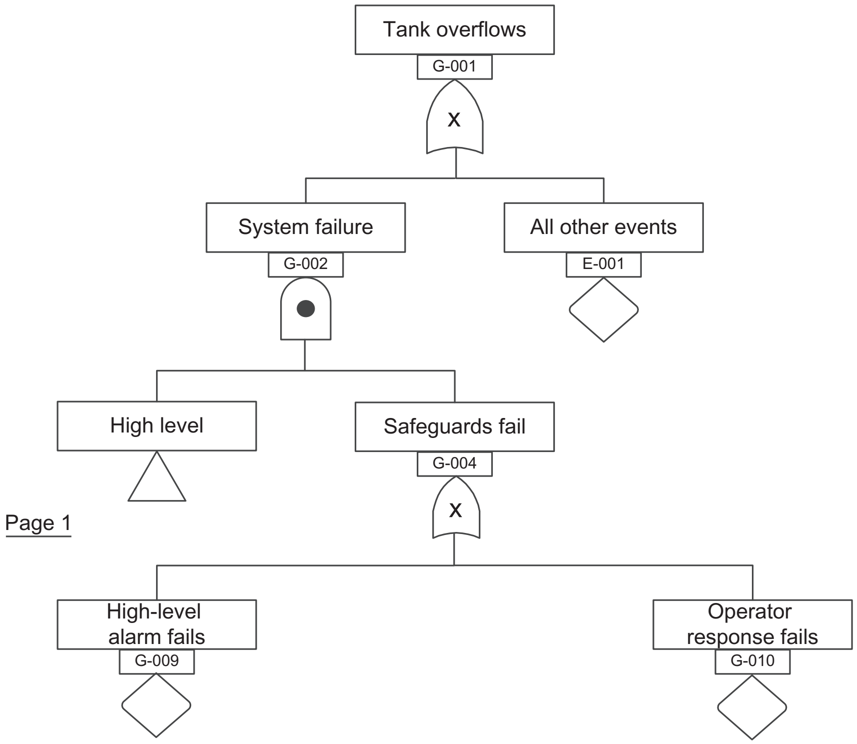


FIGURE 15.19

Third level of development 2.

At the conclusion of the analysis all of the Intermediate Events (except for the "All Other Events" term) will have been converted into gates or Base Events.

The decision as to when to stop the expansion of an Intermediate Event usually depends on the extent to which that event contributes to the overall risk. Another reason for not developing an Intermediate Event is that, if further expansion leads into areas of high uncertainty, there is little point in continuing. On page 2 of the tree is the Intermediate Event "Operator Response (fails to notice high level)." There may be two reasons for this:

1. He is busy elsewhere, and so fails to spot the T-100 high-level scenario.
2. He reads the wrong gauge.

Since it will be difficult to determine the likelihood of these individual items, it is probably best to stop the development of this term at this point.

3. Identify the Cut Sets

Development of a fault tree in the manner shown in the previous pages is very useful in that everyone is forced to think through logically ways in which events may interact with one another in a

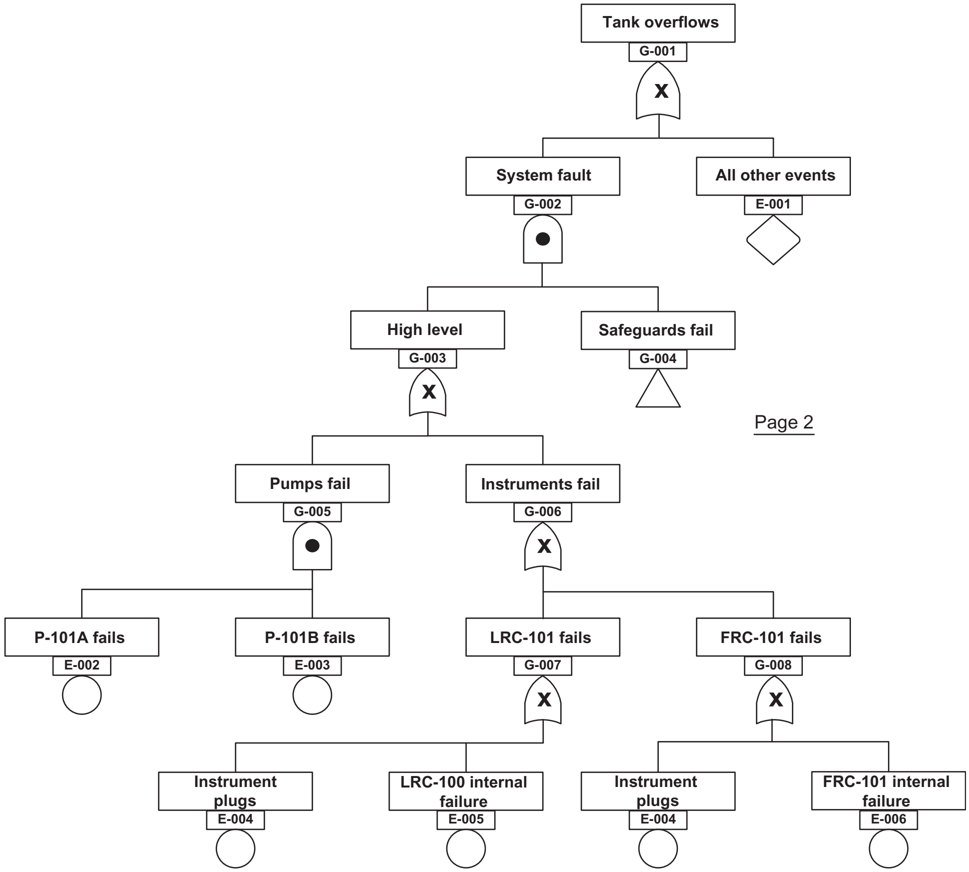


FIGURE 15.20

Final fault tree (page 1).

complex manner to create an unacceptable incident. However, it can be seen that a tree could quickly become difficult to follow and understand as more events and gates are added. Also, inspection of Figures 15.20 and 15.21 does not give any immediate insights as to what are the leading factors in the risk associated with tank overflow. (These figures do, however, give a visual Gate-by-Gate picture of the overall risk.)

In order to simplify and summarize the lessons to be learned from FTA, and in order to provide a basis for quantifying the Tree, the next step in the analysis is to develop Cut Sets, which are defined as follows:

> A Cut Set is a collection of Events such that, if all the Events in that Cut Set were to occur, the Top Event would occur.

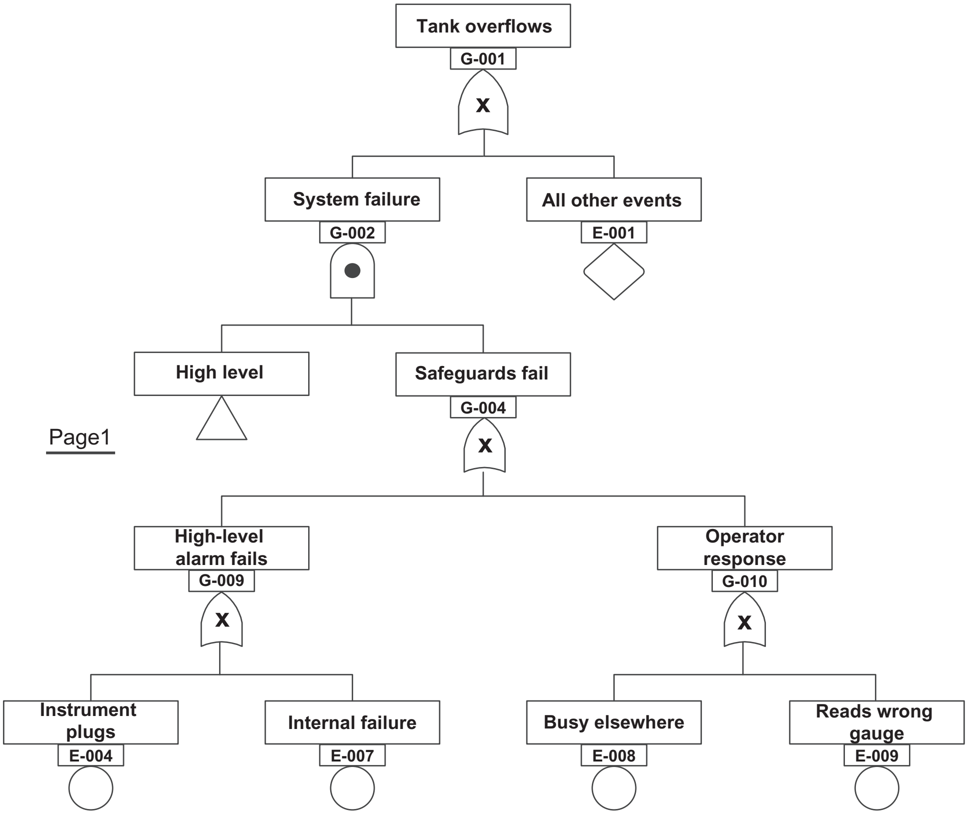


FIGURE 15.21

Final fault tree (page 2).

The convention used in this book is to show cut sets as being within curly braces { }. Using the example, the first cut set, which is simply the Top Event is:

$$\{E\text{-}001\}$$

which becomes:

$$\{G\text{-}001\}$$

Events which constitute an OR Gate are shown on separate lines, where each line represents a cut set, as shown below based on the information in “Figure 15.18.

$$\{G\text{-}002\}\text{—System Failure}$$

$$\{E\text{-}001\}\text{—“All Other Events”}$$

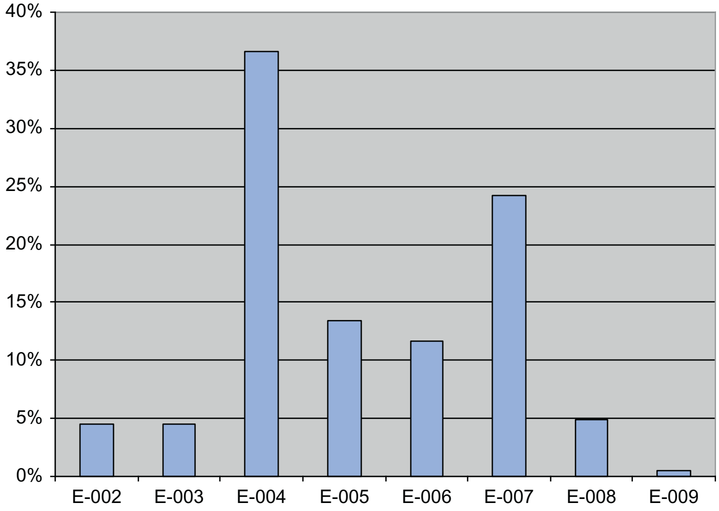


FIGURE 15.22

Risk ranking.

Events that enter an AND GATE are developed horizontally as shown for the expansion of G-002 (Figure 15.18). All the events on a line must occur for the cut set to deliver a positive output. The cut sets are now:

$$\{G\text{-}003\ \ G\text{-}004\}$$

$$\{E\text{-}001\}$$

The Gate G-002 has now disappeared from the analysis; it has been replaced by G-003 and G-004.

G-003 is an OR GATE that, on expansion, creates two new cut sets. The system is now:

$$\{G\text{-}005\ \ G\text{-}004\}$$

$$\{G\text{-}006\ \ G\text{-}004\}$$

$$\{E\text{-}001\}$$

Repeating the above actions for all events, the full set of noncondensed Cut Sets for the final tree of Figures 15.22 and 15.23 is shown in Table 15.2. All the gates, i.e., those terms starting with the letter “G,” have been transformed into base events.

The aim now is to develop *minimal* cut sets, which show just the minimal number of events and combination of events that are needed for the TOP EVENT to take place. The following process is followed:

- Eliminate repeat cut sets
- Eliminate repeat events with a cut set
- Eliminate redundant events.

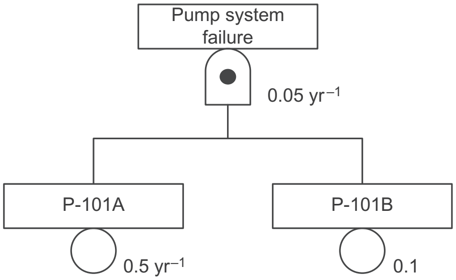


FIGURE 15.23

Pump system.

Table 15.2 The Complete Noncondensed Cut Sets

1. {E-002 E-003 E-004}
2. {E-002 E-003 E-007}
3. {E-002 E-003 E-008}
4. {E-002 E-003 E-009}
5. {E-004 E-004}
6. {E-004 E-007}
7. {E-004 E-008}
8. {E-004 E-009}
9. {E-005 E-004}
10. {E-005 E-007}
11. {E-005 E-008}
12. {E-005 E-009}
13. {E-004 E-004}
14. {E-004 E-007}
15. {E-004 E-008}
16. {E-004 E-009}
17. {E-006 E-004}
18. {E-006 E-007}
19. {E-006 E-008}
20. {E-006 E-009}
21. {E-001}

4. Eliminate Repeat Sets

Cut sets have the mathematical form of an OR GATE. Therefore, if a cut set occurs more than once, duplicates can be eliminated. In other words, the statement "IF A OR IF A" can be reduced to "IF A." For example, in Table 15.13 the cut set {E-004 E-007} occurs twice (lines 6 and 14).

Table 15.3 repeats Table 15.2, but with the duplicate cut sets removed.

Strikethrough lines have been drawn through the duplicate cut sets, which are thereby eliminated from the analysis. The number of cut sets has been reduced from 21 to 17.

Table 15.3 Repeat Cut Sets Removed

1.	{E-002 E-003 E-004}
2.	{E-002 E-003 E-007}
3.	{E-002 E-003 E-008}
4.	{E-002 E-003 E-009}
5.	{E-004 E-004}
6.	{E-004 E-007}
7.	{E-004 E-008}
8.	{E-004 E-009}
9.	{E-005 E-004}
10.	{E-005 E-007}
11.	{E-005 E-008}
12.	{E-005 E-009}
~~13.~~	~~{E-004 E-004}~~
~~14.~~	~~{E-004 E-007}~~
~~15.~~	~~{E-004 E-008}~~
~~16.~~	~~{E-004 E-009}~~
17.	{E-006 E-004}
18.	{E-006 E-007}
19.	{E-006 E-008}
20.	{E-006 E-009}
21.	{E-001}

5. Eliminate Repeat Events in a Set

Repeat events within a Cut Set are redundant, and can be eliminated. In this example, this occurs just once where {E-004 E-004} becomes {E-004}. In words, the statement "IF E-004 occurs AND E-004 occurs" becomes "IF E-004 occurs."

After the repeat events have had a strikethrough line put through them, the further reduced cut set list is shown in Table 15.4.

6. Eliminate Redundant Events

Redundant terms within a cut set can be removed. For example, the sets:

{A B C}

{A B}

become:

{A B}

because both A and B are a sufficient and necessary condition for the cut set to be initiated; the occurrence or nonoccurrence of event "C" has no effect on the final outcome.

After the redundant events have had a strikethrough line put through them, the further reduced cut set list is shown in Table 15.5.

The final minimal cut sets are shown in Table 15.6, which is a repeat of Table 15.5 showing only the remaining cut sets.

Table 15.4 Repeat Cut Sets Removed

1.	{E-002 E-003 E-004}
2.	{E-002 E-003 E-007}
3.	{E-002 E-003 E-008}
4.	{E-002 E-003 E-009}
5.	{E-004 ~~E-004~~}
6.	{E-004 E-007}
7.	{E-004 E-008}
8.	{E-004 E-009}
9.	{E-005 E-004}
10.	{E-005 E-007}
11.	{E-005 E-008}
12.	{E-005 E-009}
~~13.~~	~~{E-004 E-004}~~
~~14.~~	~~{E-004 E-007}~~
~~15.~~	~~{E-004 E-008}~~
~~16.~~	~~{E-004 E-009}~~
17.	{E-006 E-004}
18.	{E-006 E-007}
19.	{E-006 E-008}
20.	{E-006 E-009}
21.	{E-001}

Table 15.5 Redundant Cut Sets Removed

~~1.~~	~~{E-002 E-003 E-004}~~
2.	{E-002 E-003 E-007}
3.	{E-002 E-003 E-008}
4.	{E-002 E-003 E-009}
5.	{E-004 ~~E-004~~}
6.	{E-004 E-007}
7.	{E-004 E-008}
8.	{E-004 E-009}
9.	{E-005 E-004}
10.	{E-005 E-007}
11.	{E-005 E-008}
12.	{E-005 E-009}
~~13.~~	~~{E-004 E-004}~~
~~14.~~	~~{E-004 E-007}~~
~~15.~~	~~{E-004 E-008}~~
~~16.~~	~~{E-004 E-009}~~
17.	{E-006 E-004}
18.	{E-006 E-007}
19.	{E-006 E-008}
20.	{E-006 E-009}
~~21.~~	{E-001}

Table 15.6 The Minimal Cut Sets

{E-002 E-003 E-007}
{E-002 E-003 E-008}
{E-002 E-003 E-009}
{E-004}
{E-005 E-007}
{E-005 E-008}
{E-005 E-009}
{E-006 E-007}
{E-006 E-008}
{E-006 E-009}
{E-001}

Disregarding E-001, "All Other Events," a first inspection of the above list suggests that the system weak spot is the Cut Set "E-004, Instruments Plug" because it will cause both the level control system to fail, and it will also defeat some of the safeguards. It is a single point failure; all the other Cut Sets require the simultaneous and independent failure of two or three items. Therefore, were the analyst to be asked for an opinion at this point as to the best way of improving system safety/reliability, his or her response initial response would likely be that instrument pluggage is the issue to be addressed. However, this result cannot be confirmed unless the risk is quantified, as discussed in the following section.

7. Quantify the Risk

Development of a fault tree as shown in the previous sections can be very beneficial because the system logic shows just how events may occur. All the same, a fault tree becomes much more useful when quantified because management will be presented with a clear understanding as to which hazards contribute the most toward risk. This insight helps determine where investment resources are best spent in order to achieve the greatest reduction to that risk.

Using the Standard Example once more, sample quantitative BASE EVENT data are shown in Table 15.7.

Mathematics of an OR Gate

The values entering an OR Gate are summed. For example, the probability of the operator failing to respond to an upset is

$$\lambda_{\text{G-010}} = (\lambda_{\text{E-008}} + \lambda_{\text{E-009}}) \tag{15.3}$$

Based on the data in Table 15.7 the probability of the operator failing to notice High Level in T-100 is estimated to be (0.1 + 0.01) or 0.11.

For n inputs to an OR Gate, the overall failure rate using just first-order terms is calculated from Eq. (15.4).

$$\lambda_{\text{G}} = \lambda_1 + \lambda_2 + \cdots + \lambda_n \tag{15.4}$$

When the probability or frequency values entering an OR Gate are high (say greater than 0.1), it is necessary to expand Eq. (15.4) to include higher order terms. For example, if an OR Gate has two

Table 15.7 Quantitative Data for Example

Label	Item	Value	Units
E-001	All other events	Unknown	yr^{-1}
E-002	P-101A fails	0.5 (once in 2 years)	yr^{-1}
E-003	P-101B fails	0.1 (1 in 10 chance of not starting on demand)	—
E-004	Instrument plugs	0.25 (once in 4 years)	yr^{-1}
E-005	Internal failure (LRC-101)	0.15 (once in 6.7 years)	yr^{-1}
E-006	Internal failure (FRC-101)	0.13 (once in 7.7 years)	yr^{-1}
E-007	Internal failure (level alarm)	0.5	—
E-008	Operator busy elsewhere	0.1	—
E-009	Operator reads wrong gauge	0.01	—

inputs, A and B, with probability values of 0.6 and 0.5, respectively, then, using Eq. (15.4), their combined value is 1.1, which is physically impossible, since the maximum value for probability can never be greater than 1.0 (i.e., 100%).

This mathematical difficulty is caused by failing to deduct the second-order term that is needed to provide for contingent failure. For example, if A has already failed, then the system is *de facto* in a failed state, so the status of B is immaterial. Since the probability of B failing when A is already failed is p(A) × p(B), the true failure rate for these two events is $p(A) + p(B) - (p(A) \times p(B))$. Using the values of 0.6 and 0.5, respectively, the overall failure rate with the second-order term included is $(0.6 + 0.5 - 0.3)$, which is 0.8, and is less than unity. Therefore, the calculated failure rate is mathematically plausible.

In practice, the second-order term is often very small, particularly when the incoming terms have values of 0.05 or less. Second-order terms do not need to be calculated in such cases. For example, if Events A and B have respective probabilities of 0.02 and 0.03, then the value of the OR Gate is $(0.02 + 0.03 - 0.0006)$, or 0.0494. The second-order term affects the result by just over 1%.

Equation (15.5) provides the value for an OR GATE with two inputs.

$$\lambda_G = \lambda_1 + \lambda_2 - (\lambda_1 \times \lambda_2) \tag{15.5}$$

where λ_G represents the failure rate for the Gate.

In general, where multiple events enter an OR GATE, and second- and third-order terms are to be considered, the output of the Gate is:

$$\lambda_G = 1 - [(1 - \lambda_1) \times \cdots \times (1 - \lambda_n)] \tag{15.6}$$

for a total of *n* inputs to the Gate.

Mathematics of an AND Gate

The product of an AND Gate is obtained by multiplying the input values of the entering events, as shown in Eq. (15.7).

$$\lambda_G = \lambda_1 \times \lambda_2 \times \cdots \times \lambda_n \tag{15.7}$$

for a total of *n* inputs to the Gate.

AND Gates always produce an output whose value is less than any of the input values (which is why they represent increased reliability and safety).

It is important to ensure that no more than one of the terms entering an AND Gate has units of inverse time. If two such events enter the gate then the product from the gate will have a value of time^{-n}, where n is greater than 1. Such a result is physically impossible.

Mathematics of a Voting Gate

The mathematics for a Two-Out-Of-Three (2oo3) VOTING Gate is shown in Eq. (15.8).

$$\lambda_G = 1 - ((1 - \lambda_1 \times \lambda_1) \times (1 - \lambda_2 \times \lambda_3) \times (1 - \lambda_1 \times \lambda_3)) \tag{15.8}$$

Other logic equations are available for other types of VOTING Gate, but such equations are not really needed since any VOTING Gate can be broken into a combination of AND and OR Gates as already illustrated in Figure 15.15 (a 2oo3 system), which can be broken down into the following three cut sets:

{A B}
{A C}
{B C}

Cut Set quantification

Quantification of a fault tree itself is normally carried out through the use of cut sets so as to avoid redundant and repeat calculations. Each Cut Set is equivalent to an AND Gate, and the cut sets combine with one another as if they are an OR Gate.

Using the cut sets developed in Table 15.7 for the standard example, the likelihood of occurrence of the Top Event using Eq. (15.8) is shown in Table 15.8. (The E-001 term has been omitted from this calculation.)

Table 15.8 Frequency of Top Event

Cut Set			Value (yr^{-1})		Predicted Frequency (yr)
E-002	E-003	E-007	$0.5 \times 0.1 \times 0.5$	0.025	40
E-002	E-003	E-008	$0.5 \times 0.1 * 0.1$	0.005	200
E-002	E-003	E-009	$0.5 * 0.1 * 0.01$	0.0005	2,000
E-004			0.25	0.25	4
E-005	E-007		$0.15 * 0.5$	0.0075	13
E-005	E-008		$0.15 * 0.1$	0.015	67
E-005	E-009		$0.15 * 0.01$	0.0015	667
E-006	E-007		$0.13 * 0.5$	0.0065	15
E-006	E-008		$0.13 * 0.1$	0.013	77
E-006	E-009		$0.13 * 0.01$	0.0013	769
Total				**0.4513**	**2.2**

The overall predicted frequency for tank overflow of 0.4513 yr^{-1}, or roughly once in every 2 or 3 years.

It would generally be agreed that a significant environmental incident such as this tank overflow occurring once every three is not acceptable. Management may decide that they want the system failure rate reduced to 1 in 10 years, or better. How this can be done is discussed below.

8. Risk Rank

In response to the desire to reduce the likelihood of tank overflow, a vendor may claim that a new type of level alarm will reduce the probability for E-007 from 0.5 to 0.05, i.e., a factor of 10 improvement. The new system risk value is calculated in Table 15.9.

The overall failure rate has now moved from once in 2.2 years to once in 3.3 years. This improvement is not all that significant, and the overall rate is still well below the target of once in 10 years. The dramatic improvement in performance of this instrument does not lead to a corresponding improvement in system performance because the instrument is one of the "unimportant many." Therefore, before purchasing the new alarm instrument, it makes sense to carry out a structured risk ranking to see which other areas may provide the best place for investment. In particular, the analysis should attempt to identify the *important few* events that contribute the most to risk according to the Pareto Principle. Risk can then be most effectively reduced by following the "Path of Greatest Resistance," i.e., identifying and correcting the items that contribute the most to overall risk.

Event contribution

The contribution of each event to overall risk is determined with the following process.

- Determine the overall system failure rate using the predicted frequency/probability values for each event.
- Set one event with a failure rate value of zero and recalculate the minimal cut set value.

Table 15.9 Frequency of the Top Event: Change to E-007

Cut Set			Value (yr^{-1})		Predicted Frequency (yr)
E-002	E-003	E-007	0.5 * 0.1 * 0.05	0.0025	400
E-002	E-003	E-008	0.5 * 0.1 * 0.1	0.005	200
E-002	E-003	E-009	0.5 * 0.1 * 0.01	0.0005	2,000
E-004			0.25	0.25	4
E-005	E-007		0.15 * 0.05	0.075	133
E-005	E-008		0.15 * 0.1	0.015	67
E-005	E-009		0.15 * 0.01	0.0015	667
E-006	E-007		0.13 * 0.05	0.065	154
E-006	E-008		0.13 * 0.1	0.013	77
E-006	E-009		0.13 * 0.01	0.0013	769
Total				**0.3028**	**3.3**

- Determine the change to the Top Event value.
- Reset the event to its former predicted frequency/probability.
- Repeat the above process for each Base Event in turn.
- Rank each event's contribution to risk by comparing the difference that each makes to the Top Event value when its own value is set to zero.

Table 15.10 summarizes the effect of following the above process. Figure 15.22 provides the same information in bar chart format.

The following conclusions can be drawn from inspection of Table 15.10 and Figure 15.22.

Important few

One event—E-004, "Instrument Plugs"—stands out as being very important indeed; it contributes 37% to the overall risk. E-007, "Failure of the Level Alarm," is the second most important contributor, contributing 24%. Together they make up about 61% of the overall risk; they are the important few. If the value of E-004 could be reduced by a factor of 10 by changing the upstream conditions or by installing an in-stream filter, then the predicted frequency of the Top Event would fall from once in 2.2 to once in 4.4 years. The next highest ranking item is E-007, Internal Failure (Level Alarm). If its failure rate is reduced by 90% also, then the overall frequency of system failure increases to 3.5 years.

If the reliability of E-004 and E-007 can be significantly improved then E-005 (LRC-101) and E-006 (FRC-101) become the new important few.

Unimportant many

Referring once more to Table 15.10, many of the events contribute almost nothing to overall risk. Even if these events could be totally eliminated by making them totally reliable the overall frequency of Tank Overflow would hardly be affected. In particular, Event E-009, "Operator Reads Wrong Gauge" contributes less than 0.5% to the overall failure rate. Therefore, any proposals to "fix the tank overflow problem by more training" can be declared dead on arrival.

Table 15.10 Risk Ranking

Base Event	Item	Top Event Value For Base Event Set At Zero	Delta From Normal Top Event Value	Ranking %
E-002	P-101A fails	0.4208	0.1180	4.5
E-003	P-101B fails	0.4208	0.1180	4.5
E-004	Instrument plugs	0.2013	0.2500	36.6
E-005	Internal failure (LRC-101)	0.3598	0.0915	13.4
E-006	Internal failure (FRC-101)	0.3720	0.0793	11.6
E-007	Internal failure (low-level alarm)	0.2863	0.1650	24.2
E-008	Operator busy elsewhere	0.4183	0.0330	4.8
E-009	Operator reads wrong gauge	0.4480	0.0033	0.5
Total				**100**

Power of the AND Gate

As a generalization, the insertion of an AND Gate into a fault tree does more to improve reliability and/or safety than reducing the failure rate of the Base Events in the Tree. It is frequently found that two low reliability items that provide redundancy for one another (through an AND Gate) provide better system reliability that having a single highly reliable item.

Importance equalization

One of the unexpected results of fault tree quantification is that all events entering a particular AND Gate have the same importance ranking, regardless of their specific failure rates. For example, in Table 15.10, Events E-002 and E-003 each have the same ranking, even though their individual failure rate values differ by a factor of two. Although this result seems counterintuitive, it stems from the fact that an AND Gate is a product term, and it does not matter which input term changes—each has the same effect on the output.

Cost–benefit analysis

It is also useful to consider cost–benefit analyses, particularly when the Top Event is to do with economics, rather than safety or environmental performance. For example, Table 15.9 shows that Event E-005, "Failure of LRC-101" has only a medium rank (12%). However, a quick and inexpensive replacement may make this instrument more reliable by an order of magnitude. Therefore, it is worth making that investment, even though the item is not high on the risk-ranking scale. In the extreme, as noted in the discussion to do with hazards analysis some findings or recommendations are "low-hanging fruit." The investment and effort required to address a situation is so low that there is little point in conducting an exhaustive analysis on that particular hazard.

IMPORTANCE RANKING USING CUT SETS

Once the availability of a system has been calculated, the next step is to determine how it could be improved. This is done by determining which equipment items contribute the most to overall unavailability. This process is referred to as ranking, an event's rank corresponds to its overall contribution to availability (Henley and Kumamoto, 1981). Three methods that are commonly used are the Birnbaum factor method, the Fussell–Vesely method and the perturbation method.

Birnbaum factor method

The Birnbaum factor for a basic event is calculated by determining overall availability with the basic event in, i.e., the item is known to be working, and then recalculating the availability with the same basic event out, i.e., it is known to be not working. The two respective probabilities of failure are 0.0 and 1.0. The Birnbaum factor for component i is calculated using Eq. (15.9).

$$B_{f,i} = p_i(1.0) - p_i(0.0) \tag{15.9}$$

where p is the availability of the system for the given state of component i. The factor is calculated for each basic event. The events are then ranked using these factors. This method is good for those cases in which a basic event is known to be failed and then known to be operating such as occurs during maintenance, when decisions have to be made as to which items of equipment should receive resource priorities.

Fussell–Vesely method

The Fussell–Vesely method is similar to the Birnbaum factor method except that the factor for each event is multiplied by its probability of failure. Therefore, Eq. (15.9) becomes Eq. (15.10).

$$\mathrm{FV}_{f,i} = B_{f,i} \times \lambda_i \tag{15.10}$$

This method is the best choice when deciding how to prioritize services such as inspection that are used when the plant is actually running.

Perturbation method

Another way of calculating ranking is to perturb the values for each basic event by a small amount, say 1%, while maintaining the values for the other basic events at their original value. This method gives the same numerical results as the Fussell–Vesely method.

COMMON CAUSE EVENTS

Common cause events are described in Chapter 1.

Figure 15.23 shows a fault tree AND Gate based on the first standard example. The gate has two inputs: failure of P-101A, which is steam driven, and failure of P-101B, which is electrically driven. (Pump A is normally operating, with B being on standby.) It is assumed that the two pumps have failure modes that are totally independent of one another, i.e., the failure of one is completely independent of the failure of the other. Pump 101-A has a predicted failure rate of once in 2 years, or 0.5 yr^{-1}; Pump 101-B has a predicted probability of failure on demand (PFD) of 1 in 10 or 0.1.

The failure rate of this simple system is (0.5 × 0.1), i.e., 0.05 yr^{-1}. In other words, the pumping system is expected to fail once in 20 years. However, those operating the above system find that it is, in fact, considerably less reliable than it "ought to be," so an investigation into common cause events is carried out. The following factors contribute toward the failure of the steam-driven P-101A.

Steam failure due to loss of electrical power: 0.125 yr^{-1}

- Steam failure from other causes: 0.125 yr^{-1}
- Corrosion in the pump: 0.1 yr^{-1}
- Other causes: 0.15 yr^{-1}.

These terms, which total 0.5 yr^{-1}, enter the fault tree through an OR gate, as shown in Figure 15.24 (all second- and third-order terms are ignored in the following calculations).

A similar analysis can be carried out P-101B. The following factors contribute to its failure:

- Electrical power failure: 25%
- Equipment failure: 50%
- Others: 25%.

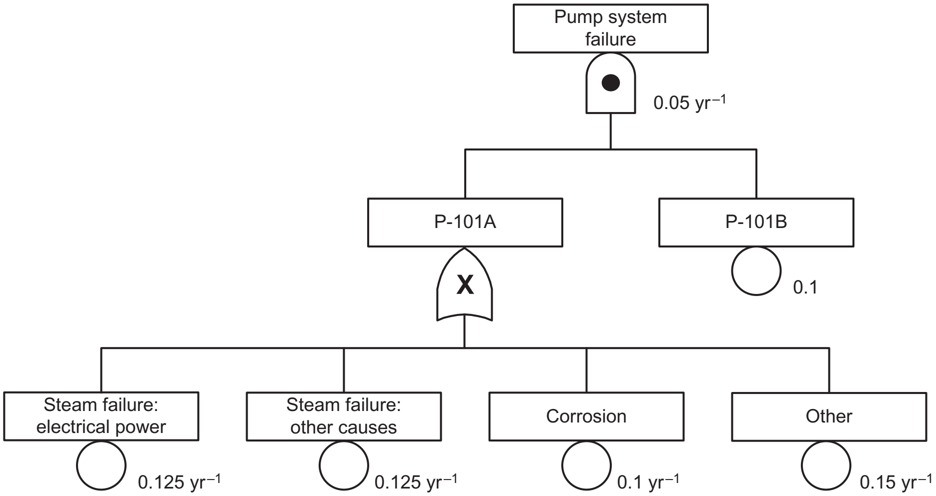


FIGURE 15.24

Expansion of the P-101A failure rate term.

(The value for electrical power not being available on demand is set at 0.25 because there is a 25% chance that power will not be available following a failure of P-101A.)

The fault tree is now expanded as shown in Figure 15.25.

Once more, the overall system failure rate appears not to have changed. Figure 15.25 does not present an accurate picture, however, because the "Electrical Power Failure" occurs twice, once to do with P-101A and once to do with P-101B. Hence it is a common cause effect: "Failure of Electricity" leads to an immediate failure of the pumping system, so the fault tree should have the structure shown in Figure 15.26.

The overall failure rate has increased from 0.05 to 0.142 yr^{-1}, or from once in 20 years to once in 7 years—an increase of a factor of three.

The development of common cause events does not stop here. Another issue that could cause both pumps to fail is the inadvertent introduction of corrosive chemicals into the RM-12 stream. When corrosion is considered, the fault tree looks as shown in Figure 15.27.

Now the overall failure rate has increased to 0.166 yr^{-1}, or once in 6 years.

FUKUSHIMA-DAIICHI

In Chapter 1, it was noted that the Fukushima-Daiichi catastrophe provides a good example of Common Cause events: the earthquake knocked out the primary cooling pumps, and the tsunami then knocked out the backup pumps. Copies of the Fukushima-Daiichi P&IDs (Piping and Instrument Diagrams) are not available. Therefore, for the sake of discussion it is assumed that there are two sets of pumps: three operating pumps (O1, O2, and O3) driven by electricity and two backup pumps (B1 and B2) that are diesel-powered and that do not require electrical power. The Fault Tree for this assumed set up is shown in Figure 15.28. It consists entirely of AND Gates.

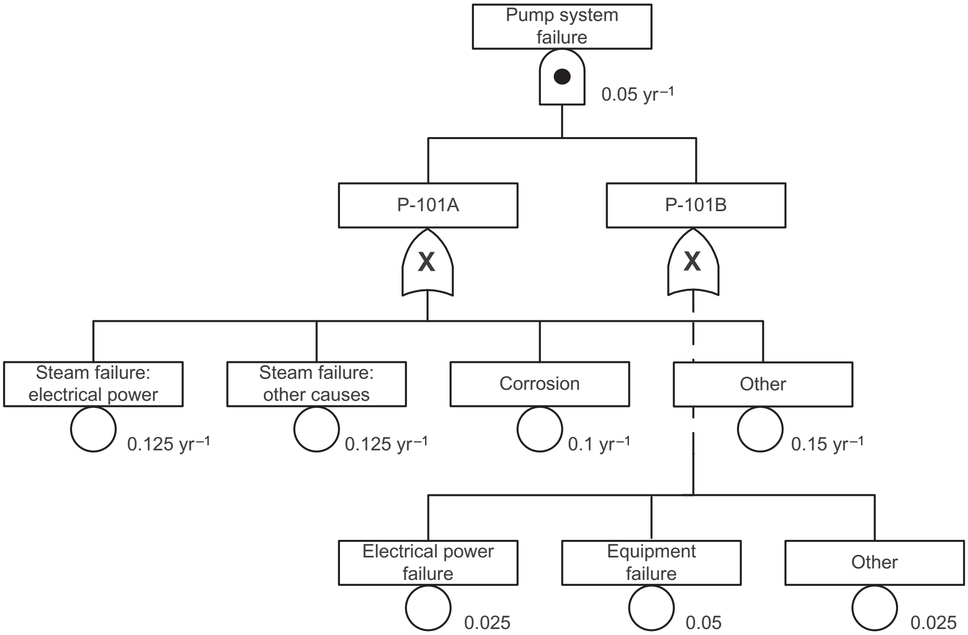


FIGURE 15.25

Expansion of the P-101B failure probability term.

The further assumption is then made that the operating pump, O1, fails twice a year and that the two backup operating pumps have a failure to start on demand of 0.05 (i.e., the likelihood that they will start on demand is 95%). Hence the overall failure rate for the operating pumps is $(2 \times 0.05 \times 0.05)$ yr^{-1}, or 0.005 yr^{-1} or once in 200 years. If this system were to fail then the backup diesel pumps would take over. Assuming a failure on demand probability for each backup pump of 0.01 then the failure rate of the backup system is 0.0001. Combining the two systems we get an overall failure rate of one in 20 million years, which is a big number.

Now comes the earthquake; it knocks out electrical power. Hence all three of the operating pumps fail due to the first common cause: Electrical Power Failure caused by the earthquake. This is bad, but the backup pumps, which together have a probability of failure of 1 in a 1000, can be trusted to work since they have their own, independent source of power (diesel). But, 40 minutes later, the tsunami disables the backup pumps due to a second common cause: sea water flooding. The reactor core continues to generate substantial amounts of heat, but there are no means of removing that heat.

GENERIC FAULT TREES

Although each system is unique, and so will have a unique fault tree, the general manner in which the trees are created will often be quite similar from situation to situation. Two generic trees are

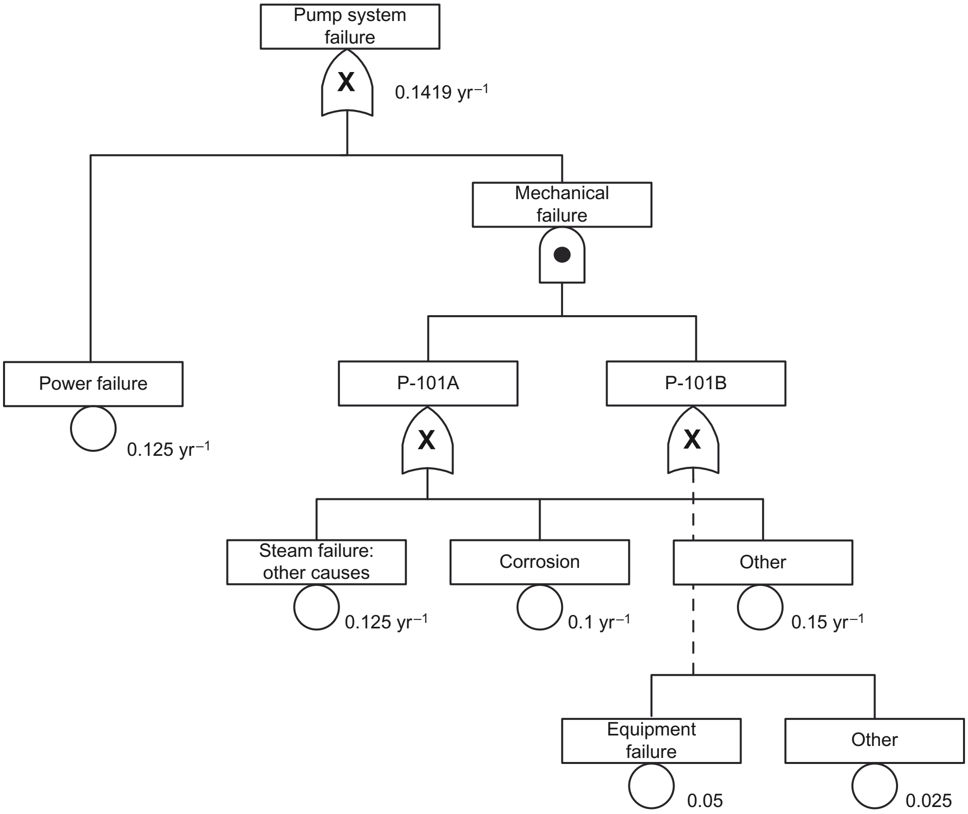


FIGURE 15.26

Electrical failure common cause.

illustrated here, one for safety and the other for reliability. Either can be used as the starting point when developing a specific model.

Generic safety fault tree

When analyzing a potential safety problem, the Top Event can often be drawn with three Intermediate Events entering it through an AND Gate, as shown in Figure 15.29.

The Top Event of a safety tree is usually of the form "Person Seriously Injured or Killed," or "Worker Suffers Lost Time Injury." The Initiating Event, whose dimension is inverse time, starts the accident sequence that could lead to the occurrence of the Top Event. Typical initiating events are:

- Leaking liquid catches fire
- Release of toxic chemical
- Explosive cloud of unburned vapor forms in furnace.

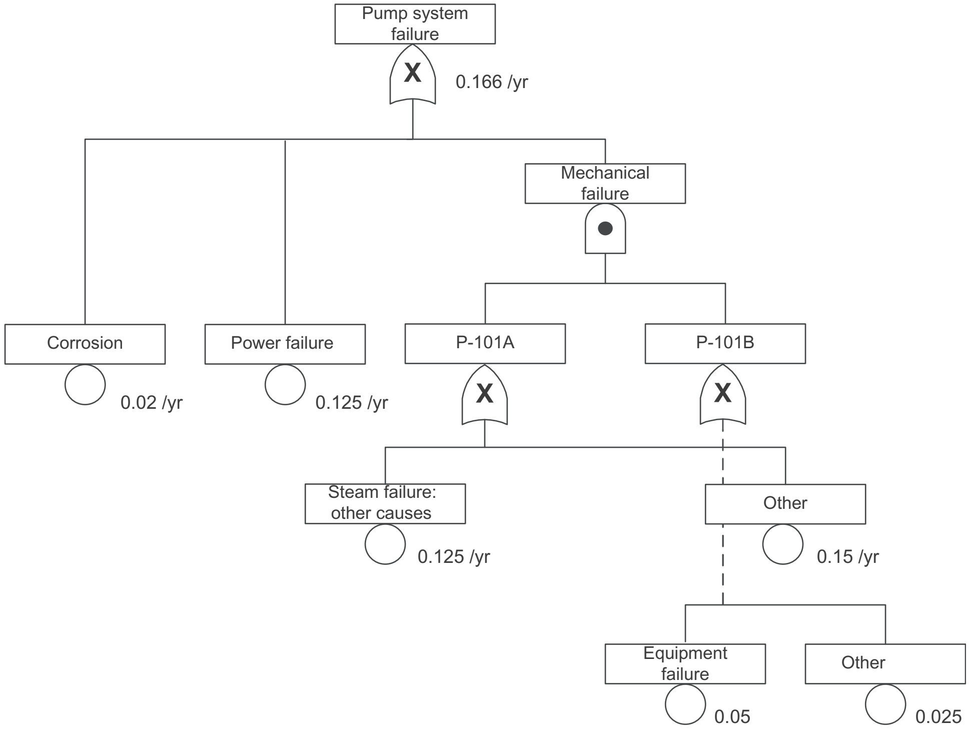


FIGURE 15.27

Corrosion common cause.

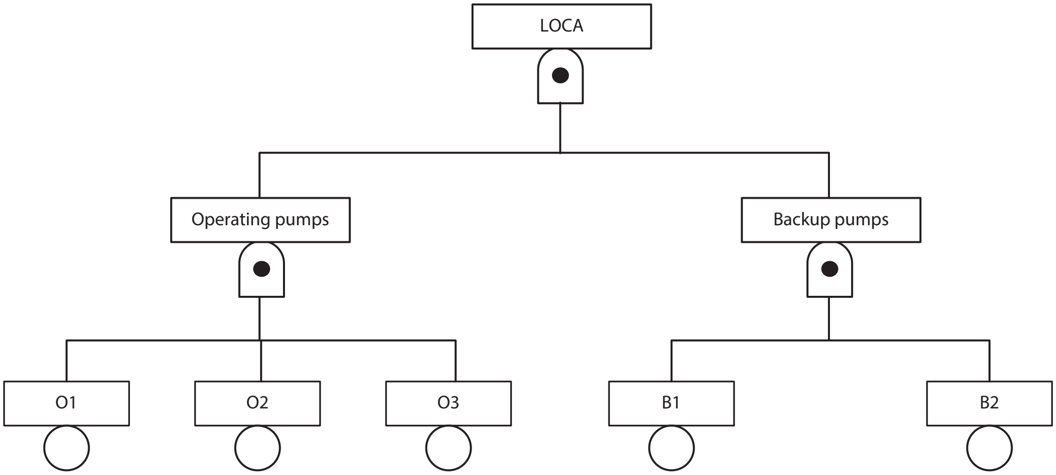


FIGURE 15.28

Fukushima-Daiichi assumed setup.

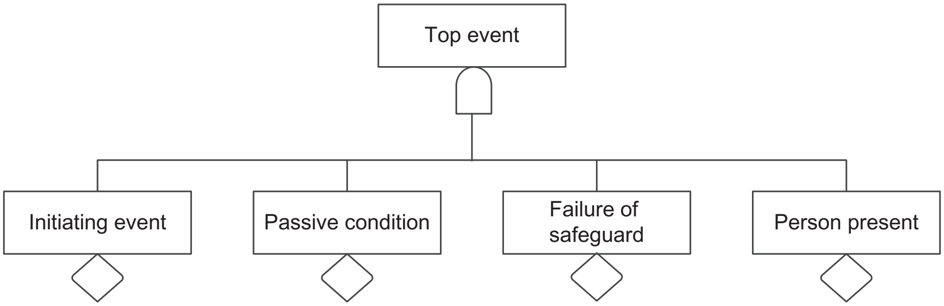


FIGURE 15.29

Generic safety fault tree.

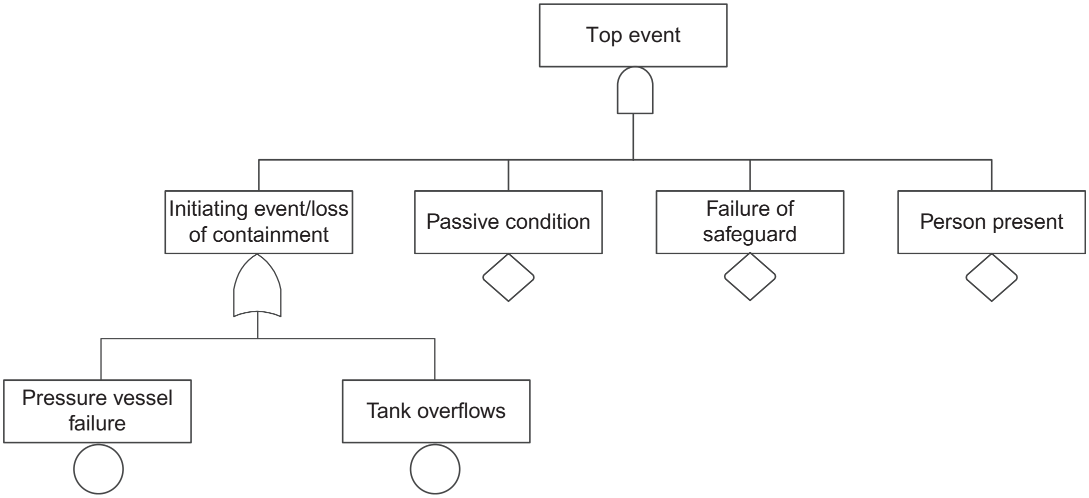


FIGURE 15.30

Generic safety fault tree development.

For the initiating event to lead to the top event, three additional factors should be considered:

1. There often needs to be a passive condition. The normal example would be a source of ignition. The release of hydrocarbon vapors (the initiating event) will not cause a fire if it cannot be lit off.
2. Safeguards, such as automatic interlocks and relief valves, must fail.
3. If a person is not present then the event cannot, by definition, be a safety problem—even if the economic loss is high.

Most accident sequences lead eventually to Loss of Containment, which usually means either that a pressure vessel ruptures or that a tank overflows. Therefore, Figure 15.29 can be expanded into Figure 15.30.

Generic reliability fault tree

For reliability work, a generic fault tree is shown in Figure 15.31, which shows three Intermediate Events entering the Top Event through an OR Gate.

The generic failures are not associated with any particular area or equipment type. Examples of these generic failures include:

- Human error
- Problems with items such as piping and sight-glasses
- Labor relations problems.

Events that are external to the system include:

- Weather (hurricanes, freezes, floods)
- Transportation failures
- Changes to raw materials.

Equipment failures can be categorized either by area or function. If different areas of the facility have very different types of equipment, then it makes sense to divide by area. However, if certain types of equipment are in use in multiple locations, the equipment can be grouped according to function and type.

DISCUSSION OF THE FAULT TREE METHOD

FTA has the following strengths:

- It provides a good, graphical picture of the hazardous situation being analyzed.
- Its logical approach is appealing to engineers and other technical people.
- It rationalizes feelings and hunches.
- It can be used as a tool in incident investigations.
- It can be both qualitative and quantitative.

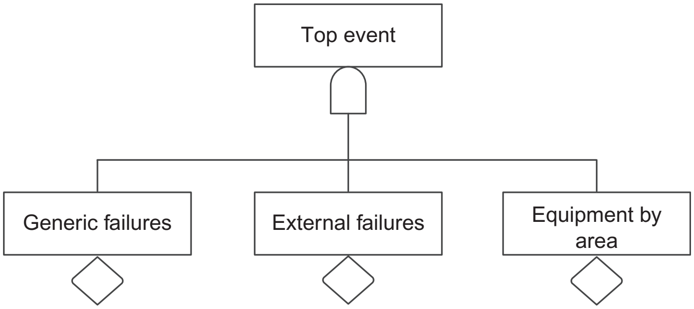


FIGURE 15.31

Generic reliability fault tree.

The method also has the following limitations:

- It can be time-consuming and expensive.
- It is difficult to incorporate real-world complexities and discontinuities such as the availability of operating and maintenance personnel over a typical 1-week shift cycle.
- For nonspecialists, the technique is not intuitively obvious, making it difficult for them to fully comprehend the insights generated.
- As the name *Fault* Tree implies, there is a tendency to focus on problems and difficulties rather than opportunities for improving an existing operation.
- Fault Trees are static—they provide a picture of a system independent of time. The method has trouble with dynamic systems, where certain events trigger other events sequentially, or where there is a time delay between the occurrence of two events. For these situations another method, such as a Monte Carlo simulation, may be a better choice.
- It is difficult to model partial failures (e.g., a pump working at lower than normal capacity) and the partial availability of maintenance resources, say, at a weekend.
- The results depend heavily on the background and skills of the analyst.
- It gives an appearance of completion—yet this may be misleading, which is why the "All Other Events" term at the top of the tree is so useful.

QUALITATIVE FTA

In the introduction to this section it was suggested that fault trees are best used to analyze and better define the hazards that have already been identified by one of the more creative hazards analysis methods, such as HAZOP. However, fault trees can also be used just to identify hazards. When used in this manner the method is known as Qualitative FTA (QFTA). Using this approach, the hazards analysis team leader, using a whiteboard develops the tree in conjunction with the team. He or she postulates the Top Event, such as Tank T-100 overflowing, and asks the team members to suggest ways in which this may happen. As the discussion develops, the leader sketches out the OR and AND Gates of the Tree, showing the combinations of events that need to occur for the Top Event to occur.

This approach to hazards analysis provides a fresh approach to hazards analysis, and so is particularly useful for those facilities that are on their second- or third-generation analyses and are looking for fresh insights. A Qualitative Fault Tree can be particularly effective at identifying common cause events. For the method to be effective, the team leader has to be "fluent" in the language of FTA. He or she must be capable of turning normal conversation into logic gates. Also the team members should have some familiarity with the Fault Tree method.

EVENT TREE ANALYSIS

ETA uses the same logical and mathematical techniques as FTA. However, whereas a fault tree analyzes how an undesirable top event may occur, an event tree considers the impact of the failure of a particular component or item in the system, and works out the effect such a failure will have on the overall system risk or reliability. Event trees use an inductive approach, whereas fault trees are deductive. Event trees were developed for the nuclear industry. They are much less widely used in the process industries.

The initiating event in an event tree will usually fall into one of the following four categories:

1. Failures or unsafe conditions in individual items of equipment
2. Human error
3. Utility failures
4. External events (such as hurricanes or earthquakes).

Figure 15.32 shows an event tree for a situation in which the pressure in a vessel rises.

Figure 15.32 starts with the event "High Pressure in the Vessel." The reasons for the occurrence of this event are not explained. There are four layers of protection, each of which has a chance of either success or failure. At the first junction the normal control system acts. If it brings the pressure to a safe state then there is no need to continue with the development of the tree. Therefore, the "Success" lines are dashed, showing that they do not need to be considered.

The "Failure" lines continue through three more layers of protection. If all the protective devices and systems fail, the tree follows the red line which leads to rupture of the vessel.

QUANTIFICATION OF AN EVENT TREE

Figure 15.33 shows an event tree developed for the second standard example. A spreadsheet is used so that calculations can be performed.

The initiating event is increased flow into Tank, T-101. At each step in the tree, the system can respond correctly or it can fail. The success lines are shown by the letter "Y" on the tree. The failure lines are indicated with the letter "N." The steps are in chronological order. For example, the correct response of FRC-101 will preempt the need for the high-level alarm.

Figure 15.33 shows the likelihood of occurrence of each branch in the tree. For example, at the first step, the likelihood of LRC-101 responding correctly to an increased level is 0.850. The corresponding likelihood of failure is 0.150.

The initial starting event has a value of 1.0, i.e., it is assumed to have occurred. The only sequence of interest is a string of "N" values, which eventually lead to system failure. Most of the other sequences have no physical meaning; for example, the high-level alarm will not be called for if the normal control system has taken care of the rising level. Therefore, even though Figure 15.33 shows the calculated value for all possible cause and effect sequences in the tree, there is really no need to calculate anything but the system failure valve.

Reading from left to right, the logic goes:

- An increased flow of liquid to T-100 occurs. This is a defined event so its probability of occurrence is unity.
- The level controller, LRC-101, detects the rising level. There is a 15% chance that it will fail to do so.
- FRC-101 opens the control valve so as to increase the flow rate out of the tank. There is a 13% chance that it will not operate correctly.

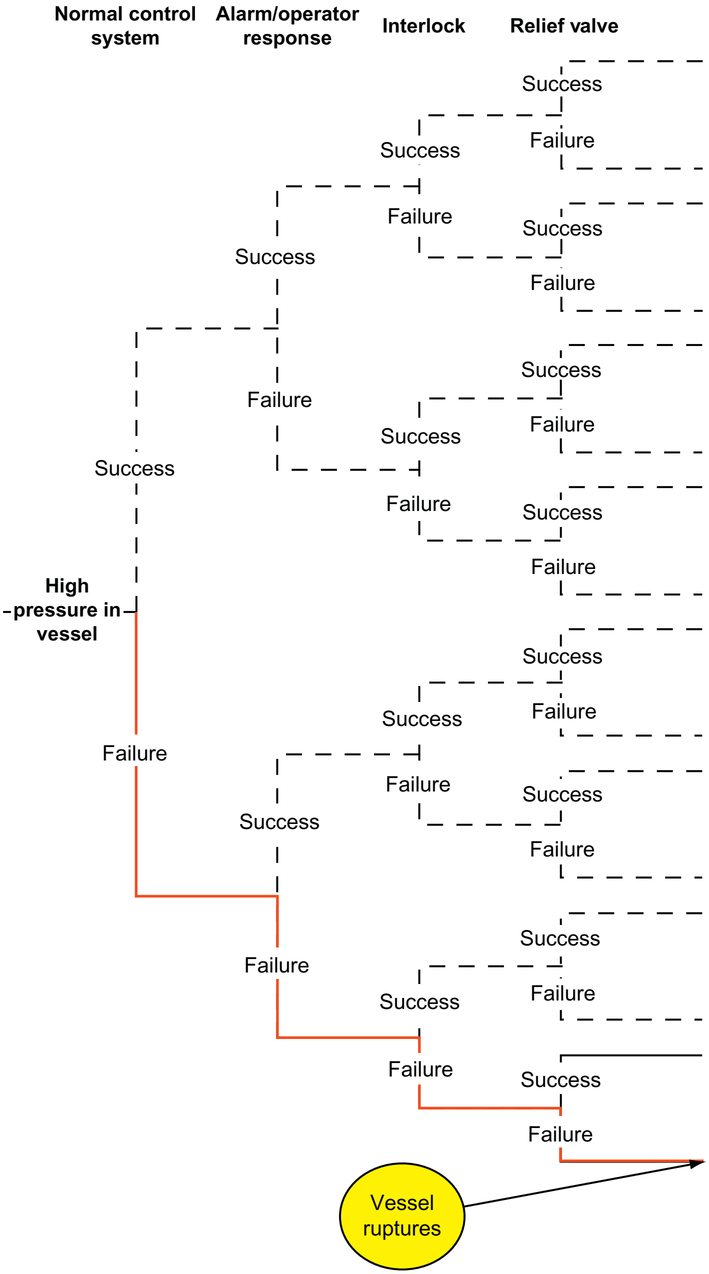


FIGURE 15.32

Event tree example.

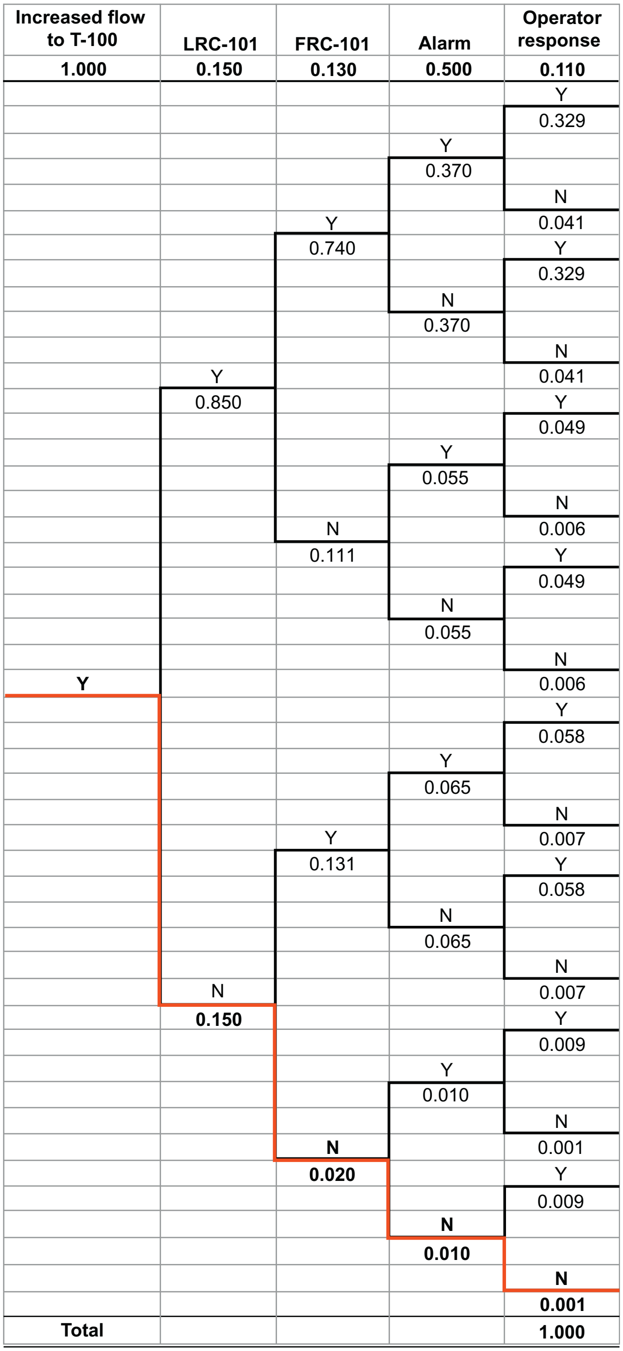


FIGURE 15.33

Event tree example.

- If the level in the tank continues to rise, an alarm sounds. This safeguard has a 50% probability of working.
- The operator responds to the alarm. The probability of a successful response is 11%.

Figure 15.33 predicts that the probability of tank overflow is 0.1%.

SCOPE OF EVENT

Different event trees can be developed for different levels of seriousness. For example, Figure 15.34 shows how an event tree can differentiate between instantaneous and prolonged releases of flammable hydrocarbons.

COMBINING EVENT TREES AND FAULT TREES

Fault trees and event trees can be combined. The gates in the event tree are treated as top events of multiple fault trees. So, for example, one of the event tree gates could be "Loss of Electrical Power." That term then becomes the top event of a "Loss of Electrical Power" fault tree. When using fault trees as subsets of event trees it is important to identify the common cause or interdependent events and to enter them separately into the tree's structure.

Figure 15.35 shows how fault trees are linked into event trees. The likelihood for some of the lines in the event tree is calculated using the top event of a fault tree.

Event trees and fault trees can also be linked as shown in Figure 15.36, which is based on ISO standard 17776 (2000).

In Figure 15.36 the fault tree (which is left to right rather than the normal bottom to top) generates a top event. This event is, in turn, the initiating event for the event tree that follows. For example, a series of equipment, human and instrument failures could lead to the top event of "Liquid overflow from a tank." The safeguards to mitigate the top event are shown in the event tree. The bow tie technique uses the same structure as Figure 15.36.

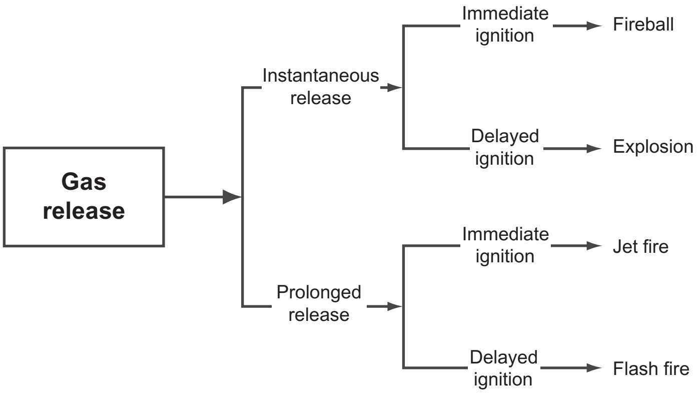


FIGURE 15.34

Flammable release event tree.

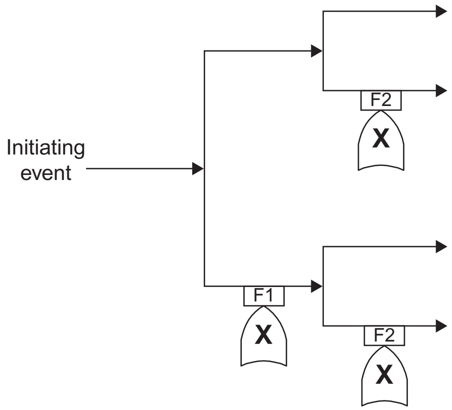


FIGURE 15.35

Events trees and fault trees.

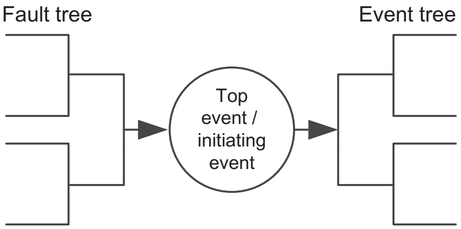


FIGURE 15.36

Events trees and fault trees.

SHORT SEQUENCE OF EVENTS

The use of the Event Tree method is most appropriate when there are many safeguards and protective layers between the initiating event and the final outcome. In the nuclear industry the scenario of greatest interest is “Loss of Cooling to the Reactor Core.” Were this event to occur, and the subsequent safeguards not to work properly then the reactor could meltdown. Obviously such a scenario is very serious, so the engineers responsible for designing nuclear power plants incorporate many layers of safety, thus making the chance of an accident remotely small. Process facilities rarely have so many layers of protection because the worst-case accidents are not usually as serious as a nuclear accident hence the corresponding events trees are much shorter.

MANY EVENTS

Although the nuclear power industry risk scenarios tend to generate long event trees, the number of trees is quite small because there are relatively few initiating events. Such is not the case in the process industries, where the technologies used are often quite complex, and so there are many starting points for accident sequences. The correspondingly large number of (short) event trees would be hard to manage.

PARTIAL SUCCESS

An event tree tends to assume an "all or nothing" situation: either the system works, or it does not work. This may be appropriate for nuclear power plants, but partial failure and reduced capacities are much more likely to occur in the process industries.

DISCRETE EVENT ANALYSIS

Broadly speaking there are two ways of calculating likelihood. The first is through the use of deterministic techniques such as fault tree and ETA as discussed above. A mathematical model of the system is created, data is entered into the model and system performance is calculated. Such an analysis is basically quite simple: either an equipment item operates as required, or it does not. Yet real-world actual equipment performance is usually much more complex.

The other approach is to use discrete event analysis. This approach is able to handle the real-world complexity of most systems. Referring to Example 1 in Chapter 1, it may be found that the availability of Pumps, P-101 A/B is not a simple number but varies according to many time-dependent factors such as when they were most recently inspected, the availability of spare parts and the operating conditions. Factors such as these can materially affect the reliability and maintainability of the pumps, often in ways that are impossible to model deterministically.

Some of the more important features of discrete event models are discussed below.

NONLINEARITIES AND COMPLEXITIES

Deterministic analysis is basically quite simple: either an equipment item operates as required, or it does not. Yet real-world actual equipment performance is usually much more complex. For example, it may be found that the availability of Pumps, P-101 A/B in the example depends on the service in which they are operating. Factors such as the viscosity of the fluids being pumped, ambient temperatures, and the quality of maintenance will affect the performance of the pumps, often in ways that are difficult to model mathematically.

Differences such as these are even more pronounced with regard to maintenance. Few facilities have equal levels of maintenance support around the clock—typically it will take longer to find maintenance help at nights, and on the weekends. There is no way that a deterministic model can incorporate complexities and variations of this type.

Yet, in practice, even greater complexities may exist. For example, the repair of Pump P-101A may require a particular spare part; if the facility warehouse has only a limited supply of that part, it may run out. Then, if the pump fails, the repair time will include the time it takes to order and ship the new part. Once more, such complexities are quite impossible to handle with deterministic models, yet stochastic models can incorporate them quite readily.

CONVEYING STATISTICAL UNCERTAINTY

Because they use random number simulations, stochastic models give a flavor of “how things really are”—they reflect the apparent randomness of life. Deterministic models, on the other hand seem like a “sure thing”—they implicitly state how things will turn out, rather than how they might turn out.

Any random number simulation requires a seed value to get it started. If the same model, using the same failure rate data and the same time scale is run twice with a different seed value in each case, then the results of the two simulations will be different. Many managers who have difficulty grasping this point—they expect that the answer to a problem should always be the same, given the same input data.

MONTE CARLO SIMULATION

One technique for modeling is to use Monte Carlo simulation. In brief, the method works as follows:

- Each equipment item (and human operator) is assigned a probability of failure and an initial operating condition.
- The computer clock is started at time = 0. Each “tick” of the computer clock corresponds to a time interval, such as 12 hours, of actual operation.
- A random number is generated for each item in the system.
- If the random number falls within a predefined range, then that item is put into a failed state.
- At the end of each iteration an examination of the cut sets determines the system’s overall operability and the resource availability.
- If an item fails during the current iteration it is taken out of service corresponding to the repair time and the availability of maintenance resources.
- Iterations are continued until a stable, overall picture of system availability is obtained.

RANDOM NUMBER GENERATORS

At the heart of any stochastic model is a random number generator. This is an algorithm that generates a series of numbers such that each successive number has an equal probability of possessing any value, and each number is statistically independent of the other numbers in the series. In real life, randomness does not exist—every consequence has a cause. However, in many cases the cause−consequence relationship is not known about, so a random sequence of events is used to simulate the real world.

No mathematical algorithm can generate a set of truly random numbers because the calculations and answers of the algorithm are, in principle, completely predictable. Such an algorithm can, however, generate *pseudo*random numbers, i.e., a series of numbers that have no discernible pattern.

A random number algorithm starts with a seed value, and generates a second number from it. This second number is then uses as the seed for a third number, and so on.

Generally, random number equations are of the following form:

$$x_{n+1} = \text{modulus}((a \times x_n + b)/c) \tag{15.11}$$

where a, b, and c are nonnegative numbers, and x_n is a number in the random number series. (A modulus returns the remainder following the division of one number by another. So mod(9/9) is 0, mod(8/9) is 8, and mod(100/9) is 1.)

The difficulty with any random number generator is that there is often some rhythm or pattern to the numbers that will start to be significant if the numbering sequence is maintained for long enough. Such a pattern may be difficult to spot, but it will always be present because, once a number is repeated, the cycle restarts. One method of addressing this problem is to restart the sequence occasionally with a new seed value, and possibly with a new algorithm.

Most computer language compilers include a random number generator. Before using one of these it is important to establish confidence in the algorithm, and its ability to generate a high degree of randomness in the number sequence that it generates.

SEED NUMBERS

The seed value for the generation of numbers can be provided by the user, or it can be taken from an external pseudorandom sources, such as the computer's clock.

SPEEDING THE SIMULATION

One of the biggest drawbacks to Monte Carlo simulation is the long run times that are often needed in order to achieve stable results. It is therefore useful to use techniques that speed up the simulations without causing the quality of the randomness of the numbers used internally to deteriorate.

One way of speeding up a simulation is to pair the generated random numbers. This is done by generating a random number, subtracting its value from unity (i.e., obtaining its dual), and then returning both numbers as arguments to the calling routine. The computer time needed for a simple subtraction calculation is very much less than the time needed to generate a new number, so the simulation will proceed much more quickly.

MARKOV MODELS

Another form of stochastic analysis is known as Markov Simulation, named after the nineteenth-century Russian mathematician. A Markov model shows all the possible system states, then goes through a series of jumps or transitions. Each jump represents a unit of time or a step in batch process. At each transition the system either stays where it is or moves to a new state.

Figure 15.37, which is derived from the first standard example, illustrates the concept for the Pump System, P-101A and P-101B. The letter "Y" means that the pump is either operating or operable; the letter "N" means that the pump is failed. (There is no direct transition from *State 3* to *State 4*, when both pumps are down, because P-101A is always repaired first.)

Figure 15.37 also shows transition values. For *State 1*, for example, there is a 0.1 probability that the system will move to *State 2* (P-101A still running, but P-101B unavailable as a spare).

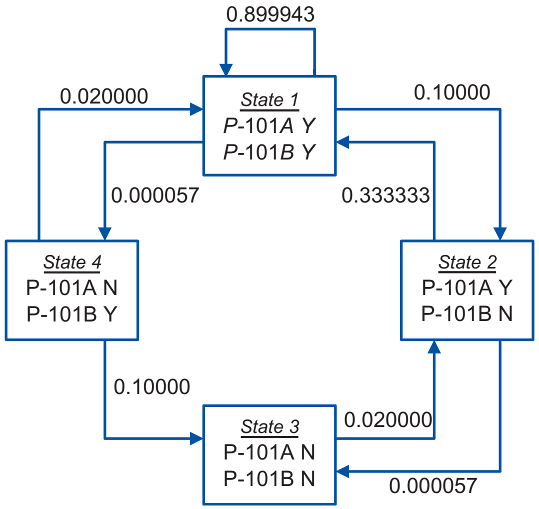


FIGURE 15.37

Example of a Markov model.

There is 0.00005707 probability that the system will move to *State 4* (P-101A fails, but P-101B successfully operates). There is a 0.899994 probability that the system will remain where it is, i.e., that both pumps will operate as required. Probability values for repair times are also shown. There is a 0.333333 chance that P-101B will be repaired (*State 2* to *State 1*), and a 0.02000 chance that P-101A will be repaired (*State 4* to *State 1*).

One difficulty with this type of model is that it is difficult to provide a probability value for an absolute repair time. For example, the Mean Downtime (MDT) for P-101B is 3 hours; this is the time it takes to repair it when it fails. It may be that this time is an absolute minimum (say due to the time it takes to isolate the pump, drain it down, repair the failure, and bring the pump back into service). Hence a simple probability value cannot truly represent this downtime.

Once a system has been set up, a simple spreadsheet matrix can be set up to calculate the probability of system states after each jump. Table 15.11 is an example of such a matrix, based on the logic and probability values shown in Figure 15.37.

The value for each cell is calculated based on initial probability and the exiting and entering probabilities. For *State 1* the transition values for the first jump can be calculated from the equations below, given that $p_1(0) = 1.0$, i.e., the starting point is for both pumps to be operating. For example, after the first transition, the value at State 1 is:

$$p_1(1) = 1.0 - (0.000057 \times 1.0) - (0.100000 \times 1.0) + (0.02000 \times 0.0) + (0.333333 \times 0.0) = 0.899943$$

Table 15.11 shows that, after 100 iterations, the system has stabilized. The overall availability for the pump system (all states excluding *State 3*) is 99.8%. Although this value is quite high, it is noteworthy that the system spends almost a quarter of its time in *State 2*, i.e., with P-101A

Table 15.11 Transition Values

	Transition Value					
Step	**1**	**2**	**3**	**4**	**Total**	**Availability (%)**
0	1.000000	0.000000	0.000000	0.000000	1.000000	100.0
1	0.899943	0.100000	0.000000	0.000057	1.000000	100.0
2	0.843232	0.156655	0.000011	0.000102	1.000000	100.0
3	0.811081	0.188751	0.000030	0.000138	1.000000	100.0
4	0.792846	0.206932	0.000054	0.000167	1.000000	100.0
5	0.782497	0.217229	0.000082	0.000192	1.000000	100.0
6	0.776616	0.223058	0.000112	0.000214	1.000000	100.0
7	0.773267	0.226357	0.000144	0.000233	1.000000	100.0
8	0.771353	0.228221	0.000177	0.000249	1.000000	100.0
9	0.770252	0.229273	0.000211	0.000263	1.000000	100.0
10	0.769613	0.229865	0.000246	0.000275	1.000000	100.0
11	0.769235	0.230197	0.000282	0.000286	1.000000	100.0
12	0.769005	0.230381	0.000318	0.000296	1.000000	100.0
13	0.768860	0.230481	0.000355	0.000304	1.000000	100.0
14	0.768763	0.230534	0.000391	0.000312	1.000000	100.0
15	0.768694	0.230560	0.000428	0.000318	1.000000	100.0
16	0.768640	0.230572	0.000464	0.000324	1.000000	100.0
17	0.768596	0.230575	0.000500	0.000329	1.000000	99.9
18	0.768557	0.230573	0.000536	0.000333	1.000000	99.9
19	0.768522	0.230569	0.000572	0.000337	1.000000	99.9
20	0.768489	0.230563	0.000608	0.000340	1.000000	99.9
21	0.768457	0.230557	0.000643	0.000343	1.000000	99.9
22	0.768427	0.230550	0.000677	0.000346	1.000000	99.9
23	0.768397	0.230543	0.000711	0.000348	1.000000	99.9
24	0.768368	0.230536	0.000745	0.000350	1.000000	99.9
25	0.768340	0.230529	0.000779	0.000352	1.000000	99.9
26	0.768312	0.230523	0.000811	0.000354	1.000000	99.9
27	0.768285	0.230516	0.000844	0.000355	1.000000	99.9
28	0.768258	0.230510	0.000875	0.000356	1.000000	99.9
29	0.768232	0.230503	0.000907	0.000358	1.000000	99.9
30	0.768207	0.230497	0.000938	0.000358	1.000000	99.9
31	0.768182	0.230491	0.000968	0.000359	1.000000	99.9
32	0.768157	0.230485	0.000997	0.000360	1.000000	99.9
33	0.768133	0.230479	0.001027	0.000361	1.000000	99.9
34	0.768110	0.230474	0.001055	0.000361	1.000000	99.9
35	0.768087	0.230468	0.001084	0.000362	1.000000	99.9
36	0.768064	0.230463	0.001111	0.000362	1.000000	99.9
37	0.768042	0.230457	0.001138	0.000363	1.000000	99.9

Table 15.11 Transition Values *Continued*

	Transition Value					
Step	1	2	3	4	Total	Availability (%)
38	0.768020	0.230452	0.001165	0.000363	1.000000	99.9
39	0.767999	0.230447	0.001191	0.000363	1.000000	99.9
40	0.767978	0.230442	0.001217	0.000363	1.000000	99.9
⋮						
100	0.767260	0.230270	0.002105	0.000365	1.000000	99.8

operating but P-101B not available if needed. Therefore, if greater reliability is required for this system, attention should be focused on P-101B rather than P-101A. In particular, the 0.1 failure rate for P-101B seems high, and is probably an area that requires attention.

TOP-DOWN/BOTTOM-UP APPROACH

Once the system and goals have been defined, the analysts and the management team need to decide if they are to develop a top-down or bottom-up approach to understanding the system whose reliability is to be improved.

TOP-DOWN

A top-down approach is used when management wants to improve overall reliability and/or does not know what the principal causes of problems may be. If a facility manager notes that production losses through unanticipated downtime are increasing, or maintenance costs for the whole facility have increased, he will probably call for a top-down analysis. He may also authorize this type of analysis when he suspects that there is a pervasive root cause problem, such as inadequate operator training, that is affecting many facility subsystems.

BOTTOM-UP

A bottom-up approach will be used when management wishes to improve the performance of a single equipment item, or small subsystem. For example, a particular compressor may be causing lots of production problems, and eating up the maintenance budget. In this case, the manager decides to analyze the compressor performance by determining issues such as (a) whether the compressor problems are associated with start-up, wear-out, or have no apparent cause, or (b) which part of the compressor system (motor, couplings, fan blades) are causing the greatest difficulties.

QUALITATIVE INSIGHTS

A good reliability model will often provide important and unexpected qualitative insights to do with the process under consideration. For example, if a facility is suffering from serious reliability problems, there is a natural tendency to attribute those problems to a particular piece of equipment that is failing frequently. However, it may turn out that the system is more complex than it appears at first blush.

The following questions may devolve from even a brief study of the problem:

- Why is the equipment failing?
- Is it being operated beyond its design point?
- Is it handling process fluids which are corrosive, and for which it was not designed?
- Are the operators running it incorrectly due to bad procedures and/or training?
- Is the item being maintained improperly, either due to maintenance errors, or the use of incorrect spare parts?
- Are external factors, such as the vibration of another equipment item, the cause of failure?
- What is the solution?
- Replace the item with a newer model?
- Improve operating and maintenance procedures/training for that equipment item?
- Add a spare, standby piece of equipment that can be used when the first item is down for repair?
- Make basic design changes that eliminate the equipment item altogether?
- If it is decided that operating errors are the cause of the equipment unreliability, how is a solution to be found?
- How is the solution to be implemented?
- Should there be more classroom instruction for the operators in the basics of operating equipment?
- Should the operators receive more field, hands-on training?
- Is there a need for new, more detailed operating procedures?
- Should the paper procedures be converted to electronic distribution?
- Is there a need for better working conditions such as improved lighting, or shorter working hours?
- Should there be more people on duty?
- Should there be fewer people on duty?

The model will show how various causes interact with one another, and it will identify which issues are causing the greatest problems.

LIMITATIONS TO QUANTIFICATION

Some of the limitations associated with risk quantification are discussed below.

MATHEMATICAL UNDERSTANDING

Risk quantification can involve the use of sophisticated mathematical techniques. Given that the ultimate “customer” for the analysis is likely to be a nonspecialist (such as a manager, regulator, or even a jury), explaining the math so that the listener or reader understands is quite a challenge. Even engineers and others who are comfortable with numbers can struggle with concepts such as “the probability of a probability,” or the fact that a “constant” failure rate does not have a straight line on a graph.

VALUE-LADEN ASSUMPTIONS

A basic tenet behind quantified risk models is that they are objective. This should mean that, if two or more people model the same scenario, their results should be more or less the same. In practice, anyone who has actually conducted hazards analyses knows that this statement is only approximately true at best. Each analyst will bring to the model his or her assumptions and values—particularly with respect to the failure rate data that they use. (The same phenomenon can be seen with respect to Hazard and Operability studies. When two teams analyze essentially similar systems, it can be startling to see how much the respective results differ from one another.)

The assertion that quantitative analyses are not nearly as objective as they may seem is supported by a study conducted by the European Joint Research Centre which states,

> When the results from a fault tree analysis were compared with historical data used by other teams for the same event, substantial differences were found.

Even without quantification, it is noticeable that any type of risk analysis is very subject to the assumptions and prejudices of the persons involved. One company, for example, conducted two HAZOPs on two very similar processes, which were in the same location, were of the same age and complexity, and had were run by the same management. An outside observer would reasonably expect that the two analyses would give roughly similar results. In fact, the opposite was the case. The findings were radically different, and the risk rankings were even more differentiated.

LACK OF EXHAUSTIVITY

Modern industrial systems are very complex, and can fail in a large number of ways. No risk analysis can possibly identify all of the failure modes (which is why the “All Other Events” event is included in the fault trees; the presence of this unknown event is a reality check).

HUMAN BEHAVIOR

Human performance is usually critical to system safety, yet, as discussed many times throughout this series of books, human behavior is essentially impossible to quantify. There is no way that a quantification analysis can incorporate the fact that an operator is distracted due to a fight he had with his wife just before coming to work, so does not take the correct actions during the course of a plant upset.

DATA QUALITY

One of the biggest difficulties with quantifying risk is that so much of the basic data (the frequency and probability values for base events) is of low quality, for the following reasons:

- Many items are inherently very reliable, so it is difficult to develop a large database for events such as pressure vessel failure.
- Even the most objective analysts tend to attribute high-frequency values to events that have actually occurred, particularly if the analyst himself has actually witnessed the event.

- Many failures are not recorded in a systematic manner, so reported failure rates are probably optimistic.
- The reliability of certain items may change. The situation where a refinery decided to replace a complete set of block valves has already been discussed.

In other branches of technology such criticisms would be taken as being so serious that there could be little confidence in the predicted results. However, with regard to risk analysis, high precision is not needed to obtain usable and credible results, again because of the Pareto Principle. Even if the results of the analysis are quite weak as a result of poor quality data, the result is the same: certain items are the major contributors to unreliability, and they are the ones that should be addressed. Even if the real failure rate distribution is, say, 70/30 rather than 80/20, the analysts' recommendations will not change.

SAFEGUARDS

Most process systems are protected by layers of safeguards as shown in Figure 15.38. The lowest layer (which is shaded) consists of normal operational controls, which are not safeguards *per se*, even though they control the great majority of deviations. The upper four layers, which are implemented in ascending order once the Safe Limit Value has been breached, represent increasing levels of safeguards.

Safeguards reduce the magnitude of either the consequence or the predicted frequency term (they do not remove the hazard). For example, a berm/bund wall around T-100 reduces the consequences of a spill from the tank. The pressure relief valve on V-101 reduces the likelihood that the vessel will rupture due to high pressure.

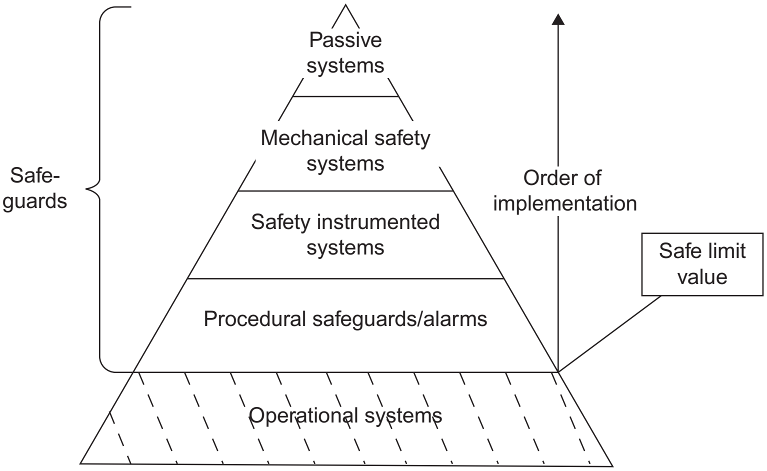


FIGURE 15.38

Levels of protection.

Safeguards can themselves create a hazard, although such hazards usually have much lower consequence than those that they are protecting against. For example, a relief valve that discharges directly to atmosphere protects against vessel rupture, but, when it opens, an employee may be affected by the discharged vapors. Another example of safeguards creating hazards occurs when unreliable safety instruments cause spurious shutdowns that in themselves create hazardous transient operations.

Some would add Emergency Response as being a sixth level of safeguard. However, if the event has reached the point where fire teams and other emergency responders are needed, the process is out of control—the incident has occurred.

Table 15.12 illustrates the types of safeguard for high level in T-101 and for high pressure in V-101. A table such as this can be prepared for any significant hazard. The first row—Normal Operations—has been shaded to indicate that responses at this level are not really safeguards; they are simply the normal operating response. Similarly, the sixth row—Emergency Response—has been shaded because, as discussed above, once the emergency situation is underway the actions taken are not really safeguards. If the situation has reached this point the safeguards have demonstrably failed.

SAFEGUARD LEVEL 1: NORMAL OPERATIONS

The first response to a hazard is for the system's normal operational and control systems to bring the situation under control. In the case of T-101, a high-level alarm will sound when the liquid

Table 15.12 Safeguards Table

Level of Safeguard	T-101 Overflow	V-101 Pressure
Normal operations	Operator responds to rising level by adjusting flow rates into and out of T-100 using normal control systems and equipment	Operator responds to rising pressure by adjusting flow rates out of V-101 using normal control systems and equipment
Procedural safeguards	Operator responds to a high-level alarm	Operator responds to a high-pressure alarm
Safety instrumented systems	Safety instrumentation takes the corrective actions needed to keep the level under control. The operator and normal control systems no longer play a role	Safety instrumented systems respond to bring the pressure back below the safe upper limit. The operator and normal control systems no longer play a role
Mechanical safeguards	An overflow pipe near the top of the tank directs spill to a safe location	The pressure safety relief valve opens
Passive safeguards	The berm can contain 110% of the tank's volume	None
Emergency response	The emergency response team works to contain the spill and to prevent further environmental or safety losses	Evacuation of the area followed by fire and spill control by the emergency response team

approaches the top of the tank. Either the operator will cancel the alarm and take the appropriate corrective action or the level control instrumentation will adjust the incoming or outgoing flow rates.

Although normal operational responses such as these will handle the vast majority of hazardous situations it could be argued that they are not true safeguards because they are not dedicated to safety. Hence the following are not true safeguards:

- Normal operating procedures and training
- Normal instrumentation and control systems
- Alarm devices that are used in the course of normal operations
- Inspection (although risk-based inspection may be an exception).

A normal operating response usually takes place before a safe limit has been breached. If the safe high level for T-101 is designated as 95% then normal operations will be conducted as the level rises *toward* the 95% value. Once the level goes above that point, the systems is, by definition, in an unsafe condition and the safeguards proper take over.

SAFEGUARD LEVEL 2: PROCEDURAL SAFEGUARDS

Procedural safeguards rely upon people either to trigger an automated safety system or to carry out the response to an ongoing situation. For example, if an operator is expected to respond to an instrument alarm, say high level in T-100, then his or her response constitutes a procedural safeguard.

Procedural safeguards are least reliable due to the relatively high chance of human error, particularly in emergencies. It has been estimated that, during an emergency, an untrained responder has an error rate of 50%, i.e., the chance of that person taking the right action (such as closing the correct valve) is only one in two. Therefore, if a person is asked to carry out "*n*" tasks during an emergency, the probability he will succeed is 0.5^n. If a person is expected to perform six tasks during an emergency, then the chance of his getting them all right is 0.5^6, which is only 3%. In other words, the person involved is virtually certain not to respond correctly.

In practice, most operators are highly trained and will have a much better response rate than that described above. Nevertheless, it is best not to rely on human response during an emergency if at all possible. The operator should initiate an automatic shutdown, then remove himself from the area of the incident if at all possible. If the incident becomes increasingly out of control the trained operator should be supported by a trained emergency response team.

Typically procedural safeguards are applied when the variable in question has gone beyond its safe limit value. In practice, alarms will often be initiated before that value has actually been reached. In other words, the alarm will sound to indicate that an unsafe condition is being approached.

SAFEGUARD LEVEL 3: SAFETY INSTRUMENTED SYSTEMS

Safety instrumented systems (SISs), with their associated Safety Integrity Levels (SILs), play an increasingly important part in assuring the safety of process plants. Referring to the standard example once more, a high-level interlock can be installed on LRC-101 such that when the level drops below, say, 5% of the tank height, a dedicated safety valve on the line from Pumps P-101 A/B will be closed.

Throughout this book emphasis is placed on the problems associated with common cause effects. In the case of safety instruments it is important to identify any problems that could simultaneously disable all the instruments. For example, solid material in a liquid stream could plug both instruments thus canceling out perceived redundancy. In order to minimize the problem of common cause events, good practice calls for different types of instrument and transmitter to be used when redundancy is called for.

SAFEGUARD LEVEL 4: MECHANICAL SAFEGUARDS

A mechanical safeguard is one that operates regardless of either instrument or human response. Two common examples of mechanical safeguards are check valves and pressure safety relief valves. They are described in Chapter 9—*Asset Integrity*.

SAFEGUARD LEVEL 5: PASSIVE SAFEGUARDS

A passive safeguard controls a hazard simply through its presence; such a safeguard does not have to do anything or to respond to unsafe conditions. An example of a passive safeguard is a tank berm.

Another common example of a passive safeguard is a flare system. Any flammable vapors that are released from the process will be burned in the flame of the flare.

SAFEGUARD LEVEL 6: EMERGENCY RESPONSE

Emergency response measures come into play *after* the incident has occurred. Therefore, such measures are not truly safeguards. They are only used when the various levels of safeguards have failed to prevent an incident from leading to actual damage and loss. Emergency response safeguards do not prevent an incident from occurring; they merely limit the consequences.

The following are typical safeguards at the emergency response level:

- Fire-fighting equipment
- The fire brigade
- Personal protective equipment (PPE) used to allow affected personnel to evacuate.

LAYER OF PROTECTION ANALYSIS

The semiquantitative technique known as Layer of Protection Analysis (LOPA) aims to address some of the practical difficulties with the hazards analysis techniques and quantification principles that have been discussed in this and the preceding chapter. A stand-alone hazards analysis, such as a HAZOP, provides only rough guidance—usually through use of a risk matrix—as to the likelihood of an event and the magnitude of its consequences. Also, in most cases, the technique discusses safeguards only in a fairly general manner, and there can be considerable disagreement among the team members as to quantitative effect of safeguards. The use of sophisticated modeling techniques for likelihood and consequence prediction tends to be resource-intensive, and the quality of their results may not be as good as hoped due to limitations in the quality of the failure rate data.

LOPA aims to address some of these concerns by positioning itself in a middle position between qualitative hazards analysis and detailed quantified studies. It takes the HAZOP results and adds a quantitative estimate as to the likelihood of occurrence and the consequences of each hazard. The calculated risk value is assessed against the company's risk-ranking criteria in order to determine if additional safeguards are required. LOPA can be particularly effective when determining if HAZOP recommendations for additional safeguards are truly warranted. Too few safeguards and the system is not safe enough; too many safeguards, and money is wasted and the additional complexity may introduce new safety issues.

LOPA can also be used to develop the quantified specifications for Safety Instrumented Levels (SILs), for SISs—a necessary step in complying with ANSI requirements). The technique is also effective at identifying safeguards—including those to do with human performance. From a regulatory point of view LOPA can provide a basis for specification of Independent Protection Layers (IPLs) and can help address the requirements of standards such as OSHA's 29 CFR 1910.119 and the Seveso II directives.

LOPA generally looks only at the risk associated with specific scenarios; it does not consider cumulative risk in the manner shown for F-N curves in Chapter 1. Nor does a LOPA normally consider the escalation of events, i.e., the change in risk values as the event develops.

The technique does require that companies put forward a value for the level of risk that they will accept ("How safe is safe enough?"). As noted with the discussion to do with ALARP in Chapter 1, the selection of such a value is fraught with difficulties.

LOPA evaluates risk in order of magnitude of selected accident scenarios. There are six basic steps in LOPA:

1. Identify the scenarios.
2. Select an accident scenario.
3. Identify the initiating event of the scenario and determine the initiating event frequency (events per year).
4. Identify the IPL and estimate the PFD of each IPL.
5. Estimate the risk of scenario.
6. Add additional IPLs to meet the company's risk targets.

THE LOPA PROCESS

The LOPA process can also be organized into the following six steps:

1. Obtain all reference documentation, including hazards analysis documentation, pressure relief valve design, and inspection reports.
2. Document the process deviation and hazard scenario under consideration by the team (in most cases, this will be taken from an already completed HAZOP).
3. Identify all of the initiating causes for the process deviation and determine the frequency of each initiating cause. The initiating cause frequencies should be based on industry-accepted and standards-compliant failure rate data for each device, system, or human.

4. Determine the consequence and likelihood of the hazard scenario. This evaluation should include an examination of safety, environmental, and economic losses (including the requirements associated with safety and environmental regulations). Based on an assessment of the overall risk associated with the identified hazard, decide if additional safeguards or Layers of Protection/Independent Protection Layers (IPL) are required. The criterion for acceptable risk could be single numerical value, or it could be determined through use of a risk matrix.
5. Identify existing IPLs or safeguards and determine the PFD for each PIL. For SISs, the PFD is a measure or risk reduction and is equivalent to the SIL.
6. Finally, the LOPA team provides specific recommendations—if required—to bring the risk to below the acceptable level.

If it is felt that a high consequence hazard has not been sufficiently evaluated, a supplemental quantitative risk analysis can be performed.

SINGLE SCENARIOS

It is critical that each LOPA scenario have just one cause and one consequence. There will always be a temptation to combine those causes that lead to the same consequence to save time in the analysis and documentation. However, the different causes will occur with different frequencies and may use different IPLs. For example, high level in a tank could be caused by failure of the level control instrument or by failure of the tank's discharge pump. These causes will have different frequencies of occurrence. They will also utilize different IPLs; for the first scenario an IPL could be a self-testing mechanism on the level instrument, for the second scenario an IPL could be an ammeter signal telling the operator that the pump had shut down.

Even if one IPL address two similar causes, it may not be equally effective against each. For example, high pressure in a pressure vessel could be caused by internal chemical reaction or external fire. A pressure relief valve is an IPL for both cases, but the sizing requirements for the valve are likely to be quite different from one another.

IPLs

An IPL is a safeguard that will prevent an unsafe scenario from progressing regardless of the initiating event or of the performance of another layer of protection IPLs can be either active or passive. All IPLs are safeguards, but not all safeguards are IPLs. Examples of IPLs include:

- Operating procedures
- Operator intervention
- Basic process control systems (BPCS)
- Alarms with defined operator response
- Critical alarms
- Safety instrumented systems
- Pressure relief devices
- Blast walls and dikes
- Deluge systems
- Flare systems

- Fire suppression systems
- Inherently safe design features
- Plant emergency response
- Community emergency response.

Each IPL must be specific, independent, dependable, and auditable. No distinction is made between safeguards that are purely for safety and those that address normal operations. For example, an operating procedure for a routine task and a pressure safety relief valve both count as IPLs.

Specific

The IPL must be capable of detecting and preventing or mitigating the consequences of specified, potentially hazardous event(s), such as a runaway reaction, loss of containment, or an explosion. A single IPL may address the multiple causes for that hazardous event; and, therefore, multiple event scenarios may initiate action of one IPL. For example, high pressure in a vessel could be caused by either a pump dead-heading into it or by external fire. For both cases the vessel's pressure safety relief valve counts as a valid IPL.

Independent

An IPL must be independent of all the other protection layers associated with the hazardous event being evaluated. Independence requires that the performance is not affected by the failure of another protection layer or by the conditions that caused another protection layer to fail. Most importantly, the protection layer is independent of the initiating cause.

A common cause of false independence occurs when a single instrument signal is used both to initiate an alarm and to operate an interlock. In this case, the alarm and interlock are not independent of one another. Another false independence is created if an operator response is treated as an IPL to an initiating error by the same person. In general, alarms that are annunciated on the BPCS are not independent of the BPCS; therefore, if the BPCS is to be treated as an IPL, then such alarms cannot be counted as an IPL.

In practice, as noted in the discussion to do with common cause effects, ensuring that two events actually *are* independent of one another can be very tricky—all sorts of unidentified causes may exist, thus creating an incorrect perception of independence. For example, high level in a tank may have two IPLs: operator response and high-level instrumentation. Superficially, these IPLs would appear to be quite different from one another. However, it may turn out that both fail due to a hidden common cause effect: an inadequate training program, i.e., the operator had not been trained in how to handle high level, and the instrument maintenance technician had not been trained to install the level alarm hardware correctly.

Dependable

The protection provided by the IPL reduces the identified risk by a known and specified amount. This does not mean that the IPL will always work—particularly with regard to human error, but an estimate as to its failure rate is available. A general rule is that the frequency reduction for an IPL should be two orders of magnitude, i.e., it has an availability of 99%. Operator response to an alarm can be one order of magnitude.

Auditable

Proof testing and maintenance of the safety system is necessary. It must be possible to verify that the IPL works as claimed (having said which, it is often difficult to check the response of personnel and some mitigating devices).

HUMAN RESPONSE

If an operator's response to a situation is to be treated as an IPL, then he or she must be allowed sufficient time to determine what is going on and then to respond.

IMPLEMENTING LOPA

Issues to consider when organizing and implementing a LOPA are discussed below.

Team makeup

A LOPA is carried out by a LOPA uses a multidisciplined team (typically including representatives from operations, maintenance, process engineering, and instrument, or electrical engineering).

Some organizations conduct LOPA as a part of the HAZOP, using same team members. This approach can be efficient because the team is familiar with the scenarios under discussion, and decisions can be recorded as part of the HAZOP recommendations. Other organizations have found it to be more efficient to capture the list of potential LOPA scenarios during the PHA, for later evaluation by a smaller team (perhaps just a process engineer and a person skilled in LOPA). The LOPA team can then report back to the PHA team on the results of their evaluation.

Timing

The LOPA technique can be used at any point in the lifecycle of a project or process, but it is most cost effective when implemented during front-end loading when process flow diagrams are complete and the P&IDs are under development. For existing processes, LOPA should be used during or after the HAZOP review or revalidation. Generally, LOPA will be applied after the qualitative hazards analysis has been completed—thus providing the LOPA team with a listing of hazard scenarios with associated consequence description and potential safeguards for consideration.

Tools

When an organization implements LOPA, it is important to establish tools, including aids like look-up tables for consequence severity, initiating event frequency, and PFD for standard IPLs. The calculation tools must be documented, and users trained. All LOPA practitioners in an organization must use the same rules in the same way to ensure consistent results.

Procedures and inspections

Procedures and inspections cannot be counted as IPLs. They do not have the ability to detect the initiating event, cannot make a decision to take action, and cannot take action to prevent the consequence. Procedures and inspections do, however, affect the probability of failure of an IPL.

Risk criteria

Implementation of LOPA is easier if an organization has defined risk tolerance criteria.

- If the result is greater than or equal to 1, the protection is adequate without any additional protection layers being required.
- If the result is less than 1 but greater than 10^{-1}, then the protection layers should be reviewed for adequacy, but an SIS or additional protection layer is not necessarily required.
- If the result is less than or equal to 10^{-1}, then the result indicates the requirement of additional protection layers, which could be an SIS.

FAILURE RATE DATA

Table 15.13 provides examples of cause frequencies (all values in events per year). Each company and facility will develop its own values for various events based on its own experience and maintenance records. In practice, the LOPA will depend heavily on the frequency estimated provided by the HAZOP team members.

CONDITIONAL PROBABILITY/BAYES' THEOREM

In many situations, some information is known about the failure rate of various equipment items, and that information improves with time as actual operating information is made available. In such situations, Bayes' Theorem can be used as a tool to update the reliability data.

The central tenet of conditional probability is that a hypothesis is rendered more probable as information confirming that hypothesis becomes available. The opposite is also true. If new information does not confirm the hypothesis, then that hypothesis is judged to be less probable. Conditional probability can be expressed in the form of Bayes' theorem, which is shown in Eq. (15.13).

$$p(T|E) = \frac{p(E|T) \times p(T)}{(p(E|T) \times p(T)) + (p(E|\neg T) \times p(\neg T))} \tag{15.13}$$

where

- T represents the theory or hypothesis that is to be tested.
- E represents new evidence that will help confirm or challenge that hypothesis.
- $p(T)$ represents the probability of T being true prior to the test taking place.

Table 15.13 Representative Event Failure Rate Data

Event	Frequency per Year
Rotating equipment failure	1E-01
Operator error (per task)	1E-01
Control loop failure	1E-02
Relief valve failure	1E-02

- $p(T|E)$ represents the probability of T being true after a positive test.
- $p(\neg T)$ represents the probability of T being false prior to the test taking place. In a two component system $p(\neg T) = 1.0 - p(T)$.
- $p(E|T)$ represents the probability of the event assuming that T is true.
- $p(E|\neg T)$ represents the probability of the event assuming that T is not true.

EVALUATION OF TESTS

Use of Eq. (15.11) can be illustrated by considering the effectiveness of a random drug screening or medical testing program. Based on experience at other facilities, management at a particular plant may have a (prior) estimate that 0.5% of their employees are using prohibited drugs. This is the prior value, $p(T)$. Since an employee can only have two "states"—either they take the drug or they do not—the prior probability that someone is not taking the drug, $p(\neg T)$, must be 0.995.

A drug screening company is hired to test the employees. The test that they use is 99% accurate, i.e., if a person is using the drug the test will identify that person 99% of the time. This is the term $p(E|T)$ in Eq. (15.11). However, the drug test can also give false positives, i.e., someone who is not taking the prohibited drug may test positive. The rate of false positives is 1%. This value is the term $p(E|\neg T)$ in Eq. (15.11).

Plugging the above data in Eq. (15.11):

$$\begin{aligned} p(T|E) &= (0.99 \times 0.005)/((0.99 \times 0.005) + (0.01 \times 0.995)) \\ &= 0.3322 \end{aligned}$$

The likelihood that an employee who tests positive is actually using drugs is only 33%. In other words, a person who tests positive is more likely to be a nonuser than a user.

This result seems counterintuitive. After all, the test is 99% accurate. The reason for the apparent anomaly is that, although the chance of a false positive is only 1%, the number of people who could have that false positive is large (99.5% of the persons tested). Therefore, the false-positive result strongly affects the overall outcome.

In order to back up the hypothesis that it is the false positives that lead to the apparently skewed results, Equation (15.13) can be tested with two new sets of numbers. First, if the reliability of the positive test is increased from 99% to 99.9% then the chance that an employee who tests positive is a drug user goes from 33.2% to 33.4%—a trivial improvement in the quality of the result. However, if the chance of a false positive falls from 1% to 0.1% the final result shifts from 33% to 83%—a significant improvement.

Equation (10.13) can also be used to evaluate the probability that a person who does take the drug will test negative. The calculation algorithm is shown in Eq. (15.14).

$$p(\neg T|E) = \frac{p(E|\neg T) \times p(\neg T)}{(p(E|T) \times p(T)) + (p(E|\neg T) \times p(\neg T))} \tag{15.14}$$

When data is entered into Eq. (15.14) the following result is obtained:

$$p(\neg T|E) = \frac{(0.01 \times 0.995)}{((0.99 \times 0.005)} + (0.01 \times 0.995)) = 0.6678$$

In other words, a person who is actually positive has a roughly 2 in 3 chance of not being detected in a single test.

SEQUENTIAL OBSERVATIONS

The first result from the application of Bayes' theorem becomes the prior value for a subsequent test. Using the drug screening example once more, the new prior value for p($T|E$) at the conclusion of the first test is 0.3322. All the other information remains the same. Running Equation (10.13) one more time with this new prior, the value for p(T|E) becomes 0.9706—a much more useful value. If this new value is used as the prior for a third test, the value increases to 0.9898.

COMBINING DATA SOURCES

Much of the data that is used in reliability work is a mixture of opinion (subjectivity) and observation (objectivity). For example, when a facility installs a new piece of equipment information to do with the reliability of that item will be based only on opinion (usually developed from knowledge as to how the equipment has worked in other applications). Once the new equipment item starts operating hard information as to its reliability becomes available. Thus, the original subjective data is gradually supplemented and replaced with objective data. The first standard example shows liquid entering a pressure vessel, V-101. The pertinent section of the block diagram is reproduced below as Figure 15.39.

Liquid leaves V-101 through a slide valve that operates in a batch manner. When the level in V-101 rises to a set value, the valve at the base of the vessel opens, the contents are drained then the valve recloses. The slide valve has a failure rate of 0.1 demand^{-1} (per demand), i.e., it fails to open one time in 10. The facility manager states that this failure rate is unacceptable, so he decides to replace the old valve with a new, more reliable model.

The vendor for the new valve claims that, in this service, the new valve will have a reliability of 0.01 demand^{-1}, i.e., it will fail only once in a 100 uses—10 times better than the existing valve. The plant manager asks his own maintenance manager to comment on this claim. The maintenance manager estimates a failure rate for the new valve of 0.05 demand^{-1}, i.e., one time in 20 uses.

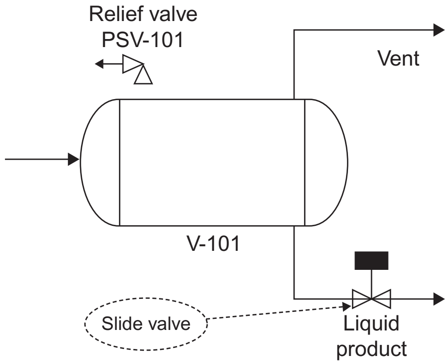


FIGURE 15.39

Sketch of the reactor drain system.

Although there is a considerable spread between these two estimates, the plant manager decides to go ahead and install the new valve because both parties judge it to be considerably more reliable than the old valve.

The plant manager has about equal confidence in the vendor (who knows the valve but not the service) and the maintenance manager (who knows the service but not the valve). Therefore, the plant manager's estimate of the overall failure rate is about 0.03 demand-1—the mean to the two estimates. It can be seen, therefore, that the estimate of the overall failure rate is made up of three subjective numbers:

- The opinion of the vendor
- The opinion of the maintenance manager
- The opinion of the plant manager concerning the previous two opinions.

The valve is installed, and on its first operation it works successfully. The plant manager now has one objective result which can be used to modify (but not replace) the opinions of the two experts.

Putting the above data into the form used in Eq. (15.13):

$$\begin{aligned} p(T) &= p(AV) \\ &= 0.50 \\ p(\neg T) &= p(AM) \\ &= 0.50 \end{aligned}$$

where $p(Ai)$ represents the probability of individual i being correct in the judgment of the facility manager (the letter "*V*" represents the vendor and "*M*" the manager).

Now, if the vendor were totally correct in his judgment, the probability of the new valve operating properly is 0.99. In other words, if the successful operation of the new valve is the observation E, then p($E|V$) = 0.99. On the other hand, if the maintenance manager's judgment is correct, the probability of the valve working is 0.95. Therefore,

$$p(E|M) = 0.95$$

For those cases in which the valve fails to operate properly, the respective probabilities are:

$$p(\neg E|V) = 0.01$$

$$p(\neg E|M) = 0.05$$

Given that, on the first operation, the valve did work, Equation (10.13) generates the following two equations:

$$\begin{aligned} p(E|V) &= \frac{0.50 \times 0.99}{(0.50 \times 0.99) + (0.50 \times 0.95)} \\ &= 0.5103 \end{aligned}$$

$$\begin{aligned} p(E|M) &= \frac{0.50 \times 0.95}{(0.50 \times 0.99) + (0.50 \times 0.95)} \\ &= 0.4897 \end{aligned}$$

Therefore, as the result of one successful operation of the new valve, the facility manager's confidence in the vendor's judgment has risen to 51%, but it has fallen to 49% for the maintenance manager. This gives an estimate for the overall failure rate as (0.5103 × 0.01) + (0.4897 × 0.05) or 2.96%, which is down slightly from the initial estimate of 3.00%.

If, on its first operation, the valve had failed, Bayes' Theorem would generate the following equations:

$$p(\neg E|V) = \frac{0.50 \times 0.01}{(0.50 \times 0.01) + (0.50 \times 0.05)}$$
$$= 0.167$$

$$p(\neg E|M) = \frac{0.50 \times 0.05}{(0.50 \times 0.01) + (0.50 \times 0.05)}$$
$$= 0.8333$$

In this case, there is a much bigger change from the initial estimates because the valve failed even though both experts believed that it would operate successfully. In particular, confidence in the vendor's opinion has changed dramatically. The overall failure rate is now estimated to be 4.33%.

Returning to the first case, in which the valve operated successfully, the new estimated failure rates are used as the starting point for the next iteration. If the valve operates successfully for a second time, then the equations become:

$$p(E|V) = \frac{0.5103 \times 0.99}{(0.5103 \times 0.99) + (0.4897 \times 0.95)}$$
$$= 0.5206$$

$$p(E|M) = \frac{0.4897 \times 0.95}{(0.5103 \times 0.99) + (0.4897 \times 0.95)}$$
$$= 0.4794$$

Once more the confidence in the vendor has increases slightly. The overall estimated failure rate is now 2.92%.

Table 15.14 shows the effect of 40 actual valve operations on estimated and actual failure rates. The first column shows the number of operations or trials of the new valve. The second column states whether the valve operated successfully or not at that trial number. The valve operates correctly up until the ninth trial. The third column shows the total number of successful operations. It shows that, after 40 trials, the valve has worked properly 38 times, thus giving an overall measured (frequentist) failure rate of 2/40, or 5.0% (which is half the rate for the old valve).

However, the Bayesian failure rate is 4.36% because the original opinions are still a factor in the overall estimate. Once the valve has operated many times, the Bayesian and statistical (frequentist) failure rates should converge because objective data will supplant personal estimates.

Although the above example involved only two initial opinions (that of the vendor and that of the maintenance manager), it is quite simple to incorporate multiple initial probabilities. For example, the plant operations manager may also have an opinion regarding the new valve. The plant manager agrees to incorporate this new opinion, but chooses to give it less credence than was given

Table 15.14 Performance of the New Valve

Iteration	Operation	Total Successes	Frequentist Rate (%)	Bayesian Rate (%)
0				3.00
1	Y	1	0.0	2.96
2	Y	2	0.0	2.92
3	Y	3	0.0	2.88
4	Y	4	0.0	2.84
5	Y	5	0.0	2.79
6	Y	6	0.0	2.75
7	Y	7	0.0	2.71
8	Y	8	0.0	2.67
9	N	8	11.1	4.13
10	Y	9	10.0	4.10
11	Y	10	9.1	4.07
12	Y	11	8.3	4.04
13	Y	12	7.7	4.01
14	Y	13	7.1	3.98
15	Y	14	6.7	3.95
16	Y	15	6.3	3.92
17	Y	16	5.9	3.88
18	Y	17	5.6	3.85
19	Y	18	5.3	3.82
20	Y	19	5.0	3.78
21	Y	20	4.8	3.75
22	Y	21	4.5	3.71
23	Y	22	4.3	3.67
24	Y	23	4.2	3.64
25	Y	24	4.0	3.60
26	Y	25	3.8	3.56
27	Y	26	3.7	3.52
28	Y	27	3.6	3.49
29	Y	28	3.4	3.45
30	Y	29	3.3	3.41
31	Y	30	3.2	3.37
32	Y	31	3.1	3.33
33	Y	32	3.0	3.29
34	Y	33	2.9	3.25
35	Y	34	2.9	3.21
36	Y	35	2.8	3.17
37	Y	36	2.7	3.12
38	N	36	5.3	4.40
39	Y	37	5.1	4.38
40	Y	38	5.0	4.36

Table 15.15 Three Initial Estimates

	Reliability Estimate (%)	Level of Belief (%)
Vendor	1.0	40
Operations manager	5.0	20
Maintenance manager	7.5	40

to the vendor and the maintenance manager. Hence the initial starting point can be based on estimates as shown in Table 15.15.

Finally, it is important to ensure that the initial probability estimates bracket the "true" final value. For example, if the failure rate of the valve in the above example turns out to be say 1 in 500, then the Bayesian estimate will never converge on that number because it can never go beyond the initial best estimate, which was 1 in 100.

CHAPTER

RELIABILITY, AVAILABILITY, AND MAINTAINABILITY 16

CHAPTER OUTLINE

INTRODUCTION

Reliability, availability, and maintainability (RAM) programs are an integral part of any risk management system. (*Note*: Some companies use the letters RAM to mean Risk Assessment Matrix.)

RAM techniques possess many similarities to those that are used for safety. However, the key difference between RAM and safety analyses is that it is possible to talk about optimum reliability, i.e., the point at which a dollar spent on improving reliability leads to less than a cost-averaged dollar in benefits, as illustrated in Figure 16.1. With safety, however, there is no real optimum value: all incidents are unacceptable. As explained with the discussion to do with ALARP, no company or government agency is going to commit to an acceptable level in the number of deaths or serious injuries. And nor should they.

Figure 16.1 shows that as funds are initially expended on improved reliability, the incremental revenue is greater than the money spent (when factored over the normal capital investment period). However, there is an optimum point, above which a dollar spent on improved reliability generates less than a dollar in life cycle incremental revenue (i.e., the slope of the curve becomes less than unity). In practice, there is rarely sufficient data to be able to develop a curve such as Figure 16.1 with precision. Nevertheless, it is useful to keep in mind that reliability program is not, in and of itself, its own justification. It has to demonstrate that an investment in reliability will lead to an increase in profits.

Process Risk and Reliability Management. DOI: http://dx.doi.org/10.1016/B978-0-12-801653-4.00016-3

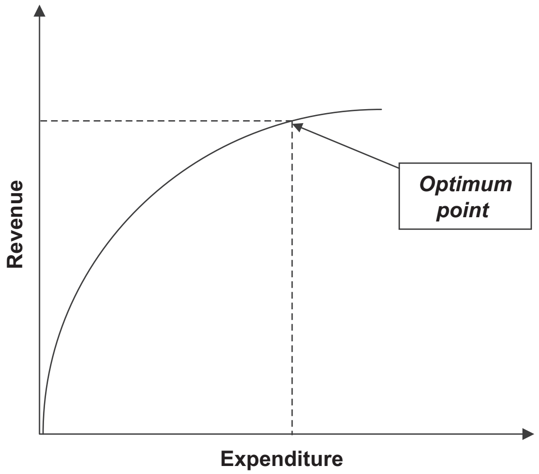


FIGURE 16.1

Reliability payout.

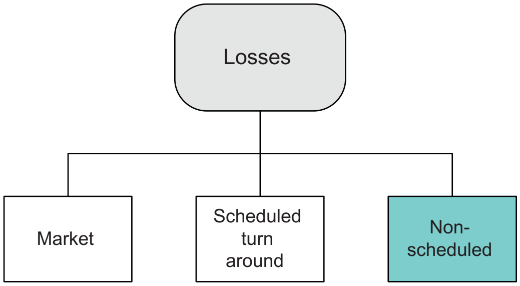


FIGURE 16.2

Loss categories.

Figure 16.2 shows three causes for losses. The first is that the sales of the product are down. Even though the facility can make product, the market is not buying it, so rates have to be cut back. The second cause in Figure 16.2 is to do with scheduled turnarounds during which equipment that cannot be maintained while it is operating is worked on. (A strong asset integrity program may help reduce the amount of time needed for such turnarounds but they are not usually part of the RAM process.) Nonscheduled losses, the third element in Figure 16.2, are the focus of this chapter.

Naturally, it is not possible to identify and correct all possible causes of production loss. Therefore, it is suggested that the Pareto Principle (described in Chapter 15) be used to find and correct the major problem areas, as shown in Figure 16.3. The focus should be on finding and correcting the important few factors that contribute toward nonscheduled downtime, and ignoring the unimportant many.

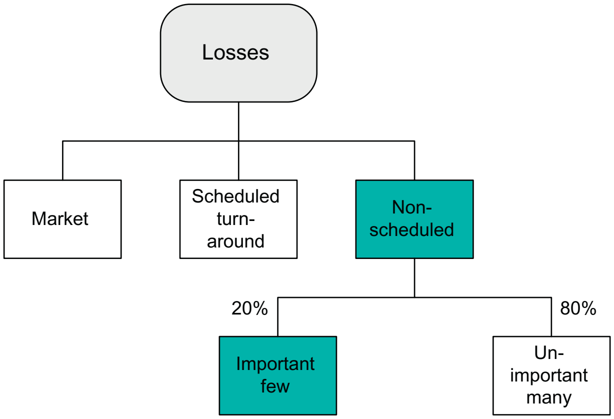


FIGURE 16.3

Use of the Pareto Principle.

BENEFITS OF A RAM PROGRAM

The benefits of an effective RAM program include the following:

- Increase production and profitability
- Increased productivity
- Reduced investment
- Lower maintenance costs
- Lower inventories
- Enhanced customer satisfaction
- Personal recognition
- Personal life
- Improved public perception.

INCREASED PRODUCTION AND PROFITABILITY

A reliable facility will make more money because it will operate for longer periods of time. The extra production will increase revenues (assuming that the facility can sell all that it makes). Furthermore, the incremental production is very profitable because all of the fixed and semifixed costs of production such as rents and salaries will have been covered by the baseline production.

Figure 16.4 shows a facility where the first 90% of the production covers fixed and semifixed costs such as payroll, taxes, equipment depreciation, and rent/lease payments. It is in the range 90–100% that the profits are made. Therefore, if availability can be increased by "only" 1% from 95% to 96%, profitability will increase by 10%.

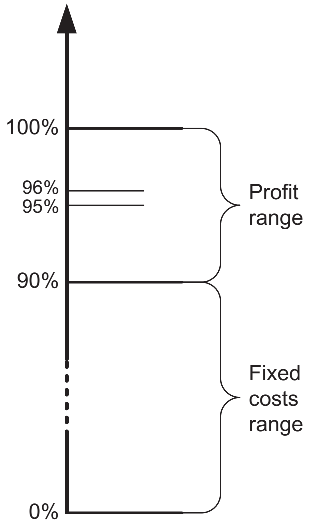


FIGURE 16.4

Reliability and profitability.

INCREASED PRODUCTIVITY

An unreliable facility will experience increased losses, most of which occur during shutdown and restart for reasons such as flaring of waste gases, recycling of off-spec products, and reduced reactor selectivities. Not only do such situations such as these result in a loss of materials, they also create an increase in energy consumption because some equipment items will have to be cooled down, and then reheated and because items such as pumps, compressors, and fired heaters have to keep operating, even though they are on total recycle.

REDUCED INVESTMENT

Productivity improvements can often be achieved with minimal investment. For example, a pump in production-critical service may fail once every 3 months. If each pump failure leads to production losses of $15,000, then the annual cost of this problem is $60,000. Investigation into the pump failures shows that the breakdown rate could be greatly reduced where a preventive maintenance system was to be implemented, so that problems can be addressed before the pump actually fails. It is predicted that the new failure rate will be once per year, equivalent to a loss of $15,000 per year. Hence the annual savings that flow from the preventive maintenance program are $45,000. If the preventive maintenance system for that pump costs say $10,000 to implement and $5,000 per year to run, then the net savings over a period of 5 years is $190,000 (ignoring the discounted value of money), and the return on investment is very high indeed.

If the RAM program is effective at squeezing more production from existing equipment, it may be possible to postpone or cancel plans to build expansion facilities.

LOWER MAINTENANCE COSTS

When a facility operates smoothly, the cost of maintenance goes down because fewer spare parts will have to be purchased, and labor costs—particularly overtime—will be reduced.

LOWER INVENTORIES

The response to reliability problems is often to increase the number of spare parts and the quantity of raw materials. As reliability improves, these inventories can be reduced.

ENHANCED CUSTOMER SATISFACTION

A facility that operates reliably will have more satisfied customers because there will be fewer problems with off-spec products and missed delivery dates.

PERSONAL RECOGNITION

Managers recognize that a smoothly operating facility makes them look good in the eyes of their bosses, whereas frequent upsets and shutdowns reflect negatively on the perception of a manager's competence. This insight was recognized by one facility manager when he was evaluating some reliability software. He said to the software salesperson, "I see what you're selling—you're selling job security." Moreover, when a facility is running smoothly, a manager has time to develop new and positive programs that develop both his or her own career and the careers of others at the facility. In addition, the development and implementation of RAM programs is often one of the few ways that a facility manager can materially improve performance. Other major expenses, such as equipment depreciation, labor rates, and taxes are usually outside the direct control of local management. However, higher on-stream performance is something that can be achieved locally.

PERSONAL LIFE

If a facility is running smoothly, the manager's personal life is likely to be more balanced, and he or she will not have to work such long hours "fighting fires" (sometimes literally).

IMPROVED PUBLIC PERCEPTION

Many problems to do with adverse public perception of the process industries relate to unreliable operations. Indeed, if a facility is operating within its environmental permits then most of the incidents that may be noticed by the public will result from unplanned upsets and shutdowns. These are the times when liquids are spilled, hazardous vapors released, and gases are flared.

RELIABILITY AND SAFETY

Although the focus of a RAM program is to improve profitability, it is also likely to enhance safety and environmental performance for the following reasons.

HAZARDOUS OPERATIONS

Shutdowns and their subsequent restarts often require that operators and maintenance personnel perform inherently hazardous activities such as opening vessels, working on electrical equipment, and lifting heavy equipment items with cranes. Moreover, during upsets and shutdowns, both the operators and the equipment are working in unusual, high stress conditions, leading to an increased chance of a serious accident taking place.

UNSAFE PROCESS CONDITIONS

Unsteady operation may inadvertently create unsafe process conditions, such as excessively high reactor temperatures.

SAFETY BYPASSES

A shutdown is often a time when operations and maintenance personnel are allowed to ignore or override safety systems such as interlocks and alarms, thus increasing the chance of someone being hurt.

TRANSIENT STRESSES

Frequent shutdowns and restarts can lead to the accumulation of transient stresses in equipment that may lead to premature failure.

REDUCED CHANCE OF CATASTROPHIC LOSSES

The safety and environmental consequences of poor reliability are usually assumed to be limited in scope. However, if a reliability issue gets out of hand, it could result in a catastrophic incident.

However, the goals of RAM and safety programs are not completely identical for some of the reasons listed below.

INCREASED SAFETY MAY REDUCE RELIABILITY

The addition of safety equipment to a process may lead to an increase in the number of shutdowns. For example, adding fire eyes to a furnace will improve its safety because they will warn of situations where a burner flame has gone out. However, fire eyes may fail internally, thus leading to spurious alarms and trips.

LOSS OF EXPERIENCE

Because a reliable plant does not undergo many shutdowns, the operators are less experienced in the actions to be taken when there is a shutdown.

ENGINEERING PRACTICES

Unsafe engineering practices can increase reliability. For example, temporary bypasses and electrical jumpers will keep a plant running during an upset, but they increase the chance of an accident. (Ultimately such shortcuts may create a major reliability problem if there is a catastrophic loss of equipment, but in the short term they are usually effective at improving reliability.)

DAILY OPERATIONS

Some safety equipment, such as personal protective equipment (PPE), can make a plant more difficult to operate and may reduce the operators' capability to respond quickly to plant upsets, thus leading to reduced reliability.

Of course, none of the above comments mean that safety work should be cut back, but it should be recognized that improving safety may mean that corresponding efforts to hold or improve reliability are also required.

DEFINITIONS

Like all other technical disciplines, reliability engineering uses specialized terms with precise meanings. Unfortunately, many of these terms also have everyday meanings—therefore, it is very important to define the terms used in formal reliability work.

RELIABILITY

> The reliability of a component or of a system is the probability that it will perform a required function without failure under stated conditions for a stated period of time.

This definition incorporates the following concepts:

- Reliability can refer to either the components in a system or the system itself (although the term *availability* is more generally used for system analysis).
- Reliability has a probability value associated with it; nothing is either certain to operate or certain to fail.
- The definition includes the term *required function*. All items and systems are designed for particular tasks or sets of tasks. If an item is called on to perform a nonspecified task, and then fails, the item itself was not unreliable.

- Similarly, the *stated conditions* must be observed. For example, if an equipment item is operated outside its design temperature range, then failure of that equipment does not mean that it was unreliable.
- Reliability covers only a *stated period of time*. Nothing can last forever; eventually everything wears out. (Sometimes the stated period of time refers to the number of cycles of operation to which an item is exposed, rather than its chronological age.)

AVAILABILITY

Availability refers to the degree with which a complete system, such as a refinery or offshore platform, is able to perform as required. It is defined as follows:

> The availability of a repairable system is the fraction of time that it is able to perform a required function under stated conditions.

Availability is used for systems—reliability for components of those systems. The difference between reliability and availability is illustrated in Figure 16.5. Over a long period of time, the value of availability levels out at (usually) quite a high number. For example, the availability of a process unit may be say 95%, which means that it is operating 95% of the time management wants it to operate. The reliability values for individual equipment items, however, trend asymptotically to zero. If an item is in service long enough, and if it is not either repaired or replaced, it will eventually fail.

Availability can be defined as shown in Eq. (16.1).

$$\text{Availability} = \frac{\text{total time}}{\text{total time} - \text{scheduled downtime}} \tag{16.1}$$

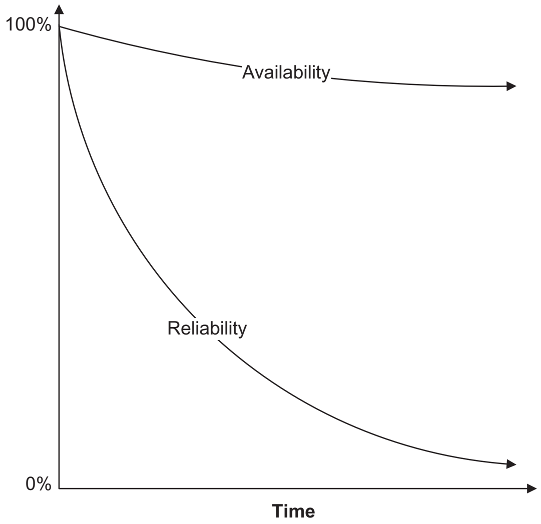


FIGURE 16.5

Availability and reliability.

For example, a facility manager may schedule 25 days a year for shutdown repairs and the installation of new equipment on a plant that can operate 365 days per year. The facility also experiences three unscheduled shutdowns totaling 8 days. Hence the system availability is:

$$(365 - 25 - 8)/(365 - 25) = 97.6\%$$

It is also possible to define availability in terms of total time, without taking any credit for scheduled downtime. Using the same sample data, the availability of the system in this case becomes:

$$(365 - 25 - 8)/(365) \text{ or } 91.0\%$$

It is important to pay close attention to repair times when aiming to improve availability even though they constitute only a small fraction of the overall operating time, as illustrated in the following example.

A system operates for 5,000 hours and then fails. The repair takes 100 hours to complete. Hence, the availability of the item is (4900/5000) or 98.0%. Management decides that they would like the availability figure to rise to 99.0%. There are two ways of doing this. The first option is to increase run times to 10,000 hours while maintaining the same 100-hour lost time for repairs. The second option is to reduce the repair time from 100 hours to 50 hours. Both approaches generate 99.0% availability. In practice, it may often turn out that it is much easier to improve repair times than to increase run times between failures.

EFFECTIVENESS

When a facility is capable of producing more product than is required by the market, then the term effectiveness is used instead of availability. Effectiveness is defined in Eq. (16.2).

$$\text{Effectiveness} = \text{Availability} \times \text{Fractional Capacity} \tag{16.2}$$

Fractional capacity represents the fraction of total production that could be made at any one time. If a facility operates all the time but is only turning out 50% of design production due to external factors such as reduced product sales, then its availability is 100%, but its fractional capacity is 50%, so its effectiveness is only 50%.

Table 16.1 shows how effectiveness can be calculated. A facility has a nameplate capacity of 500 tons per day. Market capacity shows the fraction of material that can actually be sold.

Days 1 and 2 are self-explanatory—the facility is available 100% of the time and can sell everything it makes, so it produces the full 500 tons per day. Its effectiveness is 100%. On Day 3, the availability falls to 75%, so the effectiveness falls to 75%. On Day 7, the facility can only sell 50% of its potential production even though it is 100% available, so its effectiveness is 50%. On Day 12, both the availability and market capacity are 50%. However, the effectiveness is 50% because the plant is available to meet sales requirements.

MAINTAINABILITY

The following definition is used for the word “maintainability.”

> The maintainability of a failed component or system is the probability that it is return to its operable condition in a stated period of time under stated conditions and using prescribed procedures and resources.

Table 16.1 Effectiveness Example

Day	Market Capacity (%)	Availability (%)	Production (tons)	Effectiveness (%)
1	100	100	500	100
2	100	100	500	100
3	100	75	375	75
4	100	75	375	75
5	100	100	500	100
6	100	100	500	100
7	50	100	250	50
8	50	100	250	50
9	50	100	250	50
10	100	0	0	0
11	100	0	0	0
12	50	50	250	50
Total			3,750	63

Most reliability analyses assume that, when an item is repaired, it is returned to service "as good as new." In fact, this assumption is rarely true; most items are restored to a condition that is somewhere between "as good as new" and "as good as old," i.e., it is in worse condition than when it was brand new, but in better condition than at the time of failure.

FAILURE MODES

It is critical that an item's failure modes be defined precisely. Issues to consider include the following.

EQUIPMENT DESCRIPTION

One of the biggest problems with reliability data, particularly when obtained from generic sources, is that an equipment item may not be fully described or its boundaries may not be fully delineated. For example, the term "pump failure" may cover just the pump itself or it may include failure of the motor, the coupling, and the foundations.

PRIMARY, SECONDARY, AND COMMAND FAILURES

Equipment failures can be primary, secondary, or command. A *primary* failure is one that occurs under normal operating conditions and for which the component itself is responsible. A *secondary* failure is one that is caused by external conditions or factors and for which the equipment item itself cannot be held responsible. For example, if a corrosive liquid is inadvertently fed to a pump, then the subsequent failure of the pump is secondary. A *command* failure is one that is caused by the equipment item's control systems. A signal from an instrument that causes the pump to shutdown is a command failure.

CATASTROPHIC, DEGRADED, AND INCIPIENT FAILURES

A *catastrophic* failure causes the item in question to be completely nonoperable. For example, if the casing of a pump fails the pump will have to be shut down and so the failure would be catastrophic. A *degraded* failure is one that causes it to perform below its design condition, but that does not prevent it from operating completely. An example of this type of failure would be erosion of a pump impeller leading to a reduction in the liquid discharge pressure. An *incipient* failure is one that has not yet caused anything worse than a marginal loss of performance. Such a failure is often a precursor of one of the more serious types of failure. An example of an incipient failure for a pump would be higher than normal vibration.

REAL FAILURES/NECESSARY REPLACEMENTS

When analyzing plant maintenance data, it is important to remember that items are sometimes replaced even though they have not yet failed. For example, whenever work is carried out on a pump the seal will usually be replaced, even if it was in good condition. Similarly, gaskets are replaced when work is conducted on piping regardless of the state of the gaskets of themselves. Therefore, a database that shows a large number of seal or gasket failures may give a misleadingly large number of events.

Total replacement of equipment can also lead to misleading failure rate data. One refinery, for example, had a set of block valves that were extremely unreliable. Management decided on a wholesale replacement of all these valves with a new brand that were much more reliable. Hence, the failure rate data prior to the replacement were completely misleading.

FAILURE RATES

The probability density function, $f(t)$, is defined as the probability of failure in any time interval dt. The cumulative distribution function, $F(t)$, is the integral of $f(t)$.

$$F(t) = \int_0^t f(t)\mathrm{d}t \tag{16.3}$$

where $F(t)$ can be either of the following two meanings:

1. For a population of a particular item, it is the fraction of all units of the original population that have failed by time t.
2. It is the probability that a particular item will have failed by time t.

$F(t)$ will generally have a shape such as that shown in Figure 16.6. It asymptotically approaches a value of 1.0.

The instantaneous failure rate of an item, i.e., the likelihood that it will fail at time t given that it has survived to that time is called the hazard rate, $h(t)$. It is defined in Eq. (16.4).

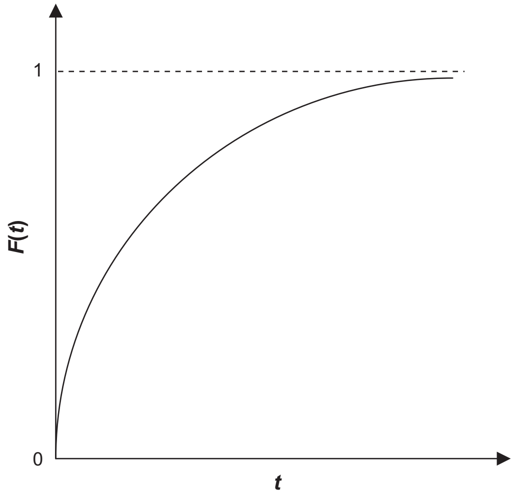


FIGURE 16.6

Shape of $F(t)$.

$$h(t) = \frac{f(t)}{1 - F(t)} \tag{16.4}$$

where $h(t)$ is not a probability and can have a value that is >1.0.

The following terms are used when calculating failure rates. (Other authorities use different definitions, particularly for MTBF (*mean time between failures*) and MTTF (*mean time to failure*), so care should be taken when using data from different sources.)

- *Mean Time to Failure (MTTF)*

  The mean of an equipment item's operating times, i.e., the time from when an item is put into to operation to the time when it fails.
- *Mean Time to Repair (MTTR)*

  The mean time it takes to repair an equipment item. It is formally defined as the "total corrective maintenance time divided by the number of corresponding maintenance actions during a given period of time."
- *Mean Downtime (MDT)*

  MDT and MTTR are often treated as being the same. However, some analysts distinguish between MTTR, which is just the repair time itself, and MDT, the total time needed to bring an item back into service, including the time for shutdown activities such as waiting for technicians to be available, transporting items to and from the work site, and the ordering of spare parts.
- *Mean Time between Failures (MTBF)*

  MTBF is the mean of the time between the failures for any particular item. It includes both operating and repair time. It relates to the other terms as shown in Eq. (16.5) and Figure 16.7.

$$\text{MTBF} = \text{MTTF} + \text{MDT} \tag{16.5}$$

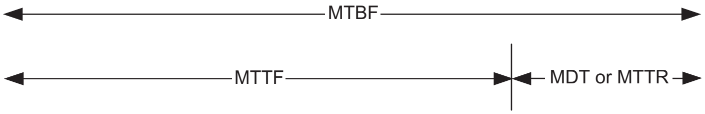


FIGURE 16.7

MTBF, MTTF, and MDT.

One potential source of confusion is the meaning of the term “failure rate.” When *f*(*t*) does not vary with time, then the failure rate is simply MDT/MTBF. If *f*(*t*) is not constant with respect to time, then either *F*(*t*) or *h*(*t*) can be defined as being the “failure rate.” In this chapter, *h*(*t*) is taken to be the failure rate.

CONSTANT/EXPONENTIAL DISTRIBUTION

The most widely used type of failure rate is the constant—or exponential—distribution. The use of the word exponential for constant failure rate seems contradictory. However, the constant failure rate refers to *h*(*t*), not *f*(*t*). In other words, as time progresses the number of items that were operable at time *t*(0) will decline. However, those items that do survive to time *t* have the same rate of failure as they had at time *t*(0).

For the constant failure rate, *f*(*t*), *F*(*t*), and *h*(*t*) are defined as follows:

$$f(t) = \mathrm{e}^{-\lambda \mathrm{t}} \tag{16.6}$$

$$F(t) = 1 - \mathrm{e}^{-\lambda \mathrm{t}} \tag{16.7}$$

$$h(t) = \lambda \tag{16.8}$$

$$\lambda = \frac{\mathrm{MDT}}{(\mathrm{MTTF} + \mathrm{MDT})} \tag{16.9}$$

where λ (lambda) is the overall failure rate.

LOGNORMAL DISTRIBUTION

The lognormal distribution is illustrated in Figure 16.8. It shows that the bulk of the failures occur early on, but that some items survive for a long time. This type of curve can be useful when considering the impact of maintenance on overall failure rates. The probability of an item being repaired in a very short time is low because it takes a finite amount of time to assemble workers and spare parts. (Figure 16.8 shows that *h*(*t*) is zero for the lowest values of *t*, indicating that MDT cannot be zero, i.e., it always takes a finite time for the item to be repaired.) At the other end of the curve, the repair time may be stretched out if a critical spare part is not available. Most of the failures occur near the peak of the curve.

BATHTUB CURVE

An item’s failure rate is generally not a single value—it will vary with time and the age of the item. The bathtub curve, shown in Figure 16.9, illustrates this phenomenon (the term “bathtub” comes from the rather fanciful resemblance of the shape of the overall failure rate to that of a bathtub).

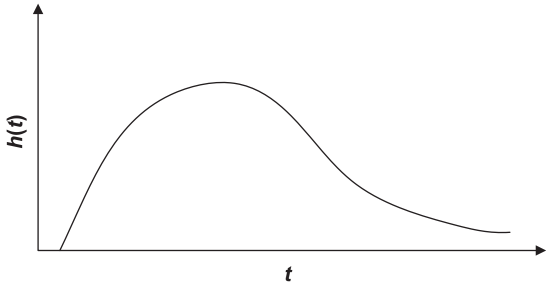


FIGURE 16.8

Lognormal distribution.

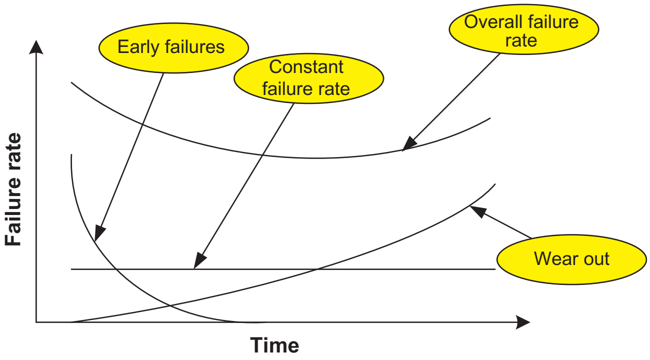


FIGURE 16.9

Bathtub curve.

In practice, few equipment items exhibit the behavior shown in Figure 16.9. For example, pressure vessels do not wear out—they generally fail due to the impact of an external event, such as the addition of corrosive materials. Nevertheless, the sketch is useful for understanding and categorizing the different ways in which equipment items can fail.

Early failures

Some components fail soon after they are placed in service. This phenomenon—sometimes referred to as "infant mortality"—usually results from problems in the manufacture or commissioning of the item. Not all equipment types exhibit wear-in behavior. For example, pressure vessels that have been fabricated and inspected to the appropriate standards are not likely to suffer from early failures.

Constant failure rate

The constant failure rate curve shown in Figure 16.9 is a straight line corresponding to the exponential failure rate already discussed. It represents random events that occur independently of time. For example, operator error that can take place at any time.

Wear-out failures

As equipment ages, particularly equipment containing moving parts, internal components will gradually wear out, thus leading to an increased failure rate. In practice, many items are prevented from reaching the wear-out point through the use of preventive maintenance and risk-based inspection programs. In other situations, the supplier of the equipment item may simply specify its "shelf life," after which the item will be replaced before it fails.

RELIABILITY BLOCK DIAGRAMS

Reliability block diagrams (RBDs) are similar to block flow diagrams (BFDs) (described in Chapter 16). A BFD shows the flow of gases, liquids, and solids through the process. An RBD illustrates the "flow" of reliability from the front of the plant to the back.

Figure 16.10 shows the simple block flow diagram that was introduced in the first standard example. The process consists of four processing areas in series (100–400), each of which receives utilities from Area 500.

The corresponding RBD is shown in Figure 16.11. In order for the system to function, it is essential that all five areas operate—if any one of them fails, then the overall system fails. The key difference between Figures 16.10 and 16.11 is that Unit 500, the utility system, is shown as being in the chain of events; if the utilities fail then the overall system fails.

A similar analysis can be carried out using the same example for the tank, pump, and vessel system (Example 2 in Chapter 1). The BFD for the system is shown in Figure 16.12.

The RBD for this system is identical to the BFD. There are two paths to reliable operation:

1. T-100/P-101A/V-101
2. T-100/P-101B/V-101.

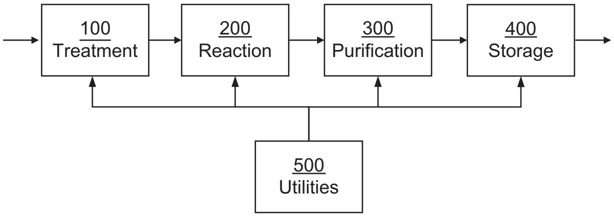


FIGURE 16.10

Process units—Block flow diagram.

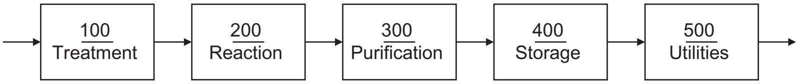


FIGURE 16.11

Reliability block diagram.

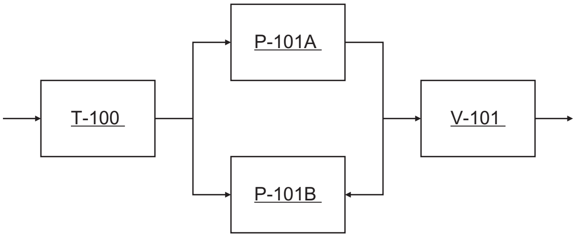


FIGURE 16.12

BFD for equipment.

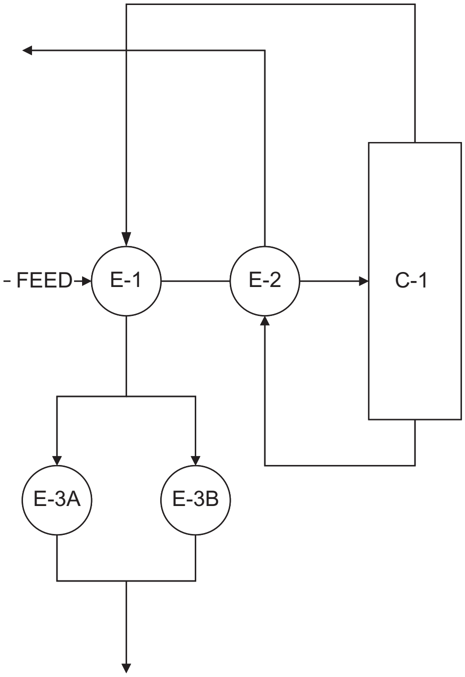


FIGURE 16.13

Heat recovery BFD.

A key difference between BFDs and RBDs is that the first can incorporate recycle streams; the second cannot. This difference is illustrated in Figures 16.13 and 16.14, which show the heat recovery system for a distillation process.

Cold feed is heated first by the overheads stream from the column in Exchanger E-1, then by the bottoms stream in Exchanger E-2. The overhead stream from C-1 is further cooled and condensed in either E-3A or E-3B (either has sufficient capacity for the full service).

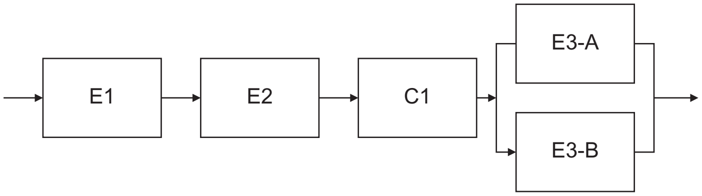


FIGURE 16.14

Heat recovery RBD.

The schematic shown in Figure 16.13 is quite complex since it involves two recycle streams. However, the RBD for this system is much simpler, as shown in Figure 16.14, because there is no recycle function in the reliability "flow." If any one of the items in the system fails (with the exception of either E-3A or E-3B), then the system fails.

ACTIVE/STANDBY REDUNDANCY

Backup equipment can be either *active* or on *standby*. If it is active, then it is operating alongside the primary item and will continue to fulfill the system function should the primary fail. However, it is more common to have a situation where the spare item is on standby. Following the failure of the primary equipment item, the backup has to be brought on line sufficiently quickly to prevent interruption to the system's function. This means that there has to be a mechanism for making the switchover—either automated for manual. In practice, the switching process can itself be a source of unreliability—particularly if it is not tested all that frequently.

Using Figure 16.14 as an example, if E-3A fails (say one of its tubes suddenly develops a large leak), then the following sequence of events must take place in order for there to be a successful (manual) switch to E-3B:

- The system instrumentation must signal that a problem has occurred.
- The operator must understand the instrument signals and correctly diagnose the cause of the problem.
- He or she needs to switch the exchangers, making sure that valves are closed and opened in the correct sequence.
- All of the above must take place in a timely manner.

The modified RBD for this new system is shown in Figure 16.15. If either E-3A or E-3B is operating, then the system is operating. However, if one of the exchangers fails, then the switchover mechanism must work properly, and the alternate exchanger must work.

QUANTIFICATION OF BLOCK DIAGRAMS

The quantification of block diagrams follows the same general principles as used for quantifying fault trees and event trees (see Chapter 15). To calculate the probability of success for each path in

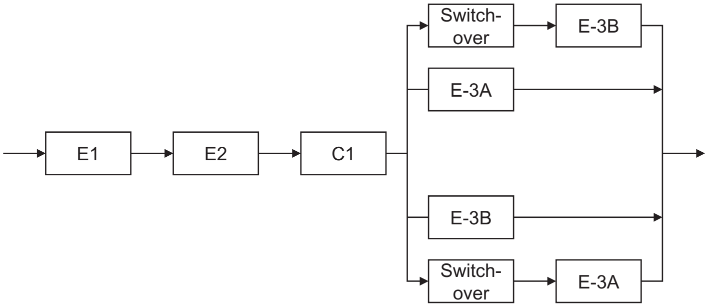


FIGURE 16.15

Heat recovery RBD with standby equipment.

a block diagram, the probabilities for each item in that path are multiplied. In the case of Figure 16.15, the probability of success for the two paths is as follows:

$$p(1) = p(E1) \times p(E2) \times p(C1) \times p(E - 3A) \tag{16.10}$$

and

$$p(2) = p(E1) \times p(E2) \times p(C1) \times p(E - 3B) \tag{16.11}$$

To calculate the probability of success for the system, the set values are added to one another. Therefore, in this example, the probability that the system will successfully operate is:

$$p(\text{System}) = p(1) + p(2) - (p(1) \times p(2)) \tag{16.12}$$

The following values are used for illustrative purposes:

p(E1)	0.95
p(E2)	0.96
p(C1)	0.99
p(E-3A)	0.90
p(E-3B)	0.80

When these values are inserted into Eqs. (16.10)−(16.12), the probability of success for each train and for the overall system becomes:

p(1)	0.813
p(2)	0.722
p(System)	0.948

It was noted in Chapter 15 that the second-order term for fault tree analysis is often not significant when probability values are low. With reliability work, where values typically are high, the second-order term must be used. If it is excluded then the probability of success is 1.535—an obvious anomaly.

HUMAN RELIABILITY

Most accidents and operating upsets involve some sort of human error. For example, Geyer et al. (1990) state that operator error is a direct cause of nearly a third of all pipework failures. (These errors consisted mostly of inadequately cleaning lines and incorrectly setting valves.)

The focus of books such as this book is on technology and the application of management principles. However, all technology and all management ideas have to be implemented through people, so it is vital that issues such as procedures, training, and performance feedback are given the same level of attention as the technical issues themselves. In addition, plant reliability is also strongly determined by human reliability.

The topic of human reliability, i.e., getting people to do the right things at the right time, presents management with a dilemma. Reliability should and can be quantified, and the management should "follow the numbers"—both engineering and dollar numbers. However, this is very difficult to do with human beings because they are not machines, and cannot be analyzed and modeled in the same manner as pumps, tanks, and instruments. Most analysis of human performance falls in the realms of psychology and sociology rather than engineering.

Yet human error and human reliability are a profoundly important part of system reliability—indeed it could be argued that, in the limit, all reliability problems are to do with human error. If a piece of equipment fails to operate properly, then possible human causes include:

- The item was not properly specified by the design engineer.
- The maintenance supervisor did not organize an effective inspection program.
- A designer may have calculated loads and stresses incorrectly.
- Management failed to implement a preventive maintenance program.
- The operator may have failed to follow instructions.

Human reliability analysis (HRA) is used to determine the probability that a task or activity will be completed successfully within a required time period, and that no other human action that could be detrimental to system performance will take place. An HRA analysis can also help identify areas where potential improvements can be made. A description of the topic is provided by the International Maritime Organization (2002).

Errors can be of either commission or omission. Errors of commission typically involve failure to follow procedures, taking a shortcut or making an (incorrect) assumption about the validity of an instrument reading. Errors of omission often occur during the response phase of an incident. For example, an operator may fail to isolate a tank that has already started to overflow.

A potentially serious human error occurs when an operator or supervisor does not realize that he or she has exceeded a safe operating limit. Not realizing how far out of control the operations have become, he or she decides to fight the problem rather than shut down and bring the facility operations to a safe state.

TYPES OF HUMAN ERROR

There are many ways of classifying human error—some are described by Mostia (2003).

The following are discussed in this section:

- Errors of intent
- Mistakes
- Slips
- Fixation
- Error in an emergency
- Incorrect response.

Errors of intent

Errors of intent are a special type of error that occur when supervision or management knowingly decide to override the normal operating or safety procedures. They may either break a rule, such as deliberately not following a procedure, or violate the intent of a standard policy. For example, an operations supervisor may choose to ignore a lab result or an instrument reading, either because they do not believe it or because they are prepared to override the implications of that undesirable piece of information.

Mistakes

A mistake (sometimes referred to as a cognitive error) occurs when a person acts on an incorrect train of reasoning, often because he was not properly informed as to what to do or how to do it. A mistake can be defined as follows:

> A mistake is a human error that is a failure in diagnosis, decision-making, or planning.

Mistakes can be further divided into those that are "procedural" and those that are "creative." A procedural mistake occurs when, for example, there is a lack of clarity in the operating instructions, thus causing an operator to misinterpret them. A creative mistake occurs when a brand-new situation develops, often during an emergency, and the operator has to develop a response on the spot, often in a very short period of time.

Slips

A slip occurs when a person makes an error, even though that person knew what to do and how to carry out a task. It is defined here as:

> A slip is a human error resulting from failure to carry out an intention, even though the person concerned had the capability, time, and equipment to successfully carry out that intention.

Slips usually occur during normal, routine, nonstress situations. For example, an operator may routinely take two samples from a certain section of the plant every shift, and he may have successfully performed this action hundreds of times. Then, on one occasion, he *slips* up and inadvertently switches the samples. Mistakes imply thinking; slips imply routine.

Worker fatigue is a common reason for the occurrence of slips.

Fixation

Most people have trouble grasping and understanding complexity, so they tend to *fixate* on the one or two solutions that they believe can resolve problems—even if those solutions are not correct. Examples of fixation include:

A plant experiences operating problems over a period of days. Different shifts witness different aspects of the problem, and so come up with different causes and proposed solutions. The people on each shift tend to discount the opinions of the other shifts because "seeing is believing"; people place more credence on their own experience than on the unwitnessed experience of others.

During an emergency, an operator is typically swamped with a large amount of information from the control panel; much of the information is confusing or apparently self-contradictory, particularly if one or two instruments are in error. In such situations, most people tend to fixate on one or two instrument readings, and then exclude all other information, regardless of its relevance. (Fixation was an important part of the Three Mile Island nuclear power plant incident, where operations personnel chose to believe a faulty instrument, even though many other instruments were indicating that the signal from the first instrument was incorrect.)

Error in an emergency

A rule of thumb is that human error rates rise to 50% during an emergency, i.e., there is a one in two chance that a person will do the wrong thing during the high stress conditions of a plant emergency. Therefore, if an operator is called upon to perform, say, six tasks during an emergency, the chance of getting them all right is 0.56, which is 1.6%—in other words, he will almost certainly fail to implement the full sequence of tasks correctly. Consequently, operators should not be expected to control a facility during an emergency. At most they should carry out a few automatic actions in which they have been thoroughly trained, and then turn over control of the plant to the instrumentation and to the trained emergency response team.

Incorrect response

The last type of error occurs when the front-line operator fails to recognize that the situation is out of control and does not respond, or else he or she fails to take the correct action.

Although this type of error is indeed an error, it is important to recognize that the person who failed to stop the chain of events is probably not the person who initiated or propagated that chain of events. He or she was merely "the last man on the bus."

HUMAN RELIABILITY ANALYSIS

An HRA usually consists of the following stages:

- Identification of key tasks
- Task analysis of key tasks
- Human error identification
- Human error analysis
- Human reliability quantification—often using THERP (Technique for Human Error Rate Prediction), as discussed below.

THERP

One method for analyzing human reliability is a straightforward extension of probabilistic risk assessment (PRA)—in the same way that equipment can fail, so can a human make mistakes and slips. One technique for predicting human error rates is the THERP, which was developed in the 1950s. As with other PRA techniques, THERP models can use either point.

A THERP analysis considers different types of error, such as not following an instruction, choosing a wrong switch or skipping a step in a sequence of activities, and forecasts the error rate for each of these tasks. If a person can make more than one type of error when carrying out a task, then the probabilities are added to one another. For example, when opening a valve an operator may:

- Open the wrong valve
- Skip the step altogether
- Open it only part way.

If the respective probabilities for these errors are 0.01, 0.03, and 0.03, then the overall error rate is 0.07 (excluding second-order terms). It is also possible to factor in recovery rates. For example, if the wrong valve is selected, then there may be a 40% probability that the operator will recognize and correct the error while there is still time, thus reducing the overall probability of error to 0.6×0.01 or 0.006.

A THERP analysis is most effective when the tasks are routine and when there is little stress.

CHAPTER

MANAGING A RISK PROGRAM 17

CHAPTER OUTLINE

INTRODUCTION

This chapter discusses the development and ongoing management of risk, reliability, and process safety management programs in the process industries.

- Clients and customers
- Program organization
- Risk management on projects.

CLIENTS/CUSTOMERS

Everyone who manages a risk program has customers or clients. Even those working in large corporations or government departments supply services and products to others, with their customers being other departments and managers within the organization. With regard to process risk and reliability programs, potential clients and customers are discussed in brief in the following sections.

SENIOR MANAGEMENT

Senior managers are concerned primarily with long-term issues. With respect to risk, they are particularly sensitive to the potential for major environmental and safety events such as the *Exxon Valdez* spill, the refinery explosion at Texas City, or the Deepwater Horizon/Macondo catastrophe.

Process Risk and Reliability Management. DOI: http://dx.doi.org/10.1016/B978-0-12-801653-4.00017-5

Such events lead to loss of life, major environmental problems, huge economic losses, very bad public relations, civil litigation, and even criminal prosecution. Senior managers do not want to be in that place—they look to the risk management program to keep them from going there.

FACILITY MANAGERS

In operating facilities, the immediate client for a risk and reliability program will be the facility or plant manager, supported by his or her operations, maintenance, and technical managers. Generally, they are less focused on big picture events than their bosses, but they do want to avoid recordable injuries and environmental citations. They are also interested in boosting profits through the use of operability and reliability programs. Moreover, they understand that a smoothly running facility will make them look good in the eyes of their superiors.

PROJECT MANAGERS AND DESIGN ENGINEERS

If a facility is still in the design or construction stage, the immediate clients for the risk management program will be the project managers and design engineers on both the client and the contractor side. These clients have two principal interests with regard to risk. First, they need to ensure safety on the project itself, particularly during the fabrication and construction phases. Second, they want to be sure that the facility that will operate safely and that it will meet its environmental and operating goals once it has been turned over to operations.

REGULATORS/AUDITORS

Modern industrial facilities are required to meet a plethora of regulations, rules, codes, and standards. Therefore, the risk management program should be organized so that its findings and results can be readily evaluated and audited by outsiders, particularly government regulators.

PROGRAM ORGANIZATION

Risk and reliability programs are organized like any other management program using a structure such as the following:

1. Determine the objectives of the program
2. Set up an organization
3. Create the metrics and baseline
4. Develop a plan
5. Implement the plan
6. Audit and improve

These steps are discussed below.

STEP 1—DETERMINE THE OBJECTIVES

Management must define the objectives that are to be met by the risk management program. These objectives must be measurable, and they should be understood and accepted by everyone working at the site or on the project. The objectives should be as concrete and specific as possible and the level of details associated with them should be tightly defined.

If a risk or reliability program is being developed from scratch, the program will typically have three phases or cycles, each with its own set of objectives. The focus of the first phase is to ensure compliance with regulations and corporate standards. During this phase, it is important to make sure that all the management elements (as described in Chapter 2) have been thoroughly implemented, that all aspects of the regulations have been addressed and that the regulatory documentation is complete.

The second phase of the program will be more concerned with achieving quantified improvements in the facility's safety and environmental results. This phase is likely to emphasize elements such as Incident Investigation and Process Hazards Analysis in order to identify weak spots in the management systems.

The third phase of the program is more concerned with the economic benefits to be obtained from implementing risk management techniques.

STEP 2—SET UP AN ORGANIZATION

The next step in the development of a risk management program is to set up an organization. This is often done through use of a steering committee, subcommittees, and a risk/process safety management (PSM) coordinator, as shown in Figure 17.1.

Management

At the top of Figure 17.1 are corporate and facility management. They are the customers or clients of the risk management program. They will also set the standards and philosophies that are to be followed in all of the risk and PSM work.

Steering committee

The steering committee provides overall direction to the risk management and PSM programs. The committee should be chaired by the facility manager and is responsible for the overall implementation of risk management at the site. Typically, the steering committee will be composed of the following persons:

- Facility manager
- Operations or manufacturing manager
- Maintenance manager
- Engineering/technical manager
- The risk management coordinator
- Safety supervisor or Health, Safety and Environment (HSE) advisor

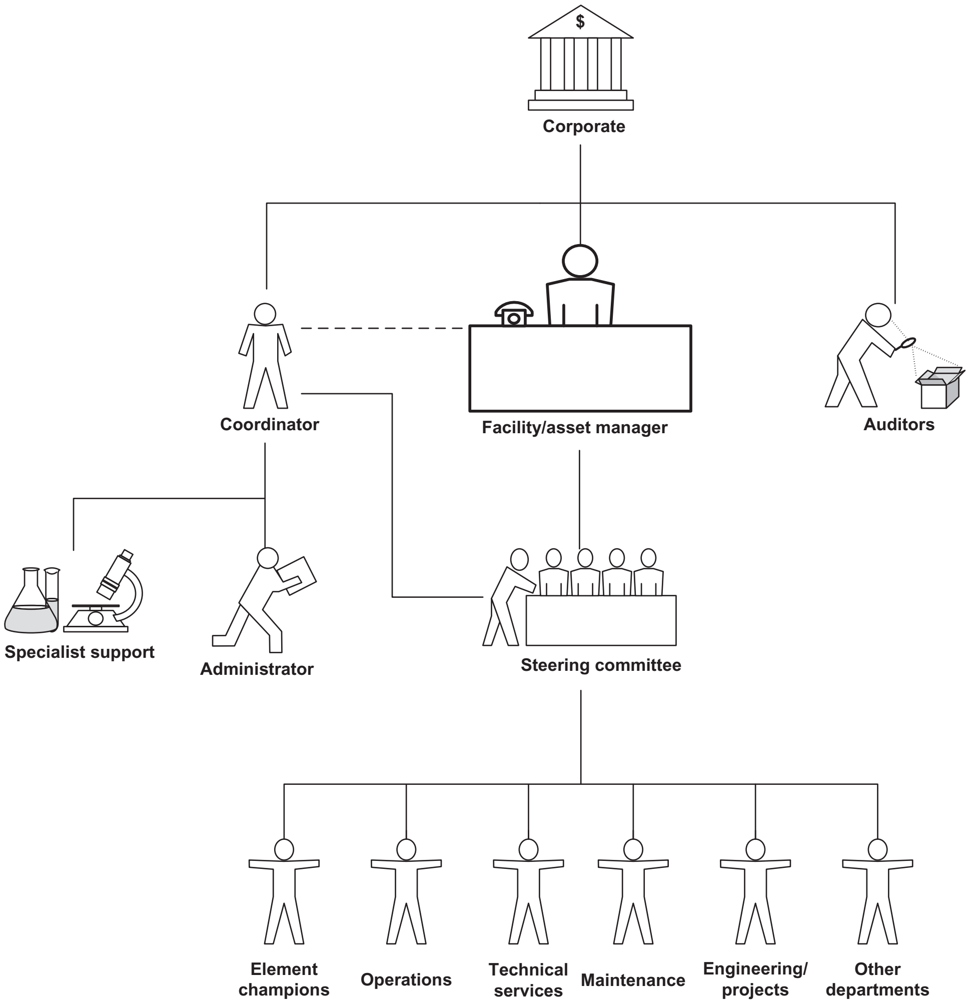


FIGURE 17.1

Representative organization.

Coordinator

The risk management coordinator runs the risk management program on a day-to-day basis. He or she assists the subcommittees and reports to management on overall progress. Responsibilities for this person include:

- Finding the right people to lead and conduct the work. The biggest challenge here is that the people who know the most and who can make the biggest contribution are typically very busy elsewhere, and in demand by many other people.

- Training participants in the elements of risk management. For example, if operators are to be rotated through the process hazards analyses, they need to be trained in the basics of this technique in order for them to participate fully. The coordinator will usually be the person to organize this effort.
- Tracking overall progress.

The coordinator is supported by an administrator who carries out tasks such as managing the risk register and scheduling training. Also supporting the coordinator are technical specialists who are called on as needed.

Subcommittees

Reporting to the steering committee are subcommittees, one for each of the major elements of the program. Each of these subcommittees will be responsible for the development of a detailed policy for their particular element of the standard within the overall company guidelines, and will also be responsible for ensuring that its element is properly implemented and maintained.

The chair of each of these subcommittees should, where feasible, remain the same person for as long as possible in order to provide continuity. However, the committee membership can constantly rotate, thus giving different people a chance to work on the different elements of the risk management program. Each subcommittee should include at least one employee representative in order to address the Employee Participation element of the PSM regulation or other legal and labor requirements.

Some of these subcommittees, for example, those to do with process hazards analysis and with asset integrity, will be very active for most of the time and will need substantial resources. Others, such as the Operational Readiness Review committee, may not have much to do except at turnarounds.

Responsibility for the management and control of each of the elements will lie with the pertinent departmental managers. For example, operating procedures will be written and updated by the operations department, engineering information will be controlled by the engineering manager, and the asset integrity element will be under the direction of the maintenance manager. These managers decide on how the program is to be implemented in detail, how training is to be conducted, and how progress is to be measured. They will usually chair the pertinent subcommittees.

An example of some of the detailed subcommittee requirements is provided in Table 17.1 for the topic of training.

Operating binders

One way of physically organizing the risk management program is to set up a library of 16 binders (either electronic or on paper): one for each element. These binders will contain information associated with that element and will each comprise a section of a master binder. They will also contain indexing information that tells the user where other information can be found. As far as possible, the binders and their contents should look the same as one another and should have similar Tables of Contents, following a layout such as shown in Figure 17.2.

Table 17.1 Organizational Responsibility for Training

	Method of Implementation	Location of Records	Responsibility
Initial Training			
Required before operating a process except for "grandfathering" those already involved in operating a process	Mix of classroom and field observation	Training Department (Documentation requires employee ID, date, and means used to verify understanding.)	Training Department
Refresher Training			
Refresher training required at least every 3 years, but the actual frequency is determined by the employee and his or her manager	Classroom and field training	Training Department	Operations and Maintenance Departments
Emergency Response and Troubleshooting Training			
All operations personnel should have at least 4 hours a year of training in Abnormal Situation Management	Emulators and Simulators	Training Department	Operations Department

- Introduction
- Objectives of the program
- Regulations
- Industry standards
- Company standards
- Protocols
- Employee participation
- Process safety information
- Administration
- Equipment items covered
- Personnel
- Use of outside companies
- Project management
- Phases of the program
- Budget
- Schedule

FIGURE 17.2

Representative table of contents for a risk management binder.

All the binders should be complete at all times. Initially, there will be very little detail in them, but they should nevertheless have a section for each part of each element of the standard. When printed, the binders should also be physically attractive and neatly organized in order to make them easy to use, and in order for them to make a good impression if the program is audited.

STEP 3—CREATE THE METRICS AND BASELINE

In order to measure progress, a system of metrics for each element is needed—there must be some way in which management can assess progress in numerical terms. In other words, instead of saying, for example, that the writing of the operating procedures is "progressing well," management really needs to be provided with a statement such as "The operating procedures are 63% complete." (The use of assessment spreadsheets, as described in Chapter 14, can be very helpful in setting up the baseline and then measuring progress.)

Figure 17.3 shows how progress on the overall risk management system can be measured. It uses the elements of PSM listed in Chapter 1.

The first column in Figure 17.3 lists the elements of the PSM program. The second column shows the man-days that it is estimated will be required for completing each element. In the case of training, the estimate is for 1260 man-days. The third column shows the number of man-days of effort that have actually been expended. For training, this value is 525. The fourth column shows the percentage completion for each element, with training being at 42%. The fifth column is the normalized fraction, i.e., it is the percentage completion weighted for the contribution that each element makes. Therefore, although Incident Investigation is 100% complete, it contributes only 0.2% to the overall total.

Figure 17.4 shows the metrics for the training element in greater detail. The facility has been divided into five operating units and a utilities area. The progress for each is shown.

A practical problem with some risk management programs is that a substantial amount of time and money is spent on them, but—particularly in the initial phases—there is very little to show for all the work that is being done. (This is particularly true if a top-down approach is followed.) Also, it is not always clear if the final product will meet the facility's requirements. For this reason, it often

	Required	Used	Fraction complete	Normalized fraction
1. Employee participation	23	11	48%	0.8%
2. Process safety information	460	96	21%	15.1%
3. Process hazards analysis	358	72	20%	11.8%
4. Operating procedures	576	114	20%	19.0%
5. Training	1,260	525	42%	41.5%
6. Contractors	40	6	15%	1.3%
7. Prestartup safety review	20	5	25%	0.7%
8. Mechanical integrity	80	29	36%	2.6%
9. Hot work permits	20	5	25%	0.7%
10. Management of change	130	20	15%	4.3%
11. Emergency planning	41	38	93%	1.3%
12. Incident investigation	5	5	100%	0.2%
13. Audits	20	0	0%	0.7%
14. Trade secrets	5	5	100%	0.2%
Total	**3,038**	**931**	**31%**	

FIGURE 17.3

Metrics (man-days).

	Number of operators	Days/ operator	Days required	Days completed	Fraction complete
Basic					
Utilities	20	2	40	20	50%
Unit 100	24	3	72	65	90%
Unit 200	24	3	72	11	15%
Unit 300	24	3	72	56	78%
Unit 400	24	3	72	60	83%
Unit 500	12	3	36	2	6%
Detailed					
Utilities	20	6	120	60	50%
Unit 100	24	6	144	80	56%
Unit 200	24	6	144	80	56%
Unit 300	24	6	144	80	56%
Unit 400	24	6	144	5	3%
Unit 500	12	6	72	5	7%
Certification					
Utilities	20	1	20	1	5%
Unit 100	24	1	24	0	0%
Unit 200	24	1	24	0	0%
Unit 300	24	1	24	0	0%
Unit 400	24	1	24	0	0%
Unit 500	12	1	12	0	0%
Total			**1,260**	**525**	**42%**

FIGURE 17.4

Training program progress.

makes sense to develop some pilot projects at an early stage. A few final products for each element are prepared, and then circulated for comment. This gives everyone a chance to make suggestions.

Some elements of the standard, such as operating procedures and mechanical integrity, lend themselves well to pilot projects. Other elements, such as employee participation and operational readiness reviews, are less amenable to this approach.

STEP 4—DEVELOP A PLAN

The material in this section should be read in conjunction with Chapter 18.

Having developed an organization and a plan, the first step in implementing a risk management program—at least on a reasonably large facility—is to develop a guide which will provide assistance as to its practical implementation at that site. Issues that could be included in such a guide are as follows:

- Define the goals
- Estimate the resources needed
- Develop a schedule
- Determine signature authority

If a company has more than one facility it can develop a set of procedures at the corporate level. These can be taken by the plants and modified so as to reflect their particular needs and circumstances.

Goals

If the goals of the program are not properly defined, then the problem of scope creep may occur. As any project progresses, it is tempting to modify the goals to reflect new ideas and to address problems that had not been considered, thus increasing the scope of work. This is a particularly serious problem with regard to process safety because there is always the feeling that any new safety problem has to be addressed and incorporated into the program—not to do so would appear to be irresponsible. Yet every additional activity will lengthen the overall time needed for completion and will increase costs.

Resources needed

The principal resources required by a risk management program are money to fund activities such as external audits and equipment inspections, and the time of key personnel to participate in activities such as hazards analyses and the writing of operating procedures. The second of these is often the most critical because the key people are busy with many other activities, including operations, maintenance, and other types of project work. Hence, the process safety schedule will often be developed around the availability of these people.

Develop a schedule

The nonprescriptive nature of process risk management means that it is difficult to develop schedules. This is one reason why it is particularly important to dividing the work into manageable subprojects, otherwise the task will seem overwhelming. Each phase of the project (and each element within each phase) should be scheduled using normal project management techniques.

A Responsible, Accountable, Consult and Inform (RACI) chart, an example of which is provided in Figure 17.5, outlines the roles of different persons on different parts of a project.

The letters in Figure 17.5 are explained below.

Accountable	A	Person ultimately responsible for the results
Responsible	R	Expected to actively participate in the activity and provide contributions
Consult	C	Persons having expertise that they can contribute
Inform	I	People who are affected by the activity, but do not participate in it

	Activity 1	Activity 2	Activity 3	. . .
Person A	A	A	C	
Person B	R	R	A	
Person C	C	—	—	
Person D	I	I	C	

FIGURE 17.5

Sample RACI chart.

Reviews and signatures

Many parts of a risk management program will call for internal and external reviews. Although reviews are necessary, there is a danger that they could become very drawn out—thus slowing down the whole program. There are two ways of addressing this problem. First, the scope of work should be defined as closely as possible. For example, the level of detail required in the operating procedures should be clarified at the beginning of the project, possibly based on the results of a pilot project.

It should be made clear to the reviewers that they are allowed only one review of the relevant document, and that their review should be completed within a certain time frame. If their comments are received late, then they will be ignored. Moreover, once they have submitted their review, further input is not allowed, except to make sure that their first comments were properly understood and incorporated in the final document. (There should always be an opportunity for people to correct factual errors, regardless of when those errors are found.)

Once the review cycle is complete, the relevant documents need to be signed before they are issued. The signing process can also turn out to be a bottleneck, generally for one of two reasons. First, it sometimes is found that too many people are asked to sign the document. Therefore, it takes a long time for that document to wend its way through the system. Second, the people who know the unit well, and whose signature is therefore of the highest importance, are also the people who are likely to have the most to do with other projects, or who are busy with day-to-day operations. It can be difficult for them to make sufficient time available to review the procedures and documents with the care and thoroughness that is required.

One way to resolve these problems is to clarify what a person's signature means, and why it is needed. In practice, there are usually just three levels of signature authority that really matter.

The first signature is from the person(s) who actually prepared the document that is being reviewed. Their signature states that the document is accurate, complete, and useable, within the extent of their capabilities.

The second signature is that of a reviewer who knows the process being described extremely well indeed. This person will often be a supervisor or senior operator. Their signature states that, to the best of their knowledge, the written procedure or document is accurate.

The third signature is that of a manager. It is unlikely that he or she will know the process well enough to comment on the technical content. What his or her signature states is that management systems for preparing and writing documents are in place, that the document being signed addresses all appropriate regulations and standards, and that these systems were followed during the execution of this assignment.

STEP 5—IMPLEMENT THE PLAN

The order in which the elements (Tables 1.1 and 1.2) will be implemented will depend on the circumstances at each facility. However, the two items that should be in place at the very beginning of the project are piping & instrument diagrams (P&IDs) and Management of Change (MOC). Accurate and up-to-date P&IDs are important because so many other aspects of risk management are based on them. They are needed for PHAs, Mechanical Integrity, Operating Procedures, and Prestartup Safety Reviews. MOC is equally important because change is constant. Therefore, as soon as one element is complete, something else will change, possibly affecting the item that was just completed. This means that the MOC process must be up and running very early on.

STEP 6—AUDIT/IMPROVE

All parties should be regularly informed as to how much progress is being made in each of the elements. The feedback should measure actual performance against the objectives.

Once a cycle of the risk management program has been completed, the next cycle should be started, using the work that has already been done as a basis. This provides an opportunity to move from strictly regulatory and safety issues toward broader topics, such as increased plant reliability and improved product quality.

CHAPTER

18 PROJECT MANAGEMENT

CHAPTER OUTLINE

INTRODUCTION

Many of the activities that have been discussed in the previous chapters are carried out as part of a project. Therefore, it is useful to review some of the basics of project management in the process industries—particularly the Phase/Gate system.

PHASE/GATE SYSTEM

Projects in the process industries are commonly divided into phases or stages such as those shown in Figure 18.1.

At the conclusion of each phase, the project management team will select one of four options:

1. Proceed to the next stage (the project is a "go")
2. Recycle the current stage (usually because insufficient information is available to make an informed decision, or because project requirements/conditions have changed)
3. Put the project on hold
4. Stop the project

Process Risk and Reliability Management. DOI: http://dx.doi.org/10.1016/B978-0-12-801653-4.00018-7

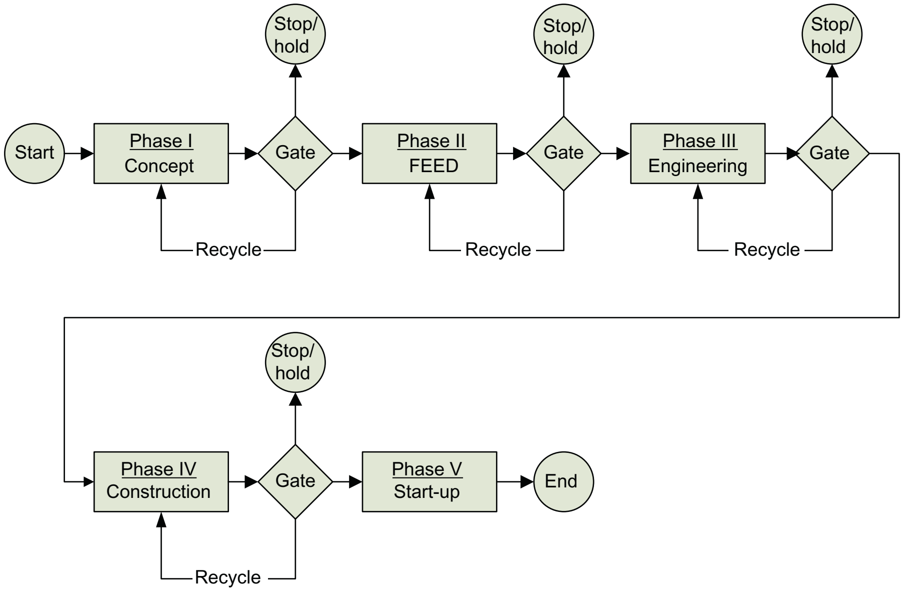


FIGURE 18.1

Project phases.

Factors that affect the phase/gate decision include the following:

- The commercial/business case for the project given the information available at that point
- Selection of the best technical options
- The need for contingency plans
- The safety and environmental risks associated with the project

The levels of funding corresponding to the phases in Figure 18.1 are shown in Figure 18.2—sometimes referred to as an “S”-curve.

Figure 18.2 shows that a decision to stop a project during Phase I or II does not have a major cost impact. However, as the project moves into Phases III and IV, management will be much more reluctant to stop it or to make major changes due to the financial commitment that has already been made.

HAZARDS ANALYSIS ON PROJECTS

When a new process is being designed and constructed, it is normal for hazards analyses to be performed at each stage of the design. The method selected will differ for each stage, reflecting the increasing amount of engineering data that is available.

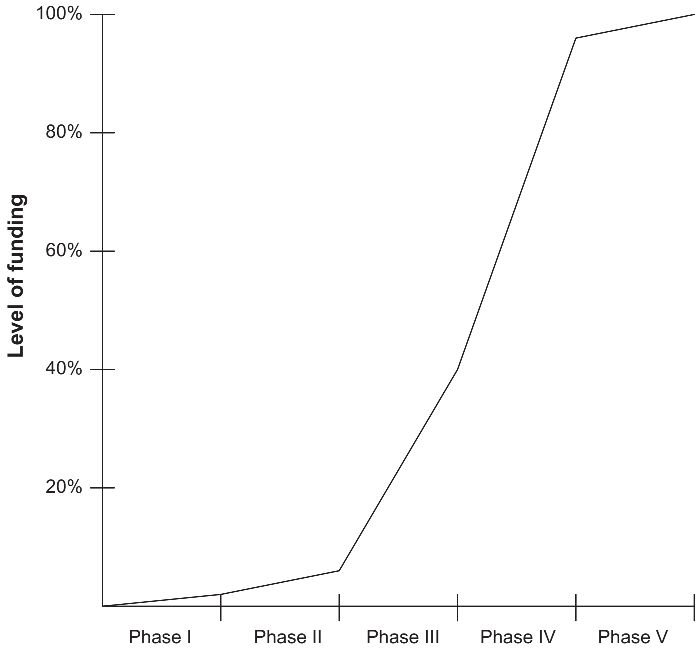


FIGURE 18.2

Levels of funding.

A hazards analysis for a facility that is in the design stage differs from a hazards analysis for a plant that is already operating in five important ways:

1. No direct operating experience is available, particularly when the basic technology is new. However, if the facility being designed and built is similar to others already in service, then the hazards analysis team should be able to find operations and maintenance personnel for other, similar plants who can provide the requisite knowledge and working experience.
2. When the facility is in the design stage, it is quite easy to make sweeping changes such as adding or removing equipment items. However, once a facility is built, even quite small changes can be very expensive, and their implementation can lead to substantial downtime and lost production.
3. Because the facility is not yet operating, the leader of the hazards analysis team is less likely to run into problems with "thinking the unthinkable."
4. In general, newer facilities will have more complex and sophisticated control schemes.
5. If the process being built uses brand new technology, then the team will probably have to delve into basic chemistry and design intent more thoroughly than is normal.

Figure 18.3 identifies some of the hazards analysis methods that are used at different stages of the project.

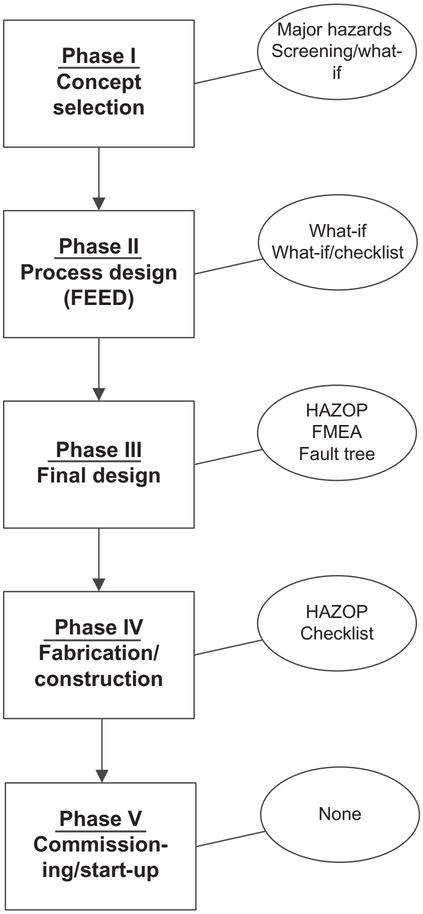


FIGURE 18.3

Sequence of hazards analysis methods.

PHASE I—CONCEPT SELECTION

The first phase of a project is usually to develop the scope for the proposed project, and then to evaluate its business justification. During this phase, senior management addresses major issues such as the technology to be used, the location of the facility, whether a brand new plant is to be built or an existing one extended, size, capacity, and environmental permitting. At the conclusion of Phase I, the management commonly decides that the project is not justified, so further work is stopped. If the project does move forward, Phase I is definitely the best time to make changes to the process because all such changes are on paper at this stage; no equipment has been purchased.

Phase I work should include a review of process safety management (PSM) issues, particularly when alternative technologies are being evaluated. Regulatory compliance and public acceptance issues at this phase often lead to the project being terminated.

Environmental issues that often come up during Phase I include the following:

- Hydrocarbon and chemical gas emissions
- Greenhouse gas emissions
- Waste management
- Groundwater protection

Technical issues can also be crucial during Phase I. For example, one company wanted to build a chemical plant based on a technology that used a highly toxic gas. Vapor dispersion analyses showed that, were the gas to be accidentally released, it had the potential to harm not only the workers at the site but also those living in the local community. At that time, no instrument manufacturer had developed a reliable sensor for this particular gas so there was no assurance that a leak would be detected in its early stages. Therefore, the operating company elected not to go forward with the project, even though the economics were very attractive. Some years later, when reliable detector technology was developed the project was given a green light to move forward.

If the project does receive approval to move into Phase II, the following parameters and issues need to be defined:

- Values and vision for the project (including the operational integrity vision)
- Project goals (principally financial)
- A resource-loaded schedule, including resource constraints
- Other constraints such as financial, political, regulatory, and logistics
- Start and end dates for the project

By the end of Phase I, the project will typically have spent <1%–2% of the overall funding; cost estimates are likely to be ±40% quality. Typically, no engineering deliverables will have been prepared up to this point, with the possible exception of a process block diagram.

DOCUMENTS

Documents that will be created by the end of Phase I include process block diagrams and preliminary process flow diagrams (PFDs), and layout diagrams.

HAZARDS ANALYSIS

During Phase I, the project team will conduct high-level hazards analyses, probably using some form of Major Hazards Screening. The team will be looking for “killer” problems that are so serious that the project will have to be canceled. The analysis will not consider details on design or the occupational safety and human factors issues discussed in the previous chapters.

PHASE II—PRELIMINARY DESIGN (FEED)

If the project does move forward into Phase II, then preliminary design work (sometimes referred to as front-end engineering design or FEED) is carried out. Also during this phase, any major technical or business issues that were not resolved during Phase I will need to be identified and resolved as soon as possible. Additionally, many of the topics discussed in earlier chapters of this book will be resolved during Phase II. For example, decisions regarding equipment sparing, fire and explosion control, and equipment layout will be made at this time.

By the end of Phase II, the project will typically have spent about 5% of the overall funding; cost estimates are likely to be ±20% quality.

DOCUMENTS

Documents that come out of Phase II include:

- Final PFDs
- Design quality P&IDs (Piping & Instrument Diagrams)
- Equipment data sheets
- Equipment layout diagrams
- Cause-and-effect charts
- Project philosophy documents

The final item in the above list is project philosophy documents. The purpose of a philosophy is to establish the preferences of the company, facility, or project on the selected topic, giving consideration to capital cost, operating costs, safety, environmental compliance, and health issues. Each philosophy should be written as part of a family of philosophies that are integrated with one another, and that are consistent with one another.

Philosophies provide high-level guidance; they do not provide detailed instructions as to what has to done or as to what resources are needed. (Some of these documents may be issued at the conclusion of Phase I.) For these reasons, philosophies are usually quite short. In general, they should not run to more than three or four pages (although the reference section could be considerably longer).

In general, a philosophy should not be quantitative. For example, a philosophy to do with the detection of toxic gas releases may state that automatic detection equipment is needed. However, the philosophy will not prescribe the value for the threshold concentration of gas that will trigger an alarm—that type of detail will be provided in the corresponding specification or standards document that will be written later on in the project.

All of the philosophies on a project should have the same overall structure and style (in other words, a "Philosophy for Writing Philosophies" is required). A representative Table of Contents for the philosophies on a project is provided in Table 18.1.

The *Introduction* section describes why the philosophy is needed. In the case of the toxic gas release, e.g., the purpose may be defined as follows:

> The purpose of this philosophy is to ensure that no persons present in the covered facility shall experience health problems due to the release of (name of the gas).

Table 18.1 Table of Contents for a Project Philosophy

Introduction
Scope
Definitions
Requirements
  Element 1
  Element 2
  Element 3. . .
References
  Regulations
  Industry Standards and Codes
  Internal Standards
  Other Philosophies, Specifications, and Procedures

The *Scope* section defines issues such as what equipment is covered, which personnel are included, and at which locations the philosophy applies. The following boilerplate material is often included in the *Scope* section.

> Any exceptions to the requirements of this philosophy or conflicts between this philosophy and other project documents shall be submitted in writing for resolution.

The *Definitions* section provides a clear description and meaning for terms such as "hazard," "code," and "emergency."

The *Requirements* section describes other resources that are needed in order to implement the philosophy. For example, if the Philosophy is to do with toxic gases, then the requirement may include MSDSs (Material Safety Data Sheets) for the chemicals under consideration.

The *References* section lists other documents that are pertinent to the development and use of the current philosophy. This includes links to other philosophies, specifications, and procedures. For example, the philosophy to do with emergency evacuation will link to the philosophy for fire fighting.

HAZARDS ANALYSIS

The hazards analysis that was conducted during Phase I will be developed in greater detail during Phase II. The available documentation will generally be limited to block flow diagrams, preliminary PFDs, and material flow diagrams (which also provide information on materials of construction). The What-If method works well at this stage because it is not too late to make major changes in the process design. The What-If/Checklist method is also a good choice at this stage. The What-If approach encourages broad-range thinking, while the Checklist questions provide a framework on which to base the analysis. Because there is no detailed engineering information methods such as Hazard and Operability (HAZOP) that require completed P&IDs are not suitable at this stage.

The hazards analysis at this stage of the project may also provide information for an insurance evaluation, and for a preliminary analysis of the emergency relief and shutdown systems.

PHASE III—DETAILED ENGINEERING

If the project clears the Phase II gate and moves forward into Phase III management or the client will generally issue a "Request for Proposal (RFP)" or "Request for Quotation (RFQ)" for the detailed engineering associated with Phase III work. It is during this phase that the detailed design is finalized; this is literally the nuts and bolts phase of the project. The detailed engineering step requires a large commitment of time and money. At its conclusion, the design team will have issued detailed documents such as P&IDs, Instrument Loop Diagrams, Layout Drawings, and MSDS.

By the end of Phase III, the project will typically have spent about 10% of the overall funding; with cost estimates likely to be in the ±10% range. It is at this point that senior management makes the major economic commitment to sanction the project.

DOCUMENTS

Documents that come out of Phase III work include:

- Final P&IDs
- Detail instrument and electrical schematics
- Structural drawings
- Civil and foundation drawings

HAZARDS ANALYSIS

The final Process Hazards Analyses—usually HAZOPs—will be carried out at this time. Also, human factors issues such as equipment layout, access to equipment, and the use of signs will be identified and resolved during Phase III.

These analyses are time-consuming because they go into so much detail, so they need to be carefully planned and sufficient time and funds allocated to their application. It is very important for the team leaders to resist attempts to redesign the facility, i.e., to make changes that should have been completed during the previous phases of the project.

If a quantified method such as LOPA or Fault Tree Analysis is to be used then it will be carried out during Phase III in order to risk rank identified hazards.

PHASE IV—FABRICATION AND CONSTRUCTION

Figure 18.2 shows that project expenditures during Phase III rise from about 5% of the total cost to the 30%−40% range. However, it is when the project enters Phase IV that the organization becomes fully committed financially to the execution of the project. It is during Phase IV that large equipment items are fabricated and the facility is constructed and installed. By the conclusion of Phase IV, the facility will be mechanically complete and about 90% of the funding will have been committed.

During this phase, the safety focus will be on the extensive construction activity that is taking place. There will also be increased activity to do with "soft" topics such as writing operating procedures and training the operators and maintenance workers.

PRECOMMISSIONING

Toward the end of Phase IV, precommissioning activities will start. There is considerable overlap between precommissioning and commissioning (discussed in Phase V). Indeed, some organizations choose not to make a distinction between the two activities. Some organizations refer to precommissioning as static commissioning—it is concerned primarily with ensuring that individual equipment items and the associated piping are properly installed and are functional. Full commissioning is then referred to as dynamic commissioning and focuses on the functionality of the equipment and instruments systems.

During precommissioning activities the following are performed:

- Hydrotest vessels and piping to their test pressure
- Check pumps and other rotating equipment for basic operational issues such as that they are rotating in the correct direction
- Check the operation of valves
- Check electrical and instrumentation systems
- Start on tasks that can take a long time to complete such as drying out refractory or loading catalyst
- Punch out all physical equipment, including piping and valves. Both the contractor and the client may have their own punch lists, operating in parallel with one another
- Verify control loops and instrument lines
- Clean out equipment and lines using steam and water
- Verify that all the documentation to do with the operation and maintenance of equipment is in place
- Function test individual components or subsystems, including instrument loop checks, cause-and-effect testing, panel function test, switchgear function tests, energizing electrical equipment, equipment alignment validation and recheck, flushing of lube/seal oil systems, motor no-load running, and control system interface testing
- Implement lubrication schedules for rotating equipment
- Check that all utilities are available as needed

PUNCH LISTS

Both the operator and contractor should each prepare their own punch lists. Each punch list will contain a list of all the work that needs to be done for a component, subsystem, or system. When an item is confirmed to be complete, it is checked off (punched out).

Items that need to be closed out can be categorized as follows:

A. Items at this level must be closed out prior to Mechanical Completion and before commissioning starts. No equipment items or systems can be energized until all Level A deficiencies are resolved.

B. Level B items must be closed out before Commissioning is complete. However, all of these items must be corrected before the Operational Readiness Review (ORR) commences.

C. These can be taken care of after the system is handed over. However, it must be closed out before hydrocarbons are introduced into the system.

D. These are issues that operations would like to see installed but that is outside the project work scope, that does not affect safety and that is not critical to process operations. Level D items do not delay system turnover or facility start-up.

TRANSFER OF CARE, CUSTODY, AND CONTROL

At the conclusion of Phase IV, the facility will be handed over to the owner/operator through the use of Turnover Packages, as described later. This activity is sometimes referred to as Transfer of Care, Custody, and Control (TCCC). This is a very important time in the project because control of the facility now resides with the operator, not the contractor. This means that the operator's safety systems now become operative. Therefore, if the contractor wishes to change anything he or she has to work through the operator's Management of Change process.

On large projects, system packages are often transferred from the operator to the contractor in phases using Turnover Packages, as described later. TCCC is also important commercially because the operator will make a major payment to the contractor for the work that has been done. Hence, any problems that may arise from that point forward are no longer the responsibility of the contractor.

DOCUMENTS

During Phase IV, many documents are prepared by both the operator, the contractor, and the subcontractors. Two document sets are particularly important: Turnover Packages and Operating/ Maintenance Procedures.

Turnover packages

Turnover packages are used as a means of efficiently transferring "care, custody, and control" from the contractor to the operator. The transfer can either be by geographical section or by functional section (such as the steam condensate system). The latter is usually the better choice. So each package represents a discrete, self-contained section of the plant, such as the instrument air header or the boiler feed water system. The operator is responsible for all activities associated with that particular package. If either the operator or the contractor wishes to make changes to the system after it has been turned over then the normal facility safe work procedures have to be followed.

The use of turnover packages improves both efficiency and safety. Efficiency is improved because the process of turning over the system to operations can start quite early on, thus saving time. Safety is improved because there is a clear definition of boundaries, with a corresponding understanding of who is responsible for what. Whenever the operations department is about to assume responsibility for a turnover package, a prestartup safety review (PSSR) can be carried out on the contents of that package.

Turnover packages are used for new plants, and sometimes when extensive changes have been made to existing plants. Each package represents a discrete, self-contained section of the plant, such as the instrument air header or the boiler feed water system. When construction has finished all of its work on that system, it turns it over to operations. Once the operations group has accepted the package, they assume full responsibility for all the equipment contained within it. By dividing up a large facility this way, the operations department can start the testing and commissioning on the packages that have been turned over. It is not necessary to wait for the entire facility to be complete before commissioning can start.

When construction transfers custody of a turnover package to operations, they are saying that *everything* to do with that system is mechanically complete. This includes instruments, painting, insulation, and all civil and structural work. The system should also have been blown free of trash before being handed over. Turnover packages can be contractually important. By transferring "care, custody, and control" from construction to operations, the responsibility for fixing problems after that time no longer belongs to the construction team.

A turnover package is prepared using a master set of P&IDs. The turnover coordinator identifies each system and then defines it in detail, usually using a colored highlighter pen on the P&ID. Generally, each package will represent a single functional entity, such as a cooling water header or a reactor. If the turnover packages are prepared early enough, they can be identified on the P&ID itself as part of the general system of line and equipment markings.

The package should be defined up to individual flange faces, and should make it clear when ownership of a line that is shared by one or more departments changes hands.

An alternative method of turning over the plant is by geographical zone. The plant is divided into sections, and all the piping and items within each section are completed and handed over to the operations department. The drawback to the geographical method of turnover is that it does not take into account the fact that the process systems, particularly those to do with utilities, reach throughout the plant. Therefore, it may not be realistic to handover just part of say the cooling water system, say, because cooling water is often found all over the facility. The geographical approach does make the handover of civil and structural work simpler.

As construction nears completion for each turnover system, the following work process is commonly followed:

- All the items associated with each package are identified and listed, usually by function. So, e.g., instruments, insulation, and flange ratings will be listed separately. This work can be done when construction is say 80% complete. The construction personnel prepare a punch list for its own use, which it will use to check the work it is finishing. They will use this list to fix the problems that they have uncovered.
- As completion approaches 100%, the operations department prepares its own punch list for that package. When the construction team members state that they are ready to turn it over, the operations department will prepare its own punch list, which will be managed in parallel with the construction checking process.
- Normally, there will still be a few items left incomplete. Operations may decide (maybe during the PSSR review) that they can accept the plant in this condition because these missing items are not important to safety, and should not be allowed to slow down progress. They can be addressed once the plant is running.
- Once the outstanding items on the work list have been completed, the construction department will prepare a formal turnover letter. This letter is signed by both Construction and Operations

> to state that Custody, Care, and Control of that turnover package are now the responsibility of operations. Once this letter has been signed, construction can no longer work on anything defined within that turnover package without obtaining permission from operations because, from that moment in time, there can be no guarantee that the turned over equipment does not contain hazardous or flammable chemicals. Hence the acceptance of Care, Custody, and Control means that standard operating safety systems, such as lockout/tagout, will be in place and have to be followed by all parties, including the construction team.

The use of turnover packages improves the speed and efficiency of the handover process because they divide the facility into sections with clearly defined boundaries—the first completed sections can be handed over while construction and testing work on other sections is still in progress. It is not necessary to wait for the entire facility to be complete before commissioning can start.

When the project team transfers custody of a turnover package to operations, they are saying that *everything* to do with that system is mechanically and electrically complete, including instruments, painting, insulation, and all civil and structural work. The piping and vessels will have been blown free of trash.

There are two types of turnover package. The first is a functional system such as the steam condensate lines and control systems in a particular area. The second type of package is geographical. The plant is divided into sections, and all the piping, equipment items, and instruments within each section are completed and handed over to the operations department. The drawback to the geographical method is that it does not take into account the fact that the process systems, particularly those to do with utilities, reach throughout the plant. Therefore, it may not be realistic to handover just part of say the cooling water system. However, a geographical approach does make the handover of civil and structural work simpler.

A turnover package is prepared using a master set of P&IDs. All equipment, instruments, and piping are defined in detail, usually using a colored highlighter pen on the P&ID. If the functional approach is used, then each package should be defined up to individual flange faces. If the turnover packages are prepared early enough, they can be identified on the P&ID itself as part of the general system of line and equipment markings.

On large projects, it is common for the project team to prepare a punch list for each functional system at around the 80% completion stage, i.e., when the system is not mechanically complete. All the items associated with each package are identified and listed—usually by function. So, e.g., instruments, insulation, and flange ratings will be listed separately.

As completion approaches 100% for that package, the Operator will also prepare a punch list and turnover package, thus providing a double check on the contractor's work.

Immediately prior to turnover, there will still be a few noncritical items such as painting and personnel protection insulation left to be done. Operations may decide that they can accept the plant in this condition because these missing items are not important to safety, and should not be allowed to slow down progress. They can be addressed during the commissioning and start-up phases.

Once the facility's management agrees that a package is ready to be turned over, the construction company will prepare a formal turnover letter. The letter, which is signed by both the construction and operations teams, states that the turned over section is ready for operations and is now the responsibility of operations. Once this letter has been signed, construction can no longer work on anything defined within that turnover package without obtaining permission from operations because, from that moment in time, there can be no guarantee that the turned over equipment does not contain hazardous or flammable chemicals. Hence the acceptance of Care, Custody, and Control means that standard operating safety systems, such as lockout/tagout, will be in place and have to be followed by all parties, including the construction team.

Procedures

During Phase IV, the operating and maintenance procedures will be written, and the technicians trained in their use. Guidance as to the writing of procedures and the development of training programs is provided in *Process Risk and Reliability Management.*

HAZARDS ANALYSIS

There should be no need for a process hazards analysis during Phase IV—all design decisions should have been pretty much finalized. A final HAZOP study and/or checklist review may be needed to close any outstanding issues and to make sure that late changes have been properly analyzed.

It will, however, be necessary to conduct many constructability reviews and safety analyses. Any changes to the process itself will be handled by the Management of Change system.

PHASE V—COMMISSIONING AND START-UP

The next stage is to commission the facility. Basically, this means that facility is brought up to operational readiness, except that it is not actually processing feed, or making product. At the end of the commissioning phase, the facility is ready for start-up, as shown in Figure 18.4.

COMMISSIONING

Commissioning brings the facility to a ready-to-go state. However, no process fluids have been introduced (although some operations may have been carried out using water, steam, nitrogen, and plant air). Commissioning activities should be carried out by a multidiscipline team of engineers and operations/maintenance personnel. They should test systems, not just the individual items or control loops as was done in precommissioning. Some simulations may be required. For example, nitrogen may be used in place of actual process gases. Also, during commissioning, most utility and life support systems will be made fully operational.

At the conclusion of the commissioning step, Turnover Packages will have been prepared and handed over and all Level A and B punch list items will have been closed out.

OPERATIONAL READINESS REVIEW

Once the TCCC step has been completed, an ORR will be carried out. (It is also called a PSSR.) The purpose of this review, which is described in detail in *Process Risk and Reliability*

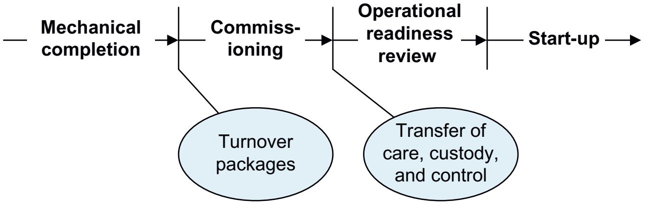

Mechanical completion
Commiss-ioning
Operational readiness review
Start-up
Turnover packages
Transfer of care, custody, and control

FIGURE 18.4

Commissioning and start-up phases.

Table 18.2 Start-Up Checklist

- Organization
- Levels of staffing as the construction and commissioning proceed
- Recruiting and personnel testing
- Training programs for the operators and maintenance technicians
- Administrative policies and procedures
- Maintenance facilities, tools, and equipment
- Operating supplies
- Spare parts and consumables
- Catalysts and chemicals
- Performance testing
- Laboratory services, particularly in the early phases of the actual start-up
- Supplementary personnel and support services

Management, is to ensure that the facility is safe to start and that the start-up step is likely to proceed smoothly. The ORR will generally be conducted by a team led by a senior representative from the Operations Department.

If the review does find significant problems, then the affected sections of the facility have to be handed back to the project team. When the deficiencies have been corrected, then handover to the operations department will take place a second time and the ORR repeated.

START-UP AND LINE OUT

Once the plant is commissioned and the ORR is complete and satisfactory, the formal start-up (sometimes called "oil in") begins. The distinction between commissioning and start-up is that start-up involves the introduction of fresh feed and the production of final product. Once the facility is started, the operation is lined out and design production rates of on-spec material is achieved.

Before committing to the start-up, it is useful to work through a list of topics such as those given in Table 18.2 in order to make sure that nothing was overlooked.

During this period, additional data is collected, including data associated with motor amperage draw, pump curve performance, interface control, and operational baseline parameters, such as noise, vibration, and performance specifications are initiated.

DOCUMENTS

Documents issued during Phase V include operating and maintenance procedures, the results of a formal acceptance test and warranties from the contractor and subcontractors.

Start-up procedures

Detailed information on the writing of operating procedures, including what needs to be done during a start-up, is provided in *Process Risk and Reliability Management.*

For a first-time start-up, it is likely that the normal operating procedures will not provide enough detail. Therefore, it would make sense to develop a block diagram or arrow diagram showing what activities occur when, and what predecessors must be complete before a particular activity can take place. Contingency procedures should be developed on the grounds that things are bound to go wrong. In particular, it is quite likely that critical equipment items will not perform to specification or that they will break down frequently.

Acceptance test

The final step in the start-up is the Acceptance Test. The facility is run for a period of say 48 hours and is carefully scrutinized during that time. Detailed records of all process parameters are collected and recorded. Production yields, utility consumption, and production rates are all checked against target values. If all is in order, the Operator signs an Acceptance Test document and the project is basically complete.

Acceptance also means that the Contractor has corrected all deficiencies that are his responsibility and he has furnished the Operator with all equipment, materials, and documents required under Contract.

Warranty

The Acceptance Test will come with a warranty from the Contractor. In it the Contractor will state that the facility, including equipment and materials furnished by subcontractors and vendors should be free from defects or failures for a period of say 1 year.

HAZARDS ANALYSIS

There should be no need for a detailed hazards analysis during Phase V.

PROJECT ORGANIZATION

Most projects have a client (operator) who will run the facility once it is complete and an Engineering, Procurement, and Construction (EPC) contractor who is responsible for the design of the facility, the procurement of equipment (mostly from vendors and subcontractors), and construction. Reporting to the contractor will be a wide range of subcontractors and vendors.

Representative organizations are shown in Figures 18.5 and 18.6.

Figure 18.6 shows that EPC will carry out all the technical, procurement, and construction activities up to the commission and start-up phases. Control of the project then passes to the operator.

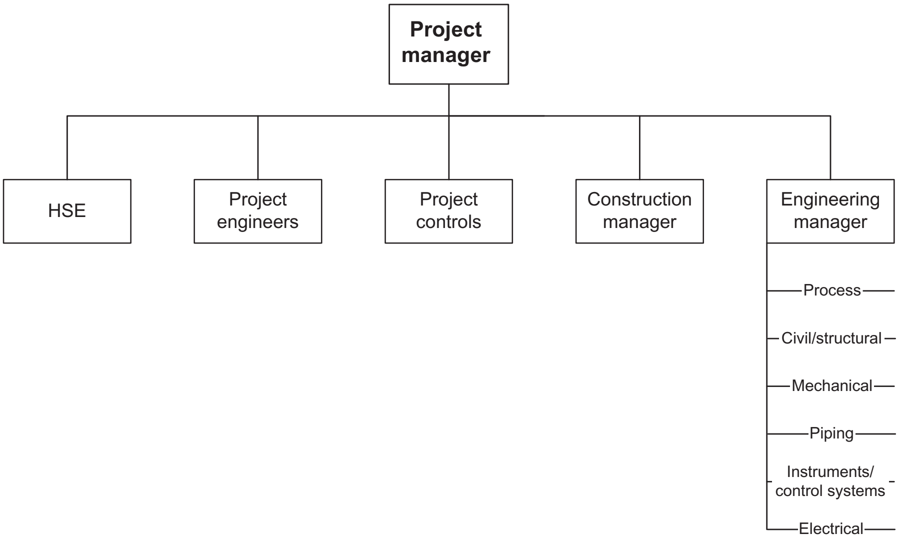


FIGURE 18.5

Representative project organization.

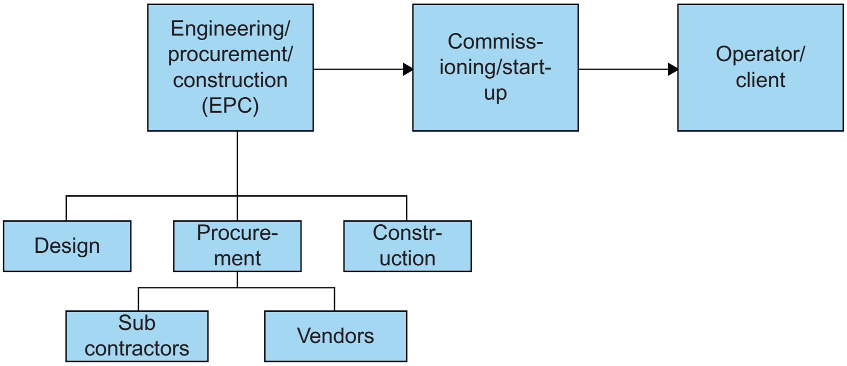


FIGURE 18.6

Contractor role.

CHAPTER

19 CONTRACTORS

CHAPTER OUTLINE

INTRODUCTION

Companies in the process industries use contractors at all levels, ranging from large companies that manage megaprojects all the way down to the single worker carrying out a simple task lasting just a few minutes. Frequently, contract workers carry out much of the work at a process facility, and they are often responsible for carrying out some of the most hazardous activities. Therefore, the management of the operator/contractor interface is very important, but it is also difficult.

The increasingly important role of contractors for offshore work is illustrated in the following chart (OGP, 2013).

Figure 19.1 shows that the number of hours worked by the owner/operator has not changed much in the last 30 years, but that the contractor work hours have increased by a factor of 15. (The chart also illustrates the costs and challenges associated with moving from simple, shall-water platforms, many of which are unmanned, to deepwater drilling and production projects.) It should also be noted that more and more of the operators' workers are themselves under contract rather than being true employees.

Companies that strive for excellent safety performance aim to treat contract workers—particularly long-term contractors—as if they are full members of the organization. However, there can be no denying that there *are* differences between permanent workers and those on contract. These differences include the following:

- Contract workers will not generally know and understand the culture of the host company. They will not know the unwritten rules and "the way things are around here."

Process Risk and Reliability Management. DOI: http://dx.doi.org/10.1016/B978-0-12-801653-4.00019-9

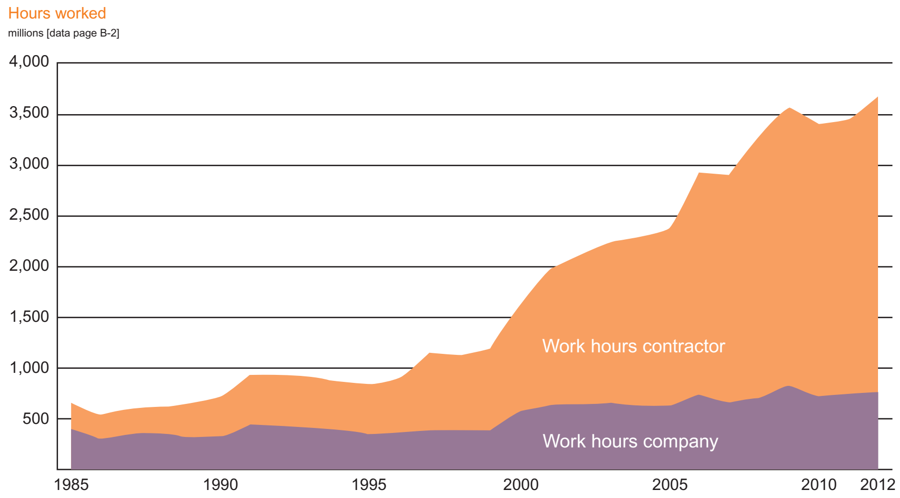


FIGURE 19.1

Increasing use of contractors.

- A contract company will often have its own procedures and systems. These may not always align with the procedures and systems of the operating company that hired them.
- Considerable effort has to be spent ensuring that each contract worker has been properly trained and is in compliance with a myriad of rules and regulations.
- Contract workers—even those on long-term assignment—are not an integral part of the facility on which they are working. Therefore, their standards and values will not necessarily be those of the host facility.
- Contract workers move on. Even if the client wishes them to stay, they will always be looking for the next assignment in the knowledge that they have no security where they are.
- Because contract workers are paid by the contract company for which they work, they will act so as to satisfy the goals of their employer, not the client facility.
- Contract workers, particularly those who are present on the site for only a short time, will not be familiar with the facility's overall safety culture, nor with its internal organization.
- Contract workers often receive instructions from both the facility supervision and their own employer. This division creates the potential for divided responsibility and confusion.
- Similarly, a contract worker often receives training from both parties, leading to the possibility of overlap, confusion, or something being left out.
- The client organization is responsible for the development and implementation of safe work practices at the work site. In many cases, the contract company will also have its own standard practices, which may not be aligned with those of the client.

On a more positive note, being outsiders, contract workers can bring an outside perspective and fresh ideas to the facility—provided the management is willing to listen.

From a legal point of view, the determination as to whether a worker is a contractor or not depends on who performs day-to-day supervision. If the supervision is mostly performed by the company personnel, then the contract workers are considered to be employees. If, however, the contract workers are supervised by their own management, if they have little interaction with the facility's process, then they would not be regarded as employees.

For example, a construction crew may be erecting a new administration building at a process plant site. The contract workers who pour the concrete and erect the steel work will not have any contact with the people who work on the processes, nor will they be directed by the site supervisors. Therefore, they are true contract workers. At the other extreme is a maintenance worker who has worked on the facility for many years and who reports directly to the facility's supervision. Even though this worker may be on contract in an administrative sense, regulatory agencies such as Occupational Safety and Health Administration (OSHA) would regard him or her as being equivalent to a full-time employee.

A hands-on worker is one who works directly with the equipment. In many cases, the work that they carry out is high risk, particularly when they are repairing or maintaining equipment. Such work often involves potentially dangerous activities such as vessel entry or accessing high-voltage electrical equipment. In these cases, the contract worker requires thorough training and indoctrination, and should be closely supervised.

Hands-on workers can be divided into two categories. The first are those who are involved in day-to-day maintenance. The need to understand the facility's safety management systems (SMSs) thoroughly because they will often be working alone and/or quite independently. The second category consists of construction workers who are present for projects and are not a part of the facility's day-to-day operations.

REGULATIONS AND STANDARDS

Because contractor management is so crucial to safe and successful operations, all industries have extensive regulations and guidance on the topic. A discussion of the standards provided by OSHA and BSEE (Bureau of Safety and Environmental Enforcement) is provided below.

OSHA PSM STANDARD

The OSHA standard and guidance to do with contractors are shown below (some administrative detail has been removed).

Standard

1. *Application*. This paragraph applies to contractors performing maintenance or repair, turnaround, major renovation, or specialty work on or adjacent to a covered process. It does not apply to contractors providing incidental services which do not influence process safety, such as janitorial work, food and drink services, laundry, delivery, or other supply services.
2. *Employer responsibilities*.
   - **i.** The employer, when selecting a contractor, shall obtain and evaluate information regarding the contract employer's safety performance and programs.
   - **ii.** The employer shall inform contract employers of the known potential fire, explosion, or toxic release hazards related to the contractor's work and the process.

iii. The employer shall explain to contract employers the applicable provisions of the emergency action plan required by paragraph (n) of this section.

iv. The employer shall develop and implement safe work practices consistent with paragraph (f)(4) of this section, to control the entrance, presence, and exit of contract employers and contract employees in covered process areas.

v. The employer shall periodically evaluate the performance of contract employers in fulfilling their obligations as specified in paragraph (h)(3) of this section.

vi. The employer shall maintain a contract employee injury and illness log related to the contractor's work in process areas.

3. *Contract employer responsibilities.*

i. The contract employer shall assure that each contract employee is trained in the work practices necessary to safely perform his/her job.

ii. The contract employer shall assure that each contract employee is instructed in the known potential fire, explosion, or toxic release hazards related to his/her job and the process, and the applicable provisions of the emergency action plan.

iii. The contract employer shall document that each contract employee has received and understood the training required by this paragraph. The contract employer shall prepare a record which contains the identity of the contract employee, the date of training, and the means used to verify that the employee understood the training.

iv. The contract employer shall assure that each contract employee follows the safety rules of the facility including the safe work practices required by paragraph (f)(4) of this section.

v. The contract employer shall advise the employee of any unique hazards presented by the contract employer's work, or of any hazards found by the contract employer's work.

OSHA PSM GUIDANCE

Employers who use contractors to perform work in and around processes that involve highly hazardous chemicals will need to establish a screening process so that they hire and use contractors who accomplish the desired job tasks without compromising the safety and health of employees at a facility. For contractors, whose safety performance on the job is not known to the hiring employer, the employer will need to obtain information on injury and illness rates and experience and should obtain contractor references.

Additionally, the employer must assure that the contractor has the appropriate job skills, knowledge, and certifications (such as for pressure vessel welders). Contractor work methods and experiences should be evaluated. For example, does the contractor conducting demolition work swing loads over operating processes or does the contractor avoid such hazards?

Maintaining a site injury and illness log for contractors is another method employers must use to track and maintain current knowledge of work activities involving contract employees working on or adjacent to covered processes. Injury and illness logs of both the employer's employees and contract employees allow an employer to have full knowledge of process injury and illness experience. This log will also contain information which will be of use to those auditing process safety management compliance and those involved in incident investigations.

Contract employees must perform their work safely. Considering that contractors often perform very specialized and potentially hazardous tasks such as confined space entry activities and nonroutine repair activities, it is quite important that their activities be controlled while they are working on or near a covered process. A permit system or work authorization system for these activities would also be helpful to all affected employers. The use of a work authorization system keeps an employer informed of contract employee activities, and as a benefit the employer will have better coordination and more management control over the work being performed in the process area.

A well-run and well-maintained process where employee safety is fully recognized will benefit all of those who work in the facility whether they be contract employees or employees of the owner.

Application

This paragraph provides guidance as to what constitutes a contract worker. Subcontractors and their employees are included.

Although OSHA separates contract workers who are providing "incidental" services from those who are working with hazardous chemicals, it is important to ensure that their work is indeed incidental to the process, and that they do not become inadvertently involved with the process in some manner. For example, if a contract worker is supplying snacks and soft drinks for the lunch room inside a plant, he or she will probably need to know about the use of basic safety clothing, and what to do in the event of an emergency.

Employer responsibilities

This paragraph highlights what the employer is expected to do when hiring and training contractors. Note that all of these requirements explicitly require the employers to be involved in the management of contractors. Companies cannot distance themselves from safety responsibilities by handing off the work to an outside contractor, and then leaving them to it.

The standard makes it clear that a contract company's safety record is to be reviewed before they are hired, and that safety record should be evaluated as part of the overall contractor selection process. Generally the contractor's OSHA 300 logs will be used for this evaluation.

BSEE SEMS

As shown in Figure 19.1, the offshore oil and gas business is especially dependent on contractors—ranging from very large companies all the way to small organizations and individuals. The agency responsible for offshore safety in the United States is the BSEE. This agency has paid particular attention to the management of contractors. Their philosophy is that the responsibility for what takes place offshore lies with the operator and that the operator therefore has to make sure that the contractors work safely and in conformance with the rules. It is up to the operator to ensure that the contractor knows what to do and that all contract workers are properly trained and evaluated.

This approach is spelled out in the following statement from the Safety and Environmental Management Systems (SEMS) rule:

> It is the intent of this rule to hold the operator accountable for the overall safety of the offshore facility, including ensuring that all contractors and subcontractors have safety policies and procedures in place that support the implementation of the operator's SEMS program and align with the principles of managing safety set forth in API RP 75.

However, in 2012 the BSEE issued a letter (BSEE, 2012) placing some of the responsibility directly on contractors. It is as follows:

> BSEE will hold lessees and operators directly and fully responsible for all activity conducted under a lease issued or maintained under OCSLA without limiting its ability to pursue enforcement actions against contractors.
>
> While the primary focus of BSEE's enforcement actions will continue to be on lessees and operators, BSEE will, in appropriate circumstances, issue incidents of noncompliance (INCs) to contractors for serious violations of BSEE regulations. The issuance of an INC to a contractor

does not relieve the lessees from liability. In fact, in instances in which INCs are issued to a contractor, INCs will also be issued to the lessee or operator.

BSEE will consider the following four factors in determining whether to issue INCs to contractors:

1. The type of violation
   Did the act or failure to act violate health, safety, or environmental requirements?
2. The harm (or threat of harm) resulting from the violation
   Did the violation directly result in, or could the violation have directly resulted in, serious injury or environmental damage?
3. Forseeability of harm (or threat of harm)
   Was it reasonably forseeable that the violation could directly result in serious injury or environmental damage?
4. The extent of the contractor's involvement in the violation(s)
   Did the contractor have control over the activity that resulted in the violation?
   Did the contractor's act or failure to act play a significant role in the violation?
   Did the contractor know or should the contractor have known that the activity may result in a violation?

It is likely that the above letter will result in legal challenges.

API RP 76

API RP 76 *Contractor Safety Management for Oil and Gas Drilling and Production Operations* was first published in 2000. The API wants to make acceptance of the new RP 76 universal in order to facilitate "Lean" and "Six Sigma" processes.

The standard includes a questionnaire of about 150 questions that contractors fill out about their health, safety, and environmental (HSE) standards and performance as part of the bidding process. The contractor need only fill out the questionnaire one time; it can then be used for multiple clients. (Not all questions apply to all contractors. For example, there are sections to do with aviation and marine. If a contractor does not work in those areas, he need not fill out the pertinent questions. There are also nation-specific questions. And contractors that perform low-risk activities will need to answer fewer questions.) Benefits of standardization include (i) elimination of redundant form filling by contractors, (ii) consistency in evaluating contractors, and (iii) freeing up more time for actually improving contractor safety.

TYPES OF CONTRACTOR

The word "contractor" is very broad in scope—covering very large organizations that can be much bigger than the host operating company down to single workers hired for a short, low-risk task. Companies that strive for excellent safety performance aim to treat contract workers—particularly long-term contractors—as if they are full members of the organization. However, there can be no denying that there are differences between permanent workers and those on contract. These differences include the following:

- Contract workers—even those on long-term assignment—are not an integral part of the facility on which they are working. Therefore, their standards and values will not necessarily be those of the host facility.
- Contract workers move on. Even if the client wishes them to stay, they will always be looking for the next assignment in the knowledge that they have no security where they are.
- Contract workers, particularly those who are present on the site for only a short time, will not be familiar with the facility's overall safety culture, nor with its internal organization.
- Contract workers often receive instructions from both the facility supervision and their own employer. This division creates the potential for divided responsibility and confusion.
- Related to the above, because contract workers are paid by the contract company for which they work they will generally act so as to satisfy the goals of their employer, not the client facility.
- Similarly, a contract worker often receives training from both parties, leading to the possibility of overlap, confusion, or something being left out.
- The client organization is responsible for the development and implementation of safe work practices at the work site. In many cases, the contract company will also have its own standard practices, which may not be aligned with those of the client.

On a more positive note, being outsiders, contract workers can bring an outside perspective and fresh ideas to the facility—provided the management is willing to listen.

From a legal point of view, the determination as to whether a worker is a contractor or not depends on who performs day-to-day supervision. If the supervision is mostly performed by the facility personnel, then the contract workers are considered to be full-time employees. If, however, the contract workers are supervised by the management of their own company, and if they have little interaction with the facility's process, then they would not be regarded as full-time employees.

For example, a construction crew may be erecting a new administration building at a process plant site. The contract workers who pour the concrete and erect the steel work will not have any contact with the people who work on the processes, nor will they be directed by the site supervisors. Therefore, they are true contract workers. At the other extreme is a maintenance worker who has worked on the facility for many years and who reports directly to the facility's supervision. Even though this worker may be on contract in an administrative sense, regulatory agencies such as OSHA would regard him or her as being equivalent to a full-time employee. The rationale behind this way of defining a contractor is that "OSHA believes that whoever is telling the worker what to do is probably in the best position to protect the worker".

Types of contractor include:

- Contract companies
- Design companies
- Subcontractors
- Contract workers
- Maintenance contractors
- Visitors/consultants

CONTRACT COMPANIES

Contract companies vary enormously in size. Some of them are small organizations that are on board just to carry out tasks that are limited in scope and number. However, other contractors—as was seen on Deepwater Horizon—are not only large, but they are responsible for much of the high-risk work that is carried out on rigs and drill rigs. Clearly, there cannot be a "one-size-fits-all" contractor management program in such circumstances.

Selecting a contract company

When selecting a company to carry out contract work, consideration should be given to the following issues:

- All of the contract workers should have received adequate basic training in the work that they are doing, and in working with hazardous and flammable chemicals. (Such training is often provided by industries, institutes, and local colleges.)
- The contracting company should have a safety program of a sufficiently high standard.
- All necessary technical and organizational information must be made available to the contracting company and to the contract workers.
- The contractor's safety logs must be up to date and show a good performance.
- The contracting company should not have a record of willful or repeat violations.
- The contracting company should have a system for recording and responding to incidents and near misses.

Knowledge as to a contractor's performance can be provided by their insurance company. They calculate an experience modification rate (EMR) for the previous 3 years. It is the ratio of the "Actual Workers Compensation Losses" to the "Expected Workers Compensation Losses."

Expected losses are determined from published tables which state the "average losses per $100 of payroll" for each of the different rating classifications and the actual payroll for that classification. A value of 1.0 for the EMR is assigned to the average contractor in their particular type of business.

Some companies will prequalify a contracting company so that there is no need to carry out qualification effort for each and every contract, particularly when the contracts are small or are of the same type. Contractors will be authorized only on those jobs for which they have been evaluated.

The contract should include a process for addressing noncompliance with HSE requirements. Issues to consider include:

- Work interruption authority
- Corrective action responsibility
- Noncompliance reporting

The contracting company, working with the facility management, should develop a contract management plan covering topics such as those shown in Table 19.1. The purpose of this plan is to ensure that all of the HSE requirements of the work have been considered and that the contract workers are fully qualified to carry out the work. The plan should be reviewed and agreed upon before the contract is awarded.

Table 19.1 Elements of the Contractor Management Plan

Management commitment and leadership
Safety committees
A head-count program
Roles and responsibilities of all workers, supervisors, and managers
Auditing
Hazard recognition
Emergency medical plan
Use of standard operating procedures and job safety analyses
Fitness for duty plan
Safety meetings
Incident reporting, analysis, and follow-up
Stop work authority/responsibility
Metrics and goals
Employee skills and training records
Entrance to property and traffic control
Violence prevention/weapons control
Use of explosives and hazardous materials

Employee participation
Inspectors
Key contacts list
Termination and warnings
Housekeeping
Hazard communication
Training
Behavior-based safety plan
Drug and alcohol control plan
Medical emergency plan
Use of PPE
Visitor orientation
Equipment inspection plan
Responsibility for compliance
Permit-required work
Emergency response plan

The contractor's emergency response plans should be designed to interface with the facility's plans. Contract employees should be adequately trained and informed of actions and expected roles they should take during emergencies. After receiving appropriate orientation and training in emergency procedures, contractor employees should participate in emergency response drills and exercises as appropriate.

Regulations generally require that employers periodically evaluate and audit contract companies and workers. If any problems or violations of company standards are observed, or if the contractor's safety record is deteriorating, the operating company must bring them to the attention of the contractors, and ensure that these problems are addressed.

Contractor HSE program

Once a contract has been signed but before the contractor begins work, facility representatives should meet with contractor representatives to discuss details of how the contractor's HSE program will be implemented. Depending on the scope of the work, this meeting might include a review of the work site to increase the contractor's familiarization with location, personnel, site HSE requirements, and emergency action procedures.

Topics that can be covered in the meeting can include the following:

- Significant HSE requirements contained in the contract
- Any change in scope or HSE requirements that might have occurred since prebid meetings
- The Contractor's Site HSE Protection Work Plan, and how it will interface with facility's HSE programs

- Clarification of HSE responsibilities of the facility employees, contractor employees, service/support personnel, and site visitors
- Reasonably anticipated hazards involved with the work and planned precautionary measures for such hazards
- The contractor's plans for conducting contract and subcontract worker orientations and training
- Emergency response and security procedures
- Considerations for permit-required work
- Chemical safety, including the use of Material Safety Data Sheets
- Container labeling requirements
- Waste management and other environmental requirements
- Accident/incident notification, investigation, and reporting requirements
- Lines of communication between facility and contractor representatives for resolving health or safety concerns
- Any significant HSE hazards which contractor employees are likely to encounter while on company premises. This disclosure should be in writing and contain sufficient information to allow a reasonable person to determine how to conduct the work in a safe manner.

DESIGN COMPANIES

The design companies hired by operators often make crucial and fundamental engineering decisions. The work that they do is often very specialized (which is one reason that they were hired in the first place) so it is difficult for the operator to evaluate the quality of that work and to be sure that the final design meets appropriate safety standards and rules.

SUBCONTRACTORS

When a contract company employs a subcontractor, the contract company is usually responsible to the client for the subcontractor's work. The client will also generally have the right to audit the subcontractor's performance.

CONTRACT WORKERS

Other contract workers, however, are present on a facility only for a short time, but may be asked to perform out high-risk activities such as vessel entry of working with high-voltage electrical equipment. In situations such as this, the operator has two tasks. First, he has to establish that the contract worker has adequate general training for the type of work that he or she is performing. Second, the operator has to make sure that the temporary contract worker has received sufficient training in the operations at the particular facility where the work is to be carried out. This validation may involve the use of bridging documents.

Some contract workers are present at a facility over a long period of time and function almost as if they are full-time workers. It is likely that these contract workers will be fully familiar with the operator's safety programs.

Each contract employer should have a facility employee who has oversight responsibility for his or her work. In some situations, assigning an individual, whether full- or part time, with direct, day-to-day involvement with the contractor's activities might be warranted.

MAINTENANCE CONTRACTORS

Maintenance contractors provide personnel, equipment, and materials as required for the upkeep and repair of company facilities and may perform general or specialized maintenance work. These workers are generally intimately involved with the facility's equipment and processes and work on high-risk tasks such as opening vessels, adjusting instruments, and replacing catalyst beds. In many cases, they are present at a site for an extended period of time—they become part of the organization and so should be provided with the training and resources that would be given to full-time employees. They also need to be very familiar with the facility's safe work practices standards.

VISITORS/CONSULTANTS

A visitor is someone who is present merely to observe what is taking place at the facility or to participate in an activity such as an audit. He or she must not touch any of the equipment or instrumentation. Visitors generally receive only a basic safety orientation; therefore, they should never be allowed to enter process areas without an escort. From a safety point of view, it is best if visitors can conduct their work in an office away from the facility. (If a man's not there he can't be killed.)

Consultants are like visitors in that they rarely have hands-on interaction with the equipment at the facility. However, they may be involved in potentially hazardous activities such as opening a vessel or changing instrument settings.

Included in this category are personnel who provide background support services such as delivering supplies to the warehouse, cleaning offices, or filling up soda machines.

BRIDGING DOCUMENTS

Contract companies do not work in isolation—they have organizational and physical interfaces with the operator of the offshore facility and with other contractors. Since each company will have its own SMS, bridging documents are needed. A bridging document is a map that links the relevant sections of the different standards. So, if the operator's plan calls for start-up procedures, then the bridging document would show where the same information is located in the contractors' documents. Any gaps would be identified, and the contractor's program would be modified to ensure that it fits with the operator's requirements.

OPERATOR/CONTRACTOR BRIDGING DOCUMENT

Figure 19.2 is an example of a bridging document between an operating and contracting company.

Sometimes, the operator will adjust his program to suit the requirements of the contractor, particularly if the contractor has specialized knowledge (which is one of the reasons that he may have

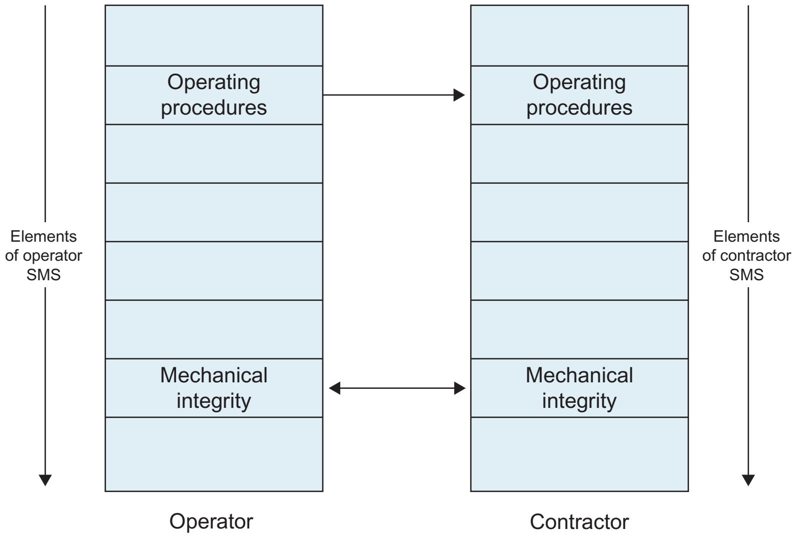


FIGURE 19.2

Bridging documents.

been hired in the first place). For example, a large operator may hire a painting contractor. Most of the information as to how to conduct safety activities will be from the operator to the contractor. But the contractor may have some special information to do with the paint being used, or how to control a fire should it ignite. In this case, the information would flow across the bridge from the contractor to the operator (which is why the Mechanical Integrity arrow in Figure 19.2 is double-headed).

BRIDGING THROUGH A REGULATION

The difficulty with developing bridging documents as illustrated in Figure 19.2 is that, given that there are many operators and even more contractors, the number of such documents could become prohibitively large. For example, in the Gulf of Mexico alone there are say 150 operators and at least 10,000 contractors (of all types) the number of potential bridging documents is 1,500,000—obviously a totally unmanageable workload. One way of getting around this is for each company to map its program to the elements of the pertinent process safety management rule—in this case, the SEMS regulation as illustrated in Figure 19.3. Then, instead of having company-to-company bridging documents they would all go through this central structure. Then, the number of documents goes down from 1,500,000 to about 10,000, i.e., one for each contractor and a few for the operators.

The central section of Figure 19.3 shows the SEMS rule. One of its sections is paragraph §250.1913 (e)(1) which is entitled “Review of and changes to the procedures must be documented and communicated to responsible personnel.” On the left of Figure 19.3 is the operator’s SMS. His standards to do with changes to operating procedures are under Sections “abc” and “xyz.” On the

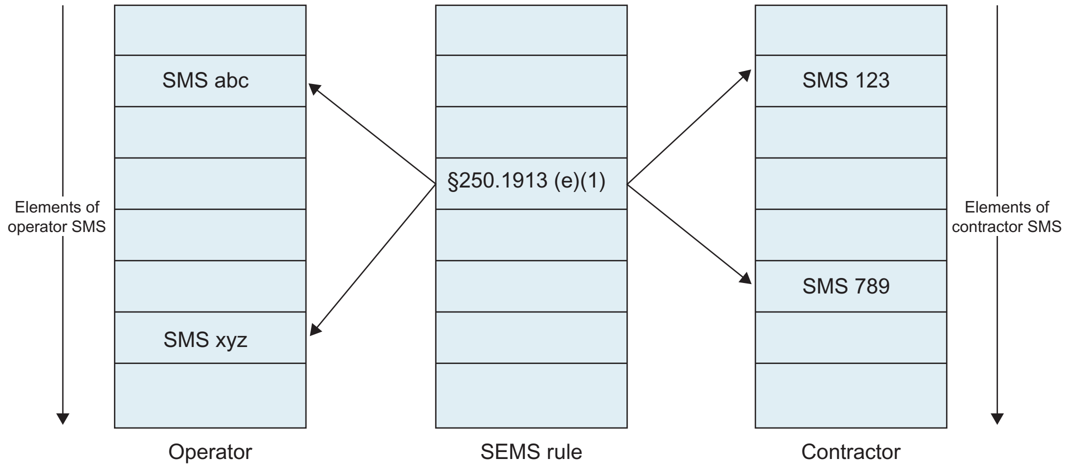


FIGURE 19.3

Central bridging structure.

right of Figure 19.3 is the contractor's program. He manages changes to procedures under Sections "123" and "789." If both operator and contractor write their programs so as to match the SEMS rule, then there is no need for a unique Operator/Contractor bridging document such as that shown in Figure 19.2.

CONTRACTOR MANAGEMENT

Management issues that the operator needs to consider include:

- Contractor selection
- Record keeping
- Contractor training
- Safety meetings
- Use of equipment
- Incident reporting
- Infractions

These topics are discussed in the following sections.

CONTRACTOR SELECTION

When writing a contract with a contractor, the operator should consider the following issues:

- Contractor's adherence to company safety and health rules
- Maintenance of independent contractor status

- Contractor's adherence to all laws and regulations
- Indemnification of operator by the contractor
- Contractor's adherence to special safety rules that may have specific importance for a particular type of work
- Operator's right to inspect contractor's work
- Accident reporting
- Furnishing equipment
- Termination of the contract if contractor breaches it in any way
- Contractor's agreement to utilize only employees with the appropriate level of training

RECORD KEEPING

The operator will need a reliable and comprehensive record keeping program. It should be designed to meet regulatory reporting requirements and to provide management with an understanding as to how each contractor is performing. Thoughts to do with the development of a record keeping systems are provided in Chapter 11.

CONTRACTOR TRAINING

The topic of Training is discussed in Chapter 7. Contract workers will often receive training from both their own company and also the operating company whose site at which they are working. The client company will generally have a two-part training program for contractors. The first part covers the general safety policies and procedures that are to be followed at all times. The second part of the training is site specific.

Contractor workers should know what to do when an emergency has been announced. In particular, they must know what to do with power tools that are in use, and where the evacuation routes are. Key elements of this training will typically include the following:

- Emergency recognition and prevention
- Safe distances
- Places of refuge
- Evacuation routes
- Site security and control
- Decontamination procedures
- Emergency medical treatment and first aid
- Emergency alerting and response procedures
- Personal protective equipment (PPE)
- Emergency equipment

SAFETY MEETINGS

Contractors should conduct periodic safety meetings for their employees and subcontractors. These meetings generally review health and safety issues but environmental issues such as waste management or spill prevention can also be addressed. Informal "tailgate" meetings can be held daily, and more formal meetings say once a week. It is a good idea to have a different person lead each of the safety meetings.

Details to do with the more formal safety meetings should be recorded. The following should be noted:

- Date of the meeting
- Presenter or facilitator
- Attendees
- Summary of topics discussed
- Action items

The operating company should review the agendas for the meetings and should participate in them as much as possible.

USE OF EQUIPMENT

Frequently, contractors will work on equipment that is the property of the operator. The operator should provide the contract workers with all the tools, materials, and PPE that is needed to work on that equipment. The contractor is then responsible for using the provided materials in the proper manner.

CONTRACTOR EVALUATION

The operator should routinely conduct audits and reviews on all of the contract companies that it employs.

At the end of each project, facility and contractor representatives should thoroughly evaluate the contractor's HSE performance. These postwork evaluations should be used for future prequalifying and selection of contractors. Evaluations should be done at or near the completion of work or upon the expiration of contracts. Topics addressed in the postwork evaluation might include:

- Accident/incident data summaries
- Environmental compliance and sensitivity
- Results of HSE reviews and audits
- Timeliness of hazard mitigation
- Integration of HSE protection in job preplanning
- Compliance with procedures and permit-required systems
- Availability and use of proper HSE equipment
- Adequacy of emergency planning and response procedures
- Commitment of contractor's management to HSE protection
- Adequacy of HSE training (level of detail and documentation)
- Submission of required data, records, and documentation

Any serious incidents that may have happened during the course of the contract should be reviewed, and future risk reduction strategies should be considered and implemented as appropriate.

Finally, the contractor should be asked for suggestions for enhancing the facility's own health and safety program.

INFRACTIONS

It is necessary to have a system in place for recording and acting on infractions of the policies and procedures that have been discussed in this chapter.

If someone working for the operator observes an infraction of safety rules, then he or she should generally contact the contractor job representative rather than deal directly with the offending employee. However, for imminent danger situations and flagrant violations, any employee can and should demand that the infraction be corrected immediately. They will then report their actions to management.

If the infraction is observed by someone working for the contractor, the same procedure should be followed. The person noting the problem should report to his or her management, unless immediate action is required.

CONTRACTOR TRAINING

The client company will generally have a two-part training program for contractors. The first part covers the general safety policies and procedures that are to be followed at all times. The second part of the training is site specific.

Contractor workers should know what to do when an emergency has been announced. In particular, they must know what to do with power tools that are in use, and where the evacuation routes are. Key elements of this training will typically include the following:

- Emergency recognition and prevention
- Safe distances
- Places of refuge
- Evacuation routes
- Site security and control
- Decontamination procedures
- Emergency medical treatment and first aid
- Emergency alerting and response procedures
- Personal protective equipment
- Emergency equipment.

SAFETY MEETINGS

Contractors should conduct periodic safety meetings for their employees and subcontractors. These sessions typically focus more on health and safety issues, but environmental issues such as waste management or spill prevention can also be addressed. Informal "tailgate" meetings can be held daily, and more formal meetings say once a week. It is a good idea to have different people lead the safety meetings.

Details to do with the more formal safety meetings should be recorded. The following should be noted:

- Date of the meeting
- Presenter or facilitator
- Attendees
- Summary of topics discussed
- Action items.

CHAPTER

THE RISK MANAGEMENT PROFESSIONAL 20

CHAPTER OUTLINE

Parts of this chapter discuss legal issues such as copyright and litigation support. Because this is a technical book, the information provided here should not be used for legal purposes. Legal advice must always be sought from a qualified attorney.

INTRODUCTION

The previous chapters of this book have discussed the development and implementation of a risk management program. They have shown that the topic is varied and covers a wide variety of topics ranging from highly technical issues, such as vapor dispersion and fault tree analysis, to management systems and human behavior. Hence, the persons charged with creating and running such a program need a wide range of aptitudes and skills. This chapter discusses some of the attributes of the ideal risk management processional, whether he or she be a direct employee, contract worker, or a consultant.

Process Risk and Reliability Management. DOI: http://dx.doi.org/10.1016/B978-0-12-801653-4.00020-5

There is no formal process risk management discipline, analogous to chemical engineering or business studies, nor is there any single educational, work, or professional background that is shared by risk management professionals, largely because they often start working in this area toward the latter half of their careers, having had many years of diverse experience working in operations, design, and engineering in a wide range of industries.

ATTRIBUTES

A successful risk management professional needs to have personal attributes that match his or her technical knowledge and skills. Some of these attributes are discussed below. Of course, no single person can possess all of them, but the list does provide an outline as to goals to aim for.

EDUCATION AND CERTIFICATION

Most risk management professionals have a technical education—often in engineering or environmental science. Such an education provides the necessary skills to handle the technical and quantitative aspects of the work, particularly with regard to the analysis or risk, fires and explosions, and gas dispersion.

TECHNICAL KNOWLEDGE

The risk management professional should have a thorough understanding of the many technical topics that the discipline covers. Obviously, no one person can be an expert in all of the technical areas that make us risk analysis, but he or she should possess enough knowledge of them in order to develop the correct parameters for risk analyses and to understand the findings and reports that the experts provide.

HOLISTIC

A person who thinks and works holistically is not limited to a single, narrow detailed specialized sphere; instead he can understand management, technical, and human systems, and how they interact with one another. A risk management professional understands how his or her profession is composed of a wide range of disparate topics such as human factors engineering, Boolean algebra, government regulations, starting up a process plant, and the design of instrument systems.

If a risk management professional is to be effective at integrating different types of knowledge, he or she must possess a good grasp of those topics. This does not mean that the professional has to be an expert in everything—such a goal is obviously unrealistic—but it does mean that he or she needs to have a working knowledge of multifarious topics, and to have a comprehension as to how they fit together. The phrase, "jack of all trades, but master of none," is usually considered pejorative. However, with regard to the risk management professional, it is a sensible job description.

NUMERATE

As has been stressed throughout this book, risk has both objective and subjective elements. The objective part of the work means that those working in the area of risk management need to be numerate; they need to be comfortable with a variety of quantitative topics such as gas dispersion modeling, the development of $F-N$ curves, and the use of Boolean algebra.

COMMUNICATION SKILLS

Risk management professionals spend much of their time communicating with others in a variety of ways such as writing reports, listening to client needs, delivering presentations, and listening to anecdotes. Hence the risk management professional must be a good speaker, writer, listener, and reader. Discussion of these topics is provided later in this chapter.

INDUSTRIAL EXPERIENCE

There is really no substitute for industrial experience. It is one thing to learn about a topic from books such as this, and by reviewing incidents that have occurred elsewhere, but it is quite another to actually learn from the school of hard knocks. Industrial experience includes not only a hands-on knowledge of industrial processes and equipment but also an understanding of the realities of client/consultant relationships, the resistance that managers have toward spending money on safety, problems at the management/union interface, and how government agencies actually enforce regulations.

KNOWLEDGE OF PAST EVENTS

The risk management professional should know about incidents and events (both good and bad) that have occurred in other companies and locations. He or she can use these events to understand and identify patterns in current operations.

The importance of understanding the past is illustrated with regard to (the fictional) Dr. Watson's ruminations as to what new friend Sherlock Holmes does for a living, not long after they first meet. Watson summarizes Holmes' attributes. The list includes the following statement:

> <knowledge of...> Sensational Literature—Immense. He appears to know every detail of every horror perpetrated in the century.

So it is for the risk management professional; he or she should possess an "immense knowledge" of incidents that have occurred and what lessons can be drawn from them. An overview of some major incidents in the process industries is provided in Chapter 1.

In this context, it is interesting to note that the recently released proposed update to the Occupational Safety and Health Administration (OSHA) process safety management (PSM) standard (see Chapter 2) relies heavily on actual incidents. Almost all of the proposed changes are justified by showing how such changes could have helped prevent the cited incident.

PROFESSIONAL INVOLVEMENT

Risk management professionals should be involved in their community. This is usually done by working with professional societies or independent trade organizations—often by helping with the organization of meetings, editing papers and articles, and writing technical standards. Reasons for being involved include the following:

- It is a way for experienced professionals to give back to their community and to help young people who are entering the field.
- Development of personal reputation and contacts within the community that could lead to more interesting and rewarding work and assignments.
- Enhancement of the reputation for the company or organization that the professional works for.
- The writing of articles and papers requires the author to carry out thorough research on the topic about which he or she is writing.
- Helping others to prepare and publish their work increases the knowledge and skills of all parties.

NETWORK

A well-known proverb states "It's not what you know, it's who you know." This proverb is only half correct—technical knowledge and personal skills are vital to any professional. Yet it is important to maintain a network of qualified contacts. In particular, when an expert has to address a challenging problem it is useful to have someone to call who can help out as a friend and colleague.

THE RESUMÉ/CV

The expert's knowledge, skills, and attributes are summarized in his or her or resumé or curriculum vitae (CV).

It is critical that the resumé be accurate and verifiable, especially with regard to statements, such as the possession of advanced degrees, or major work experience. Accuracy of the resumé is particularly important when the risk management professional is involved in litigation. He or she must expect to have his qualifications challenged because, if the resumé can be discredited, then the expert‘s statements can be discredited also.

Many professionals fail to keep their resumés up to date. It is a good idea to check it and modify as needed every 3 months or so, particularly when new types of work or project are being carried out.

Level of detail

An expert's resumé can become very lengthy because he or she is likely to have years of experience in a wide range of tasks and projects. Such length has its drawbacks—it can make the resumé difficult to read and lacking in focus. For this reason, it is often a good idea to have a short (say half page) summary at the start of the resumé, supplemented by an attachment that provides the detailed information.

Publications

An expert's resumé is greatly enhanced if he or she has published professional papers, articles, and books. Books, in particular, can make a very strong impact—the risk management professional can say "I wrote the book on that. Here it is!"

Involvement with professional societies, as discussed in the previous section, also looks very good on the resumé.

Gaps/negative facts

After many years of work experience, no one will have a perfect work record. Everyone's career hits the occasional bump in the road. In particular, there will often be gaps in the work record for the times that the professional was unemployed or was trying to land new contracts. These gaps can be filled with information to do with background work such as the preparation of seminars or professional papers, or with time spent on continuing education.

Multiple resumés

Some risk management professionals have multiple resumés, with each version emphasizing particular qualities. For example, one version may stress say design experience, whereas another may place a greater emphasis on field operational work.

Although this practice may help in specific situations, it is generally best not to have more than one resumé. This is particularly true with respect to litigation work because an opposing attorney may use the two documents to "demonstrate" that the witness is not to be trusted, particularly if the professional appears to have a "plaintiff resumé" and a "defendant resumé."

Declining experience

One of the traps that experts can fall into is that, if they fail to keep up with the latest knowledge and practice in their field, they may not really be qualified to help a client in an area that is shown on their resumé. The expert may fail to recognize that his or her knowledge and judgment is out of date.

A related problem is that some process risk experts may have worked for just one company for the duration of their careers. On retirement they seek to become consultants with other companies, but find that their deep, but narrow, experience can be quite limiting.

PROFESSIONAL ENGINEER

Most nations have a system whereby engineers can be licensed. In the United States, the licenses are issued by individual states.

Professional engineers working in the process industries in California face a challenge: most licensed activities have to be carried out by civil engineers, regardless of the work that is being performed; chemical engineers have comparatively little status (Parkinson, 2013).

CONSULTANTS

Companies hire consultants to help them with their risk management programs for the following reasons.

- Some of the elements of the program may be new to a company; in such cases, a consultant can help them get started. For example, in the late 1980s and early 1990s Process Hazard Analyses (PHAs) were a new technique in most facilities. Hence, a small consulting industry began to conduct PHAs, develop software, and to train clients in their use and application. Now that PHAs are part of the furniture for most companies, the need for this particular consulting service is not so great (although many of the same people continue to assist with the implementation of the PHAs—but as such they are serving as contract workers, not consultants).
- A company may be struggling with the logistics of its risk management program. Costs may be out of hand and/or the program may be way behind schedule. A consultant can work with the management team to bring the project back on track.
- Consultants often make good auditors. Their expert knowledge of the principles of risk management of process safety regulations provides a solid foundation for their findings. And consultants are particularly well qualified to conduct assessments of a facility's risk management program.
- A consultant can provide fresh ideas as to how to perform well-understood tasks. For example, in Chapter 5, it was pointed out there is a wide variety of PHA techniques that can be used. If a company has become stuck with one method, say the Hazard and Operability technique, a consultant can help them evaluate and use other methods such as What-If or failure mode and effects analysis.
- A company may require detailed help concerning the interpretation of a regulation or ruling. A consultant can provide benchmarks from other companies. Indeed, one of the most common questions that consultants have to answer is "How do other people do it?" where the word "it" refers to an activity that they themselves are having trouble addressing.

TRUE EXPERTISE

Consultants must be true experts. Many people know "quite a lot" about a topic, but that does not make them true experts. In the example quoted above concerning PHAs, by the early 1990s many engineers and other technical specialists had become very familiar with the process of leading hazard analyses. This did not, however, qualify them to become PHA consultants. Their experience merely qualified them to lead hazards analyses, not to design, implement, and run PHA systems.

THE CONSULTANT AS OUTSIDER

The consultant should be an outsider. This is important because he or she may be called upon to present unpalatable truths to management. In many situations, the cause of a problem such as a deteriorating safety record is understood by the people at the working level. However, no one within the organization feels that they can present "the truth" to management for fear of retribution. (This is not always a management problem, however. The consultant may find that management is quite flexible and willing to adopt new techniques. The resistance may come from supervisors and working level people who have become entrenched in the current mode of operating.)

A consultant may be able to successfully present bad news more effectively than an employee for three reasons. First, the worst that the client company can do is to terminate the consultant's contract. Since the consultant usually has other assignments, this loss of work is not as critical as it would be to full-time employee. Second, outsiders are often perceived as being more credible than insiders, even though they present exactly the same facts. (This is why consulting companies themselves sometimes have to hire consultants to tell them "the truth." It is also the rationale behind the quotation "An expert is someone who is more than 50 miles away.") The third advantage of using an outsider to present bad news is that management is not quite sure where to "place" the consultant. Consultants are often perceived as being "above" line employees, particularly if it is suspected that they have the ear of senior management. Therefore, comments from consultants are often treated with a good deal of respect and consideration.

The importance of being an outsider raises a concern about the use of "internal consultants"—a phrase which some might regard as being an oxymoron. If the consultant and the client work for the same organization, sooner or later their chains of command will meet. Hence, neither is truly independent from the other. Furthermore, as their respective careers progress, it is possible that they will find themselves working for or with one another. This knowledge is likely to cloud the objectivity of the client–consultant relationship.

The consultant should also be an outsider because it is his knowledge of "how other people do it" that can be so valuable to an organization that has become trapped in its own systems and ways of thinking.

Ironically, one of the problems that consultants can run into is that they themselves can become stuck in their own rut; they may have trouble accepting that other people's ideas may be as good as or even better than theirs. Therefore, it is important to make sure that the consultant is truly up to date, and that he or she is constantly evaluating and testing their own ideas, and abandoning those that are out of date. This being the case, one question that the client company may want to ask a consultant before hiring him or her is "Which of your opinions and ideas have you changed during the last few years?"

CONSULTANTS—NOT CONTRACTORS

An appropriate analogy can be made here with respect to education and training, as discussed in Chapter 7. Someone who is educated in a topic understands its fundamental principles, whereas someone who is merely trained in that topic knows "how to do it." So it is with consultants and practitioners. Consultants provide insights to do with fundamental principles; practitioners, however, simply know what to do.

The third aspect of consulting is that it is concerned with advising, not doing. A consultant looks at organizational issues and advises management on how to address them. This is why the end product of most consulting contracts is a report and a presentation to management. If he or she is asked to implement some of the recommendations contained in the report, he or she has switched roles from being an adviser to a doer.

Good consultants work by generalizing from the specific and then drawing specific conclusions from their generalizations. They go into a situation and investigate the facts of the current situation. From these facts, they come up with a general analysis from which they develop specific recommendations. This ability to form general conclusions is also an important attribute of an incident investigator.

Consultants must possess good client-relations skills. They have to be aware not only of technical issues but also of the internal company dynamics and politics. Process safety consultants frequently have a technical background—many of them are chemical engineers—and therefore tend to perceive the world as being rational and objective. They may fail to grasp that their clients, like all customers, base many of their decisions on a combination of both emotion and fact.

The distinction between “doing” and “consulting” can be frustrating for many consultants. Many of them have had a career in industry, often at quite senior levels. They are used to taking charge and having their ideas put into practice. Hence, the need to persuade rather than command can be a challenge for such consultants, particularly when the client chooses to ignore the consultant’s recommendations.

A facility may choose to use contract help with many of its risk management activities, particularly those that are labor intensive, such as writing operating procedures. Using consultants or contract workers in this manner moves away from the principles of employee participation and involvement.

CUTS GORDIAN KNOTS

In the fourth century BC, King Midas in the city of Gordium in what is now the nation of Turkey tied his ox-cart/chariot to a post with an intricate knot. It was prophesied that whoever could undo the knot would become the next king of Persia. In 333 BC, Alexander the Great attempted to untie the knot. He could not find an end to the rope, so he simply cut through the knot with his sword. He went on to conquer most of the known world, including Persia.

The story symbolizes the resolution of an intractable problem with a swift, unconventional stroke. Good consultants have the ability to cut the Gordian knots that clients have created for themselves.

QUICK STUDY

Although a consultant may be an expert in many areas of business or technology, but he will never possess the detailed technical knowledge to do with every task he or she faces. For example, each new assignment will require him to work with a new type of chemical process technology. This means that an effective consultant is a quick study, i.e., he or she must be able to enter a situation, learn it sufficiently well to understand the management issues involved, and then make sensible recommendations. This is analogous to what a trial lawyer does. He will learn the details of a case very rapidly, organize the case that is to be presented to the court, make the presentation, and then almost immediately forget the details as he moves on to the next case.

ROLE OF THE CLIENT

The client must realize that the success of the consultant’s work will depend largely on the attitude and degree of cooperation provided by the facility employees. In particular, client personnel must try to be open-minded and objective. The consultant has been hired because he or she represents an outside point of view. Hence, the findings are likely to upset some people on the client side because old and comfortable ways of doing business will be challenged. The client should try to understand that there may be new and better ways of operating; in particular, everyone should try to avoid using the phrase “we’ve always done it that way and it’s never been a problem” (with the implication that it never will be a problem).

RESPONSE TO CRITICISM

Consultants must have thick skins. It is almost certain that their ideas and recommendations will be critiqued and criticized. Oftentimes, the people doing the criticizing will be considerably less qualified than the consultant. Also they will have spent less time studying the problem being analyzed and will probably have motives and agendas of their own. In these situations, the consultant must work as hard as possible to communicate the findings of the analysis to all concerned, but he or she must also recognize that the client is paying the bills, and ultimately makes the final decisions. The consultant is an advisor, not a decision maker.

MARKETING

Consultants must market their services. At the same time, they must maintain a professional profile. For most consultants, their marketing will be based on a web page that provides information on services offered. This will be supplemented by direct mails and carefully managed email campaigns (which are best done through a service that provides full opt-out capabilities).

Social media also provide an opportunity for professional marketing. By writing articles and blogs for LinkedIn and other similar sites, the professional gains exposure (and also develops his or her own ideas).

Maintaining a professional and independent profile is particularly important for consultants who serve as expert witnesses (a topic that is discussed below). He or she has to avoid the perception that he is a “professional expert”—a hired gun.

COMMUNICATING WITH MANAGEMENT/CLIENTS

Risk management professionals report to managers or clients. Therefore, they must know how to communicate information, findings, and insights quickly and effectively. This is generally done in one of three ways:

1. Presentations
2. Discussions in meetings
3. Written reports

PRESENTATIONS

When making a presentation, the following guidance should be considered:

- Visual aids must always support what is being communicated. They are not an end to themselves.

- They should be simple—like Goggle or amazon.com pages.
- Each visual should be shown for about 60–90 seconds. It is best to avoid fancy graphics or animation, cartoons, and humor.
- Although a discrete use of color makes sense, the visuals should never be garish.
- The presentation should be practiced as much as possible. It should be fluent and somewhat conversational.
- It is possible to make remarks that would not be written down. For example, there is little place for humor in professional publications. However, during a presentation it may be appropriate to make a few gently humorous comments.

MEETINGS

Professionals can spend a large amount of time in meetings. Many risk management issues—particularly in the area of safety—require team input and consensus, and such input and consensus usually requires that those involved get together in a meeting. Therefore, the effectiveness with which a professional can carry out his or her work depends, to a considerable degree, on the manner in which he or she participates in meetings and is able to lead multidisciplinary discussions.

Meeting participants should always focus on the leader/facilitator and show respect to other attendees.

Meetings are expensive. In order to emphasize this point, one company installed special "clocks" in each of their meetings rooms. At the start of any meeting, the leader entered the number of attendees into the "clock." A dollar value was assigned for each man hour. As the meeting progressed, the clock displayed the cost of the meeting so far. So, if a meeting had eight attendees, with a cost of $50 per man hour and the meeting duration is 1 hour, the clock displays a total meeting cost of $400.

Given that meetings are expensive and time-consuming, those calling meetings should ask two questions of themselves: "Is this meeting necessary?" and "What would be the consequences were it not to happen?" The cost of the meeting is also why people should be punctual. If a person is late for a meeting, or leaves early, then they have wasted not only their own time but the time of everyone else at the meeting. This practice is both discourteous and inefficient.

REPORT WRITING

The end product of much risk management work is a report. It is vital to recognize that the timeliness and quality of the report itself are as important as the work that went into its creation. All too often a report is delivered late. The report itself may be incomplete, cryptic, either too long or too short, and hard to follow. Guidance to do with clear writing is provided in Chapter 6. Additional thoughts are provided here.

Strunk and White's *The Elements of Style* (Strunk and White, 2000) provides excellent guidance with regard to writing. Although first published before World War I, this book is as useful and relevant now as it was then. (The last update was published in the year 2000.)

Brogan's *Clear Technical Writing* (Brogan, 2000) provides guidance for technical writing in general. One quick way of checking the quality of the writing is to read out loud what has been written. If what has been written seems to flow smoothly and clearly expresses the author's message, then it is probably readable.

DRAFT REPORT

Having collected the information—say for an audit or a hazards analysis—the report writer must write the draft report as quickly as possible. No matter how effective and thorough the auditor's note taking may have been, there will always be some observations and facts that were not fully recorded in the auditor's notes, or that are not easily understood a few days after the audit has concluded. In order to capture these thoughts, and to clear up any potential ambiguities, the auditor must write the draft report right away.

In spite of the need for speed in preparing the draft report, it is equally important to make sure that it is accurate, complete, and presentable. There is a well-known proverb in the consulting business that "There is no such thing as a draft report." If a draft report contains errors, especially egregious or silly errors, the people reading it will fixate on them to the exclusion of all other factors. Furthermore, they will never forget these problems. No matter how high the quality of the final report, an indelible image of poor quality will remain. As they say "You don't get a second chance to make a first impression." It is particularly important to watch for "obvious" errors. If the auditor uses the wrong name for an important piece of equipment or places the plant in a different city from the one it is actually in, the report will instantly lose credibility. In the words of another saying "Vice Presidents can add up, but they can't multiply." In other words, it is vital not to make obvious or silly mistakes.

Once the draft report is complete, the auditor must ask a colleague to check it. Failure to do this is an invitation to some of the problems just discussed. The internal reviewer probably will not know the facility being audited. Nevertheless, he or she can at least assess the overall tone and style of the audit, and check for internal inconsistencies. The reviewer can also make sure that all the findings are cross-referenced against the appropriate regulation or standard. In general, the internal reviewer should check for the following potential problems:

- Factual errors or inconsistencies
- Inappropriate language
- Opinions masquerading as facts
- Completeness
- Incorrect references to regulations or standards

Draft documents should be disposed of as soon as they are no longer relevant or correct. All drafts should be destroyed prior to the issue of a final report or document. Not only does this practice reduce the potential for problems in an investigation, it also reduces the chance of internal confusion. The control of draft documentation is difficult to enforce. It is likely that each person involved with the program will have his or her own copies of documents such as piping & instrument diagrams (P&IDs) and operating procedures. They will also probably have made notes in their diaries and files. If there is an accident, those notes become part of the official record. Yet people are reluctant to throw such documents away because "you never know when they might come in handy." Nevertheless, these documents must be discarded. (In this regard, the increased use of electronic document management systems should reduce dependence on old printed reports.)

LANGUAGE OF THE REPORT

The report should be written in a neutral style. If problems are found, the report should make it clear that these problems are to do with management systems, not specific individuals. (Sometimes the auditor will find a hazardous situation that can be attributed to one individual. In these cases, the auditor should probably communicate that concern verbally.)

The vocabulary used in the report should be careful and objective. Problems that are uncovered should be referred to as "exceptions," rather than "deficiencies" or "faults." Words such as "dangerous" and "willful" are inappropriate unless applied very specifically. Other words, such as "negligent," often have a legal connotation that should be avoided by nonlawyers. The report writer should also avoid words such as "dishonest" which impute a person's character, unless there is very clear evidence that justifies doing so. The report language should also meet the red face test, i.e., could it create embarrassment if it is read out in a court setting?

COMPLETENESS/THOROUGHNESS

The report must be complete and thorough, and should contain enough detail to explain the findings and provide the background discussions. What may appear obvious and self-explanatory at the time of the PHA meetings may be anything but when someone who was not on the team reviews the work 2 or 3 years later. As already stressed, it is almost impossible to provide too much detail and explanation, particularly when explicating and justifying findings and recommendations.

PERSONAL INFORMATION

Those reporting information must be careful not to reveal personal information such as the age of the persons involved or whether their performance was affected through substance abuse. If such information has to be recorded, then the incident investigation software must have the capability of creating private fields for information such as this. In all cases, it is vital to recognize a person's right to privacy—a right which is often upheld by law. It is particularly important not to include a person's face in any photographs that are taken of the incident site.

WRITING STYLE

A comment that is sometimes heard during the report writing process is "We're not writing Shakespeare, you know." Obviously such a statement is true—even though the person making the statement probably fails to appreciate the rather sad irony behind the statement. But the implication of such a statement that the report writer need not pay much attention to writing style is regrettable.

Nonemotional language

The report must not contain language that is inflammatory, emotional, or judgmental. All statements should be based on facts, not feelings. Therefore, words such as "dangerous," "tragic," "unacceptable," and "fatal" should only rarely be used, and then only with the greatest care.

Some report writers try not to include nouns that hint at serious problems. They tend to avoid references to "fires," "explosions," and "release of toxic gas." Such an approach is counterproductive; if a hazard has the potential for creating a fire, then the report should say so. Writing style is subordinate to results; the writer has a responsibility to the reader to deal in honest and clear language.

It should be noted that not all managers agree with the need to be circumspect with regard to the communication of hazards analysis results. Once a hazard has been identified as being serious enough to require action, words that attenuate the recommendations will not make any difference if the incident actually occurs—the company will still be faced with a situation where a hazard was known about but had not been addressed. "Fine words butter no parsnips."

Minimalist writing—Make every word tell

Although he did not use the term "minimalist writing," the concept was excellently described by Professor Strunk in the year 1918.

> Vigorous writing is concise. A sentence should contain no unnecessary words, a paragraph no unnecessary sentences, for the same reason that a drawing should have no unnecessary lines and a machine no unnecessary parts. This requires not that the writer make all his sentences short, or that he avoid all detail and treat his subjects only in outline, but that every word tell.

His use of engineering design as an analogy for writing style is should resonate with those writing operating procedures.

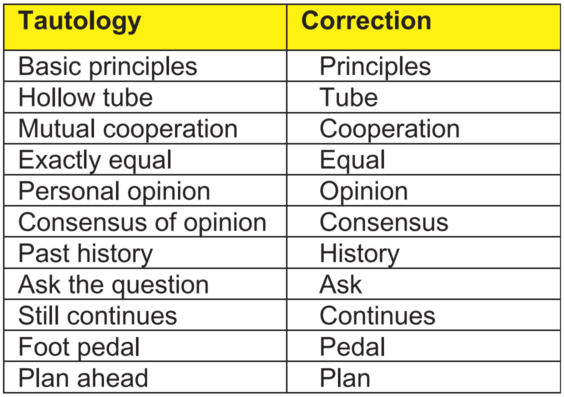
Minimalist writing does not mean that a large number of words cannot be used where needed. If a hazards analysis team has uncovered a very serious issue that is also difficult to quickly understand, then a lengthy description should be provided in the report. Nevertheless, the writer of the report should still "make every word tell."

Omit needless words/tautologies

The omission of needless words (which also comes from Professor Strunk's book) is one of the keys to minimalist writing. Similarly, tautologies should be avoided (a tautology is "a needless repetition of the same sense in different words"). Figure 20.1 provides some examples of tautologies and their corrections.

Short, simple words

Many reports could be made shorter were the writers to use simple words and phrases at every opportunity. Some examples are shown in Figure 20.2. In the first column, a nonminimalist word is provided; in the second column, a shorter "translation" is shown.



Tautology	Correction
Basic principles	Principles
Hollow tube	Tube
Mutual cooperation	Cooperation
Exactly equal	Equal
Personal opinion	Opinion
Consensus of opinion	Consensus
Past history	History
Ask the question	Ask
Still continues	Continues
Foot pedal	Pedal
Plan ahead	Plan

FIGURE 20.1

Tautologies.

Minimize "soft" materials

Many reports are cocooned in a cloud of "soft" materials such as statements of the company's commitment to quality, safety slogans, and Mission Statements. None of these materials help the reader understand the report's contents any better; instead they pad the report with material that gets in the way, and increases the time it takes to find useful information. The minimalist approach eliminates as much as possible of these soft materials.

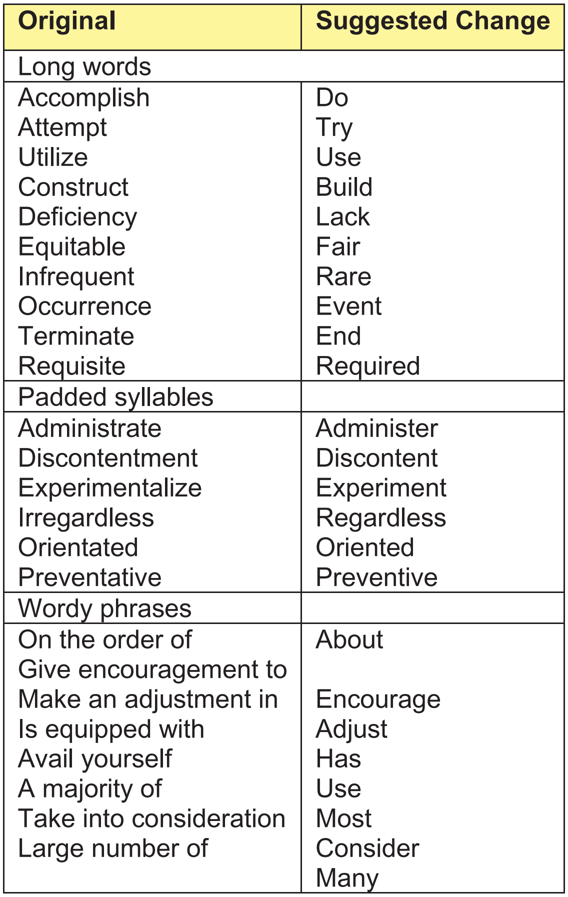
Eschew obfuscation

In general, simple words should be used. They will make the report more readable, and give it more accessible, conversational tone. However, it is important to use a mixture of words, particularly as certain specialized words such as "risk," "safe," and "failure" are likely to crop up over and over again in a report, thus making it rather tedious. The word processor's thesaurus can help add variety to the language of the report as long as the clarity of the report's meaning is not threatened.

The use of the Fog Index to measure grade writing level is discussed in Chapter 8. Whereas an eighth grade level may be suitable for operating procedures, 11th or 12th grade equivalency is more likely to be suitable for professional reports (this chapter is written at an 11th grade level).

Develop a theme

In the 1980s, one of the best-known sports broadcasters in the United States was Howard Cosell. He was particularly well known as one of the commentators for the Monday Night Football program. One of the reasons for his success was that he developed a theme for each game before the game started. For example, one team may have had a young, inexperienced quarterback, while the other team had a very strong defensive line. The theme would then be how well the young quarterback could play under the pressure of such a strong defense.



Original	Suggested Change
Long words	
Accomplish	Do
Attempt	Try
Utilize	Use
Construct	Build
Deficiency	Lack
Equitable	Fair
Infrequent	Rare
Occurrence	Event
Terminate	End
Requisite	Required
Padded syllables	
Administrate	Administer
Discontentment	Discontent
Experimentalize	Experiment
Irregardless	Regardless
Orientated	Oriented
Preventative	Preventive
Wordy phrases	
On the order of	About
Give encouragement to	
Make an adjustment in	Encourage
Is equipped with	Adjust
Avail yourself	Has
A majority of	Use
Take into consideration	Most
Large number of	Consider
	Many

FIGURE 20.2

Redundant words.

The same approach can be used when writing a report. After collecting the facts to do with a situation, the writer of the report can develop overarching themes for what he or she has observed, and organize the material of the report around these themes.

Modifiers

In general, it is generally best to avoid the use of modifiers (adjectives and adverbs) altogether. For example, the adjective "large" in the phrase "Large fire" does not provide specific guidance as to how bad the fire was. However, the phrase "Fire resulting in loss of Pump, P-101" is specific, and could therefore be used in the report. The more specific a statement is, the less likely it is to be misconstrued.

It is generally a good idea to avoid modifiers, i.e., adjectives and adverbs, when writing technical reports, particularly when the modifiers are nonquantitative. For example, the statement “An explosion occurred” is better than “A large explosion occurred.” In this context, the word “large” is not meaningful. However, if the qualification can be quantified, then its use would be more acceptable. For example “An explosion equivalent to 5 pounds of TNT occurred” provides additional information.

Adverbs are even more prone to misinterpretation than are adjectives. For example, a statement such as “the temperature rose quickly” can mean different things to different people. However, the statement “the temperature rose 100ºC in 5 minutes” is unambiguous. Similarly, a phrase such as “I read the report carefully” implies that other documents may not have been read carefully. It is better simply to say “I read the report.”

No typos

With the advent of modern word processing software, there is no reason for the report to contain any type of error in grammar or syntax. In particular, there is no excuse for misspellings, nor for misspellings.

Date format

One potential source of confusion concerns the manner in which dates and times are formatted. Different companies and nations use different formats. For example, 03/5/06 could represent March 5, 2010 (United States) or 3 May 2010 (United Kingdom). In order to circumvent these difficulties, the international convention ISO 8601 (ISO 2004) can be used. It calls for dates to be formatted as follows: YYYY-MM-DD. So, May 3, 2010, would be 2010-05-03.

Active/passive voice

Most authors of style books recommend that writing be in the active voice. However, a mix of active and passive may be most appropriate. The passive is slightly more “professional,” whereas the active voice is more energetic, as can be seen from the following examples:

- The operator opened the valve (active).
- The valve was opened by the operator (passive).

He/she

In recent years, writers have been encouraged to avoid the use of just the male gender. The problem that this raises is that there is no neutral, singular word in the English language for a person of either gender. Hence, attempts to make writing more balanced and equitable also tend to make it more clumsy. There are four possible ways of addressing this issue.

The first is simply to ignore the problem. Although there has been a significant increase in the number of women working on process facilities, the fact remains that, at present, the great majority of workers are men, and the great majority of people who are hurt in industrial accidents are men.

A second approach is to use the word “they,” even when referring to persons in the singular. This is a little awkward, and it is grammatically incorrect. However, it can work quite well in some situations.

The he or she construct can make the overall writing very clumsy and unattractive. Also, it is possible to use the words “he” and “she” interchangeably (although this might break the train of thought of someone who is used to seeing the word “he” all the time).

Finally, it is often possible to finesse the issue by using words that describe the person’s actions or functions. If the text is discussing the work of scientists, e.g., it may often be feasible to use the word “scientist” rather than he or she.

You/I

One of the most important decisions regarding style is whether or not to use the word “you,” and hence speak directly to the reader, or else write in a more abstract manner. This decision probably depends on the nature of the audience and the subject matter it covers. For most professional reports, which are describing facts, situations, and considered opinions, use of the word “you” is not generally appropriate.

The word “I” should also be avoided unless it is clear that the writer is making a personal statement—e.g., in a report written by an expert witness.

Choice of words

When the French-speaking Normans invaded England in the year 1066, the native population was Saxon, and the language that they spoke was Anglo-Saxon (with other sources such as Scandinavian). This mixture of Saxon and French formed the foundations of modern English, and is one of the reasons that it is such a rich language: there are often two words that describe the same object, but each word has a slightly different connotation. For example, the Saxon word “cow” is used for the live animal walking around in a field. When it is killed and prepared for the table of the Norman rulers, it becomes “beef,” derived from the French word “boeuf.” Similarly, the animal “sheep” (Saxon) becomes mutton (French: “mouton”).

Even now, the social distinction between the two sources of words exists. Day-to-day English tends to use Saxon words. The use of French-based words suggest sophistication. Saxon words tend to be shorter and more pithy, whereas the French words are often longer, suggesting learning and culture.

Use of humor

There is no place for the use of humor in any professional report or publication for the following reasons.

Humor depends on surprise to make its effect. Given that a professional report is likely to be read many times, the surprise effect is quickly dissipated. After the first reading, the humor will become irritating and simply a nuisance. It is nonminimalist.

Generally, humor makes its effect by challenging the established order of things. To some degree, almost all humor is antiauthoritarian. Yet most reports are directed toward a professional community. Their aim is to improve existing systems, not to overturn them.

Some humor makes its impact by picking on differences among groups of people. Such an approach has no place in a professional report.

COPYRIGHT

Copyright law grants to the copyright holder exclusive control over the distribution and reproduction of that material. Copyright Law attempts to balance the intellectual property interest of authors and publishers with society's need for the free exchange of ideas. The pertinent U.S. law reads as follows:

> . . .lawful reproduction of protected materials requires the copyright owner's permission, except for copying which is authorized as "fair use" and for certain reproduction by qualified libraries.

"Fair use" copying has all of the following characteristics:

- The copy is made in lieu of taking manual notes.
- The copy is the reasonable portion of a given work. Reasonable portion is defined as nor more than 10% of the total pages, or one chapter of a published work that is not <10 pages, and is not an artistic work.
- The copy has a temporary use, primarily for study and use.

It is not fair use to:

- Make a copy to avoid purchasing an original
- Engage in systematic copying to avoid purchase or subscription
- Make multiple copies of material for distribution
- Use copies of copyrighted material in a company document, proposal, newsletter, manual, or employee newsletter without copyright clearance

RESPONSIBLE DOCUMENT CREATION

When writing documents, including emails, it is vital to make sure that what is written is accurate and is not likely to embarrass either the author or the company for which he or she works. The following guidance can help minimize potential problems.

- Before transmitting a document, examine it with "third party eyes" to see if it could be misconstrued or misinterpreted by a third party, maybe many months after the document was written.
- The language and the tone of the communication are important. They should be able to survive the "red face" test. If read to a jury, the communication should be calm in tone and defensible in content.
- Limit what is written to statements of fact. Sometimes, opinions have to be written down, but the document should never be emotional.
- It is a good idea to take a break before pushing the "send" button on an email that could be controversial or that is emotional in tone.
- Statements from others should always be relayed with qualification language such as "The contractor claims. . ." or "It is alleged."
- In particular, do not accept criticisms from third parties as being the factual truth.
- Do not write informally.
- Never use humor, satire, or irony.

- Minimize the number of people who are copied on an email.
- Emails are retrievable and discoverable. Any sensitive information should be conveyed by letter or in person.

ANECDOTES/STORYTELLING

> A man walks into a pet store and says “I want a talking parrot.”
>
> The clerk says “Yes sir, I have several birds that talk. This large green parrot here is quite a talker. He taps on the cage, and the bird says ‘The Lord is my Shepherd, I shall not want.’ He knows the entire Bible by heart. This one here is young, but he’s learning. He prompted ‘Polly want a cracker’ and the bird repeated back ‘Polly want a cracker’. Then I’ve got a mynah bird but he belonged to a sailor, so if you have children you won’t want that one.”
>
> The man says “I’ll take the young one if you can teach me how to make him talk.”
>
> “Sure I can teach you” says the clerk. He sat down with the man and spent hours teaching him how to train the parrot. Then he put the bird in a cage, took his money, and sent the man home.
>
> After a week, the man came back into the store very irritated. “That bird you sold me doesn’t talk.”
>
> “He doesn’t? Did you follow my instructions?” asked the clerk.
>
> “To the letter,” replied the man.
>
> “Well, maybe the bird is lonely. I’ll give you this little mirror to put in the cage. The bird will see his reflection and he will start talking right away,” responded the clerk.
>
> The man did as he was told but 3 days later he was back in the shop. “I’m thinking of asking for my money back, that bird still won’t talk.”
>
> The clerk pondered a bit and said “I bet the bird is bored. He needs some toys. Here take this bell—no charge. Put it in the bird’s cage. I’ll bet he will start talking as soon as he has something to do.”
>
> A week later the man was back, angrier than ever. He was carrying a shoebox. “That bird you sold me died.” He opened the shoebox and there was his poor little dead parrot. “I want my money back.”
>
> The clerk was horrified. “I’m so sorry, I don’t know what happened. But... tell me... did the bird even *try* to talk?”
>
> “Well,” said the man, “he did way one word, right before he fell off his perch and died.”
>
> “What did he say?” the clerk inquired.
>
> The man replied “F-o-o-d.”

Process risk analysts spend immense amounts of time communicating with charts, reports, slide packs, and safety meetings, i.e., with the mirrors and bells of the above story. These are important tools, but people need food—they need to have their feelings and emotions touched. And that is done through the use of stories.

For example, with regard to automation, a writer could say

> Modern process facilities are becoming so automated that there is very little need for human intervention.

Or else she could say

> When you fly over the offshore platform of the future you will see just two living beings: a man and a dog. The man’s job is to feed the dog; the dog’s job is to make sure that the man does not touch anything.

A fine example of effective storytelling is provided in a paper (Espinosa-Gala, 2004) that features the Deepwater Horizon/Macondo tragedy in human terms.

STORIES

The lesson to do with the importance of storytelling was recently driven home when your author when reading the first part of the Book of Exodus as part of a homework assignment. It's a real page turner, replete with the infant Moses in the bullrushes, the Pharaoh's daughter, the Nile full of blood, plagues of frogs and boils and locusts, the slaughter of first-born sons, and lambs' blood on doorposts. All of human life is there.

As part of the same study I read a modern, earnest, thoroughly researched book that explained these phenomena in sensible terms (e.g., the "blood" in the Nile could have been red soil washed down from the mountains of Ethiopia). The book further pointed out that there is little non-Biblical evidence of an exodus from Egypt. Guess which book caught my attention? The one that told the story, of course. The other book? Worthy as it was, I remember neither its title nor the name of the author.

ELEMENTS OF A STORY

A properly structured story has five elements:

1. Characters
2. Setting
3. Plot
4. Conflict
5. Resolution

Characters

Stories are about people. In the process industries, we cannot generally reveal names and personal details for both ethical and legal reasons. However, we can often identify the persons involved with a job title such as "Operations Superintendent" or "Lead Instrument Engineer." These titles usually give the reader enough information to visualize the persons involved and what their roles and responsibilities were likely to have been.

Setting

The setting is where the action takes place. The location for process safety events is usually clearly defined and can often be associated with pictures or videos. (There are exceptions. If one of the causes of an event was a design error, then the setting is likely to be a nondescript, air-conditioned office in a suburban office park.)

Plot

Events in the process industries may not have a plot in the sense of anticipating what happens. After all, it is usually the conclusion in the form of a fire or explosion that raises the initial awareness. Nevertheless, the multiple parallel timelines that converge on the final event provide the makings of an excellent plot.

Conflict

It is unusual for a process safety event to involve conflict between people (although it was a factor in the Deepwater Horizon catastrophe). However, conflicting departmental goals are often a factor—particularly the perceived clash between safety and "getting the job done." We may instill the mantra "There's always time to do a job safely" into people. But they do not always behave that way.

Resolution

The stories we tell should have a resolution. In the case of major events such as Piper Alpha or Deepwater Horizon, the resolution could be new ways of managing safety (Safety Cases) or the introduction of new regulations (SEMS). Even less dramatic stories should always provide guidance to better behaviors or improved management systems.

SENSITIVITY

Anecdotes—being a source of analogies—can be extremely valuable in illustrating what went wrong, and what actions can be taken to avoid a repeat of such incidents. The problem that those writing about such incidents have—particularly writers of public domain documents such as this chapter—is that information to do with real events is often sensitive, and may be controlled by the facility's legal department. One response to this difficulty is to create incidents which are loosely based on actual events, but where sufficient detail has been changed to protect confidentiality. However, this approach to the use of examples does not cover the use of pictures. With modern digital cameras, it is now extremely easy to take high quality pictures of the aftermath of an event. However, extreme care has to be taken with regard to the use of such pictures.

COMMUNICATING WITH THE PUBLIC

Industrial facilities do not operate in isolation; they are part of a larger community—a community that is often skeptical about their "polluting, dangerous" neighbor. Even remotely located facilities such as offshore oil and gas platforms have to be sensitive to public concerns. Therefore, effective public outreach and communications are an important and essential component of any safety management program.

Because risk is fundamentally a subjective topic: no single, mutually agreed upon value can be assigned to the term "acceptable risk," as discussed in Chapter 1. Therefore, the manner in which risk is communicated to members of the public has a profound effect as to the degree to which such risk will be accepted. If people *feel* that a risk is too high, then that risk *is* too high. People who actually work at a facility often have a good understanding as to the risks involved, and have usually learned to accept them. Moreover, the facility workers derive a direct benefit in the form of a paycheck from the operation, thus making the associated risk much more palatable. However, the general public is likely to be both much more ignorant about what is going on within a process facility, and far less willing to accept risks from which they derive little or no direct benefit. In many cases, the public's concern is often exacerbated by their lack of faith in the integrity of large institutions.

THE COMMUNITY

At the core of the topic of public communication lies a basic divergence of goals. On the one hand, the company managers wish to install and operate an industrial process to make money. The associated risk is part of the overall enterprise and can be managed in an objective, rational, and reasonable manner. The public, on the other hand, perceives that they are the ones actually exposed to the risks associated with the pipeline, yet they, as individuals, gain little or nothing from the existence of that pipeline. Although a good risk communication program can help close the gap between these two perspectives, it must always be recognized that the gap exists, and can never be entirely closed. Members of the public are not going to be "reasonable" if they feel that the safety or themselves or of their families is in jeopardy. Hence, any formal discussion in a public forum about the four elements or risk (hazards, consequence, likelihood, and safeguards) could easily create an impression that a smokescreen of words is being created, and that the communicator is dodging the real issues. Similarly, mathematical analyses of risks could create a problem that they, the managers of the pipeline, don't care about "our" feelings. The mathematical analysis may look like obfuscation. The public does not really understand the concept of probability—they only want certainties. Therefore, when talking with the public, the credibility of the communicator is more important than the objective facts associated with the communication.

Professionals analyze risk in an objective manner; they know that risk can never be eliminated—only controlled. The public, however, treats risk almost entirely in subjective and emotional terms. Management knows that risk can never be eliminated—only managed.

If an incident does take place, the more the public feel that they had been informed about the facility, the less likely they are to pursue aggressive litigation. (This may sound unlikely, but it has happened.)

The public, however, is not so analytical, as can be seen by the nature of questions such as the following:

- "What is the worst thing that can happen?"
- "How many people could be killed?"
- "How much material could get out?"
- "Could another Bellingham/Bhopal/Three Mile Island/. . . happen here?" (These names refer to industrial accidents that developed a high public profile.)
- "I live one block away, would I survive if this dangerous chemical is released?"
- "Are there any long-term health impacts?"
- "How do I know my child is safe when he or she is at school?"
- "How much have you spent to reduce emissions?"
- "Would you live here?"
- "What about sabotage?"
- "Do the emissions from your plant cause cancer?"

Many questions of the type listed above demand a “yes” or “no” answer; the inevitable nuances that a manager has to raise are treated as evasion.

In spite of the difficulties listed above, it is a premise of most risk management programs that communication is desirable. Such an assumption is a fundamental premise of much legislation, including the Seveso Directive and the EPA RMP. Nevertheless, many managers must wonder whether they should even bother trying to establish good relations with the public. These managers could take the attitude that they will do what they have to do to meet legal requirements, and leave it at that.

OTHER BUSINESSES

In addition to the public and the workers at a facility, other businesses in the area need to be informed as to the risks that are present, and to be invited to comment on those risks. In addition, if a cluster of industries in an area are part of a mutual support team, they must have quite detailed technical communications to do with their mutual risks.

THE MEDIA

Recognizing that much of the exposure that the community has to emergency issues is through the news media, key issues, or concerns that were raised by the news media may need to be addressed. Newspapers, television, and radio can all help inform the public about what to do in the event of an emergency. At the same time, facility managers must recognize that the goal of any media manager is to increase circulation or audience, and an effective way of doing this is to sensationalize problems and potential problems at industrial facilities.

REGULATORS/NONGOVERNMENTAL ORGANIZATIONS

The public often has a distrust of industry and agencies. Concern over the need for a facility to emphasize safety over profit, adhere to safe operating practices, and maintain the proper functionality of mitigation systems may be key issues for the public.

A strong risk communication program can also assist a company if there is a serious accident. The more the public knows ahead of time about the facility, the less likely they are to feel outrage. Also, the existence of the risk communication program will support the defense in any ensuring litigation.

TYPES OF PUBLIC COMMUNICATION

Public communications fall into two broad categories. First, the public has to be informed about the industrial process itself, and—in general terms—what risks it poses to the community. The second type of communication with the public concerns the public’s involvement in emergency response. Were the worst to happen, and there were to be a serious incident (either a fire or release of toxic materials), the correct response of people living in the neighborhood could easily be a matter of life or death. Community emergency notification, warning, and response issues should be addressed as part of the risk communication process.

DEVELOPING A RISK COMMUNICATION PROGRAM

Build relationships immediately.

- Interface contacts for community awareness are defined, documented, and understood.
- A program is in place to keep employees and the community informed regarding relevant safety, health, and environmental issues. Support units participate appropriately in the program of the primary operating organization.
- Employee and local community questions and concerns about company operations and facilities are solicited, evaluated, and addressed.
- Communication training is provided for personnel with employee and public communications responsibilities concerning company issues.
- Community awareness efforts are coordinated at sites occupied by more than one operating organization.
- The effectiveness of the community awareness program is regularly evaluated.
- Identification and notification procedures are in place for company facilities (e.g., pipelines) that are in the community.

COMMUNICATING NEW PARADIGMS

One feature of contemporary society is that people may intellectually understand issues such as Peak Oil or Global Warming, but they fail to internalize what they know and to change their own lives in response. The Business as Usual paradigm reigns. It could be that one reason for this lack of personal acceptance of these events is that almost all of the communication is in the form of reports, charts, and statistics, i.e., the bells and mirrors of the Dead Parrot story. Stories are needed.

In his post *Return of the Space Bats*, John Michael Greer (Greer, 2014) states "Most of what's kept people in today's industrial world from coming to grips with the shape and scale of our predicament is the inability to imagine a future that's actually different from the present… one way out of that trap is to learn more stories—not simply rehashes of the same plot with different names slapped on the characters… but completely different narrative structures that, applied to the same facts and logical relationships, yield different predictions."

TRADE SECRETS (OSHA)

The OSHA standard contains 14 elements. Of these, the topic of Trade Secrets is the only one that is basically nontechnical. OSHA wants to ensure that employees have access to the information that they need to carry out their job safely, regardless of Trade Secret concerns. A Trade Secret is some knowledge that is not formally patented, but that nevertheless gives companies a competitive edge. The term is defined by OSHA as follows:

A trade secret may consist of any formula, pattern, device or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it. It may be a formula for a chemical compound, a process of manufacturing, treating or preserving materials, a pattern for a machine or other device, or a list of customers. It differs from other secret information in a business (. . .) in that it is not simply information as to single or ephemeral events in the conduct of the business, as, for example, the amount or other terms of a secret bid for a contract or the salary of certain employees, or the security investments made or contemplated, or the date fixed for the announcement of a new policy or for bringing out a new model or the like. A trade secret is a process or device for continuous use in the operations of the business. Generally it relates to the production of goods, as, for example, a machine or formula for the production of an article. It may, however, relate to the sale of goods or to other operations in the business, such as a code for determining discounts, rebates or other concessions in a price list or catalogue, or a list of specialized customers, or a method of bookkeeping or other office management.

Secrecy

The subject matter of a trade secret must be secret. Matters of public knowledge or of general knowledge in an industry cannot be appropriated by one as his secret. Matters which are completely disclosed by the goods which one markets cannot be his secret. Substantially, a trade secret is known only in the particular business in which it is used. It is not requisite that only the proprietor of the business know it. He may, without losing his protection, communicate it to employees involved in its use. He may likewise communicate it to others pledged to secrecy. Others may also know of it independently, as, for example, when they have discovered the process or formula by independent invention and are keeping it secret. Nevertheless, a substantial element of secrecy must exist, so that, except by the use of improper means, there would be difficulty in acquiring the information. An exact definition of a trade secret is not possible. Some factors to be considered in determining whether given information is one's trade secret are: (i) the extent to which the information is known outside of his business; (ii) the extent to which it is known by employees and others involved in his business; (iii) the extent of measures taken by him to guard the secrecy of the information; (iv) the value of the information to him and his competitors; (v) the amount of effort or money expended by him in developing the information; and (vi) the ease or difficulty with which the information could be properly acquired or duplicated by others.

Novelty and Prior Art

A trade secret may be a device or process which is patentable, but it need not be that. It may be a device or process which is clearly anticipated in the prior art or one which is merely a mechanical improvement that a good mechanic can make. Novelty and invention are not requisite for a trade secret as they are for patentability. These requirements are essential to patentability because a patent protects against unlicensed use of the patented device or process even by one who discovers it properly through independent research. The patent monopoly is a reward to the inventor. But such is not the case with a trade secret. Its protection is not based on a policy of rewarding or otherwise encouraging the development of secret processes or devices. The protection is merely against breach of faith and reprehensible means of learning another's secret. For this limited protection, it is not appropriate to require also the kind of novelty and invention which is a requisite of patentability. The nature of the secret is, however, an important factor in determining the kind of relief that is appropriate against one who is subject to liability under the rule stated in this Section. Thus, if the secret consists of a device or process which is a novel invention, one who acquires the secret wrongfully is ordinarily enjoined from further use of it and is required to account for the profits derived from his past use. If, on the other hand, the secret consists of mechanical improvements that a good mechanic can make without resort to the secret, the wrongdoer's liability may be limited to damages, and an injunction against future use of the improvements made with the aid of the secret may be inappropriate.

The following situations may require that employees have access to material that may be protected by Trade Secret law.

- Development and compilation of Process Safety Information
- A PHA investigation
- Development of Operating Procedures

- Incident Investigation
- Preparation of Emergency Plans
- Audits

The PSM regulation concerning Trade Secrets is provided below. The key words in terms of implementing process safety are in the final clause of paragraph (1).

1. Employers shall make all information necessary to comply with the section available to those persons responsible for compiling the process safety information (required by paragraph (d) of this section), those assisting in the development of the PHA (required by paragraph (e) of this section), those responsible for developing the operating procedures (required by paragraph (f) of this section), and those involved in incident investigations (required by paragraph (m) of this section), emergency planning and response (paragraph (n) of this section) and compliance audits (paragraph (o) of this section) without regard to possible trade secret status of such information.
2. Nothing in this paragraph shall preclude the employer from requiring the persons to whom the information is made available under paragraph (p)(1) of this section to enter into confidentiality agreements not to disclose the information as set forth in 29 CFR 1910.1200.
3. Subject to the rules and procedures set forth in 29 CFR 1910.1200(i)(1) through 1910.1200(i)(12), employees and their designated representatives shall have access to trade secret information contained within the PHA and other documents required to be developed by this standard.

Usually, a Trade Secret is used to protect some technique or operation that the company has developed to give itself a competitive advantage. Unlike, new technology, ideas, and techniques covered by Trade Secrets cannot be patented. OSHA recognizes that there is a potential conflict between the Workforce Involvement of the PSM standard and a company's right to protect its competitive advantages. OSHA insists that employees must have access to the information that they need to carry out their work safely. However, there are ways in which employers can protect their rights.

When preparing the process safety standard, OSHA realized that Trade Secrets could be used by employers to prevent employees from learning information critical to the safety of the facility. Therefore, OSHA explicitly stated that Trade Secrets cannot be used as a reason for not complying with the process safety standard—which includes operating procedures.

In practice, this restriction need not be a significant problem. First, an employer can ask employees to sign a confidentiality agreement. In this agreement, employees (including contract workers) will agree to use the protected information for safety purposes only, and they agree not to divulge it to anyone outside the company. Second, a company need only reveal the information necessary for safety. For example, if the employees need to know the flash point for a chemical, but this does not mean that the company must also reveal the formula of that chemical. Third, companies can use code words to hide sensitive information. If they have a proprietary catalyst, e.g., they may simply choose to identify as X-12, rather than revealing its correct chemical name.

Table 20.1 provides an example of a Trade Secrets secrecy form that an employee could be asked to sign.

A trade secret is any information that can be used in the operation of a business or other enterprise that is sufficiently valuable and secret that it affords an actual or potential advantage over others

A trade secret can consist of any of the following:

- A formula
- A pattern

Table 20.1 Sample Trade Secret Form

I, ________________________ (name, address, and other personal information here) agree to keep all information in confidence relating to the design of equipment, process flow schemes, and yields less than six months old that I might learn from the records and files of COMPANY, and not to transmit or discuss this information with persons or organizations that have not entered into a secrecy agreement with or release from COMPANY. This agreement is in exchange for being allowed to enter the files and records of COMPANY for information pertaining to §1910.119, Process Safety Management of Highly Hazardous Materials.

- Compilation of data
- Software
- A device or device design
- Marketing or pricing techniques
- Customer lists and customer information
- A method, technique, or process
- Other forms of economically valuable information

Some of the steps that can be used for protecting trade secrets are listed below.

- Determine what is a trade secret so that the correct information is protected
- Put a trade secret stamp or label on secret material or data
- Ensure that confidentiality and nondisclosure agreements have been entered into with anyone who may access the information
- Apply a “need to know” system
- Use passwords and other devices to secure computers
- Ensure that all hard copy information is locked up
- Shred and dispose of any hard copy information that is no longer needed
- Require all employees and other workers with access to information to sign a confidentiality or nondisclosure agreement, and have the agreement resigned every year
- Audit confidential information to see if anything is missing or changed

When preparing the PSM standard in the late 1980s, OSHA realized that Trade Secrets could be used by employers to prevent employees from learning information critical to the safety of the facility. Therefore, OSHA explicitly stated that Trade Secrets cannot be used as a reason for not complying with the process safety standard.

In practice, this restriction need not be a significant problem. First, an employer can ask employees to sign a confidentiality agreement. In this agreement, employees (including contract workers) will agree to use the protected information for safety purposes only, and they agree not to divulge it to anyone outside the company. Second, a company need only reveal the information necessary for safety. For example, if the employees need to know the flash point for a chemical, but this does not mean that the company must also reveal the formula of that chemical. Third, companies can use code words to hide sensitive information. If they have a proprietary catalyst, e.g., they may simply choose to identify as X-12, rather than revealing its correct chemical name.

LITIGATION SUPPORT

This is a technical book. Guidance to do with legal matters should be provided by a qualified attorney.

Professionals working in the process risk and PSM areas will sometimes be called upon to provide litigation support. They may serve as witnesses to fact, i.e., they provide information concerning the incident being litigated. Or else, as expert witnesses, they provide independent opinion as to the causes of an incident. Whatever their role, the risk management professional must never forget that he or she is a technical expert only; it is the attorneys and judges who are the experts in law. He or she should never offer legal opinions or try to direct the case in any way. However, the technical expert cannot allow the attorneys to tell him what to say or write.

Both types of witness should keep careful records of what they said, when they said it, and what was said to them during the duration of the case. However, after consultation with the attorneys, the expert may choose to discard draft reports.

Generally, technical professionals work one another in a reasonably cooperative manner; their goal is to find the most effective ways of minimizing health, safety, and environmental problems, not to win a dispute. Attorneys, however, want to win, which means that they want the other side to lose. Consequently, attorneys will aggressively challenge risk management experts by challenging their technical expertise and by trying to prove them wrong in any way possible. The courts are not primarily interested in raising the standards of process risk and safety management—they are interested in resolving differences of opinion. This disputatious atmosphere means that most technical professionals do not find that working with attorneys is their favorite pastime. For example, experts can become defensive when their credentials and expertise are challenged (particularly if such a challenge is indeed unfair). Yet such challenges will inevitably occur. Indeed, the attorney asking the questions may intend to upset the witness so as to reduce his or her credibility before the jury.

USE OF LEGAL SERVICES

It is important that employees know when to inform their legal department whenever there has been a significant event or if there has been a communication with an outside party that could have legal consequences. These circumstances include the following:

- Incidents involving fatalities, serious personal injuries, a major environmental event, or property damage that could result in significant financial exposure.
- When an incident has occurred that could result in either the Company or an employee of the Company being exposed to legal action.
- During an incident investigation.

TYPES OF LITIGATION

A risk management professional is most likely to be involved in one of the following three types of litigation.

1. Follow-up to a citation from a government agency. (Most citations are resolved before litigation commences, but the risk management expert may still be involved in the negotiating process.)
2. Involvement in civil suits brought against a company. Examples include worker compensation claims or responding to a public interest group claiming that a release has caused serious damage to the environment.
3. The third type of litigation is criminal prosecution. In the event of a very serious incident, the authorities may charge a company and/or individuals within that company with a criminal violation.

THE PARTICIPANTS

The principal participants involved in a lawsuit are listed below (this list is based on the Anglo-American system of justice where a jury normally makes the ultimate decisions with regard to the facts of the case).

- The judge
- The jury
- The plaintiff
- The defendant
- The attorneys on each side
- Witnesses to fact
- Expert witnesses

TIMELINE/STORY LINE

Major incidents usually require that an unusual, even bizarre, set of events take place because most of the predictable accident scenarios have already been considered, and corrective action taken. Given, therefore, that most incidents are complex and even strange, one of the most important roles of a risk management professional is to explain to the court just what happened in terms and language that they can understand.

The story line should be factual and not offer analysis or opinion. If assumptions are made, they should be clearly stated.

DOCUMENTATION

When documenting risk management work, it is important to understand that the information recorded may, if there is a serious accident or an audit, be introduced brought into the formal investigation process (unless protected by client/attorney privilege). Documentation may be called for by agency representatives, such as OSHA, or counsel representing plaintiffs in litigation. Therefore, the following points should always be considered:

- Documentation should confine itself to facts and sound engineering judgment. It should not contain any speculation, particularly to do with major accident scenarios. Any estimates as to possible incidents (such as occurs during a PHA) should be based on professional judgment and plant experience.
- Draft documents should be disposed of as soon as they are no longer relevant or correct. All drafts should be destroyed prior to the issue of a final report or document. Not only does this practice reduce the potential for problems in an investigation, it also reduces the chance of internal confusion. The control of draft documentation is difficult to enforce. It is likely that each person involved with the program will have his or her own copies of documents such as P&IDs and operating procedures. They will also probably have made notes in their diaries and files. If there is an accident, those notes become part of the official record. Yet people are reluctant to throw such documents away because "you never know when they might come in handy." Nevertheless, these documents must be discarded. (In this regard, the increased use of electronic document management systems should reduce dependence on old printed reports).
- All recommendations and action items must be followed through to closure in a timely manner, and the closure should be properly documented.
- Documentation should avoid the use of emotional or potentially inflammatory language. Generally, words such as "catastrophe" and "tragic" should be avoided. Documentation should also avoid judgmental words like "serious" or "unacceptable." However, there is nothing wrong with using factual words or phrases such as "fire" or "rapid corrosion."
- When selecting a recommendation from a variety of solutions, it is important to show how it was chosen, especially if it happened to be the cheapest option.
- There should never be any indication that safety was traded off against cost, nor that a safety recommendation was not implemented because it was too expensive.
- The documentation should not imply that levels of "acceptable risk" have been determined. Instead the use of risk matrices, as discussed earlier in this chapter, should show that high risk items are being addressed before those of lower risk—there is no attempt to determine absolute risk.
- All personnel should be taught how to answer audit questions, i.e., how to be open and honest but not to volunteer any information that has not been asked for.

THE DISCOVERY PROCESS

The early stages of a suit involve the discovery of information pertinent to the case. Both sides search for documents that can help support its case. These documents include drawings, training records, log books, contracts, data sheets, letters, emails, reports, and design calculations.

Relevant documents must never be destroyed. Nor should there be any suggestion that such documents be destroyed, concealed, or altered.

DEPOSITIONS

Generally, the first formal phase of the litigation process is for witnesses (fact and expert) to be deposed. They are questioned by attorneys of both sides, usually in a conference room setting. A judge is not present. Their deposition is videotaped for possible use in later stages of the trial.

The questioning in depositions is often wide ranging—the attorneys are often fishing for ideas and information. Once the deposition is complete, the witness is asked to read and sign a copy of what he or she said.

Many cases are resolved "on the court house steps," i.e., a negotiated agreement is reached before going to trial. This means that the expert's involvement goes no further than being deposed and writing a report for the attorneys he is working for.

WITNESSES TO FACT

A witness to fact tells the court what he or she observed—he or she is neither required nor allowed to offer interpretation or analysis. For example, when testifying to an event in a process plant, the witness to fact is allowed to state that the pressure in a reactor rose very rapidly, and that it ruptured soon afterwards. He or she is not allowed to add a comment such as "...the pressure rose rapidly as a result of a runaway reaction in this reactor." Such a comment is an interpretation of events, not a mere statement of observed facts.

Sometimes, technical experts who work at a facility and who are called on to provide factual information only are frustrated that they are not allowed to present their opinions. After all, there are probably few people who know more about the process in question than they do.

A witness to fact may be able to offer an implicit analysis. For example, the facility's mechanical engineer is not allowed to say "The relief valve failed to open due to internal corrosion." In this statement, the engineer is creating a cause and effect. His analysis may be correct, but is not an observation. However, what the engineer can say is "The relief valve failed to open. When the relief valve was removed following the accident, I observed that its internals were corroded."

THE EXPERT WITNESS

Most cases involving safety, environmental, and health problems are highly technical. Such cases often require the services of an expert witness to explain the issues involved. Unlike the witness to fact, the expert witness has no first-hand knowledge of the facts of the case. His knowledge is limited to postevent information sources, such as the depositions, reports of other experts, laboratory tests, and site inspections. The expert is being asked to offer his or her opinion, and to interpret a complex set of events so that the court can make a well-informed decision. (Not all experts testify. A nontestifying consultant will provide advice to the party by which he is retained. However, this type of consultant will neither be deposed, nor be asked to appear in court.)

The most common reasons for using an expert witness include:

- A law or regulation was not followed, and a government agency is taking action against the alleged offender (which could either be a company or individuals working within the company).
- Someone is injured or killed in an industrial accident. They or their family claim damages through the court system.
- An accident leads to serious financial loss, resulting in a claim for damages from a customer, or someone else who suffers follow-on loss. (Insurance companies may also reduce payment, depending on the nature of the accident.)

In order to make an informed and fair decision, the court (the judge and jury) often have to evaluate complex, technical facts that are outside their own areas of expertise. An expert witness helps the court understand and evaluate complex and specialized topics. For example, if a worker is injured, and sues his employer for damages, at least three types of expert are likely to be needed:

- A doctor or medical specialist to explain the nature of the worker's injuries, and the likely effect on his or her ability to work in future.
- An engineer or scientist to explain how the accident happened, and where blame should be placed.
- An economic expert to evaluate the effect of the accident on the worker's financial future.

If a technical expert is asked to serve as an expert witness, there is absolutely no obligation to agree to do so, particularly if he feels that he may be expected to make statements that do not square with the facts. (Many technical experts refuse to serve as expert witnesses at all—they feel that their integrity will inevitably be compromised.) The expert should also feel personally comfortable working with his or her attorneys. In particular, the expert must feel that the attorneys are allowing him or her freedom to state their honest opinion. If an expert does feel that he or she cannot continue with the case, then he should do so as soon as possible. After all, most experts are retained (i.e., paid) by one set of attorneys, so those experts can be faced with a potential conflict of interest.

In most cases, the technical expert will be called upon to help the court answer one or more of the following three questions:

1. What happened?
2. What were the causes?
3. Who was at fault?

They typically carry out calculations and analyses, perform tests or measurements, and they evaluate or critique the work of others—including other expert witnesses.

ACCEPTANCE BY THE COURT

Before an expert witness can testify in court, he or she has to be accepted by the court—specifically by the judge. Only then does his or her testimony become admissible. The expert witness does not need to be overly concerned about the criteria for being accepted; he or she should concentrate on his or her own professional expertise.

Before accepting the testimony of an expert witness, the judge will want to know that the expert really is an expert, and will the expert's knowledge and expertise help the judge and jury reach the proper decision regarding the outcome of the trial. Therefore, the judge may hold a hearing to evaluate the credentials of the expert witness. The statements made by the expert during the hearing can be used later in the deposition process and in the trial. During the hearing, the judge will want to know if the expert's knowledge is current, tied to widely accepted principles in that area of specialty, and grounded solidly in both theory and day-to-day practice.

DAUBERT AND *FRYE* RULES

In the case of *Daubert v. Merrell Dow Pharmaceuticals, Inc.* (1993), the U.S. Supreme Court ruled that the trial judge should function as a gatekeeper who allows the jury access to expert testimony only after the court has made an initial determination regarding the scientific reliability and relevance of that testimony, and of the proposed experts witnesses. The *Daubert* Rule applies to federal courts and to some states. It is gaining increased recognition and use.

The judge may hold a hearing to evaluate the credentials of the expert witness. The statements made by the expert during the hearing can be used later in the deposition process and in the trial. During the *Daubert* hearing, the judge will want to know if the expert's knowledge is current, tied to widely accepted principles in that area of specialty, and grounded solidly in both theory and day-to-day practice.

The *Frye* Rules, which do not apply to all states, are used to validate expert testimony. They require the following criteria:

- Established, recognized methods and standards should be used wherever possible.
- New or innovate procedures or test methods require verification through third party analysis and publication.

PRIOR TESTIMONY

With regard to prior testimony and his or her resumé, the expert has a decision to make. Including information about such testimony will be a convenience for the opposing attorney, and may help him or her find prior statements made by the expert that conflict with the current testimony. However, if the expert is to be true to himself, he should identify cases in which he was involved, otherwise he is opening himself up to the question "Since you have hidden this work experience, what else are you hiding—indeed why should the jury trust you at all?"

TIMELINE/STORY LINE

Most incidents to do with process risk and safety are unusual and complex—after all, most of the predictable accident scenarios have already been considered and corrective action taken. This means that one of the most important roles of an expert witness is to explain to the court just what happened in terms and language that they can understand. The story line should be factual and not offer analysis or opinion. If assumptions are made, they should be clearly stated.

As the case progresses, an expert witness can help the attorneys identify which documents are needed, particularly as more is learned about the circumstances of the accident or event. The expert will often try to recreate a sequence of events based on limited data or information.

THE REPORT

The expert witness will probably be asked to write a report. This report will be shared with the opposing attorneys and can be referred to in depositions. All of the comments to do with careful report writing discussed above should be followed. In particular, the report should confine itself to facts and sound engineering judgment. It should not contain any speculation, but it can contain professional judgment.

ATTRIBUTES OF AN EXPERT WITNESS

It is suggested in this chapter that an expert witness should follow the four guidelines listed below, and amplified in the following Volumes:

- To Thine Own Self Be True
- Be Prepared
- Be a True Expert
- Be a Teacher

To thine own self be true

Because he or she is offering an opinion, an expert witness must follow Polonius' precept "...to thine own self be true." An expert has to be honest in his or her opinions. If he or she states that "such and such is my professional opinion," that statement really must represent his or her opinion. An expert witness must be a person of integrity—no ifs, buts, or maybes.

The potential primary conflict of interest issue to be addressed by expert witnesses is that they are expected to provide objective analysis, yet their fee is being paid by an attorney representing one of the parties to the case. The expert can support his or her client, while maintaining integrity, by realizing that he or she is not obliged to present all sides of the case. All questions must be answered truthfully, and all reports must be complete and correct, but the expert is not obligated to present information that is advantageous to the other attorneys. In addition, all parties to a lawsuit are entitled to legal representation. This representation includes the opportunity to have an expert represent those parties.

Be prepared

Being an expert witness is hard work. He or she must study all the pertinent documentation, appropriate rules and regulations, and the depositions that have already been taken. He must try to avoid ever being taken by surprise by the revelation of some fact that he should have known about.

Be a true expert

Part of being "true to yourself" is in deciding if they are qualified to assist with the case in hand. It is not enough to know "about" the matter in hand—the expert really must be an expert. One of the traps that experts can fall into is that, if they fail to keep up with the latest knowledge and practice in their field, they may not really be qualified to testify—even though they believe that they are. They may fail to recognize that their knowledge and judgment is out of date.

Be a teacher

One of the central roles of an expert witness is to explain to the court (particularly the judge and jury) the circumstances of the case. Therefore, the expert must concentrate on communicating his or her expertise to a group of people who have little or no knowledge in the specialist area. This means that the expert has to strike a balance between explaining technical concepts in simple terms, and being perceived as “talking down” to the jury. Therefore, the expert must avoid any perception of arrogance, and he or she must be very careful not to use technical words that may not be familiar to the court (or that have a specialized meaning that differs from normal language). The expert must be sensitive to the fact that words used technically can have different meanings to the general public. For example, the word “risk” has been defined throughout this book in considerable detail. Yet members of the public use the same word in a much more general sense.

The expert must always remember that he or she is imparting neutral information and opinion, and must try not to become emotional, or to get into an argument with the questioning attorney (this is easy to say, but hard to do).

“Reasonable” risk

The concept of “acceptable risk” has been discussed in Chapter 1. Given that risk is, at its root a subjective concept, terms such as “acceptable risk” and “reasonable risk” will necessarily mean different things to different people. Engineers and scientists are used to thinking of risk in terms of 90%−99% confidence levels. However, the public and the legal community may consider a risk to be reasonable if it is merely >50%.

PRIVILEGE

Experts working with attorneys will often use the concept of attorney−client privilege. As always in this chapter, the comments provided below are general in nature; specific guidance should be obtained from a qualified attorney.

The basic idea behind attorney/client privilege is that communications with a professional legal advisor can be held in confidence (similar types of privilege can exist between a husband and wife or a religious counselor and a parishioner). Privilege protects communications, not facts. For example, if someone is asked if the valve was open immediately prior to an incident he or she cannot respond “I discussed that with my attorney, and hence the information is privileged.” However, the witness can claim privilege if asked “What did you tell your attorney about the status of the valve?”

Attorney−client privilege is commonly invoked if the event led to serious injury, death, or large economic loss. The attorney work−product privilege protects an attorney’s investigation, preparation, and evaluation of a potential claim or actual lawsuit. These privileges permit a company’s attorney to learn in confidence all facts about a legal matter so that the attorney can then provide legal advice to the company. It can be lost by divulging, to a third person, the subject matter of the communication. The following is a representative company policy statement with regard to privilege.

> Communications between attorneys and clients, where legal advice is being sought and rendered, is privileged. This would include communications concerning an incident or its investigation and analysis of an incident between attorneys in Legal Services and the Company or employees/agents of the Company. In order to preserve this privilege, such communications may not be distributed outside the incident investigation team and other specifically designated personnel. Written communications between the attorney(s) working on the investigation and analysis and

members of the incident investigation team and other designated personnel concerning the incident analysis shall be marked as follows:

PRIVILEGED AND CONFIDENTIAL

ATTORNEY CLIENT COMMUNICATION

Any documents bearing this marking must be stored and maintained in a confidential and secure location, which is not open to review by individuals outside the scope of the investigation and analysis. This privilege does not protect the disclosure of the facts involved in the incident.

In order to create and maintain privilege, the following guidelines can be followed:

- Maintain separate files for project activities and legal advice
- Privileged documents must be stamped: "attorney/client work product. Privileged and confidential. Do not disclose, mark on, or copy"
- Create a system for labeling, recording, and controlling investigation-related documents
- Report directly to the attorneys, not the normal line managers
- Do not discuss the event with anyone outside the investigation team, the designated facility management, and the company attorney assigned to the investigation
- Limit access to the legal advice files
- Clearly mark privileged documents as such (however, merely marking documents as such does not make them privileged)
- Recognize that facts that are otherwise discoverable on their own are never privileged
- Do not circulate communications beyond the individuals necessary for making decisions or gathering necessary information
- Ensure that the mechanism of communication is secure

References

Allen, G., 2011. Limit the damage from a vapor cloud loss. Hydrocarbon Processing.

American Industrial Hygiene Association, 2009. ERPG/WEL Handbook.

ANSI (American National Standards Institute), 2005. Overview of the U.S. Standardization System.

API (American Petroleum Institute), 2013. Recommended Practice for Qualification Programs for Offshore Production Personnel Who Work with Safety Devices. Recommended Practice T-2.

API (American Petroleum Institute) RP 754, 2010. Process Safety Performance Indicators for the Refining and Petrochemical Industries.

Arendt, S., 2009. Evaluate HSE/Process Safety Culture. LAI/MEP Forum, Lake Charles, LA.

Ayral, T., de Jonge, P., 2013. Operator training simulators for brownfield process units offer many benefits. Hydrocarbon Processing.

Baker, J., 2007. The Report of the U.S. Refineries Independent Safety Review Panel.

Baybutt, P., 2003. Major hazards analysis: an improved method for process hazards analysis. Process Saf. Prog.

BOEMRE (Bureau of Ocean Energy Management, Regulation and Enforcement), 2010. 30 CFR Part 250.

BOEMRE (Bureau of Ocean Energy Management, Regulation and Enforcement), 2011. Report Regarding the Causes of the April 20, 2010 Macondo Well Blowout.

Bradley, V., 1996. Empowering safety teams. Texas Chemical Council Safety Seminar, Galveston, TX.

Brander, R., 1995. The Titanic Disaster: An Enduring Example of Money Management vs. Risk Management. <http://www.cuug.ab.ca/˜branderr/risk_essay/titanic.html>.

Broadribb, M., 2008. 3 Years on from Texas City. In: 4th Global Congress on Process Safety.

Brogan, J.A., 2000. Clear Technical Writing, Career Education.

BSEE (Bureau of Safety and Environmental Enforcement), 2012a. Draft Safety Culture Policy Statement.

BSEE (Bureau of Safety and Environmental Enforcement), 2012b. Interim Policy Document. Issuance of Incident of Non Compliance (INC) to Contractors.

Carpenter, C., 2013. Abnormal situation management in offshore operations. J. Petrol. Technol.

CCPS (Center for Chemical Process Safety), 1994. Guidelines for Implementing Process Safety Management Systems.

CCPS (Center for Chemical Process Safety), 2003. Guidelines for Investigating Chemical Process Incidents. American Institute of Chemical Engineers, New York, NY.

CCPS (Center for Chemical Process Safety), 2007. Process Safety Leading and Lagging Metrics. American Institute of Chemical Engineers, Center for Chemical Process Safety, New York, NY.

CCPS (Center for Chemical Process Safety), 2011. Auditing Process Safety Management Systems, second ed.

Coast Guard (United States Department of Transportation), 2001. Chemical Hazards Response Information System (CHRIS).

Crumpler, D., Whittle, D., 1996. How to effectively revalidate PHAs. Hydrocarbon Processing.

CSB (U.S. Chemical Safety and Hazard Investigation Board), 2007. Investigation Report No. 2005-04-I-TX Refinery Explosion and Fire.

Cullen, D., 1990. The Public Inquiry into the Piper Alpha Disaster. Department of Energy, London.

Davenport, J.A., 2006. History of the Loss Prevention Symposia: Forty Years, 1967–2006. Process Saf. Prog.

DeWitt, L.A., 2005. Developing, Implementing and Managing a Risk-Based Safety and Health Auditing Process. American Society of Safety Engineers.

Dow's Fire & Explosion Index Hazard Classification Guide, seventh ed. 1994. American Institute of Chemical Engineers (AIChE).

Dow's Chemical Exposure Index Guide, first ed. 1998. American Institute of Chemical Engineers (AIChE).

Einolf, D.M., Menghini, L., 2007. Acquisition of the PSM-Subject Facility: Considerations in Due Diligence.

Espinosa-Gala, L., 2004. The Final Tipping Point. Society of Petroleum Engineers. Aberdeen, Scotland.

Farrell, K.V., 2008. Investigation Process for Industrial Accident Scenes. Mary Kay Process Safety Center.

Gano, D.L., 2007. Apollo Root Cause Analysis. Atlas Books.

Gell, C., Schilling, L., 2008. Empowering Young Professionals to Lead After "The Big Crew Change." Society of Petroleum Engineers. Paper No. 115341.

Geyer, T., et al., 1990. Prevent pipe failures due to human errors. Chem. Eng. Prog.

Goldacre, B., 2008. Bad Science. Faber and Faber.

Greer, J.M., 2014. Return of the Space Bats. Available from: <http://thearchdruidreport.blogspot.com/2014/01/return-of-space-bats.html>.

Hadden, S., 1990. Risk communication: some guidelines. Chem. Process.

Henderson, P., 2013. Will Dreamliner drama affect industry self-inspection? Reuters.

Henley, E., Kumamoto, H., 1981. Reliability Engineering and Risk Assessment. Prentice Hall, Englewood Cliffs, NJ.

Hipple, J., 2008. Improving Check Listing with Predictive Failure Analysis.

Holder, J., 2004. Environmental Assessment: The Regulation of Decision Making. Oxford University Press, New York, NY.

Hopkins, A., 2000. Lessons from Longford: The Esso Gas Plant Explosion. CCH Australia Ltd.

International Maritime Organization (IMO), 2002. Guidelines for Formal Safety Assessment (FSA) for Use in the IMO Rule-Making Process.

ISO 17776:2000(E), 2000. Petroleum and natural gas industries—Offshore production installations—Guidelines on tools and techniques for hazards risk assessment.

Juran, J.M., 1951. Quality Handbook. McGraw-Hill, 1999 (Republished).

Kletz, T., 1993. Lessons from Disaster: How Organizations Have No Memory and Accidents Recur. Institution of Chemical Engineers, Rugby, UK.

Kletz, T., 1997. Reliab. Eng. Syst. Saf. 55 (3), 263.

Knowlton, R., 1992. An Introduction to Hazard and Operability Studies, The Guide Word Approach.

Lapp, S., 2005. Applications of fault tree analysis to maintenance interval extension and vulnerability assessment. Process Saf. Progress.

Lawley, H.G., 1976. Size up plant hazards this way. Hydrocarbon. Processing.

Lees, F., 2004. Loss Prevention in the Process Industries. Elsevier, Burlington.

Maher, S., Norton, K., Surmeli, S., 2011. Using the HAZID Study, HAZOP Study and LOPA to generate ideas for inherently safer designs. AIChE.

Mannan, M., West, H., Krishna, K., Aldeeb, A., Keren, N., Saraf, S., et al., 2005. The legacy of Bhopal: the impact over the last 20 years and future direction. J. Loss Prevent. Process Ind. 18 (4–6).

Mostia, B., 2003. Avoid error. Chem. Process.

Muhlbauer, W., 2003. Pipeline Risk Management Manual, third ed. Gulf Professional Publishing.

NEB (National Energy Board), 2013. Draft Safety Culture Definition and Framework.

NFPA 704, 2012. The Standard System for the Identification of the Hazards of Materials for Emergency Response.

Nelms, C.R., 2007. The Problem with Root Cause Analysis.

NIOSH (the National Institute for Occupational Safety and Health, 2004. Chemical Listing and Documentation of Revised IDLH Values.

NRC (Nuclear Regulatory Commission), 1975. Reactor Safety Study: An assessment of accident risks in U.S. commercial nuclear power plants.

OGP (International Association of Oil & Gas Producers), 2011. Recommended Practice on Key Performance Indicators. Report No. 456.

OGP (International Association of Oil & Gas Producers), 2013. Safety Performance Indicators 2012.

Olesky, J., 2012. Diminishing Returns, Diminishing Awareness. The Overuse of Reflective Vests.

OSHA (U.S. Department of Labor, Occupational Safety & Health Administration), 1992. Process Safety Management of Highly Hazardous Chemicals. 29 CFR 1910.119.

Ostrowski, S., Keim, K., 2008. A HAZOP methodology for transient operations. In: 11th Annual Symposium, Mary Kay O'Connor Process Safety Center.

O'Toole, M.F., Nalbone, D., 2005. Is the Safety Climate a Barometer of Safety Results? American Society of Safety Engineers.

Overton, T., Berger, S., 2008. Process safety: how are you doing? Chem. Eng. Progress.

Paradies, M., 2008. TapRooT® - Changing the Way the World Solves Problems.

Parkinson, G., 2013. Professional bureaucracy. Chem. Eng.

Pasquill, F., 1961. The estimation of the dispersion of windborne material. Meteorol. Mag. 90 (1063).

Philley, J., 2011. Structured What-if Approach to Process Hazards Analysis. 24th Annual TCC/ACIT EHS Seminar.

Pitblado, R., 2008. Global process industry initiatives to reduce major accident hazards. In: 11th Annual Symposium, Mary Kay O'Connor Process Safety Center.

Sanders, R.E., 1992. Small Quick, Changes Can Create Bad Memories. Chemical Engineering Progress.

Saraf, S., 2009. Forecast for process safety in the 21st century. Hydrocarbon Processing.

Schubert, P., 2011. Lessons learned from inspection of 25,000 upstream oil and gas wells and associated plants. In: 7th Global Congress of Process Safety.

Slovic, P., 1992. Perception of risk: reflections on the psychometric paradigm. Soc. Theories Risk 95−108.

Soczek, C., 2011. A key factor in hazardous processes: safety culture. In: 7th Global Congress on Global Safety.

Stahl, M., Kenady, K., 2011. A frequency based approach to hole size selection for consequence analysis. In: 7th Global Congress on Process Safety.

Strunk, W., White, E.B., 2000. The Elements of Style. Longman.

Sutton, I.S., 1997. Process Safety Management. Sutton Technical Books, Houston, TX.

Sutton, I.S., 2008. Use root cause analysis to understand and improve process safety culture. Process Saf. Progress.

Taleb, N.N., 2007. The Black Swan: The Impact of the Highly Improbable.

Thomas, P., Reidar, B., Bickel, J., 2013. The Risk of Using Risk Matrices. Society of Petroleum Engineers.

Toghraei, M., 2014. Principles of P&ID Development. Chem. Eng.

Transportation Research Board Special Report 309: Evaluating the Effectiveness of Offshore Safety and Environmental Management Systems, 2012.

Vancauwenberghe, W., 2011. The Basics of Safe Maintenance: What Can We Learn from a Survey on Safe Maintenance? BEMAS—Belgian Maintenance Association.

Vesely, W., 1981. Fault Tree Handbook.

Vincoli, J.W., 1997. Making Sense of OSHA Compliance.

Walker, V., 2009. Designing a Process Flowsheet.

Whipple, T., Pitblado, R., 2008. Applied risk-based process safety: a consolidated risk register and focus on risk communication.

Wilson, A., 2013. Safety-management leading indicator results in unintended consequences. J. Petroleum Technol.

Index

Note: Page numbers followed by "*t*" refers to tables.