3 SYSTEM MODELS FOR RISK MANAGEMENT

Risk Model - A framework of processes and activities concerned with identification and management of the system risks, arranged in a sequence of overlapping stages, and which acts as a common reference for communication and understanding.
Adapted from ISO/IEC 15288: 2002

The concept of risk and the various categories of risk have been described in Chapter 1. The subject of risk management is very large. Process risk management, while forming a subset of the overall topic, is in itself vast. It integrates scientific, engineering, behavioural and general management functions into a single framework, focusing on identification, assessment, treatment and control of risk.

Most people take a narrow view of process risk management, within the constraints of their area of specialization, or area of responsibility. From an organisation's perspective, it is not only necessary to take the broader view, but ensure that all the different organisational functions (production, engineering, procurement, product storage and distribution) gain an appreciation of the broad picture, and an in-depth understanding of risks in their respective areas.

In the traditional view, risk management is viewed as part of general project management or a production management function. In recent years, it has been recognised that risk affects every stage of a process facility life cycle, and therefore managing risks should become an integral part of the overall management system.

Many system models have been developed for process risk management. The basic components of them are similar, namely identification of hazards, assessment of risk, and development of control measures to manage the hazards.

3.1 LIFE CYCLE RISK MANAGEMENT

Risk is present in every aspect of the life cycle of a facility. Therefore it requires us to identify and manage the risks in every stage of the life cycle and develop methods to manage them. The integrated approach to life cycle management has become the focus in recent years, but has not been universally adopted by the industry.

We need to focus on two aspects of life cycle, as the term "life cycle" has been used both in the context of process systems risk management, and environmental impact assessment. There is some overlap of the life cycle components, but these two aspects of life cycle are essentially different.

Life cycle stages for any generic industry are defined as concept, development, production, utilization, support and retirement stages (ISO/IEC 15288: 2002). We have used slightly different terms that are more familiar in the process industries to define life cycle stages for a process facility, but consistent with ISO 15288.

3.1.1 Process Facility Life Cycle

The life cycle components listed and discussed here are from the viewpoint of a new facility in a greenfield site, and would vary slightly for extensions to brownfield facilities. The major stages are outlined in Figure 3-1.

The process gets complex as a number of contracting companies may be involved during the various stages. There may be delays between Stages 2 and 3 during the capital investment funding and approval process.

Stages 4 and 5 (sometimes stages 3 to 5) generally go together, following a tendering process. The stage directly managed by the corporation is Stage 6, and even here, outsourcing of maintenance is being increasingly practised. The common thread that runs through Stages 1 to 5 is the project management team from the corporation (client representation). Achieving consistency and alignment to corporate practices during the different stages requires special skills and extensive planning.

A risk management model should consider all stages of the facility life cycle. For instance, a decision made at the design stage to reduce capital expenditure may increase the operating cost over the entire operating life of the facility.

It is also essential that decommissioning and site remediation requirements are taken into account at the design stage as part of an integrated design approach (Hicks et al. 2000).

A detailed discussion on managing risks through the life cycle of a facility is provided in Chapter 12.

3.1.2 Environmental Life Cycle

The control of environmental pollution from process industries has been receiving ever increasing attention and legislation since the 1970's. However, the analysis of

the environmental impacts has not been holistic, using a life cycle approach (LCA). There have been a number of recent calls to undertake LCA in environmental impact assessment and management (Nicholas et al., 2000). Standards have been developed to assist in the assessment (ISO 14001-1998).

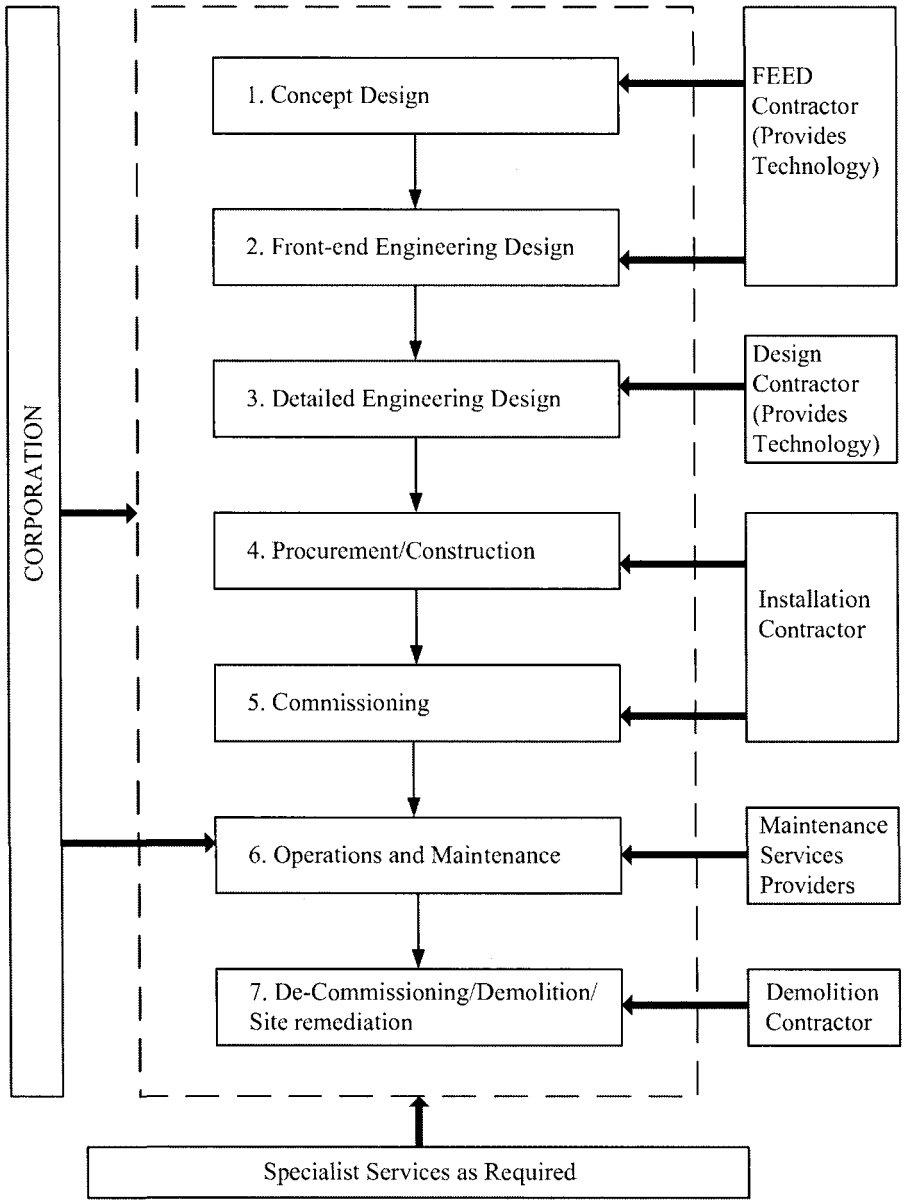

FIGURE 3-1 FACILITY LIFE CYCLE

Life cycle assessment has been defined as a scientific and technical methodology to assess, analyse and evaluate environmental and other impacts of a product, product group or material (Khan et al., 2002).

In the LCA, the environmental impact assessment of extraction of raw materials (pre-manufacturing), receival and storage, handling and processing of raw materials, intermediates, products and final waste disposal is considered from a 'cradle-to-grave' perspective. From primary supply through to ultimate disposal. Environmental fate of the disposed waste is also considered. The assessment covers both quantities handled and energy flows though the process.

For an organisation desiring to design, construct and operate a process facility, it would be difficult to take into account the pre-manufacturing stage of raw material extraction, which essentially forms the product of the raw material supplier.

From a process systems perspective, the environmental life cycle for a process facility consists of the steps shown in Figure 3-2. For each step of the life cycle, emissions during normal operations (stack discharges, aqueous effluents, wastes) and emissions from abnormal operations (spills, releases and all loss of containment), are considered for each material, along with flows of energy.

The facility life cycle and the product environmental life cycle complement each other and should be considered synergistically, as a loss of containment affects both process safety and the environment.

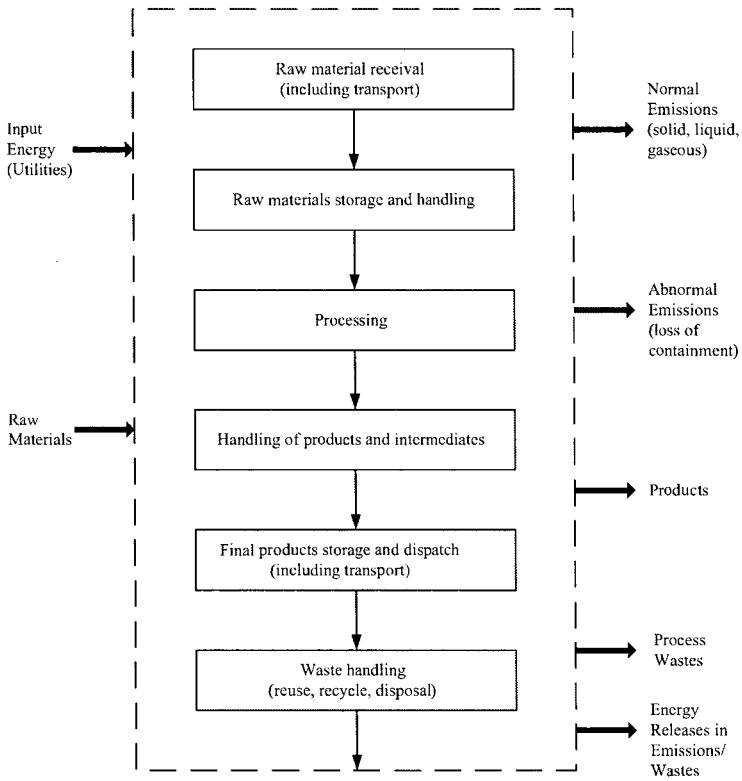

FIGURE 3-2 PRODUCT ENVIRONMENTAL LIFE CYCLE IN A FACILITY

3.2 ONE AND TWO DIMENSIONAL MODELS OF RISK

A number of risk management models are available in the literature. Many of the models have originated from the insurance industry. In a broad framework, the models used by the insurance industry and the process industry appear similar, and in some cases identical. When it comes to filling the boxes in the framework, the details are quite different.

There are two dimensions from which risk can be managed, and a model is presented for each.

3.2.1 One-Dimensional Model

This is a simple, linear model where the hazards are identified, analysed, evaluated for their impacts, and decisions are taken for appropriate reduction of risk (see Figure 3-3).

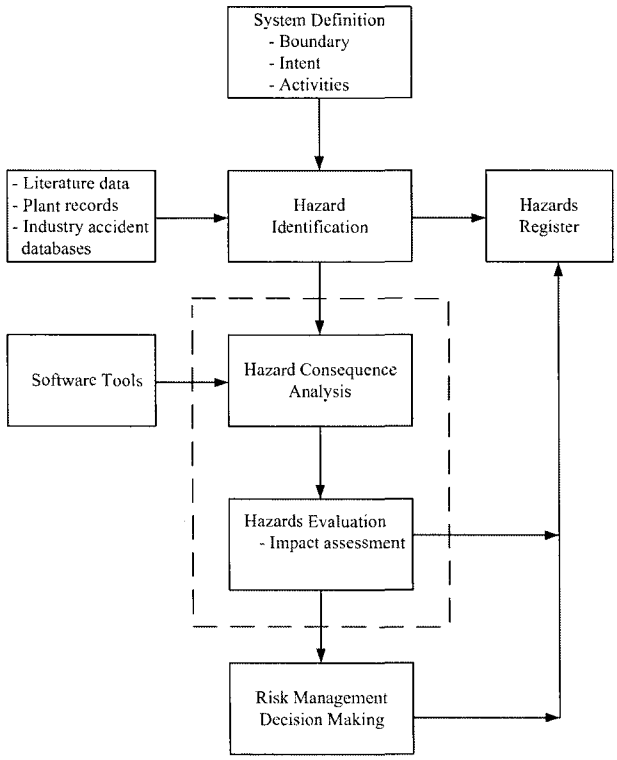

FIGURE 3-3 ONE-DIMENSIONAL MODEL FOR PROCESS RISK MANAGEMENT

The linear model has 4 steps (the consequence analysis and impact assessment combined as a single step). Some of these steps are common to more complex models that are discussed later on, and will not be repeated.

Step 1: System definition

System definition constitutes three elements:

a) system boundary
b) system objectives or intent and
c) activities that occur within the system boundary

It is essential to mark the system boundary clearly, along with interfaces of the boundary with other systems. If this step is not undertaken with clarity, the result will be a muddle of interacting systems which is difficult to analyse systematically.

The next element is defining the objectives of the system. This can be a simple box model, which describes the intent of the system, along with the inputs and outputs.

The final element is a list of activities that occur within the system. This may be the "methods" by which the system objectives are achieved.

EXAMPLE 3-1 DEFINING SYSTEM BOUNDARIES

Figure 3-4 illustrates the system boundary and how the selection of boundary influences the study, with respect to a simple example, a semi-batch process to manufacture ethanolamines (EA) by reacting ethylene oxide (EtO) with ammonium hydroxide solution.

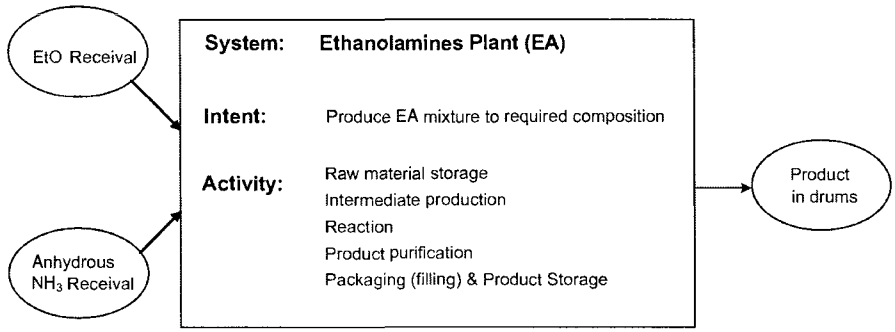

FIGURE 3-4 LARGE SYSTEM WITH SINGLE BOUNDARY

If we take the system into the next step of hazard identification, it is clear that the system boundary is too large to make an effective start. In a system with a large boundary, the subsystems become activities. Unless each activity is analysed in detail, along with interactions between activities, the hazard identification step becomes difficult, and some hazards can be missed.

In Figure 3-5, the large system has been broken down into subsystems with interactions shown. The activities of the large system become the subsystems. If the intents and activities are listed for each of the subsystems, a more detailed picture emerges, that facilitates hazard identification.

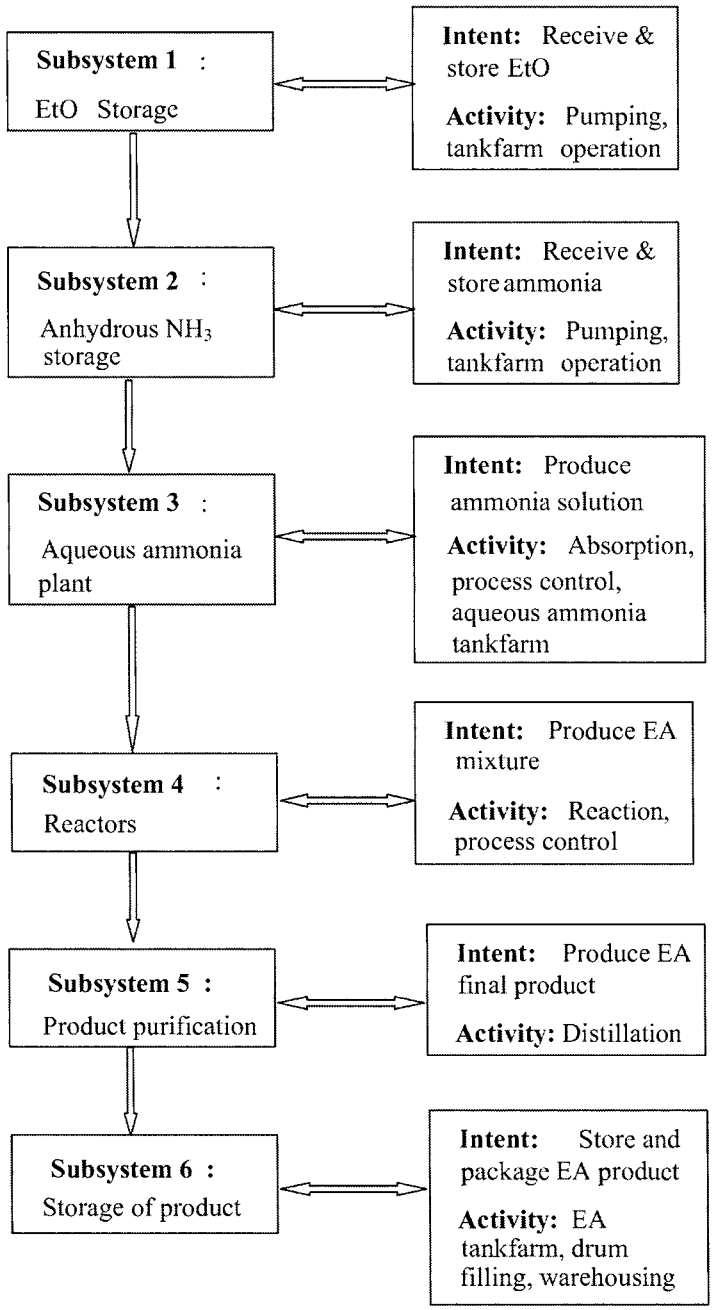

FIGURE 3-5 SUB-SYSTEMS WITH SMALLER BOUNDARY WITH INTERFACE TO OTHER SUB-SYSTEMS

Step 2: Hazard identification

By following the definition of hazard in Chapter 1, we do not confine the hazard identification to safety aspects alone. The hazard identification would include all aspects such as safety, environmental impairment, production interruption, asset loss etc.

The hazard identification is the most crucial step in the entire process of risk management. A hazard not identified may come to haunt the management sometime during the life cycle of the facility. It resides as a "latent" factor in the system. This step cannot be and should not be rushed.

A number of systematic hazard identification tools are available. These tools, which are discussed in Chapter 4 include:

- Checklist of generic hazards
- Process Hazards Identification Matrix
- 'What if' analysis
- Concept Hazard Analysis (CHA)
- Failure Mode and Effects Analysis (FMEA)
- Failure Mode Effects and Criticality Analysis (FMECA)
- Hazard and Operability Study (HAZOP)
- Scenario Based Hazard Identification

It should be borne in mind that no single technique is capable of identifying the hazards for *all* types of facilities and *all* stages of the facility life cycle. The selection of appropriate tool, or combination of tools is vital to the success of the hazard identification step. Details of the methods and recommended selection criteria for different situations are provided in Chapter 4.

Step 3a: Consequence analysis of hazards

Once the hazard identification step is complete, the next step is to estimate the magnitude of the consequences, should the hazardous event occur. The assessment of severity consists of two-step process:

1. Assessment of effects of the incidents (release of hazardous materials, fires, explosions, toxic impacts). These are the immediate consequences of the incident. Well established predictive tools are available, with new and ever growing research material. Details are given in Chapters 5 and 6.
2. Assessment of vulnerability of targets, using the outputs from effects assessment. These include effect on people exposed, effect on plant structures and equipment, and final consequences such as injury, fatality, asset damage, loss of production, environmental impairment etc. This is an area where there is considerable research in progress to minimise uncertainty in the estimates. Details are given in Chapters 5, 6 and 7.

Step 3b: Vulnerability assessment

In this step, the results of consequence analysis are evaluated in terms of potential impact on personnel, public, property and business activity. A ranking based on severity can be undertaken.

It is essential that this evaluation covers the life cycle. For instance, a significant delay in commissioning may cost dearly with interest on capital borrowings accruing and no revenue to service the investment loan.

It is also necessary to ensure that the impact of final plant decommissioning be considered up front, especially where potential environmental impairment over a long period of operation is identified such as soil or groundwater contamination that requires significant remediation. Many organisations do not generally allow for this cost in the discount rate and use risk-free capital value in the economic analysis. As pointed out by Hicks et al. (2000), decommissioning and remediation costs can be about 4-5% of the total assets for the chemical/petroleum process industries, 8-9% for offshore oil and gas production and as high as 25% for nuclear installations.

Step 4 (1-D Model): Decision Making

This step is not easy. By attempting to mitigate the consequences of an event, it is not clear how far one should go. That is, how safe is safe enough? Where possible, one could decide that all incidents that have an offsite impact on the public would be mitigated to the extent of no offsite impact.

Where there is insufficient information to make decisions, especially those involving high capital expenditure, it would be prudent to use the two-dimensional model of risk management rather than the one-dimensional model. Only the subset of hazards where decision making is fraught with uncertainty, need to be carried forward to the 2-dimensional analysis.

One of the important aspects of decision making is the question: "Can the process be made safer at the design stage?"

This brings us to the area of inherently safer design (ISD), further discussed in Section 3.6, and Chapter 12.

EXAMPLE 3-2 ETHANOLAMINE PLANT ANALYSIS

The one-dimensional model is applied to the manufacture of ethanolamines, following on from Example 3-1.

System definition: The overall system in Figure 3-4 has been broken into subsystems in Figure 3-5, with boundaries of the subsystem shown.

Hazard identification: There is no fixed formula for hazard identification. Systematic hazard identification methods are described in Chapter 4.

Reactive chemical hazards must be identified in the process, besides conventional hazards such as fire, explosion and toxicity hazards from loss of containment.

For the purpose of illustrating the one-dimensional model, the main hazards are:

- Fire from ethylene oxide leak and ignition (highly flammable material)
- Vapour cloud explosion from ethylene oxide leak (atmospheric boiling point is about 10°C, and a release may flash and form a vapour cloud under higher ambient temperatures)
- Toxic impact from anhydrous ammonia release
- Loss of containment of corrosive materials (ammonium hydroxide, ethanolamines)
- Runaway reaction (highly reactive chemical)

The hazard identification above is for illustrative purposes and is not comprehensive. Detailed hazard identification methods are shown Chapter 4, using different hazard identification techniques.

Analysis: The analysis involves identifying possible causes for each hazard, estimating the consequences and developing possible prevention and mitigation measures. A tabular format is preferred, as shown in Table 3-1.

Evaluation: The hazard prevention and mitigation measures are evaluated for their adequacy, whether additional measures are required and associated costs of these measures. For instance, one measure of suppressing runaway reaction is automatic dumping of water into the reactor through a water valve actuated by the temperature sensor reading high temperature.

Decision making: The decision making is based on the extent of consequence minimisation that can be achieved by the control measure. There may be a tendency to depend too much on operator action or intervention as a way of reducing the cost of instrumentation. This can be a problem when the operator is involved in other duties. A balance is required, and additional information may become necessary to make informed judgements. This will typically involve the dynamic behaviour of the process.

The inherently safer design question should be asked and answered before a decision is made. For our example, the question is "Can we eliminate anhydrous ammonia storage and handling by importing aqueous ammonia in road tankers?". This will eliminate the hazard, but adds additional capital in terms of aqueous ammonia storage, and additional transport costs during the facility's operating life.

■ ■ ■

TABLE 3-1 HAZARD ANALYSIS OF ETHANOLAMINES MANUFACTURE

No	Hazard	Causes	Consequences	Prevention/ mitigation measures
1	Ethylene oxide release	• Material failure • Flange gasket leak • Pipe rupture • Corrosion • Mechanical impact • Failure during transfer from transport vehicle	• Fire • Vapour cloud explosion potential • Incident escalation potential (intermediate consequence) • Toxic impact of ethylene oxide on exposure to personnel	• Storage design integrity • Mechanical integrity inspections • Transfer procedures • Active fire protection • PPE • Protection against mechanical impact
2	Anhydrous ammonia release	• Stress corrosion of pressure vessel • Flange gasket leak • Pipe rupture • Mechanical impact • Flexible hose failure during transfer from road tanker	• Toxic cloud • Potential for serious injury/ fatality on exposure • Fire potential low compared to toxicity impact	• Storage design integrity • Mechanical integrity inspections • Transfer procedures • Personal protection equipment • Emergency shutdown system (ESD) • Emergency response procedures • Protection against mechanical impact
3	Runaway reaction	• Loss of cooling water during reaction • Agitator failure • Human error • Temperature control failure • Incorrect reaction mixture	• Rapid temperature/ pressure rise in reactor • Potential for reactor vessel failure • Serious injury/ fatality potential	• Reactant addition control • Temperature monitoring • High pressure protection • High temperature protection • Pressure relief • Operating procedures (batch recipes)

No	Hazard	Causes	Consequences	Prevention/ mitigation measures
				• Operator training • Preventive maintenance
4	Release of corrosive materials	• Flange gasket leak • Pipe rupture • Corrosion • Mechanical impact • Spill during product packaging	• Skin injury on exposure • Irritant vapours causing injury (eyes, inhalation)	• Mechanical integrity inspections • Selection of materials of construction • Protection against mechanical impact • PPE

Advantages of the one-dimensional model

There are a number of advantages with the one-dimensional model, and it is useful for application to workplace safety in simple facilities with low consequence impact of incidents. The features include:

- simple to use
- can be qualitative, with some quantitative assessment of consequences
- less uncertainty in the model as more refined consequence assessment software is becoming available at affordable costs
- analysis can be carried out by a trained engineer using relevant software for consequence modelling
- focuses on consequence prevention and mitigation, and has a more direct effect on hazard control

Disadvantages of the one-dimensional model

There are a number of disadvantages and hidden problems with this linear model:

- does not consider the likelihood of incidents and hence decision could be biased, at a cost, on directing too much effort on controlling very low likelihood events
- cannot prioritise the decisions in terms of importance in hazard control as the probabilities of the events have not been assessed
- how far should one go down the path of hazard control is the question the simple model cannot answer (the question of 'how safe is safe enough?' remains unanswered)
- uncertainties are not accounted for in decision making
- if there are several options giving approximately the same level of consequence mitigation, in the absence of likelihood estimation, cost

alone cannot be the criterion for decision making, as the reliability of the hazard control measures could vary significantly

The one-dimensional model is useful as a first-pass assessment to generate an understanding of the hazardous events and their consequences, but more sophisticated models are necessary for decision making and life cycle management of risk in major hazard facilities.

3.2.2 Two-Dimensional Model

As described in Section 1.2.2, risk has two dimensions, the severity of the consequences of an event and the likelihood (or probability) of occurrence of that severity.

In the two-dimensional model, both the severity of the hazardous occurrences and their likelihood are assessed to obtain a magnitude of risk. A model is shown in Figure 3-6. References to various chapters in this book are indicated in the figure to show the linkages.

The first three steps on the 2-D model are identical to the 1-D model described in the previous section.

Step 4 (2-D Model): Estimation of Incident Likelihood

The power of the 2-D model becomes obvious when step 4 is undertaken. This assessment of likelihood is a major source of uncertainty in the risk assessment process, and different analysts may produce different results, often due to unavailability of statistically valid reliability data.

For incidents related to occupational injuries (slips, trips and falls, working at heights, materials handling etc), there is sufficient epidemiological data to make reasonable predictions. However, for process incidents that can result in major consequences, often the initiating event could be a loss of containment of hazardous material, and event propagation through to a fire or explosion, and incident escalation. While these events are fortunately few, the final outcome probability for a specific facility cannot be predicted by actuarial data on fires and explosions. There are simply too many variables involved, depending on the mechanical integrity of plant and equipment, operating parameters, the quality and effectiveness of the process safety management system, and human error contributions.

A qualitative estimate can be made within an order of magnitude, based on actuarial data. One example is that there is a 1-10% chance of occurrence of an incident in a given year, provided operating conditions and practices do not change. For a first pass, this may be adequate.

If a quantitative estimate of the likelihood is required in terms of a probability or frequency of occurrence, then the analysis becomes complex. Techniques such as fault tree and event tree modelling or Markov techniques may need to be used. Details of methods for both qualitative and quantitative estimation of probability are given in Chapter 8.

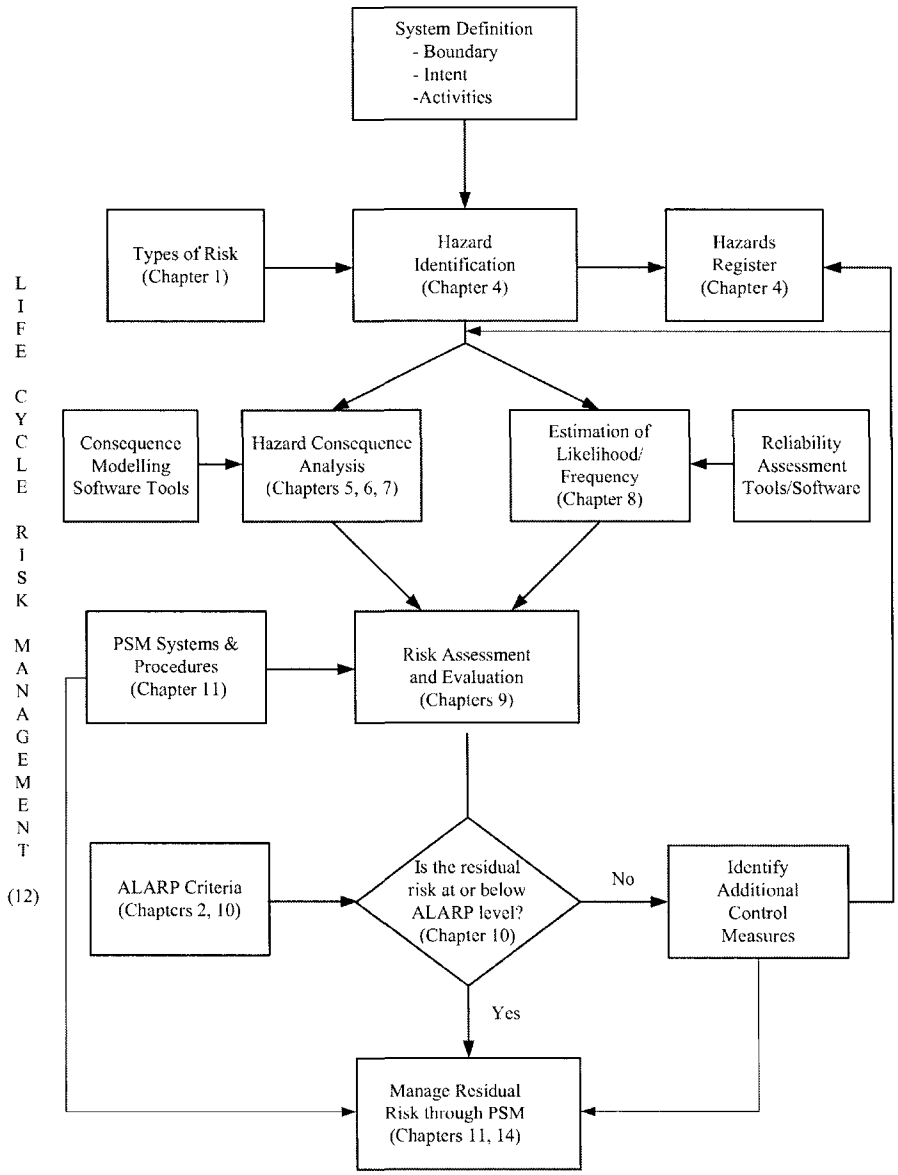

FIGURE 3-6 TWO-DIMENSIONAL MODEL FOR PROCESS RISK MANAGEMENT

In all estimations of likelihood, the following precautions should be observed:

1. Clearly list the assumptions made in doing the analysis, and provide the source and justification for the assumptions. The justifications may be based on:

- historical records
- actuarial data
- reliability databases
- actual plant data from maintenance records
- experienced judgement of plant personnel with several years of operating/ maintenance experience on the plant
- engineering judgement of the analyst (the analysts' own experience in being able to make good assumptions needs to be scrutinised)

2. Conduct a sensitivity analysis on the assumptions to identify how sensitive the assessed risk is to the assumptions. Critical assumptions can be further scrutinised, and further attempts may be made to reduce uncertainty.

If steps 1 and 2 are not undertaken, then the risk predictions can be questionable. The corporation is often at the mercy of the risk analyst, who can be an external service provider, and it is essential for the client representative to work with the analyst and question the assumptions made, in order to achieve a 'best estimate' outcome from the analysis.

Step 5: Evaluation of risk tolerance

Once the risk is estimated qualitatively or quantitatively, the next step in the risk management process is to examine if the risk is tolerable, using the criteria outlined in Section 2.4.

If the risk is deemed tolerable, then the residual risk is managed by the Process Safety Management (PSM) system. If not, one needs to identify further risk reduction measures. Risk reduction measures may comprise -

- Mitigation of consequences to reduce severity
- Additional layers of protection systems to reduce likelihood of the severity occurring
- A combination of both of the above
- Iterative estimation of risk, as a sensitivity analysis with the risk reduction measures in place to determine the adequacy and effectiveness of the risk reduction measures proposed
- Repetition of the above actions until a satisfactory strategy is evolved

Step 6: Decision Making

Armed with the consequence severity and incident probability information, the decision making on implementing a set of risk reduction measures becomes easier. Details of decision making under uncertainty are covered in Chapter 10.

The main considerations in decision making are:

- For new projects, can the design on paper be changed to incorporate more inherently safer design (ISD) features to eliminate some risks? (For details of ISD, see Chapter 12).
- If there are regulatory criteria for risk tolerability, as is the case in several countries, does the risk assessed meet the tolerability criteria? The criteria is generally set by regulatory authorities in connection with land use safety planning for process facilities located in proximity to populated areas (see Chapter 16).
- Does the risk meet the corporate risk criteria for personnel safety, environmental protection and business continuity? Many large national corporations and transnational corporations have developed corporate risk criteria for risk tolerability as part of their process risk management strategy.
- Is a cost-benefit analysis necessary to determine where the 'stop' sign should be placed in the risk reduction process? What is the *de minimis* criterion?

Ultimately, risk tolerance is based on the concept that we do not have to remove every hazard, but make the risks 'as low as reasonably practicable'. Kletz (1999) describes the ALARP concept as follows:

"We weigh in the balance the size of the risk and the cost of reducing it, in money, time and trouble. If there is gross disproportion between them, the risk being insignificant compared with the cost, we do not have to reduce it".

This concept has legislative backing in the UK, and is used as an 'in principle' concept by regulators in other countries. The ALARP concept is further discussed in Chapter 10, as a tool for decision making.

The two-dimensional model can be extended to a 3-dimensional model by adding the cost of losses (Grose, 1987).

Step 7: Managing residual risk

The attitude of people regarding "risk acceptance" varies among different countries, and among the types of industry/activity. In some cases, there are legal and emotive problems when it comes to assessing the risks of fatality from process incidents. For this reason, a quantitative risk analysis (QRA) is sometimes discouraged on the argument that "How can one place a value on human life?" What the antagonists of QRA tend to ignore is that the tool is very valuable for addressing loss of asset, and business interruption risks, even if potential loss of life is not quantified.

It must be recognised by corporations and regulators alike that as long as a process facility storing and handling hazardous materials is operational, the risk from the facility cannot reduce to zero, whatever the semantics of the argument may be. This means that after every attempt is made to reduce the risk levels from a facility to ALARP level, the residual risk must be managed. The most significant tool for day to day management of residual process risks is the Process Safety

Management (PSM) system. Details of developing and implementing a PSM program are described in Chapter 11.

The PSM is sometimes referred to as Safety Management System (SMS). The SMS may integrate elements of OH&S management within it, as there are some overlaps. We have used the term PSM and SMS interchangeably in this book, to denote process safety management as distinct from OH&S management system.

3.3 LAYERED PROTECTION MODELS

The layered protection model uses a hierarchy of hazard control measures, from basic control to physical protection of plant and equipment (Dowell, 1999). An overview is shown in Figure 3-7.

In principle, if the risk can be managed by lower level layers (inner layers in Figure 3-2), then an additional layer may not be necessary. However, in practice, codes and regulations demand some coverage of all layers.

Layer 1: Process design

In this layer, inherent safety features that can be built into the design are considered. Key features include:

- Selection of process technology with minimum inventories
- Selection of reaction pathways minimizing intermediates or complex reaction sequences
- Selection of a process with less hazardous materials
- Selection of a process with less severe operating conditions (e.g. temperature, pressure)
- Mechanical integrity
  - Materials selection
  - Corrosion allowances
  - Pressure rating (allow for possible range of pressures under process deviations)
  - Temperature rating (allow for possible range of temperatures under process deviations, including cryogenic conditions for low volatile hydrocarbons)
- Better access, isolation provisions

Layer 2: Basic process control, process alarms and operator monitoring

The process is controlled by a programmed logic controller (PLC) or distributed control system (DCS) system, with high and low alarms for control variable deviations. When the alarm is raised, the operator may make some process adjustments to control the deviation.

Often the alarm is raised by the same sensor that is performing the process control function, which can be seen in some old, but still operating plants designed in the 1970's.

This layer depends entirely on the operator's monitoring of the process, ability to diagnose causes of process deviations, and mount an appropriate response in

time. If alarms fail or if there is inadequate response such as human error or insufficient time to respond, the incident could escalate.

Layer 2 is necessary for routine process control and monitoring, but by no means adequate for hazard control, especially for systems with reactive hazards or systems where an external event such as a fire can cause serious incident escalation.

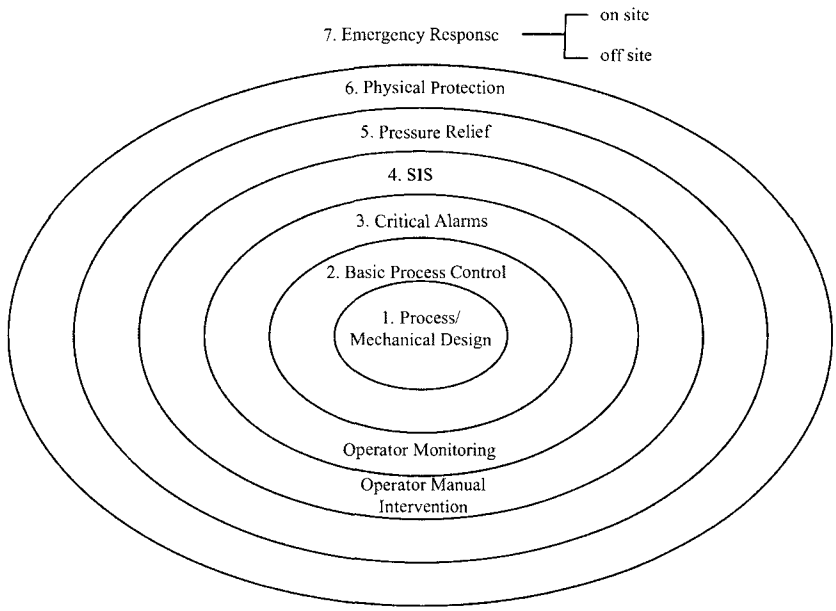

FIGURE 3-7 OVERVIEW OF LAYERED PROTECTION MODEL

Layer 3: Critical alarms and operator manual intervention

Layer 3 is similar to Layer 2, but alarms are given a priority or criticality rating. Critical alarms would require operator intervention, and possible manually initiated process shutdown of selected areas.

Key features of Layer 3 are:

- Independent sensors for process parameters such as pressure, temperature, flow, level and composition. These are separate to the sensors used for process control
- Critical alarms
- Interlocks
- Adequacy of isolation such as double isolation valves or double block and bleed valves
- Redundancy where appropriate

Details on safety integrity levels (SILs) are given in Chapter 8.

In Layer 3 operation, the operator would have to make a quick diagnosis and take quick decision on the intervention level. Process diagnosis and abnormal situation management (ASM) is a vital part of the risk management framework (Venkatasubramanian et al., 2003a,b,c). As in layer 2, it depends on effective diagnosis and response time available, and the experience of the operator. Layers 1 to 3 alone are not sufficient for hazard control in major hazard facilities.

EXAMPLE 3-3 OIL REFINERY, CRITICAL ALARMS

In an ageing oil refinery, the operating philosophy was based on Layer 2 protection. For the crude oil heater in the crude distillation plant, in the case of loss of feed to the crude heater, the following practice was adopted:

- a low flow alarm would be raised in the control room (priority high alarm)
- control room operator would contact the field operator by radio and ask for the standby pump to be brought on line
- field operator starts the standby pump by lining up the relevant manual isolation valves.

On one occasion, the field operator was pre-occupied with a problem in another area of the plant and could not respond quickly. By the time the standby pump was started, the skin temperature of the tubes in the furnace reached failure levels and the tube ruptured.

Layer 4: Automatic action through safety instrumented system or emergency shutdown

Layers 1 to 3 are often adequate for day-to-day running of the process. However, if the consequence of an incident is assessed to be severe, or the overall risk is assessed to be high (a qualitative assessment is often sufficient at this stage), a safety instrumented system (SIS) can be designed that will undertake actions to initiate an emergency shutdown (ESD) (IEC 61598 1998; IEC 61511 2003).

This layer is one level more sophisticated than Layer 3 in that it does not rely entirely on operator response, but conducts an automatic process action.

In Layer 4, there is also provision to initiate an ESD from the control room or from selected locations in the plant, by push-button operation.

EXAMPLE 3-4 CRITICAL ALARMS

If we apply Example 3-3 to Layer 3, on low flow of feed, the following automatic actions could be designed:

- the standby pump starts automatically. This requires some automation of the valves.
- if the standby pump does not start within a specified time, monitored by a timer in the process control system, there would be a furnace burner trip.

In the above arrangement, there is room to retain the original operating philosophy of field operator starting the standby pump, if so desired.

Main features are:

- Automatic activation of standby or redundant system
- Automatic isolation of process section through actuated valves, independent of control valves
- Location of valves
- Location of ESD push-button stations ensuring that the stations would be accessible, and would not themselves by impaired in the incident
- Separating the control system and the protection system which include sensors and isolation valves
- Safety integrity level (SIL) assessment for the SIS
- Emergency depressuring system such as instrumented system that rapidly relieves the pressure to the flare or a scrubber
- Fail-safe design of actuated valves on power or instrument air failure

Details on safety integrity levels are given in Chapter 8.

Layer 5: Pressure relief systems

For pressurised systems, pressure relief of the equipment is a pressure vessel code requirement, and often a statutory requirement.

Operation of pressure relief, while protecting the equipment, can cause environmental problems through atmospheric discharge. Therefore, an instrumented system for pressure protection (Layer 4) precedes the pressure relief layer. This is recommended by American Petroleum Institute (API 14C 2001) for all offshore oil and gas facilities.

The main features are:

- Selection of pressure relief type (e.g. pressure safety valve, rupture disc)
- Sizing of the relief system for single phase or two-phase discharge
- Selection of relief discharge point such as atmospheric discharge, scrubber system or flare system

Layer 6: Physical Protection systems external to the process

The protection systems are physical systems to mitigate the incident severity and escalation prevention. Typical protection systems are:

- Bunded or diked areas to retain losses
- Gas detection for flammable and toxic gases
- Gas knock down or dispersion agents such as water sprays and steam curtains
- Fire detection (flame, smoke, heat detection)
- Active fire protection including firewater system, foam, gaseous or powder fire suppressants
- Passive fire protection such as thermal lagging of equipment and structures, firewall and blast wall

Layer 7: Mitigation system based on procedures (Emergency response)

This layer essentially consists of

- Emergency response procedures as part of the safety management system
- Emergency preparedness based on pre-incident plans
- On-site emergency response
- Off-site emergency response

Layers 1 to 3 are used for day-to-day operation and control of the process plant, and Layers 4 to 7 are for managing major incidents that could occur in the plant.

The selection of higher layers exceeding Layer 3 depends on a number of factors:

- Regulatory requirements. If a regulation requires a level of protection to be provided that falls into layers beyond Layer 3, it must be provided.
- Standards and recommended codes of practice. Some of these may be advisory and not mandatory under a regulation, but the concept of 'industry best practice' requires compliance with these codes and standards.
- Nature of the process and operations. From the time a process deviation occurs, how much time is available before manual intervention and control becomes impossible? If the time is inadequate, then resorting to Layer 4 and above becomes a necessity.
- Effectiveness of the safety management system. How much credit can be given to the skill and diligence of the operators, remembering that the safety management system should be 'system dependent' and not 'individual dependent'? To answer this question, we need to ask - "What is the consequence of the deviation, if left uncontrolled, or responded to in an incorrect manner?" If the consequence severity is high, go to Layer 4 and above.

Experience has clearly shown that a major hazard facility would need all the layers of protection in varying degrees.

3.4 RISK RANKING MODELS

We have seen in the 2-dimensional model of section 3.2.2 that it requires an assessment of risk for decision making. This assessment can be either qualitative or quantitative. A qualitative assessment is very useful at the hazard identification stage, to enable a rapid ranking of risks (Tweeddale 2003).

Rapid risk ranking has the following advantages:

- It helps to prioritise the risk and highlights higher risk events that need more detailed analysis.

- It helps to screen out some low risk events that can be managed routinely by the safety management procedures.
- It is particularly useful at the hazard identification stage, in order to define the scope of future safety analysis that possibly require quantitative assessments.
- It provides a useful input to the layer of protection analysis (LOPA) (see Chapter 12 for more details on LOPA).
- If a criticality assessment is required in the Failure Mode and Effects Analysis (FMEA) in hazard identification, then the rapid risk ranking helps to assign the criticality. See Chapter 4 for more details.

The qualitative assessment of risk may be conducted using a *risk matrix*. A risk matrix is a graphical representation of the risk as a function of probability (likelihood) and consequence (severity). Section 2.1.2.1 introduced the idea.

A widely used matrix in Australia and New Zealand, across a wide range of industries has been the standard Australian/New Zealand (AS/NZS 4360 1999). Figure 3-8 shows such a risk matrix that is appropriate to the process industries. It is interesting to note that "almost certain" and "likely" events have a high or extreme risk ranking regardless of the severity. Similarly, high severity incidents "Major" and "Critical" have a higher risk ranking regardless of likelihood. The risk allocation in the various cells in the matrix ensures that high severity events cannot be screened out because of perceived low frequency at the qualitative evaluation stage, but they need to be carried forward for further analysis.

The most recent version of the generic risk matrix (AS/NZS 2004a, 2004b) has downgraded the 'extreme' risk category in a number of cells to 'high' or 'very high'. It is however noted that the risk categorization is dependent on the application area. For the process industries Figure 3-8 represents an appropriate categorization.

Rule sets should be developed for allocation of severity and likelihood scale. A probability scale is suggested in Table 3-2.

Severity scales can be developed for several categories of risk, including safety, environmental performance, impact on business, and impact on corporate reputation. A comprehensive severity scale is shown in Table 3-3. Each organisation may define its own rule sets, based on corporate requirements and experience.

The advantage of the risk matrix is that events which require priority action from management to reduce the risk from a higher level to a lower level, as far as reasonably practicable, can be easily seen using this graphical method.

Likelihood or Frequency	Consequence Severity				
	Low	**Minor**	**Moderate**	**Major**	**Critical**
Almost Certain	High	High	Extreme	Extreme	Extreme
Likely	Moderate	High	High	Extreme	Extreme
Possible	Low	Moderate	High	Extreme	Extreme
Unlikely	Low	Low	Moderate	High	Extreme
Rare	Low	Low	Moderate	High	High

FIGURE 3-8 EXAMPLE OF RISK MATRIX

The judgement of the participating team from the corporation is essential in order to use the risk matrix for risk allocation and ranking. There should be at least one management representative in the team to be able to make judgements of costs associated with business interruption risks and risks of damage to corporate reputation.

The application of the risk matrix is described in Chapter 4 under hazard identification.

The risk matrix appears easy to use on the face of it, but in practice, can raise a number of difficulties. Some of the pitfalls and methods to overcome these are described in Chapter 9 under risk assessment.

TABLE 3-2 EXAMPLE OF LIKELIHOOD SCALE (WITH PERMISSION FROM BLUESCOPE STEEL PTY LTD)

Likelihood	Description	Frequency Scores*
Almost Certain	Event expected to occur in most circumstances	Does Occur Definite history of occurrence Frequency between once and ten times a year
Likely	Event will probably occur in most circumstances.	Possible history of occurrence Probably occur once per decade and history of near miss Frequency between 1 every 10 years and 1 per year
Possible	Event should occur at some time.	May happen once in plant lifetime Possible history of near miss Frequency between 1 every 100 years and 1 every 10 years
Unlikely	Event could occur at some time.	Low likelihood of occurrence Frequency between 1 every 1000 years and 1 every 100 years
Rare	Event may occur, but only under exceptional circumstances.	Very Low likelihood of occurrence Frequency between 1 every 10,000 years and 1 every 1000 years

* The frequency descriptions must be generated for each specific risk assessment, so that the time range is appropriate to the level of detail of the risk assessment.

TABLE 3-3 EXAMPLE OF SEVERITY SCALE (WITH PERMISSION FROM BLUESCOPE STEEL PTY LTD)

Low	Minor	Moderate	Major	Critical
Injury and Disease (includes workers and community)				**SAFETY**
Minor injury. No medical treatment e.g. cuts, bruises, no measurable physical effects	**Significant injury.** Medically Treated Injuries from which recovery is likely. e.g. burns, broken bones, severe bruises, cuts.	**Serious Injury**. Moderate permanent effects from injury or exposure. e.g. serious burns, serious internal and/or head injuries, gassings that require hospitalisation.	**Single fatality** and/or, Severe permanent injury, paralysis, brain damage, life threatening exposure to a health risk	**A Multiple fatality** and/or, Significant irreversible exposure to a health risk that effects greater than 10 people

Environmental effects			ENVIRONMENT	
Low Pollution No observable effect to plants or animals. No requirement to inform authorities. No visible discharges observed offsite	**Minor Pollution** Minor effects on plants & Animals. Required to inform authorities. May involve a cleanup. Visible discharge observed offsite.	**Moderate Pollution** Moderate effects on plants & animals. Physical impact on the public. Required to report to authorities. Extensive cleanup may be required.	**Major Release** Major effects on Plants & Animals. Substantial cleanup costs. Personal & business prosecution possible	**Extreme Event** Permanent effects on the environment. Potential loss of licence to operate. Prosecution of company and directors possible.
Social / cultural heritage				
Low-level social or cultural impacts. Low-level repairable damage to commonplace structures.	Minor medium-term social impacts on local population. Minor damage to structures / items of significance. Minor infringement of cultural heritage. Mostly repairable.	Ongoing social issues. Permanent damage to structures or items of cultural significance, or significant infringement on cultural heritage / sacred locations.	On-going serious social issues. Significant damage to structures or items of cultural significance, or significant infringement and disregard of cultural heritage.	Very serious widespread social impacts. Irreparable damage to highly valued structures, items or locations of cultural significance. Highly offensive infringements of cultural heritage.
Operational impact			**PLANT / BUSINESS ($)**	
Easily addressed or rectified by immediate corrective action. No loss of production. No damage to equipment.	Minor or superficial damage to equipment and/or facility. Minor loss of or impact on production.	Moderate damage to equipment and/or facility. Significant loss of production.	Major damage to facility requiring significant corrective/preventative action. Serious loss of production.	Future operations at site seriously affected. Urgent corrective/remedial action required. Major loss of production.
Financial / Marketing / Customers				
Can be easily absorbed through normal activity.	Consequences can be absorbed, but management effort is required to minimise impact. Minor delivery delays	Significant event, which can be managed under Special circumstances. Some customers seek alternative supply for short term. Normal circumstances.	Major event, with prioritised and focused management will be endured. Some customers lost to alternative supply.	Extreme event with potential to lead to failure of most objectives or collapse of part of business. Key customers lost to alternative supply.
Legal				
Low-level legal issue. Technical non-compliance. Prosecution unlikely.	Minor legal issues, non-compliances and breaches of regulation. Minor prosecution or litigation possible. On the spot fine.	Serious breach of regulation with investigation to report to authority. Prosecution and/or moderate fine.	Major regulatory breach with potential major fine. Investigation and prosecution by authority. Major litigation.	Investigation by authority with significant prosecution and fines. Very serious litigation, including class actions.
Total Business Cost Impact				
< $50k	**$50k - $500k**	**$500k - $5M**	**$5M - $25M**	**> $25M**

Community / government / media / reputation				OUTRAGE
Public concern restricted to local complaints. Ongoing scrutiny / attention from regulator. Individual concern. No discernable impact on reputation.	Minor, adverse local public or media attention and complaints. Significant hardship from regulator. Reputation is impacted with a small number of people.	Attention from media. Heightened concern by local community. Criticism by local NGOs. Significant difficulties in gaining approvals. Reputation impacted with some key stakeholders.	Significant adverse national media / public / NGO attention. Licence to operate suspended or not gain approval. Reputation impacted with significant number of key stakeholders. May lose licence to operate or not gain approval. Environment / management credentials are significantly tarnished.	Serious public or media outcry (international coverage). Damaging NGO campaign. Licence to operate threatened. Reputation impacted with majority of key stakeholders.

(NGO = Non Government Organisation)

3.5 INTEGRATED SYSTEMS MODELS

There have been attempts to develop integrated risk management models. Two general forms of model exist.

In the first type, management of safety, both process safety and occupational health & safety, environment and quality are integrated into a single framework, taking into account the overlapping elements among them.

In the second type, the traditional source-pathway-receptor model for environmental risk from release of environmental pollutants is extended to cover process risk (Marshall and Ruhemann 1997).

3.5.1 Integrating Safety, Environment and Quality

Many organisations have attempted to have a single integrated system for quality, safety and environmental management. While some success has been achieved in integrating the quality, environmental system and OH&S system, the integration of PSM into the framework has proved difficult. One of the main problems is that the coordination responsibilities for quality, environment and process safety lie with different groups in the organisation, presenting logistic difficulties in integration.

An alternative is to interface the disciplines of quality, OH&S, environment and process safety, rather than integrate them. The overlaps can then be managed by an information management system and inter-discipline coordination.

A simple interface model is given in Figure 3-9.

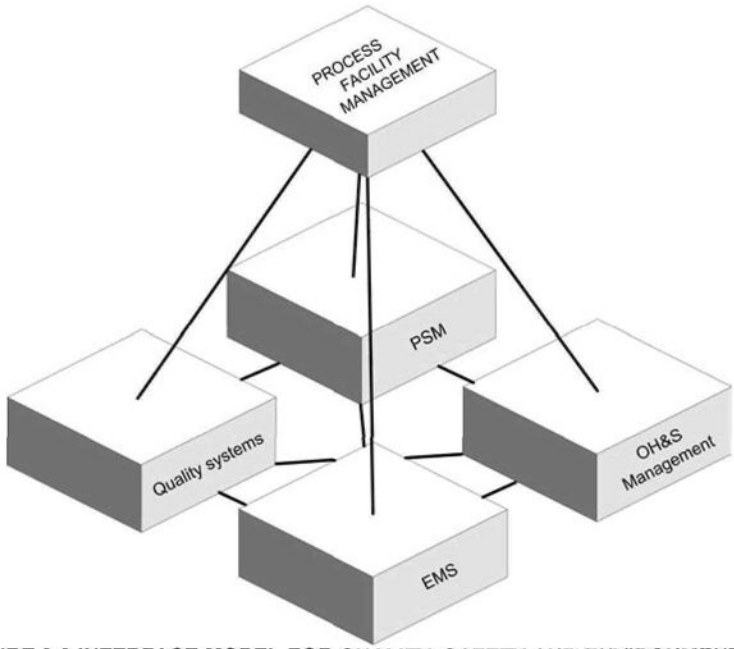

FIGURE 3-9 INTERFACE MODEL FOR QUALITY, SAFETY AND ENVIRONMENTAL MANAGEMENT

It is essential that this integration occurs for the design stage of a new facility, where safety, reliability and environmental performance are to be addressed simultaneously. It should be an on-going integration across the process life cycle. Currently, in many instances, the safety analysis studies, reliability studies, the environmental assessment studies and the project quality requirements are fragmented in their approach, and the synergies are not exploited at the time of design.

The common elements among the modules, expressed in terms of the quality elements are (ISO 9001):

- Management responsibility
- Design control
- Document control
- Process control
- Control of non-conformances
- Corrective action
- Handling storage, packaging and delivery
- Training
- Audits

The modules of quality, environmental management, OH&S management and process safety management under the umbrella of the facility management can share the same information on common elements from the organisation's information database.

This aspect is discussed further in Chapter 11 under process safety management systems.

3.5.2 Generalised Hazard System Model

The source-pathway-receptor model has been traditionally used for many years in environmental risk assessment (Pritchard 2000). In this model, an emission occurs from a source (e.g. a stack), the environmental receptors are people, atmosphere, surface water, groundwater, and soil, and there are many pathways by which the emission can reach the receptor. See Section 5.2.1.

Marshall and Ruhemann (1997) extended this concept to a generalised hazard system, consisting of four elements:

1. A hazard source, capable of emitting hazardous material or harmful energy
2. Receptors, that have the potential to be harmed by absorption of such emissions - people, structure and biophysical environment
3. Transmission paths via both a route and a medium by which the harmful matter or energy can reach the receptor.
4. Barriers that have the potential to attenuate the emission or attenuate the absorption by the receptor.

In some instances a receptor can become a secondary source, emitting to yet another receptor, and so on. Therefore the main issues in transmission pathways in highly coupled process systems are:

- Process deviations
- Information pathways created by control system designs
- Generation of 'domino' sequences created by human error
- Thermal response of structures to fires
- Structural response to explosions
- Competing dynamic processes of incident escalation and emergency response
- Integrity of barriers in the transmission pathways

A sneak analysis for the pathways can help to identify hidden hazards (Whetton 1993). A model for competing dynamic processes of incident escalation and incident control by emergency response is described by Raman (2004).

EXAMPLE 3-5 OIL AND GAS PRODUCTION

An oil and gas production facility produces sour gas which is a mixture of methane, hydrogen sulphide, carbon dioxide, and small amounts of nitrogen and other hydrocarbons. The gas, with some natural gas liquids is received into a separator where the gas is separated from the liquid, and sent to carbon dioxide removal and drying.

Let us say the primary source (S_1) is the gas pipework, from which a gas leak occurs. The gas is both flammable and toxic. The primary receptor (R_1) is a

maintenance worker undertaking maintenance work nearby. The transmission path is the atmosphere whereby gas disperses.

Let us postulate that due to some fault in the maintenance equipment (R_2), the gas finds an ignition source and a jet fire results. The maintenance worker's equipment now becomes a secondary source (S_2). The receptor to the fire is a field operator doing routine surveillance work (R_3). There is also another receptor to the fire, which is the separator vessel (R_4), on which flame impingement may occur. The failure of separator vessel results in incident escalation which becomes a tertiary source (S_3) and so on.

There are toxic gas detectors in the plant, which raise an alarm. The maintenance worker carries an escape breathing unit, which is worn when the alarm is raised and the person evacuates the area. This provides one barrier (B_1). The maintenance worker is operating under a permit to work system, using approved electrical equipment for the classified hazardous area (Barrier B_2). Finally, the separator is protected by a fixed deluge system initiated by fusible plugs (Barrier B_3) that would either prevent failure or delay failure before which time the emergency shutdown system would isolate the leak.

The system is described in Figure 3-10.

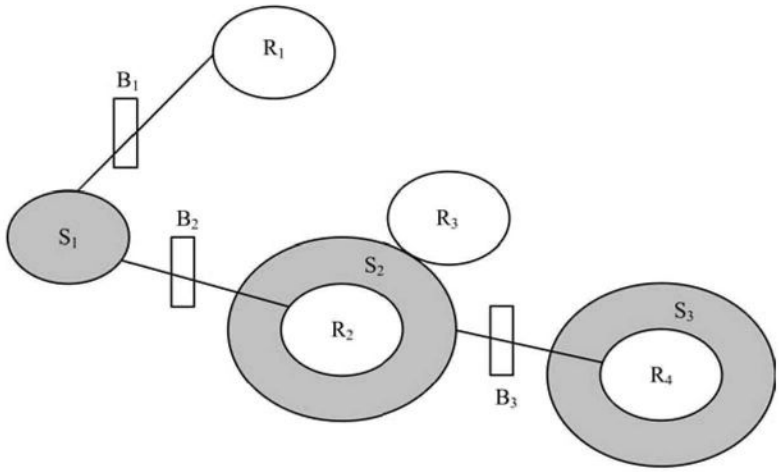

FIGURE 3-10 GENERALISED HAZARD MODEL FOR GAS SYSTEM

The representation in Figure 3-10 is convenient for tracing accident sequences and in identifying where a barrier may be missing or inadequate. Quantification of sources and impact on receptors still needs conventional consequence analysis, as described in Chapters 6 and 7. Software packages have been developed with the generalised hazard models, where the emissions from given sources, and dose-response relationships for receptors have been built-in, along with failure rate databases.

Advantages of the integrated hazard models are:

- Software can be used by non-experts with basic input of sources and receptor characteristics (e.g. population distribution).

- Provides a good first-pass risk assessment for decision making in issues such as facility location and land-use planning.

The disadvantages are:

- The software is essentially a "black box" over which there is very little control, especially for the non-expert.
- In the absence of appropriate software, the various stages of risk assessment have to be carried out individually, and the advantage of 'integration' is lost.
- Since detailed information on the risk assessment process is lacking, the process is not transparent for verification and auditing purposes.

There have been continual efforts in the industry to develop the integrated software, but these have not found universal acceptance due to their complexity and apparent lack of flexibility and transparency.

In theory, an integrated model is very attractive as it provides a holistic picture of hazards and their impact, but in practice, the individual steps are carried out separately with relevant interfaces, in order to have a transparent process, and at the same time, exercise better control over the whole process.

3.6 HIERARCHY OF MANAGING PROCESS RISK

In managing process risks, the following hierarchy applies.

1. Application of inherently safer design (ISD) principles (Kletz 1998)
2. Process control and critical alarms
3. Provide safeguards
4. Manage residual risk

The above steps are linked to the layered protection models, as summarised in Table 3-4.

Table 3-4 does not fully cover activities associated with the installation, commissioning and decommissioning part of the life cycle. Details of each of the activities in Table 3-4, and other activities of the life cycle stages, are discussed in the life cycle risk management, Chapter 12.

TABLE 3-4 PROCESS RISK MANAGEMENT HIERARCHY AND LAYERED PROTECTION MODEL

Activity	Protection Layer in Figure 3-7	Inherent safety	Process control and alarms	Safeguards provision	Manage residual risk
Eliminate hazard by design	1	✓			
Intensify, substitute, attenuate, simplify process	1	✓			
Segregate/ separation of plant areas	1	✓			
Process/ mechanical design	1	✓			
Process control	2		✓		
Critical alarms	3		✓		
Detection	4			✓	
Prevention (SIS)	4			✓	
Pressure relief systems	5			✓	
Consequence mitigation (passive protection)	6			✓	
Consequence mitigation (active protection)	6			✓	
Procedural safeguards (PSM)	7			✓	✓
Risk Transfer	7				✓

3.7 REVIEW

In Chapter 3, we introduced the concept of managing risk over the entire life cycle of the facility. Distinctions between facility life cycle and product life cycle have been highlighted. A number of risk management models have been introduced. The definition of the system boundary with system objectives and activities, together with comprehensive hazard identification, is common to all models. It is the foundation of system models.

The one-dimensional model focuses on consequence analysis of identified hazards, and decision making for consequence mitigation. It is in itself inadequate by not considering the corresponding likelihood of occurrence of hazardous incidents, and hence the inability to assess the risk, and prioritise risk management requirements.

The two-dimensional model in Figure 3-6 provides a comprehensive tool for managing risks, along with linkages of the model to various chapters in this book. A third dimension of cost can be added, but we have refrained from making the model too complex. Cost-benefit analysis is a decision making tool, described in Chapter 10.

The layer of protection model is an alternative representation of how incident prevention and mitigation systems are progressively developed around the process facility design and operation. This model also links to the Layer of Protection Analysis (LOPA), described further in Chapter 8.

The risk matrix model for qualitative assessment and ranking of risks has been introduced. This model, while appearing to be simple on the surface, needs some experience to use successfully. The difficulties in using this model and the methods to overcome these difficulties are described in the discussion on risk assessment in Chapter 9.

Some integrated models are presented. These have not found wide application and are still being developed by the process industry and practitioners.

The hierarchy approach to risk management and linkages to the layered protection models has been described. The concept of inherently safer design (ISD) has been introduced. More details on ISD are provided in Chapter 12, under life cycle risk management. The material covered in this chapter is applicable to a wide range of process industries, including upstream oil and gas production, downstream oil and gas processing, and the chemical process industry.

3.8 REFERENCES

American Petroleum Institute. *Recommended Practice for Analysis, Design, Installation and Testing of basic Surface Systems for Offshore Production Platforms*, American Petroleum Institute, API 14C:2001.

Dowell, A.M. 1999, 'Layer of Protection Analysis and Inherently Safer Processes', *Process Safety Progress*, vol. 18, no. 4, pp. 214-220.

Grose, V.L. 1987, *Managing Risk - Systematic Loss Prevention for Executives*, Prentice Hall, 1987.

Hicks, D.I., Crittenden, B.D. and Warhurst, A.C. 2000, 'Addressing the future closure of chemical sites in the design of new plant', *Transactions of Institution of Chemical Engineers*, Part B, Loss Prevention and Environmental Protection, vol. 78, pp. 465-479.

International Electrotechnical Commission. *Functional Safety of electrical/electronic/programmable electronic safety-related systems, Parts 1 to 7*, International Electrotechnical Commission, Switzerland, IEC 61508:1998-2000.

International Electrotechnical Commission. *Functional Safety - Safety instrumented systems for the process industry sector, Parts 1 to 3*, International Electrotechnical Commission, Switzerland, IEC 61511:2003-2004.

International Organization for Standardization. *Environmental management systems - life cycle assessment - principles and framework*, International Organization for Standardization, Geneva, ISO 14001:1998.

International Organization for Standardization. *Quality management systems - Requirements*, International Organization for Standardization, Geneva, ISO 9001:2000.

International Organization for Standardization. *Systems engineering - System life cycle processes*, International Organization for Standardization, Geneva, ISO/IEC 15288:2002.

Khan, F.I., V. Raveender and Husain, T. 2002, 'Effective environmental management through life cycle assessment', *Journal of Loss Prevention in the Process Industries*, vol. 15, pp. 455-466.

Kletz, T.A. 1998, *Process Plants: A Handbook of Inherently Safer Design*, 2nd edn, Taylor & Francis, Philadelphia, USA.

Kletz, T.A. 1999, 'The origins and history of loss prevention', *Transactions of Institution of Chemical Engineers*, Part B, Process Safety and Environmental Protection, vol. 77, pp. 109-116.

Marshall, V.C. (Late) and Ruhemann, S. 1997, 'An anatomy of hazard systems and its application to acute process hazards', *Transactions of Institution of Chemical Engineers*, Part B, Process Safety and Environmental Protection, vol. 75, pp. 65-72.

Nicholas, M.J., Clift, R., Azapagic, A., Walker, F.C. and Porter, D.E. 2000, 'Determination of 'best available techniques' for integrated pollution prevention and control: a life cycle approach', *Transactions of Institution of Chemical Engineers*, Part B, Process Safety and Environmental Protection, vol. 78, pp. 193.

Pritchard, P. 2000, *Environmental Risk Management*, Earthscan.

Raman, R. 2004, 'Accounting for dynamic processes in process emergency response using event tree modelling', *19th CCPS International Conference*, Orlando, Florida, pp. 197-213.

Standards Australia. *4360 Risk Management*, AS/NZS:1999.

Standards Australia. *4360 Risk Management*, AS/NZS:2004a.

Standards, Australia. *HB436 Risk Management Guidelines*, AS/NZS:2004b.

Tweeddale, M. 2003, *Managing Risk and Reliability of Process Plants*, Gulf Professional Publishing.

Venkatasubramanian, V., Rengaswamy, R., Yin, K., and Kavuri, S.N. 2003a, 'A review of process fault detection and diagnosis Part 1: Quantitative model-based methods', *Computers and Chemical Engineering*, vol. 27, no. 3, pp. 293-311.

Venkatasubramanian, V., Rengaswamy, R., Yin, K., and Kavuri, S.N. 2003b, 'A review of process fault detection and diagnosis Part 2: Qualitative models and search strategies', *Computers and Chemical Engineering*, vol. 27, no. 3, pp. 313-326.

Venkatasubramanian, V., Rengaswamy, R., Yin, K., and Kavuri, S.N. 2003c, 'A review of process fault detection and diagnosis Part 3: Process history based methods', *Computers and Chemical Engineering,* vol. 27, no. 3, pp. 327-346.

Whetton, C. 2000, 'Sneak Analysis of Process Systems', *Transactions of Institution of Chemical Engineers*, Part B, Process Safety and Environmental Protection, vol. 71, pp. 169-179.

3.9 NOTATION

ALARP	As Low As Reasonably Practicable
API	American Petroleum Institute
AS/ NZS	Australian Standard/ New Zealand Standard
CHA	Concept Hazard Analysis
DCS	Distributed Control System
EA	Ethanolamine

EPA	Environmental Protection Agency
ESD	Emergency Shutdown
EtO	Ethylene Oxide
FMEA	Failure Mode and Effects Analysis
FMECA	Failure Mode Effects and Criticality Analysis
HAZOP	Hazard and Operability study
IEC	International Electrotechnical Commission
ISD	Inherently Safer Design
ISO	International Standards Organisation
LCA	Life Cycle Approach
LOPA	Layer of Protection Analysis
NGO	Non-Government Organisation
OH&S	Occupational Health & Safety
PLC	Programmable Logic Controller
PPE	Personal Protection System
PSM	Process Safety Management
QRA	Quantitative Risk Analysis
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SMS	Safety Management System