CHAPTER

Operational integrity management

1

CHAPTER CONTENTS

INTRODUCTION

The first edition of this book was published in the year 1997 with the title *Process Safety Management (PSM)* (Sutton, 1997). At that time process safety regulations in the United States had been in force for just a few years so companies in the process industries were developing and implementing the programs needed to address the new regulations. The need for process safety regulations had arisen as a result of a number of very serious process plant incidents that occurred in the 1970s and early 1980s. (Some of these incidents are listed in Table 1.4.) In the United States process safety legislation was included in the amendments to the Clean Air Act of 1992. This legislation directed the Occupational Safety & Health Administration (OSHA) and the Environmental Protection Agency (EPA) to 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 general 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 1986. 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.

Considerable progress to do with process safety 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 it is likely that, over the course of the last 20 years, there have been greater improvements in occupational safety than in process safety (Whipple, 2008). (The different types of safety are discussed on page 18.) In addition, new concerns—such as the increased shortage of experienced employees—have come to the fore as being a potential source of decline in process safety performance. 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.

Many companies are now looking to go beyond mere regulatory compliance to expand their PSM programs, to increase performance not just in safety, but also in environmental compliance, quality control, and profitability. In other words, they are moving into the broader topics of *Process Risk and Reliability Management*—the title of this book. Another term that describes the same transition is *Operational Integrity Management* (OIM)—the title of this chapter.

This book was written to assist those managers and technical professionals who are seeking to make this transition from PSM to the management of risk and reliability. (However, in recognition of the fact that regulatory compliance is always an issue, Chapter 15—*Process Safety Management Compliance*—discusses what needs to be done to abide by the PSM rules and regulations.)

OPERATIONAL INTEGRITY/EXCELLENCE

Operational integrity management is rooted not just in process safety management, but also in the 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 the following:

- RAM (reliability, availability and maintainability) programs that focus on achieving maximum profitability;
- HSE programs covering the broad spectrum of Health, Safety and Environmental work;
- Statistical Process Control;
- Quality standards such as ISO 9000; and
- 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. 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.

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 was the case with traditional process safety management. OIM can be

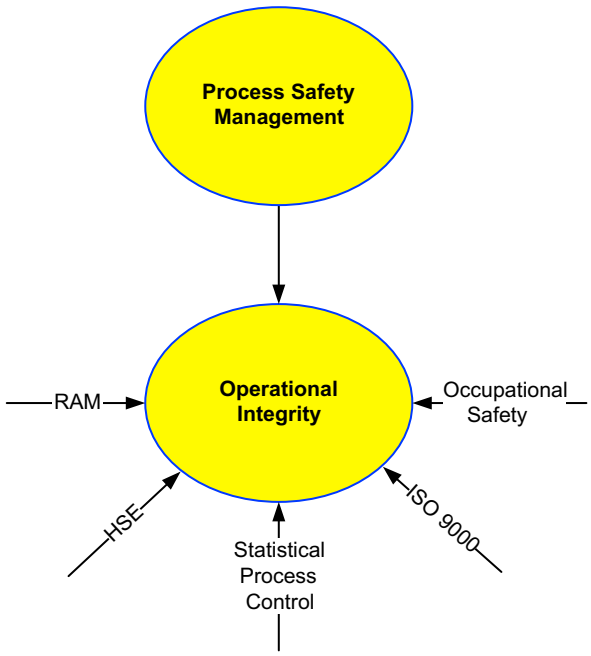


FIGURE 1.1

Operational Integrity Management Programs.

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 non-technical management systems that can affect safety and operability. These include distribution, inventory management, outsourcing, supply chain management, and procurement.

PROCESS SAFETY MANAGEMENT

Figure 1.1 shows that process safety management 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, but the standard promulgated by OSHA (the United States Occupational Safety & Health Administration) is widely used (OSHA, 1992). The development of the standard involved considerable input from the leading operating companies of the time, and has often been applied, regardless of whether a facility fell under OSHA's jurisdiction. OSHA divided process safety into the 14 elements listed in Table 1.1.

The topics listed in Table 1.1 were not new. Companies have always carried out activities such as the writing of procedures, planning for emergencies, training of

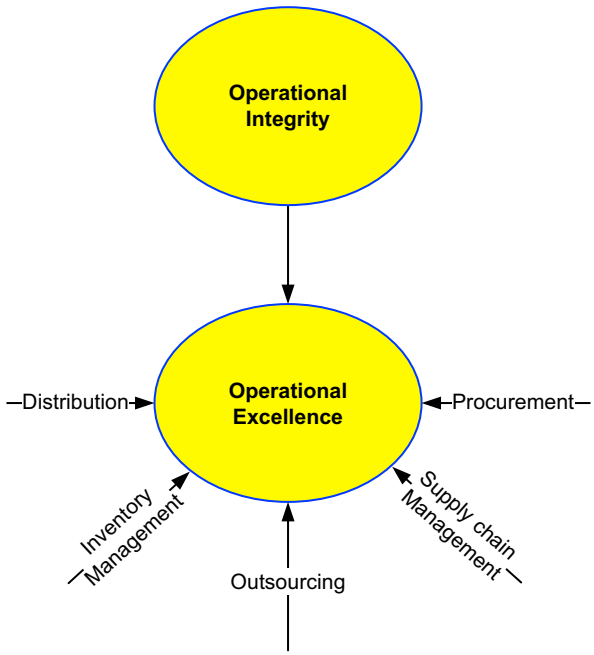


FIGURE 1.2

Operational Integrity to Operational Excellence.

Table 1.1 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

operators, and the investigation of incidents. However, the regulation did have the following effects.

- It forced companies to complete their process safety work. 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 management's feet to the fire.
- Companies were required to initiate work on elements such as Management of Change and Process Hazards Analysis that they may not have performed previously.
- PSM activities were increasingly seen as an integrated whole in which the elements all interacted with one another.

As companies have gained more experience with the implementation of PSM they have found that the list in Table 1.1 has some limitations. A modified list published by the Center for Chemical Process Safety (CCPS, 2007a) is shown in Table 1.2.

Table 1.2 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

Some of the elements in Table 1.2, such as Management of Change, are identical to those in Table 1.1. Others are modified—for example, Prestartup Safety Review becomes Operational Readiness. But some of the elements listed in Table 1.2, 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 structures put forward by OSHA and the CCPS many organizations, such as the American Petroleum Institute (API) and the American Chemistry Council, have offered their own methods for organizing PSM programs. Many larger companies also have their own systems, which typically are similar to what is shown in Tables 1.1 and 1.2.

The organization of the chapters of this book, which is shown in Table 1.3, is based on Table 1.2.

MAJOR EVENTS

Major steps in the development of process safety management (and hence of operational integrity management) have often taken place following the occurrence of serious accidents. Some of the more significant of these are listed in Table 1.4.

Table 1.3 Organization of This Book

Chapter 1	Operational Integrity Management (this one)
Chapter 2	Culture and Employee Involvement
Chapter 3	Hazard Identification and Risk Management
Chapter 4	Consequence and Likelihood Analysis
Chapter 5	Technical Information and Industry Standards
Chapter 6	Asset Integrity
Chapter 7	Reliability, Availability, and Maintainability
Chapter 8	Operations and Maintenance
Chapter 9	Operating Procedures
Chapter 10	Training and Competence
Chapter 11	Emergency Management
Chapter 12	Incident Investigation and Root Cause Analysis
Chapter 13	Management of Change
Chapter 14	Audits and Assessments
Chapter 15	Process Safety Management Compliance
Chapter 16	Managing a Risk and Reliability Program

Table 1.4 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 lead 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 2500 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.*

Further information to do with major events is provided by various agencies and companies, including the following, as listed by Balasubramanian and Louvar (2004):

- National Response Center (NRC);
- Major Accident Reporting System (MARS);
- Accidental Release Information Program (ARIP);
- Bureau of Labor Statistics (BLS);
- Census of Fatal Occupational Injuries (CFOI); and
- Marsh & McLennan Summaries.

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.

Example 1—facility design

A process consisting of four operating units and a utilities section. A schematic of the system is shown in Figure 1.3.

Example 2—process flow

Figure 1.4 shows part of Unit 100 from Figure 1.3. 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 shown in Table 1.5.

Summarizing Table 1.5 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.

Example 3—heat exchanger

Figure 1.5 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.

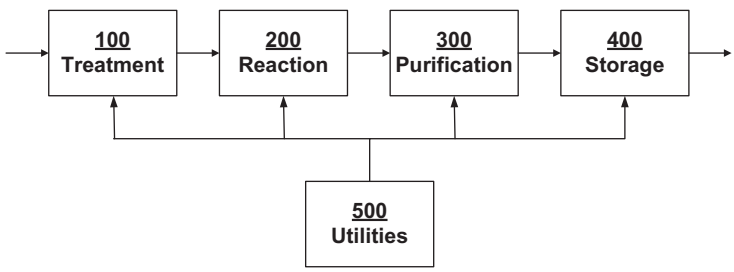


FIGURE 1.3

Process Units.

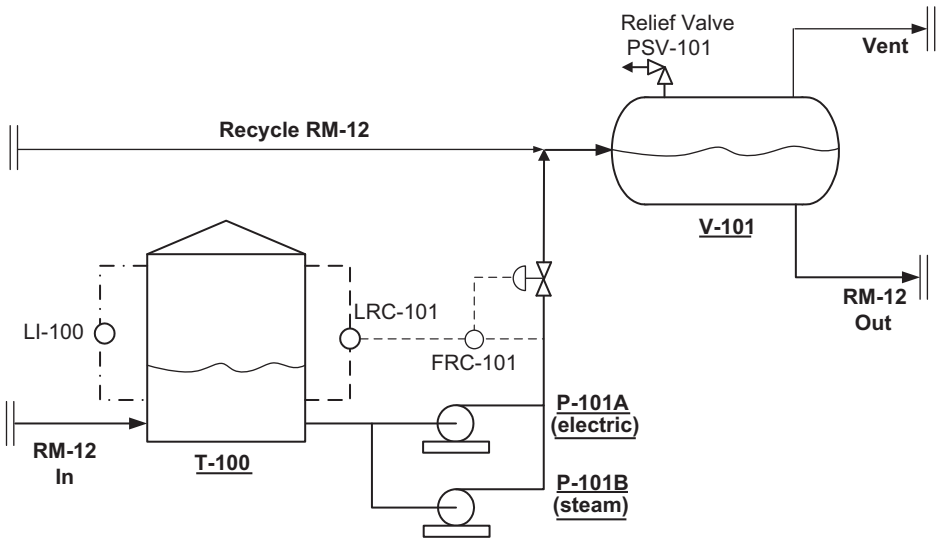


FIGURE 1.4

Process Flow Example.

Example 4—risk management workflow

The third example is used for discussions of the management of risk. Figure 1.6 illustrates the major steps in the development of a representative risk management program.

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.

Table 1.5 Failure and Repair Times

Item	Failure Rate, yr^{-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

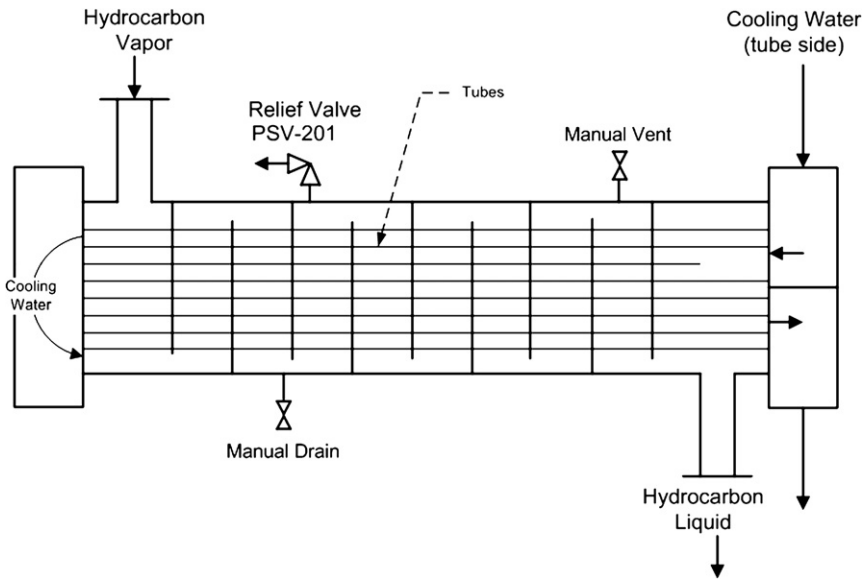


FIGURE 1.5

Heat Exchanger Example.

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".)

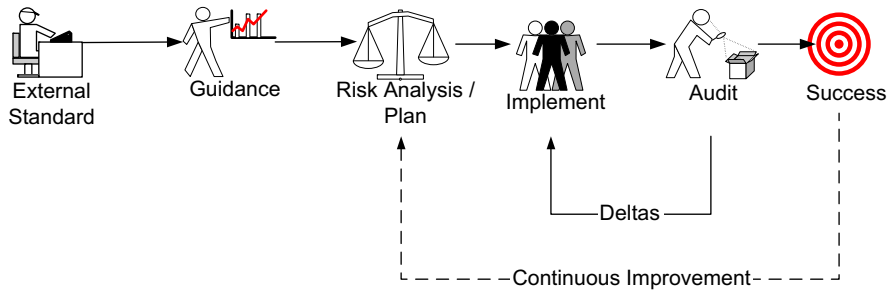


FIGURE 1.6

Risk Management Workflow Example.

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.

FUNDAMENTALS OF PSM

The nature of Process Safety Management (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.

Some of the fundamental features of a successful PSM program are discussed below. These fundamentals also form the basis of operational integrity management work.

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 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 1.6 provides some examples for safe limit values for the first standard example (Figure 1.4). Not only is a numerical value provided, but some discussion as to why that value was chosen is provided.

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 1.6 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 shown in Table 1.7 are commonly used to ensure that only compatible chemicals 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 1.7 lists five chemicals: A-E. It shows which chemicals can and cannot be mixed with one another safely.

Table 1.6 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.			

Table 1.7 Mixing Scenarios and Safe Limits

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

The symbols in Table 1.7 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; and

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 1.7 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.

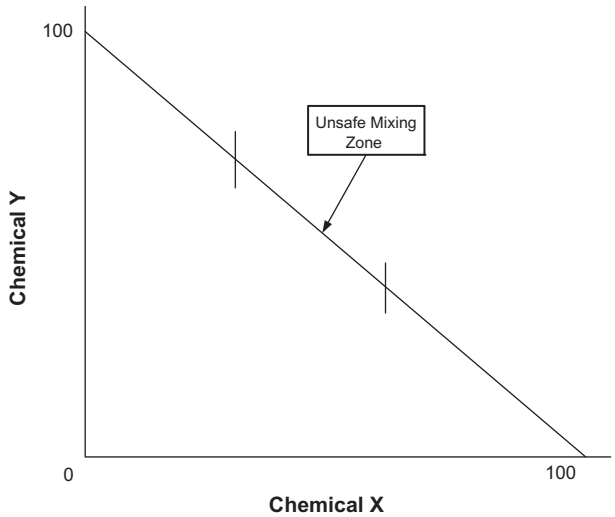


FIGURE 1.7

Unsafe Mixing Range.

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

Set point values

Figure 1.8 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 °C, 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 1.9, which shows that the set point has been raised from 147 to 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.

Operating, safe and emergency limits

The concept of safe limits can be extended to include operating and emergency limits, as illustrated in Figure 1.10, which shows values for a process variable such as pressure, temperature, level, or flow rate.

The innermost range of Figure 1.10 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.

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 1.10 the operating range is 235-245.

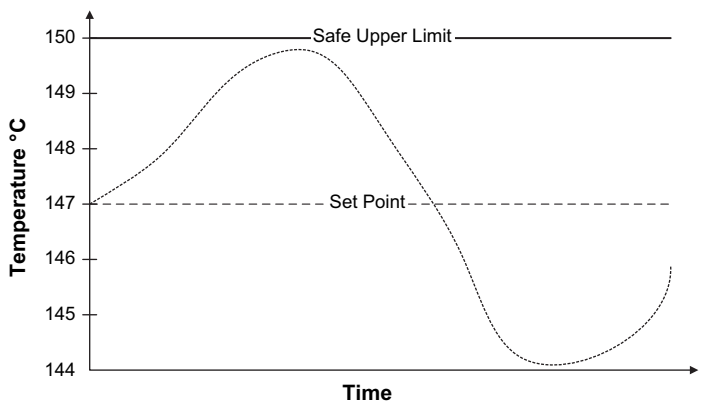


FIGURE 1.8

Safe Limit and Set Point Values.

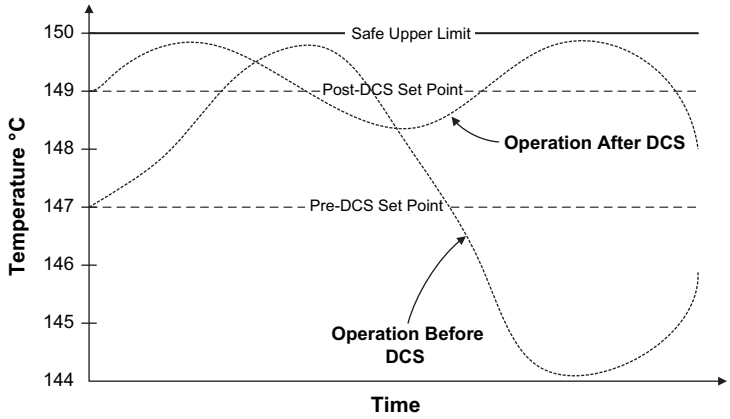


FIGURE 1.9

Effect of DCS on Set Point Values.

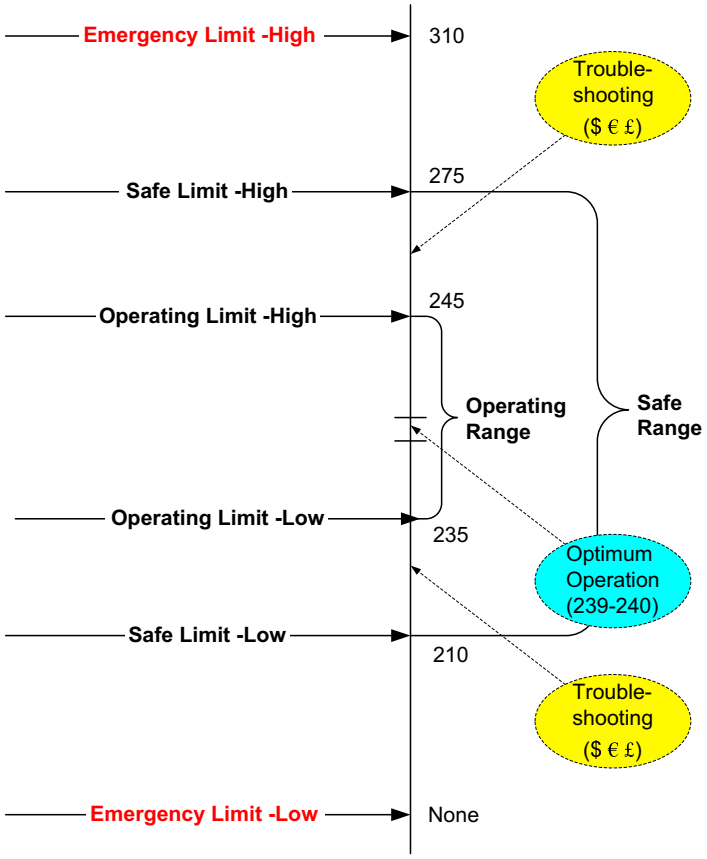


FIGURE 1.10

Operating, Safe and Emergency Limits.

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 the following:

- Excessive energy consumption;
- Product quality problems;
- Unusually high use of spare parts; and
- 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 1.10, were 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 1.10 the upper emergency limit is 310, there is no lower emergency limit. The relationship between operating, safety, and emergency limits is shown in Table 1.8.

The first two columns in Table 1.8—Operational Deviation and Safety Deviation—have been discussed in previous chapters. The third column—Emergency Operation—covers the reaction that operators take to bring an emergency situation under control. The fourth column describes the actions taken if the emergency gets out of hand and emergency response teams have to be mobilized.

Further discussion to do with emergency response is provided in Chapter 11—*Emergency Management.*

Non-prescriptive

Process safety management programs are largely non-prescriptive; that is, the regulations and standards in this field generally provide very little specific detail as to what has to be done. Basically they say, "Do whatever it takes on your facility not to have accidents". It is up to the managers, technical experts, and the operations/maintenance personnel to determine how this should be done. This lack of detail explains why the OSHA PSM standard is so short—the technical section of the regulation is only about 10 pages long. The PSM standards simply require that programs be in place, that they be adhered to, and that they work.

Although each facility is unique, many operations, such as starting a pump or training a contract worker, are really quite similar from site to site and from company to company.

Table 1.8 Types of Non-standard 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 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. The instructions 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.

Therefore it is possible to develop high quality, generic systems that can be used in a wide variety of situations. Doing so saves time and money, and improves quality.

Performance/risk based

Non-prescriptive management programs have to be performance-based because the only measure of success is success. Hence the only true measure of success of the program is not to have incidents. But, from a theoretical point of view, such a goal is impossible to achieve. No matter how well run a facility may be accidents will occur; risk can never be zero. For this reason, some PSM professionals choose not to use the terms "compliance" on the grounds that true compliance can never be realized. This insight means, therefore, that OIM and PSM programs are on-going activities that never end. Because risk can never be zero, there are always ways of improving safety and operability.

Process—not occupational—safety

It is important to distinguish between process safety and occupational safety. Process safety is primarily 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.

The Center for Chemical Process Safety (CCPS, 2007b) 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; and
- The release must be acute, i.e., it must occur over a short period of time.

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 Triangle shown in Figure 1.11. 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 events are much more

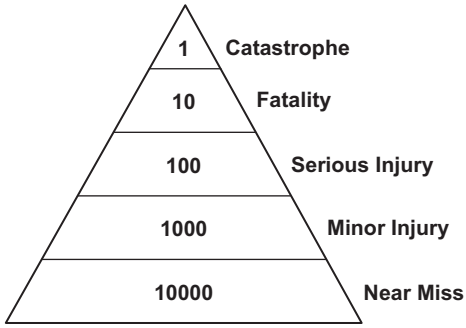


FIGURE 1.11

Incident Triangle-1.

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.

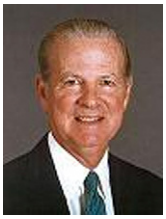
Figure 1.11, which uses created data, shows five levels of seriousness to do with worker safety (similar categories can be used for environmental and economic loss). Single order of magnitude steps are used. Hence it is estimated that, for every 10,000 near misses there will be a 1000 minor injuries, a 100 serious injuries, 10 fatalities, and one 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 personal protective equipment, and the improper use of machinery. Major events, however, are more often caused by *process* safety problems such as incorrect instrument settings, corrosion, or the 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.)



James Baker, *1930-*

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 the following:

- 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 Personal Protective Equipment (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 1.11 can therefore be modified as shown in Figure 1.12. 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.

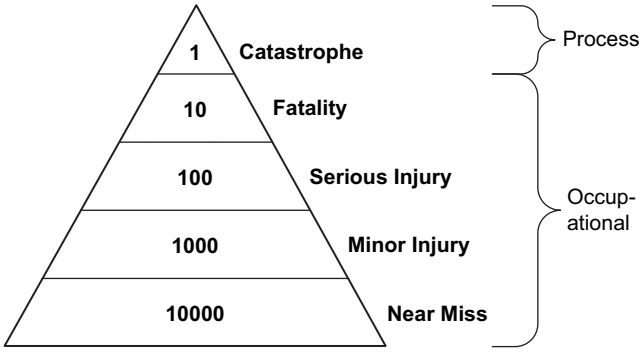


FIGURE 1.12

Incident Triangle-2.

Involvement and thoroughness

OIM 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.

PSM regulations 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 in Table 1.2—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 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* is the "most important" because, if the employees do not participate, the process safety 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. The real point, of course, is that they are all important and necessary, and that they all rely on one another to be effective.

Definition of process safety management

The definition for Process Safety Management provided by the Center for Chemical Process Safety (CCPS 1992) is:

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

Based on the discussions in the previous pages, the following alternative definition is offered:

> *Process Safety Management is an on-going 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.*

Trends

Pitblado (2008) showed that there has been a steady improvement in occupational safety in the process industries, as illustrated in Figure 1.13. 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 USA or EU, although the data

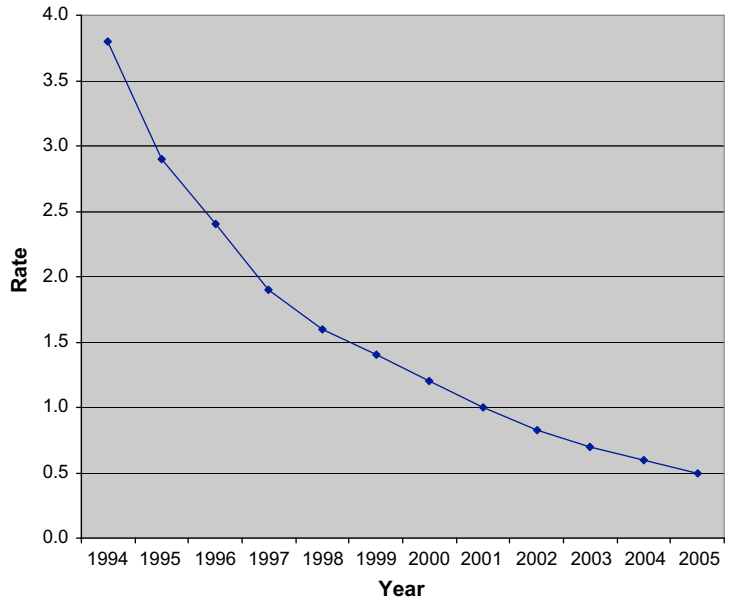


FIGURE 1.13

Occupational Injury Trends.

is noisy and some successes do exist—notably the UK 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.

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 also the title of the well-known three volume series Loss Prevention in the Process Industries (Lees, 2004).

Although Health, Safety and Environmental activities are often grouped together, and are often directed by a single manager, the three topics are actually quite distinct from one another. Table 1.9 shows who or what is covered by each of the elements of HSE, and outlines the geographical scope and time line 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

Table 1.9 Elements of HSE

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

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, it is argued, to have as little long-term impact on the environment as possible, and, where possible, 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 was identified as a potential problem in the late 1970s, but only now is it becoming widely recognized and addressed. Indeed the phenomenon has developed so gradually, and the global climate is affected by so many other poorly understood variables that many responsible professionals believe that the phenomenon of global warming either does not exist, or that its causes have not yet been fully identified. It will be many years before these disagreements are resolved.

Environmental performance is largely driven by regulations because no company is big enough to address such issues alone. Also, whereas PSM programs are non-prescriptive, 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 time line 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). Discussion to do with health and industrial hygiene is provided in Chapter 8—*Operations, Maintenance and Safety.*

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—asbestos abatement in particular—are propelled by litigation, particularly in the United States. In other words, standards developed through the use of law suits 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 event shown in Table 1.4 led to the death of thousands of people in the local community.) In general, the time line in which safety events take place is short, often covering just a fraction of a second.

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 to maintain the consistency of how the product is made and 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 “fire fighting” every time that 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" (Pearch, 2000). 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 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

For every complex problem there is an answer that is clear, simple — and wrong.
H.L. Mencken, 1880-1956

The topics of risk analysis and risk management thread through much of what is written in this book. An effective risk management program has three elements. First, the program must be properly grounded in theory. Modern process systems are large and complex. As the above quotation from H.L. Mencken suggests, the most obvious ways of reducing risk in such systems may turn out to be wrong, misleading, or inefficient. Risk can only be managed properly if it is properly analyzed and understood in terms of its basic principles.

Second, risk management has to be practical. Many risk analyses are theoretically interesting, but they do not provide much practical help to managers, operators, and engineers working on operating facilities and on projects. An effective risk management program is useful at eight o'clock on Monday morning, both in an operating facility and in a design office.

The third element in an effective risk management program is the appropriate use of both "hard" and "soft" approaches to both analysis and follow-up. The "hard" approach relies on the use of formal models, quantitative data, and an objective examination of equipment and instrumentation. The "soft" approach is oriented more toward understanding people and their behaviors. The best risk management programs combine both approaches. For example, the well-known Hazard and Operability technique (HAZOP) that is described in Chapter 3 is based on a "hard" structured approach to hazard identification through the use of carefully organized deviation guidewords. At the same time, a well-led HAZOP creates a "soft" environment in which the team members can "dream up" previously unthought-of accident scenarios.

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

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

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

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

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 consequence and likelihood terms can be reduced in size, 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 term in Eqn (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.

Table 1.10 lists some of the hazards associated with the second standard example.

One of the greatest difficulties to do with practical risk analysis is defining the scope of the hazard term. For example, with respect to the second hazard in Table 1.10—the overflow of T-100—simply to say that RM-12 overflows from T-100 is not enough.

Table 1.10 Hazards from the Example 2	
1	Tank T-100 is pumped dry.
2	Tank T-100 overflows.
3	P-101A seal fails.
4	V-101 is over-pressured.
5	Liquid flows backward from V-101 into T-100
6	Other.

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 onto the ground and then flow into the local waterways. Realistically, these two scenarios represent not different consequences, but different hazards.

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 listed in Table 1.10 is "Other". This term is included as a reality check. No risk management team, no matter how well qualified the members may be or how much time they put into the analysis, 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/likelihood

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; and
3. Economic.

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

Each event has a predicted frequency of occurrence, such as once in a 100 years. The frequency term always has units of inverse time, such as number of events per year.

Figure 1.14 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.

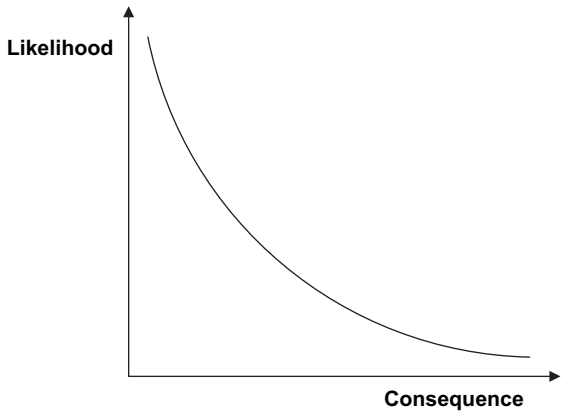


FIGURE 1.14

Likelihood vs Consequence.

The total risk associated with a facility is 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 1.15 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). In Figure 1.15 it is projected that the organization will have a fatality about

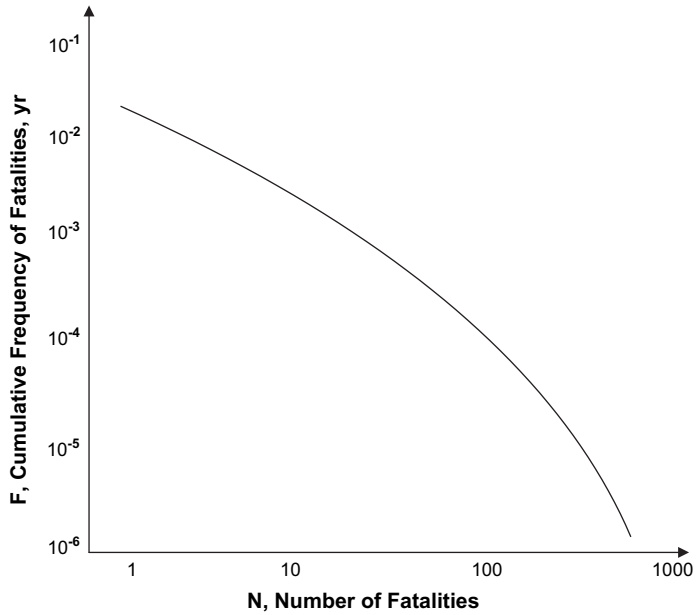


FIGURE 1.15

Representative FN Curve.

once every 50 years, whereas a major event (say more than 10 fatalities) will occur every 1000 years or so.

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 1.16, which compares technologies A and B.

Bow-tie method

Another way of looking at risk is through use of the "bow-tie" technique (Philley, 2006), which is basically a fault tree followed by an event tree.

Figure 1.17 shows the structure of a bow-tie diagram. At the left of the diagram is the hazard, say a vessel containing hydrocarbons stored under pressure. Threats are events such as corrosion, external impact, and operating error, which could create an undesired event, in this case a release of hydrocarbons from the vessel. Between the threats and the undesired outcome are barriers such as operator training, relief valves, and instrumentation.

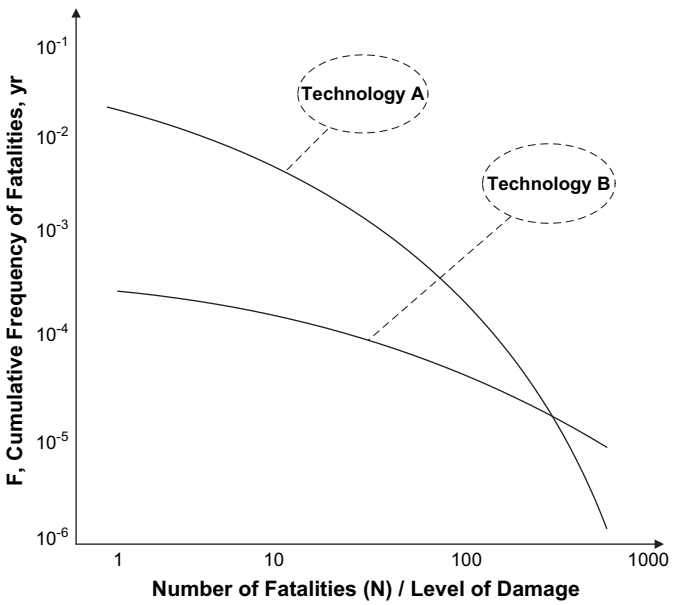


FIGURE 1.16

Comparative FN Curves.

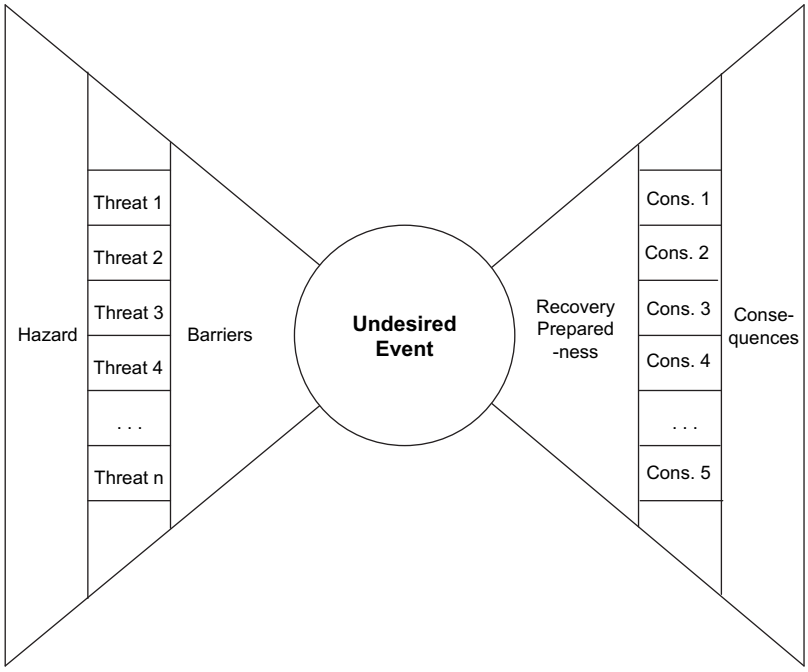


FIGURE 1.17

Bow-Tie Diagram.

Moving to the right side of the diagram, if the top event does occur, various recovery and preparedness measures limit its impact. In the case of the over-pressured vessel, these measures could include emergency blowdown or the triggering of a deluge system. If these protective measures do not work, a range of consequences such as fire or the release of toxic materials to the atmosphere will take place.

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 4. 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:

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

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).

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; that is, they pre-judge situations rather than trying to analyze the facts rationally and logically. People jump to pre-conceived 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.

The subjective component of risk becomes even more pronounced when the perceptions of non-specialists, 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.

Factors that affect risk perception include the following:

- Degree of control;
- Familiarity with the hazard;
- Direct benefit;
- Personal impact;
- Natural vs. man-made risks;
- Recency of events;
- Effects of the consequence term; and
- Comprehension time.

These terms are discussed below.

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 risks 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

Equation (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 Eqn (1.1), a hazard resulting in one fatality every 100 years has the same risk value as a hazard resulting in 10 fatalities every 1000 years. In both cases the fatality rate is one in a 100 years, or 0.01 fatalities yr^{-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 Eqn (1.1) can be modified so as to take the form of Eqn (1.3).

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

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 Eqn (1.3) for the two scenarios just discussed—the airplane crash and the highway fatalities—becomes Eqns (1.4) and (1.5), respectively.

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

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

The 500 airplane fatalities are perceived as being equivalent to over 11,000 automobile 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 Eqn (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.

Quantification of risk

There are three kinds of people: those who can count, and those who can't count.

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, the words frequency, probability, and likelihood tend to be used interchangeably, 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 two years, or $0.5\ \text{yr}^{-1}$.

Frequency can 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 $0.01\ \text{batch}^{-1}$. 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 do 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 7.

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 $0.5\ \text{yr}^{-1}$; 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 $(0.5 * 0.1)\ \text{yr}^{-1}$, 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 $0.1\ \text{yr}^{-1}$. 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 yr^{-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 are 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 non-functioning of a specific item of equipment; "Fault" refers to the non-functioning of a system or sub-system. 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 non-occurrence 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, so, that event is said to occur at random.

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 shown in Table 1.11 for its design personnel. 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.

Gillard (2009) states that the concept of acceptable risk is different once a facility is in operation. Management of operating facilities should take "all reasonable precautions" (ARP). For example, having all the operators trained and having critical instrumentation properly maintained would certainly fall under ARP. However, protection against highly unlikely weather conditions (such as heavy snow falls in Houston, Texas) would not constitute ARP.

As low as reasonably practical—ALARP

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 1.18 which is an FN curve family (see Figure 1.15).

Table 1.11 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	$<1 \times 10^{-6}$

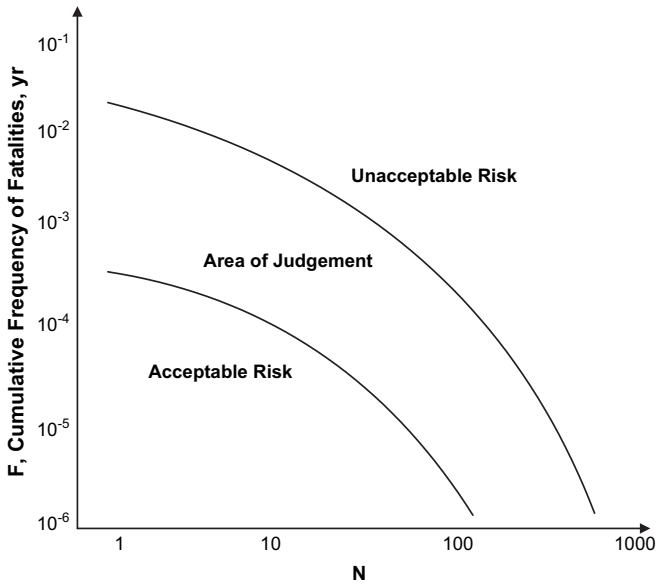


FIGURE 1.18

Risk Boundaries.

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 such as that shown in Table 1.14 are frequently 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.

One panel has developed the following guidance for determining the meaning of the term "As Low as Reasonably Practical".

- 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; and
- 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.

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 United Kingdom Health

and Safety Executive (HSE) chose in the year 2006 to minimize its emphasis on 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). Such a practice establishes engineering performance criteria based on established codes, standards, and recommended practices.

The development of RAGAGEPs for a particular company or facility includes the following steps:

1. Identify the relevant federal, state, county, and local regulations;
2. Identify local codes and standards (such as building and fire codes);
3. Identify the pertinent industry consensus standards;
4. Review all of the above with legal, safety, and environmental staff;
5. Incorporate proprietary experience and standards; and
6. 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.

RAGAGEP can be used to provide a basis for regulatory action (or the defense to such an action). For example, the EPA Risk Management Plan (RMP) General Duty clause provides very little guidance regarding the management of "extremely hazardous substances". If the EPA were to cite a company under this clause, the company could defend itself by showing that it was following recognized good engineering practices.

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 with 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 the following:

- Consequence Matrix;
- Frequency Matrix; and
- Risk Matrix.

Consequence matrix

A representative consequence matrix is shown in Table 1.12. 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 do not provide sufficient flexibility and differentiation, but five

Table 1.12 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 remediation 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

levels imply a level of accuracy that is probably not justified. The steps in Table 1.12, from "Low" to "Very Severe", are roughly in 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 shown in Table 1.12 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. 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 shown in the third column of Table 1.12, 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 shown in Table 1.12. In practice environmental issues are normally controlled by rules and regulations rather than an objective analysis of risk.

Economic loss

The final consequence category in Table 1.12 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; and
- Clean-up.

Economic loss can either be one time (say the destruction of a piece of equipment) or on-going, in which case the value shown in Table 1.12 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 1.12 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 shown 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 imply a degree of accuracy that probably could not be justified (precision is not the same as accuracy).

As with the consequence matrix, the steps in Table 1.13 are roughly an order of magnitude greater than the one before it.

Table 1.13 Frequency Matrix

	Frequency	Comments
Low, 1	<1 in 1000 years	Essentially impossible: "Once in a blue moon" or "meteor falling out of the sky".
Moderate, 2	1 in 100 years to 1 in 1000 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.

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 world-wide, 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 shown in Table 1.14, 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 1.14 is as follows.

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 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

Table 1.14 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

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.

In addition to the four letters shown in Table 1.14, 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 1.12. 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 non-conformance 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 non-controversial. 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.)