PROCESS RISK MANAGEMENT

By IAN SUTTON

March 2007

1st Edition

This is a SAMPLE of the 272 page book available at …
http://www.bin95.com/ebooks/risk_tree_analysis.htm

Synopsis by Chapter:

Chapter 1 - Risk Management provides an overview of risk management in the process industries. Terminology - such as the important distinction between the words 'frequency' and 'probability' - is explained, as are fundamental concepts, such as the role of safeguards in a process safety management system.

Chapter 2 - Hazards Identification describes how hazards can be identified, usually in a team environment. The role of the team leader (facilitator), scribe and department specialists is discussed, as is the all important topic of writing the final report. The chapter points out some of the limitations of typical hazards analyses, and discusses how hazards analysis fits into the overall topic of process safety management.

Chapter 3 - Hazards Analysis Techniques describes some of the more commonly used methods for identifying hazards. The Hazard and Operability (HAZOP) method is discussed in depth, as are Failure Modes & Effects Analysis (FMEA), Checklists and the What-If approach. The strengths and limitations of each technique are described.

Chapter 4 - Consequence Analysis provides an overview of some of the major consequence issues facing the process industries. These include fires, explosions, and toxic gas releases.

Chapter 5 - Likelihood Analysis provides a background to the difficult yet important issue of risk quantification. The chapter starts by discussing the Pareto Principle, then discusses the Fault Tree Analysis method in some depth. The final section of the chapter outlines some of the limitations that are inherent in quantification work.

(**Note:** The fault tree content of this chapter is available in an expanded form in Fault Tree Analysis .)

Chapter 6 - Common Hazards explains that many hazards are common to a wide variety of processes and technologies. A wide range of such common hazards are listed in this chapter.

CONTENTS

CHAPTER 1 — RISK MANAGEMENT

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

INTRODUCTION


H.L. Mencken

Excellent safety and environmental performance in the process industries does not happen by chance; after all, most process facilities handle large quantities of toxic, flammable and explosive materials, often at high temperature and pressure. Such processes are inherently hazardous. Therefore process risk must be properly understood and managed.

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 quotation from H.L. Mencken at the head of this chapter suggests, the 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 based 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.

The third element in an effective risk management program is the appropriate use of both the '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, on the other hand, 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 on page 127 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. They are encouraged to 'think the unthinkable'.

ABOUT THIS SERIES

This ebook is part of a series of publications provided by Sutton Technical Books.

Ebooks

Ebooks in this series are full-length publications that are available for purchase. Typically, they are more than 300 pages (8½ x 11", single-spaced) in length.

Books

Sutton Technical Books also publishes printed books, typically based on the corresponding ebook.

Engineering Minutes / Events

A variety of Engineering Minutes can be downloaded at no cost from www.stb07.com. The Engineering Minutes provide a brief overview of some specialized topic to do with the process industries. Typically they are around 10 pages long.

The Events section provides information on some of the major events that have occurred in the process industries, particularly as they affect safety and environmental issues.

Reference

The final major section of the Sutton Technical Books contains links to reference material and commercial terms. The page www.stb07.com/citations.html shows the reference material used for all of the publications in this series.

WORKED EXAMPLE

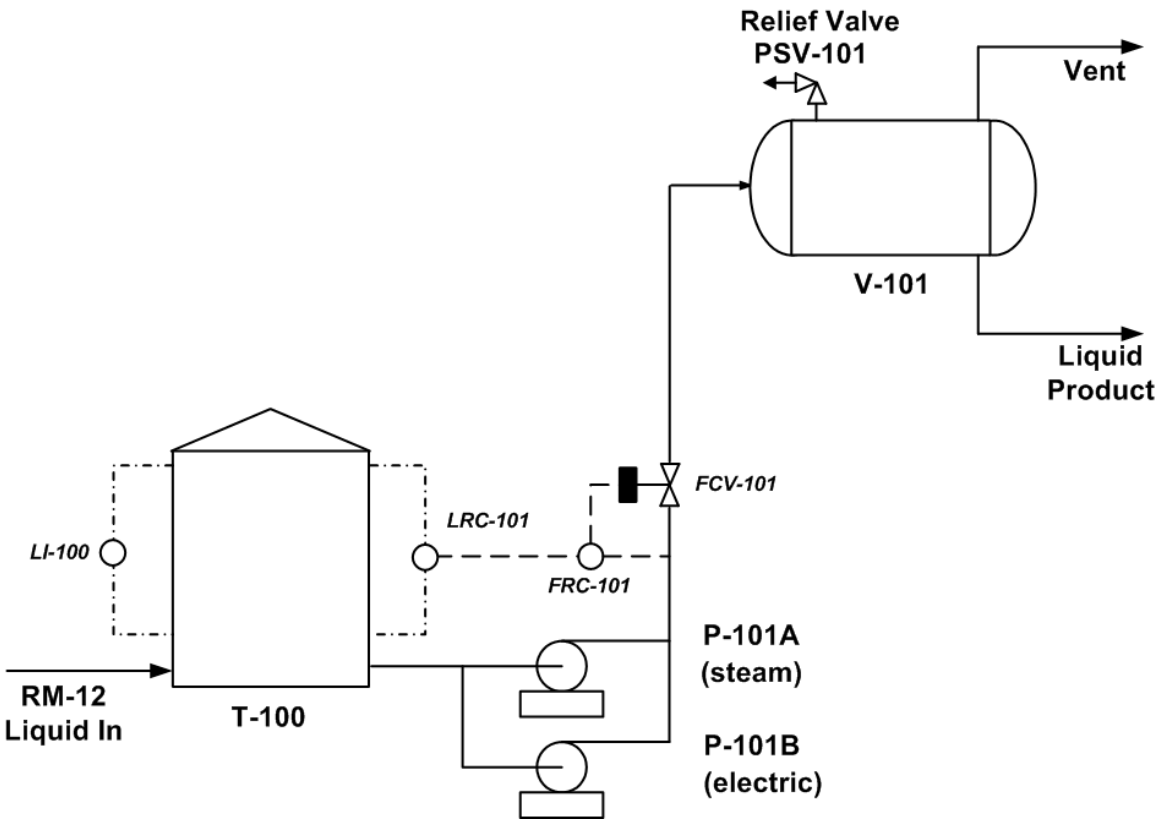
In order to illustrate concepts as they are introduced throughout the remainder of this ebook, a simple example to do with the transfer of a hazardous chemical to and from a storage tank is provided below. The example is taken from the *Ebook 1: Worked Examples,* which can be downloaded at no cost from www.stb07.com/e1-examples.html. For convenience the first example in that ebook is repeated below (some detail has been removed).

Figure 1 shows liquid flowing into an Atmospheric Tank, T-100. The liquid is called Raw Material Number 12 — abbreviated to RM-12. It is both flammable and toxic. 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 predicted failure rate for Pump A is once in two years, or 0.5 yr^{-1}; the predicted probability that the Pump B will not start on demand is 1 in 10, *i.e.,* 0.1 (this term is dimensionless). The predicted repair time (Mean Downtime) for P-101A should it fail is 8 hours; the predicted repair time for P-101B should it not start is 3 hours.

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 determined manually using the sight glass, LI-100.

V-101 is protected against over-pressure by safety instrumentation (not shown) that shuts down both pumps, and by the pressure safety relief valve, PSV-101.

Figure 1
Process Flow Example



CLIENTS / CUSTOMERS

Before starting the development of a risk management program it is important to identify the program's client or customer so that the program can be structured to meet their needs. Potential clients are listed below.

Senior Management

Senior managers are concerned primarily with 'big picture' issues. With respect to process risk, they are particularly sensitive to the potential for major environmental and safety events. They are also concerned about relations with outside groups such as investors, regulators and members of the public. Therefore senior managers are interested not only with the actual results of the risk management program, but also in the way in which those results are communicated to the outside world.

Facility / Plant Managers

In operating plants the immediate client will usually be the facility or plant manager, supported by his or her operations, maintenance and technical managers. Although these line managers will be concerned about the big picture issues discussed above, they will generally be more focused on meeting shorter-term goals. With regard to risk management, they particularly want to avoid lost-time and recordable injuries and environmental citations. They also want a risk program that helps them improve plant reliability and on-stream performance.

In most cases, it is the facility manager who will have to fund the risk management program. Therefore he or she will want to know that these funds (along with other resources such as the time of skilled personnel) are being invested wisely, and that any findings are properly addressed in a timely and cost-effective manner.

Project Managers

If a facility is still in the design or construction stage the immediate client for the risk management program will be the project managers on both the client and the contractor sides. They will have two principal interests regarding risk management. First they will want to ensure safety on the project itself, particularly during the fabrication and construction phases. Second, the project managers want to be assured that the facility that will operate safely and that will meet its environmental and operating goals once it has been turned over to operations.

Regulators / Auditors

Modern industrial facilities are required to meet a plethora of regulations, rules, codes and standards. Therefore the risk management program should be organized so that its findings and results can be readily evaluated and audited by outsiders, particularly government regulators.

MALICIOUS ACTS

The discussions to do with risk and risk management throughout this ebook are predicated on the assumption that everyone working on the design or operation of a process facility wants to do a good job, and that all employees and managers wish to foster a safe and productive environment. Therefore risk analyses do not generally consider malicious acts, whether they be internal sabotage or external attack; it is assumed that accidents truly are accidents.

In point of fact industrial facilities are potential targets for malicious acts. Hence management needs to create and implement a Security Vulnerability Analysis as a supplement to the normal risk management program.

HEALTH, SAFETY & ENVIRONMENTAL (HSE) PROGRAMS

Risk management programs are usually part of a facility's Health, Safety and Environmental (HSE) program. (Some companies use the initials in a different order, *i.e.,* SHE, HES, or EHS. The choice is not important. In the United Kingdom, the letters 'HSE' generally refer to the regulatory agency the Health and Safety Executive.)

Although Health, Safety and Environmental issues are often grouped together, and although HSE activities are often directed by a single manager, the three topics are actually quite distinct from one another. Table 1 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.

Table 1
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

Environmental and Sustainability Programs

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

term goal should be, 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 is only now is it becoming widely recognized as an issue that must be dealt with. 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 full identified. It will be many years before these disagreements are resolved.

From the point of view of an HSE professional, much environmental work consists of formal compliance with regulations from a myriad of government agencies, not all of which are properly coordinated with one another. Compliance work is expensive and time-consuming, and hence is sometimes perceived by management as being merely a burden and an expense. Nevertheless, these mangers have no choice — regulatory compliance work must be carried out if the company or facility is to receive operating permits, avoid compliance penalties, and minimize legal liabilities. As noted above, a facility's risk management program must be organized so that outside auditors can check that the rules and regulations are being followed.

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

Worker Removing Asbestos

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 (although some poorly understood health issues may take longer than that to diagnose and understand).

Health and environmental concerns often overlap. For example, if a company is discharging a toxic gas such as sulfur dioxide (SO_2) on a routine basis, then the company will have to be concerned about meeting the *environmental* rules to do with SO_2 emissions. Going beyond mere regulatory compliance however, the company may then elect to conduct analyses to determine what impact the SO_2 may be having on the *health* of the local community. The

results of such a study may encourage the company management to implement control measures that are more stringent than are legally required.

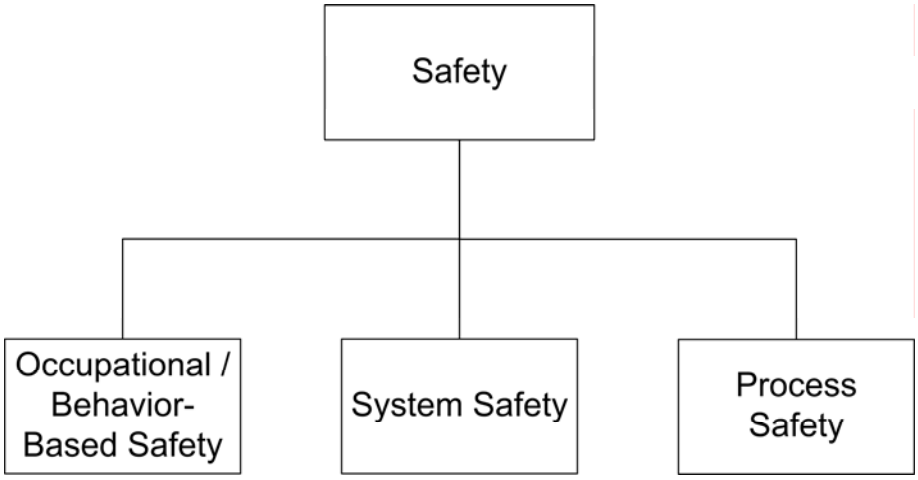
Whereas environmental compliance is typically driven by legislation, many health programs — asbestos abatement in particular — are driven by litigation, particularly in the United States.

Safety

Safety issues generally affect only facility workers. (There are important exceptions to this statement; sometimes an industrial accident can impact public safety. In particular, the Bhopal event in the year 1984 led to the immediate death of thousands of people in the local community.) In general, the time line in which safety events take place is short, often just momentary.

Safety programs can be divided into three major categories, as shown in Figure 2.

Figure 2
Types of Safety



Occupational and Behavior-Based Safety are the topics that most people think of when they hear the word ‘safety’. These topics include issues such as training, safe work practices and the use of personal protective equipment (PPE). System safety is concerned with the understanding of complex industrial systems, and the ways in which they can fail. Fault tree analysis, the focus of Chapter 5 of this ebook, is one of the techniques used to understand

system safety. Process safety focus on management systems such as hazards analysis, auditing and incident investigation. Most companies include these activities in their Process Safety Management programs, as discussed below.

Process Safety Management

Process Safety Management (PSM) widely used in the 1990s, particularly in the United States. The Occupational Safety & Health Administration (OSHA), the Environmental Protection Agency (EPA) and various state agencies introduced process safety regulations during that decade.

As the term implies, process safety management focuses primarily on issues to do with process operations and design, as distinct from say occupational or behavior-based safety. PSM programs are divided into management elements; the fourteen elements of the OSHA PSM standard are widely used; they are listed below in Table 2.

Table 2
OSHA's PSM Structure

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

PSM is not a management program that is handed down by management to their employees and contract workers; it is a program involving everyone. The key word is *participation* — which is much more than just *communication*. All managers, employees and contract workers are responsible for the successful implementation of PSM. Management 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 PSM is fundamentally a line responsibility.

The concept of process safety management can be further understood by examining its component words.

Process

The first word in the phrase PSM is *Process*. PSM is concerned with process issues such as reactor temperatures and the properties of chemicals, as distinct from *occupational* safety issues, such as trips and falls.

Safety

The second word in the phrase PSM 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.

Management

The third and final word in the phrase PSM 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. Control of an operation can only be achieved through the application of good management practices.

PSM is an on-going activity that never ends; it is a process, not a project. Because risk can never be zero, there must always be ways of improving safety and operability. Process safety management cannot be viewed as being a one-time fix.

Non-Prescriptive

Process safety management programs are non-prescriptive which means that the regulations and other standards in this field generally provide very little detail as to what needs to be done. For example, the technical section of the OSHA PSM standard is only about ten pages long.

Basically, PSM rules say 'do whatever it takes *on your facility* not to have accidents'. It is up to the managers and employees to determine how this should be done. There are no universally 'correct answers' as to what needs to be done to achieve a safe operation. What is appropriate in one location may or may not be appropriate in another. The PSM standards simply require that programs be in place, and that they be adhered to. (In this regard, PSM is similar to ISO 9000 and other quality standards, which also require that companies set their own standards, and then adhere to them.)

Performance-Based

Programs that are non-prescriptive are, of necessity, performance-based. This means that the only true measure of success is not to have upsets or accidents. Consequently, from a theoretical point of view, it is impossible to achieve 'compliance'. The only truly acceptable level of safety is zero accidents. Yet, no matter how well run a facility may be a zero accident rate is a theoretically unattainable goal. In spite of the fact that many companies set a target goal of 'zero accidents', risk can never be zero, and accidents can always happen. Indeed, if a unit operates for long enough, it is *certain* — statistically speaking — that there will be an accident. Hence, even though the stated PSM goal may be 'zero accidents', in practice, management has to determine a level for 'acceptable safety' and for realistic goals.

ELEMENTS OF RISK

Risk 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).

$$Risk_{Hazard} = Consequence * Predicted\ Frequency \quad .....(1)$$

Risk is not the same as uncertainty. Events which have a desirable outcome may contain a high level of uncertainty, but they do not create risk. Risk implies some type of negative outcome.

Equation (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, but they can never be eliminated, as illustrated in Figure 3, in which both axes are approached asymptotically, *i.e.,* they never reach zero. The only way to achieve a risk-free operation is to remove the hazards altogether (or, with respect to safety, to remove personnel from the site).

Figure 3
Likelihood vs. Consequence

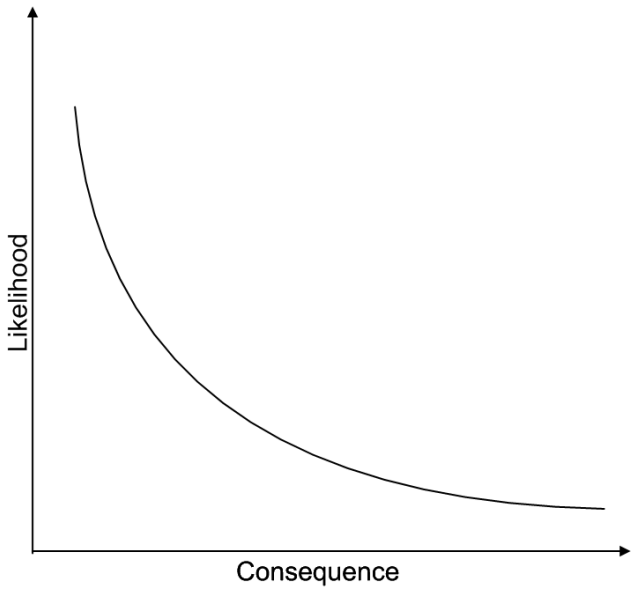
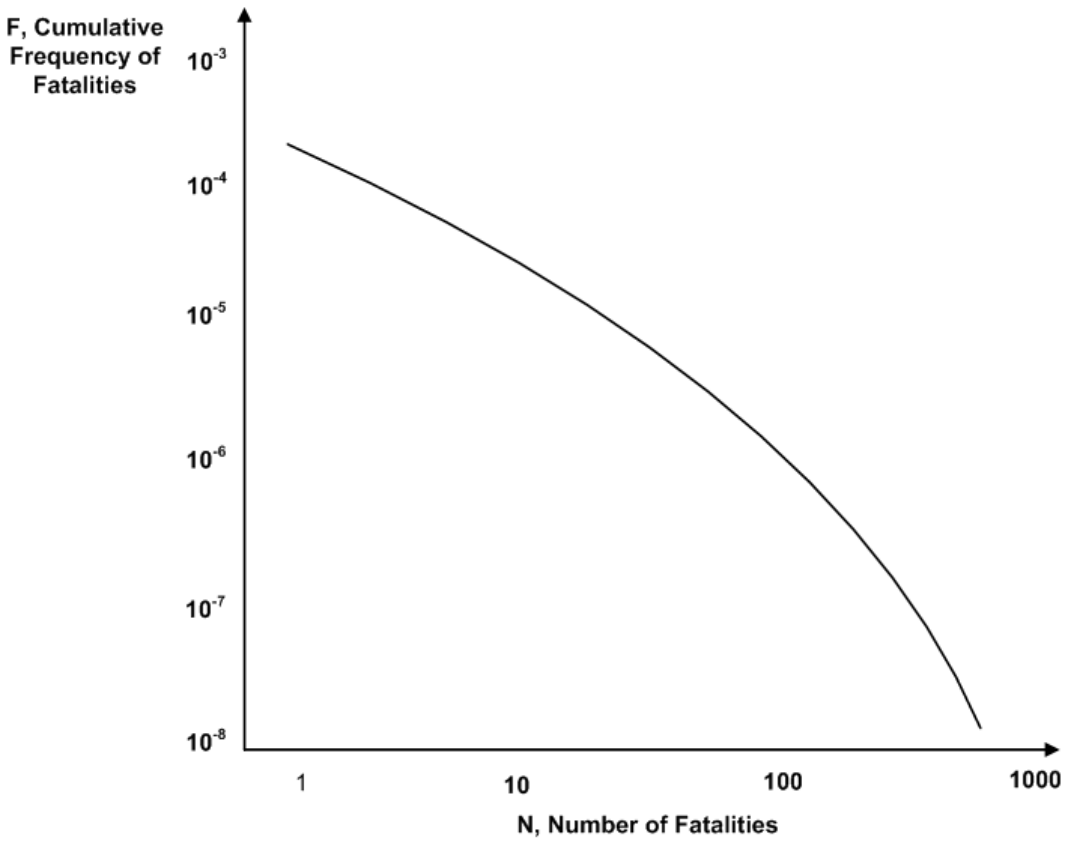


Figure 3 also shows that an inverse relationship generally exists between consequence and frequency. For example, a serious event such as the failure of a pressure vessel may occur only once every ten years, whereas simple trips and falls may occur weekly.

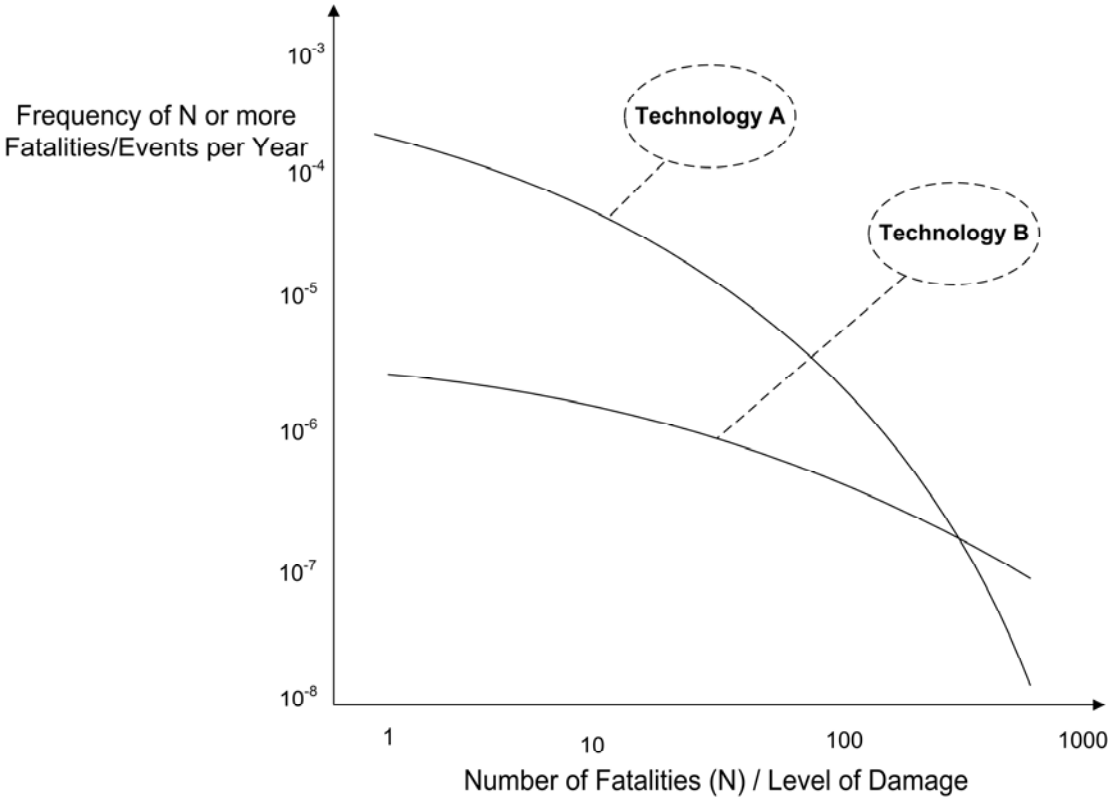
The total risk associated with a facility is obtained by calculating the risk value for each consequence, and then adding all the individual risk values together. The result of this exercise is sometimes plotted in an FN curve as shown in Figure 4 in which the ordinate represents the cumulative frequency (F) of fatalities or other serious events, and the abscissa represents the consequence term (usually expressed as N fatalities). 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 a family of 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.

Figure 4
Representative FN Curve



FN curves are generally used when making industry-wide decisions; FN curves would not generally be calculated for individual process plants. However, if two types of technology are being considered their respective FN curves can be compared, as illustrated in Figure 5, which compares two technologies: A and B (such as determining the overall risk associated with moving from gasoline to hydrogen powered cars).

Figure 5
Family of FN Curves



HAZARDS

The first term in Equation (1) is the hazard. A hazard is a condition that has the potential to cause harm. The key word in this 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 3 lists some of the hazards associated with the example shown in Figure 1.

Table 3
Hazards from the Standard Example

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.

Hazard Scope

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 the list above — the overflow of T-100 — simply to say that RM-12 overflows from T-100 is not enough. Clearly there is an enormous difference between having a few drops spill into a closed drain system, and having thousands of liters of the chemical pour on to the ground and then flow into the local waterways. 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 3 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 ebook an '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'.

Safe Limits

Where possible, hazards should be precisely defined through the use of safe limit values for process parameters such as flow, temperature, pressure and level. If the value of a variable moves outside its safe range then, by definition, a hazardous situation has been created.

Table 4 provides some examples for safe limit values for the standard example.

Table 4
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 is not provided so a minimum level in the tank must be maintained to prevent pump cavitation leading seal leaks.			
P-101	Flow	kg/h	N/A	500
	The upper limit for flow is set by the capacity of the pumps. 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 250C)	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.			

Figure 6 provides another illustration of the safe limit concept (the values shown in Figure 6 could be for any process parameter such as pressure, temperature, level or flow).

Figure 6
Example of Safe Limit Range

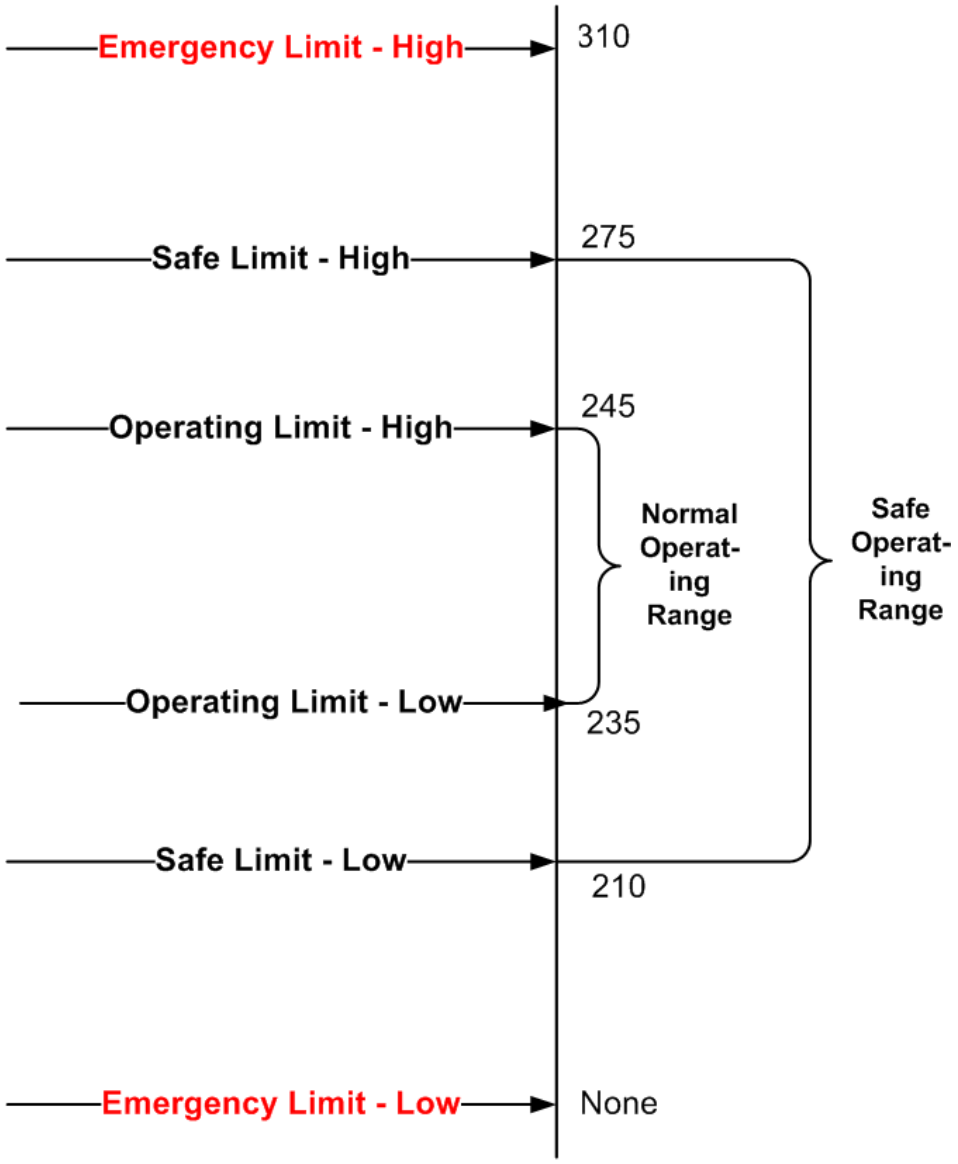


Figure 6 shows three ranges for the process parameter in question. The first is the normal operating range; it lies between 235 and 245 (in whatever the units of measurement are). Normal operations are carried out within this envelope. If the value is allowed to go outside the range it is likely that production or quality problems will crop up.

The second range lies between the safe upper limit and the safe lower limit (210 – 275 in Figure 6). If the value of the parameter goes outside this range then the process is, by definition, unsafe, and action must be taken. The option of doing nothing is not an option. It is likely that, once these safe limits are breached, safety devices — particularly instrumentation systems — will be activated. Operations personnel should understand the consequence of exceeding the limits; they should also be provided with procedures and training as to what actions to take to bring the variable back into the safe range. If the

operations team wishes to operate outside the safe range, say to increase production rates, they can only do so after implementing the Management of Change process (*see* page 124).

The third range shown in Figure 6 defines emergency conditions. If a variable value goes outside the emergency limit range, urgent action is required. It is probable that an excursion outside the safe limits will lead to activation of emergency instrumentation and mechanical safety devices (such as pressure relief valves).

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 4 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.

Maximum Allowable Working Pressure (MAWP)

One particularly important safe limit value to understand is that of Maximum Allowable Working Pressure (MAWP) for pressure vessels. Since the concept of MAWP is so important, and since it is not always well understood, the following guidance, based on ASME terminology using V-101 as an example is provided.