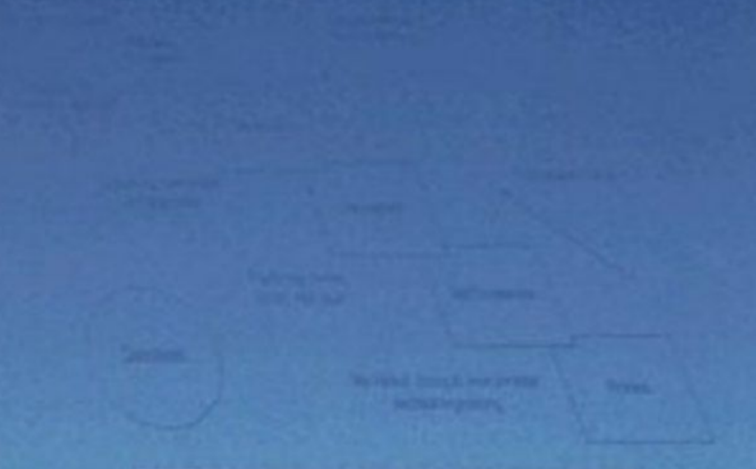
ELSEVIER
ACADEMIC
PRESS

Ian Cameron
Raghu Raman

# Process Systems Risk Management



PROCESS SYSTEMS ENGINEERING
Volume 6

# PROCESS SYSTEMS RISK MANAGEMENT

**PROCESS SYSTEMS ENGINEERING**
**A Series edited by George Stephanopoulos and Efstratios Pistikopoulos**

Volume 1
Mathematical Modeling
Rutherford Aris

Volume 2
Data Processing and Reconciliation for Chemical Operations
José A. Romagnoli and Mabel Cristina Sánchez

Volume 3
Linear Algebra and Linear Operators in Engineering
Ted H. Davis and Kendall T. Thomson

Volume 4
Process Modelling and Model Analysis
Katalin Hangos and Ian Cameron

Volume 5
Computational Flow Modeling for Chemical Reactor Engineering
Vivek V. Ranade

Volume 6
Process Systems Risk Management
Ian T. Cameron and Raghu Raman

# PROCESS SYSTEMS RISK MANAGEMENT

**Ian T. Cameron**
*Department of Chemical Engineering*
*Computer Aided Process Engineering Centre*
*University of Queensland*
*Brisbane, Australia*

**Raghu. Raman**
*Safety Engineering and Risk Management*
*Kellog Brown & Root Pty Ltd*
*Sydney, Australia*

2005

ELSEVIER
ACADEMIC
PRESS

Amsterdam – Boston – Heidelberg – London – New York – Oxford
Paris – San Diego – San Francisco – Singapore – Sydney – Tokyo

ELSEVIER B.V.
Radarweg 29
P.O.Box 211, 1000 AE
Amsterdam, The Netherlands

**ELSEVIER Inc.**
**525 B Street, Suite 1900**
**San Diego, CA 92101-4495**
**USA**

ELSEVIER Ltd
The Boulevard, Langford Lane
Kidlington, Oxford OX5 1GB
UK

ELSEVIER Ltd
84 Theobalds Road
London WC1X 8RR
UK

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

First edition 2005

ISBN: 0-12-156932-2

♾ The paper used in this publication meets the requirements of ANSI/NISO Z39.48-1992 (Permanence of Paper).
Printed in The Netherlands.

# ACKNOWLEDGEMENTS

No book appears without the involvement and help of many in the background, least of all our families. To them we owe a huge vote of thanks for their support and patience over the time of preparation.

We are thankful to the reviewers who took the time to read early draft chapters and to make helpful suggestions for improvements. These included Michael Cass at Shell Global Solutions, Steven Sylvester at Sinclair Knight Merz, Tim Routley at URS Group, Allen Gargett at Petrochem Consulting Services, colleagues Paolo Grillo and John Bertram at Kellogg Brown & Root, and to many friends and colleagues for their 'pick your brain' contributions.

To Jesper Deleuran we acknowledge his generosity in allowing us to use several of his cartoons to good effect. Please visit his website at http://www.jesperdeleuran.dk/ to see more of his work.

To Barry Maher we acknowledge the assistance he gave with some of the word processing features.

To Stephanie Peake for unrelenting web search and inter-library liaisons in accessing relevant references and information in time, every time.

The authors thank the International Electrotechnical Commission (IEC) for permission to reproduce information from its International Standard IEC 61508-5. All such extracts are copyright of IEC, Geneva, Switzerland. All rights reserved. Further information on the IEC is available from www.iec.ch. IEC has no responsibility for the placement and context in which the extracts and contents are reproduced by the authors, nor is IEC in any way responsible for the other content or accuracy therein.

To Christine Smith we owe an enormous "thank you" for preparing the initial chapters and then putting up with all the revisions, inclusions, deletions, swapping and changing that took place over many, many months. Without her expert help and dedication the book would not be a reality.

# PREFACE

Risk management is a vital systems activity across design, implementation and operational phases of a process system. This integrative systems perspective is often missing or poorly emphasized in much of the risk management literature. The purpose of this volume is to present a holistic approach to process risk management that is firmly grounded in systems engineering employing a life cycle approach. Throughout this volume there is a recurring emphasis on a comprehensive "cradle to the grave" approach.

Risk management has now become a central corporate issue due to a plethora of important drivers, amongst which are legislative compliance, duty of care, financial viability and public perception of industrial and commercial enterprises. The last 10 years has seen substantial changes and enhancements to legislative regimes in Europe, USA and Australasia, with the aim of improved industrial risk management practice driven in most part by public demands following highly publicized major accidents. Public risk aversion to industrial operations remains a major issue where in fact perception has become reality. These and many other issues are addressed and discussed in this volume.

Modern process risk management practice involves all levels of personnel within a corporation as well as interaction with many levels of government – from national to state and local authorities. Risk management also cuts across a wide range of professional interests – from engineers, through safety and health professionals to town planners and government administrators. Risk management also spans the purely technical through financial, social and human factors. This realization enforces a much broader perspective to the risk management challenge than given by a purely technical systems approach. Of necessity, effective risk management must consider the integration of these components with appropriate emphasis on all components as they relate to the application area.

There are many excellent reference volumes available for the risk management professional, which often require substantial effort in gaining an in-depth understanding and application of the basic concepts. Much new material has appeared in this area over the last 10 years. The present volume emphasizes the principal concepts of risk management and the practical outworking of those concepts, such that it will appeal to a wide ranging audience.

This volume will find substantial use with engineering professionals who have specific responsibility in risk management. It provides a succinct, yet comprehensive coverage of the key components of risk management applied to the process and manufacturing industries. The subject matter of risk management is often not dealt with convincingly in undergraduate university courses and this volume provides a systems approach to teaching the material. It will be useful for both undergraduate and graduate training with a full set of presentation material being available on the web[1]. Aspects of risk management are often the subject of intensive, short courses, which tend to be highly focused. As such this volume provides a broader, integrative systems approach to the area.

Health professionals as well as government administrators and town planners will also find this volume helpful in understanding the key industrial procedures that take place in order to establish, implement and maintain effective risk management systems. The contents deal with the interaction between operational location, process design, operation and land use planning issues.

Much of the material presented in this volume has been taught regularly at The University of Queensland, Australia. As well, the authors have presented the concepts in many short courses over the last 15 years to industry, government, planning and consulting professionals from a wide range of industry backgrounds. This has taken place within and also outside Australia.

Between them the authors have almost 40 years of experience in risk analysis, assessment and management, with applications in both on-shore and off-shore operations. Many of the examples used in this volume are drawn from actual consulting studies done by the authors or familiar to the authors. They cover on-shore and off-shore sites, vehicular and rail transport as well as pipeline systems. As such there is wide coverage of topics typical of many common industrial and related applications.

The authors are well aware that their views and practice have been shaped by influential colleagues who are themselves experts in the field. We are grateful to them for their impact into our professional practice. As always, the responsibility of the views and material presented remain with the authors. So too are the omissions and errors that manage to get through the review process! We hope that a wide range of readers will find the material illuminating, instructive and eminently useful in improving risk management of process and related activities over a wide area of application areas.

[1] http://www.cheque.uq.edu.au/psdc/risk

# CONTENTS

## 1 Managing Risks from Process Systems

## 2 Risk - Estimation, Presentation and Perception

# 3 System Models for Risk Management

# 4 Identifying Hazards and Operational Problems

# 5 Analysing the Consequences of Incidents

# 6 Effect Models for Consequence Analysis

# 7 Vulnerability Models

# 8 Estimating the Likelihood of Incidents

# 9 Risk Estimation

# 10 Decision Making under Uncertainty

## 11 Process Safety Management Systems

## 12 Life Cycle Risk Management Tools

## 13 Management of Major Hazard Facilities

# 14 Auditing Process Safety Management Systems

# 15 Land Use Planning Risk Management

This page is intentionally left blank

# 1 MANAGING RISKS FROM PROCESS SYSTEMS

*"Although my commitment to the goal of immortality is unswerving, I am not positive that a zero risk society is yet in the scientific cards"*

*Daniel I. Koshland, Jr.*
*Nature, 17 April 1987*

A quick look through the daily newspapers shows that all human activity is surrounded by hazards and associated risks. Road accidents, disease, fires, financial collapse are all part of human existence.

In personal affairs, we tend to manage risks implicitly. In a visit to the local grocery store on foot, we tend to avoid high traffic routes, cross roads at traffic lights or pedestrian crossings to minimize risk of injury or death. When it comes to managing risks to stakeholders in an enterprise, more formal and explicit measures are required.

Risk management has been practised for millennia in all areas of human activity. The earliest concept of loss prevention was self-defence to save one's possessions and property against attacks by enemy tribes. Since the industrial revolution, and in the aftermath of industrial disasters costing multiple lives, there has been a gradual, though not necessarily systematic improvement in work place safety. With the advent of major public companies in the 20th century and the depression of the 1930s, the need for financial risk management and protection of shareholders' interests has evolved as a separate field of study.

In the meantime, the insurance industry has been engaged in risk management in its own way. The focus has been largely on minimising losses in the aftermath of an accident event, and hence reducing the magnitude of claims by policy holders, rather than proactive prevention of loss incidents. Industries have also come to realise that an insurance policy is not a panacea against loss events, as the policy would not compensate for the full extent of the loss. For instance, in a major fire resulting in loss of assets, the insurance policy may replace the assets, but not the loss of market share due to prolonged downtime.

With the rapid development of modern technology, the level of complexity in industrial activities increased in the latter half of the 20th century. Correspondingly, the scale of loss events has increased, as has the extent to which they can affect not only the industrial facility and its employees, but also the surrounding local population. Classic examples are the chemical factory explosion at Flixborough in England (1974); the Three Mile Island (1979) and Chernobyl (1986) incidents involving nuclear power generation plants; the major gas explosion in Mexico City (1984) with loss of hundreds of lives; the major toxic gas release at Bhopal, India (1984) resulting in loss of lives and injuries running into thousands and the Piper Alpha oil platform disaster in the North Sea (1988). It is not surprising that most of the major industrial accidents were in process facilities, due to the hazardous properties of materials stored and handled.

Each major incident prompted the legislators to tighten up safety regulations, the insurers to seek more informed risk management techniques, and the industry to adopt formal risk management systems as part of ensuring operational integrity in day-to-day operations. Thus the subject of risk management has been steadily gaining prominence in the last 25 years.

## 1.1 WHY RISK MANAGEMENT?

There are many reasons why the technical and operational risks in an organisation must be assessed systematically.

### 1.1.1 Regulatory Requirements

Regulations covering the various aspects of risks from process operations exist in all industrialised countries and most developing countries covering the various aspects of risks from process operations. Regulatory compliance requires a dedicated organisational structure to undertake risk assessment and management to protect the health and safety of employees and the public, and the biophysical environment.

### 1.1.2 Common Law Duty of Care

In addition to complying with the statutory regulations, there is the all-embracing 'duty of care' on the part of the corporation, to protect the health and safety of its employees and the public from the corporation's activities.

The requirement is on the organisation to demonstrate that all reasonable care has been taken in identifying the hazards associated with the facility and its operations, and that adequate hazard control measures have been put in place.

Where the duty of care has not been visibly demonstrated, there is potential for criminal liability on the part of the company, should an incident occur resulting in serious injury or fatality to employees or the public, as a result of the activities of the company.

### 1.1.3 Commercial Reasons

There are strong commercial reasons for minimising business interruptions and equipment damage. Systematic risk management not only identifies the hazards, but also helps to rank the allocation of resources in a cost and time effective manner. Such an approach also assists in minimising the organisation's overall costs.

EXAMPLE 1-1 GAS PRODUCTION

A gas producer has contracted to supply natural gas to a distributor at a high availability. This is generally an onerous task, as a major incident in the gas production facility can interrupt gas supply for extended periods.

In September 1998, an explosion occurred at the gas processing plant of Esso Australia in Longford, Victoria. The accident resulted in loss of gas supply to consumers for several weeks, with significant consequential losses. The Royal Commission of inquiry into the accident attributed one of the causes to the failure of the risk management process in place (Hopkins 2000).

The accident showed that, without a systematic hazard identification study and an 'effective' risk management system, it is not always possible to meet the contractual obligations.

### 1.1.4 Evaluation of Alternative Options

In project feasibility evaluations, several alternatives are initially considered. The options may be related to siting of the facility, the process technology to be adopted, logistics of raw material supply and product distribution, availability of skill base, etc. The final short list of options would generally be based on locational and commercial considerations.

However, if we make an assessment of the risks associated with each of the options, an additional dimension of input to decision making emerges. It is possible that the options initially arrived at may have to be reconsidered based on risk.

EXAMPLE 1-2 VETERINARY CHEMICALS FACILITY

A producer of animal health and veterinary chemicals decided to construct a new formulation plant near a major metropolitan area. Three possible locations were selected. All the locations were suitable in terms of area of land, land prices and proximity to markets.

Before making a final decision on purchase arrangements for a specific piece of land, the company decided to undertake a preliminary risk assessment study of the impact of the proposed manufacturing and storage on the surrounding areas.

For near identical operations, each of the sites revealed quite different aspects of risk. These were related to environmental issues such as proximity to sensitive waterways, and transportation issues such as movement of toxic chemicals along highly populated thoroughfares. It also became apparent that the costs of mitigating the risks in the three sites were so different that, when these costs were included in the cost-benefit analysis of the project, there was only one clear winner.

If a risk management survey had not been undertaken, and a piece of land had been purchased without consideration of this additional dimension, not only might the project have become financially non-viable, but there could also have been a number of difficulties in obtaining the necessary planning and environmental approvals from statutory authorities.

The following sections introduce some of the basic concepts surrounding modern risk management practice. In particular an emphasis is given to systems approaches to process risk management within the framework of the process life cycle.

## 1.2 HAZARD AND RISK

The terms 'hazard' and 'risk' appear extensively throughout this book and it is vital to be clear about what we mean by these terms. In popular parlance they are often used interchangeably. However in the context of process systems we make a clear distinction between these two complementary terms.

### 1.2.1 Hazard

In the case of 'hazard' we understand this to be an attribute of a thing or activity that has the potential for harm or loss. The term 'risk' relates to chance or probability of harm or loss. The following sets out formal definitions of the terms, giving a range of examples to illustrate the concepts.

*Hazard* can be formally expressed as:

"a source of potential harm or a situation with a potential to cause loss."

This is a definition in-line with that developed by safety professionals (Jones, 1992) or national standards like AS4360 (Standards Australia 2004). The key ideas embodied in the definition are:

a source or situation - meaning an inherent property of a thing or a set of circumstances that come into play.

a potential - implying that given the right circumstances or conditions some effects can be realised.

harm or loss - implying unwanted effects that could impact on people, property, environment or other nominated receptors such as corporate reputation, financial situation, heritage values, and the like.

**EXAMPLE 1-3 HAZARDS IN INDUSTRIAL OPERATIONS**

In the context of an industrial operation the following can be regarded as hazards:

(i) The presence of high pressures or temperatures in the system
(ii) The act of smoking in certain areas
(iii) Explosive properties of a material
(iv) Inappropriate behaviour of staff
(v) Storage of large quantities of toxic substances
(vi) Industrial operations near to high population density urban areas.

It is important that identification of hazards be comprehensive and thorough in addressing loss issues. This is the topic of Chapter 4.

It needs to be emphasized that hazard is a *potential* for harm or loss not a *realized* harm or loss. The role of risk management is to ensure that the potential is not realized, and should it be realized, then the consequences are mitigated.

Hence, the storage of large amounts of liquefied petroleum gas (LPG) for commercial use is designed and operated to ensure that the flammable and explosive potential of the material does not lead to harm or loss.

### 1.2.2 Risk

Risk is often associated with the likelihood of an adverse outcome. It is a rather vague term used widely in common language across many contexts. The English word has its origins in Latin (riscare) where it meant to "run into danger". A few examples help to illustrate the point.

**EXAMPLE 1-4 SKY DIVING**

We all know that sky diving is a risky sport. The risk here is the potential for serious injury or loss of life in the event of an accident. However, the activity itself does not mean that there is certainty of loss of life, but that the chance of an incident happening and its severity are relatively high compared to other sports. While the severity of a loss is recognised, people still undertake these activities because safeguards have been developed to reduce the chance of an accident. In other words, the likelihood of a loss is minimised. This is done by having redundant parachutes for sky divers, so that in the event that the primary parachute does not open, the spare one would. The chance of both not opening is considered very low. In other words, the 'risk' has been reduced to levels that people involved in the sport would accept.

**EXAMPLE 1-5 TOXIC GAS RELEASE IN BHOPAL, INDIA**

In December 1984, there was an accidental release of the toxic chemical methyl isocyanate from a pesticide manufacturing plant in Bhopal, India. The gas spread over a few square kilometres in the vicinity of the plant. This happened in the early hours of the morning when most people were in their homes asleep. The gas killed more than 2000 people in the surrounding community and injured tens of thousands of others. The incident had several implications:

- serious injury to, and loss of life of thousands of members of the public
- criminal prosecution of the company
- loss of assets for the company as the plant was never allowed to re-open
- extensive court battles and compensation costs.

This event also brought into focus the high risk nature of these industrial activities. Here the loss was not only material and financial, but also irreplaceable loss of human lives, and the devastation of an entire community. In terms of risk management, the following factors emerged:

- the nature of the material stored and processed, and its potential effect on humans on exposure
- the design and operational safeguards in place to prevent the event, or minimise the chance of its happening to very low levels
- the adequacy of the risk management systems in place and their effectiveness
- the lack of an off-site emergency response plan
- the problems of ensuring an adequate buffer distance between a hazardous facility and populated areas, especially in high population density developing countries
- the various risk exposures of the company whose magnitude had not been foreseen
- the high public costs associated with immediate payment to surviving victims and families of the dead, cost of investigation, heavy toll on the local infrastructure (hospital staff etc.). If the incident had not occurred, the money could have been spent on other community projects.

■ ■ ■

This is an example of an incident where the potential loss may have been recognised, but the likelihood of occurrence of the event had been grossly underestimated.

### EXAMPLE 1-6 AMMONIUM NITRATE EXPLOSION AT AZF, TOULOUSE, FRANCE

In September 2001 an explosion at the fertilizer works of ATOFINA and Grande Paroisse resulted in 30 deaths and around 2500 injuries. Some 40-80 tonnes of ammonium nitrate exploded with the resultant shock wave causing significant damage to surrounding commercial buildings, residences and the Toulouse town centre some 3 kilometres away. Of the 30 deaths, 8 were outside the plant. The blast created a crater some 40 metres in diameter and up to 7 metres deep. Surrounding site buildings were destroyed and tanks containing other substances were damaged or ruptured. Liquid ammonia and chlorine storage facilities were fortuitously shielded by buildings which were themselves destroyed.

The accident highlighted the risks associated with inappropriate urban planning decisions and residential "creep" towards major hazard facilities. Other important risk related factors included better technical knowledge of risks, improved quality of hazard studies, improved land-use planning practices as well as better information to the public.

■ ■ ■

The above examples illustrate that risk has two dimensions:

- the *severity* or *magnitude* of the loss event
- the *likelihood* or *probability* of occurrence.

The combination of both dimensions is what constitutes risk. However, risk perception by the public of high technology industrial activities tends to be associated more with the severity dimension rather than the probability dimension.

To a large extent, the occurrence of high loss events around the world in the past, and vivid memories of those events, have contributed to this perception. It has led to the idea that risk is the hazard plus the outrage that accompanies it. We discuss risk perception and risk communication in Chapter 15.

It is essential to appreciate the two-dimensional nature of risk. This gives a two-pronged approach to managing risks–namely minimise the extent of loss or severity of the incident, and minimise or eliminate the likelihood of the event.

We are now in a position to develop a definition of risk. One obvious definition incorporates the concept of loss and the two-dimensional nature of risk.

*Risk* can be formally expressed as:

"the probability of occurrence of an event that could cause a specified level of harm to people, property and the environment or financial loss over a specified period of time".

The key concepts embodied here are:

a probability or likelihood - hence some frequency or chance of occurrence of the event.

a risk receptor - meaning a nominated target for the impact, not only limited to people, property, environment or financial impacts but to other issues such as corporate reputation, heritage value or legal action.

a level of harm - indicating a specific level of impact being considered. For people it could be fatality or injury. Within injury levels we can nominate such issues as the degree of burn, level of toxic impact and the like.

a time frame - typically over a period of a year, although other measures are often used.

The following examples illustrate the risk concept:

**EXAMPLE 1-7 RISK IN COMMERCE AND INDUSTRY**

a) Very large oil tankers transport crude oil from production fields to the oil refineries in many parts of the world. If there is an accidental release of oil, there is potential for major environmental damage as was seen in the Exxon Valdez incident in Alaska, and the incident involving a Spanish tanker in the Shetlands, off the coast of Scotland. If we apply the above definition of risk in this context, the risk in super tankers carrying oil is the probability of a specified quantity of oil leaking into the ocean over a given period of time, say 1 year or 10 years, depending on the scale chosen.

b) Hundreds of people work in underground mines everyday around the world. Underground mining is associated with the risk of serious injury or fatality by roof/ground fall or fires and explosions. If the management of the mining company wishes to define the major risk to employees, and apply the above definition of risk, it may define the risk as the probability of a fatal accident in a given time period, say 1 year.

c) A mineral processing company has a target production to be met for the year. One of the important steps in the operations is the crushing of raw material ore to size for further processing. A large ball mill is used to crush the ore. This is critical equipment, and should a major failure occur in this section of the plant, the downstream processing will have to be shut down, and considerable loss of production could occur. By applying the above definition of risk to the operation, the following measures might be developed:

- Probability of 10% loss of production for 1 week.
- Probability of total loss of production for 1 month.

d) A construction company has a contract to complete a railway overpass that can carry heavy vehicle traffic. The turnkey project is a lump sum contract and is to be completed within an agreed date. A cost penalty would apply for delays. The financial reward is obviously higher for earlier completion. The integrity of the installation is critical as the consequential costs of a structural failure is very high.
The construction company can adopt a number of risk measures such as:

- Probability of project completion delay by a specified period (1-2 months).
- Probability of budget overrun by 15%.
- Probability of a structural failure during the operational life of the overpass.

■ ■ ■

### 1.2.3 Risk as an Ascribed Quantity

Risk is not a physical entity that one can measure. As mentioned before, risk is a very broad concept and can mean different things to different people. Therefore, the concept of risk can be interpreted differently by different people. Here are three examples:

a) Risk as perceived by a safety professional
A safety professional may interpret risk in a given industrial facility as the chance of a major fire or explosion, or structural failure, with consequent injury or fatality.

b) Risk as perceived by a production manager
A manager in charge of production operations may see risk as the likelihood of a major business interruption resulting in loss of production, resulting from an accident, equipment breakdown, or industrial dispute.

c) Risk as perceived by a fund manager
The fund manager's perspective is quite different. The fund manager may interpret risk as fluctuations in the market, bond rate and interest rate variations, and volatility in foreign exchange rates that could undermine the value of the investment, or affect overseas borrowing, against which hedging is necessary.

Risk is subjective. No one knows what will happen in the future, not even statistically. But, if we assume that the relevant working conditions in an industrial plant and patterns of behaviour of employees at the work place do not change, it is reasonable to assume that some value, R1, equals the corresponding loss rate observed in the past; we can then reasonably assign the same value to R1 for predicting future losses. This is so common a situation that we often talk of 'estimating' the risk. But risk doesn't exist the way a thing or physical attribute such as energy does. Indeed, in many situations, there is either something significant that cannot be assumed constant or there is insufficient data. Therefore it is then important not to assume that risk can be measured, estimated or calculated in all situations.

The subjective nature of risk raises many questions about the credibility of risk analysis, which we deal with in Chapters 9 and 10.

## 1.3 THE NATURE AND ROLE OF RISK MANAGEMENT

Risk management is the co-ordinated set of activities that direct and control an organization with respect to risk (ISO/IEC:73, 2002). It is the encompassing activity for a range of other tasks that include at the very least:

- Risk assessment (analysis and evaluation)
- Risk treatment (elimination, mitigation, transfer)
- Risk acceptance (tolerability/acceptability criteria)
- Risk communication (information sharing with stakeholders)
- Risk monitoring (auditing, evaluation, compliance).

Figure 1-1 shows a schematic representation of risk management concepts similar to the Australian Standard AS4360 2004. Risk management is a life cycle concept, since it is both multifaceted in addressing a range of risks; it is active throughout the life cycle of the process or product; it is multidisciplinary since it can cut across all levels of the corporation, government authorities and local communities; it is dynamic in nature due to an ever-changing environment of legislation, expectations, technology and business pressures.

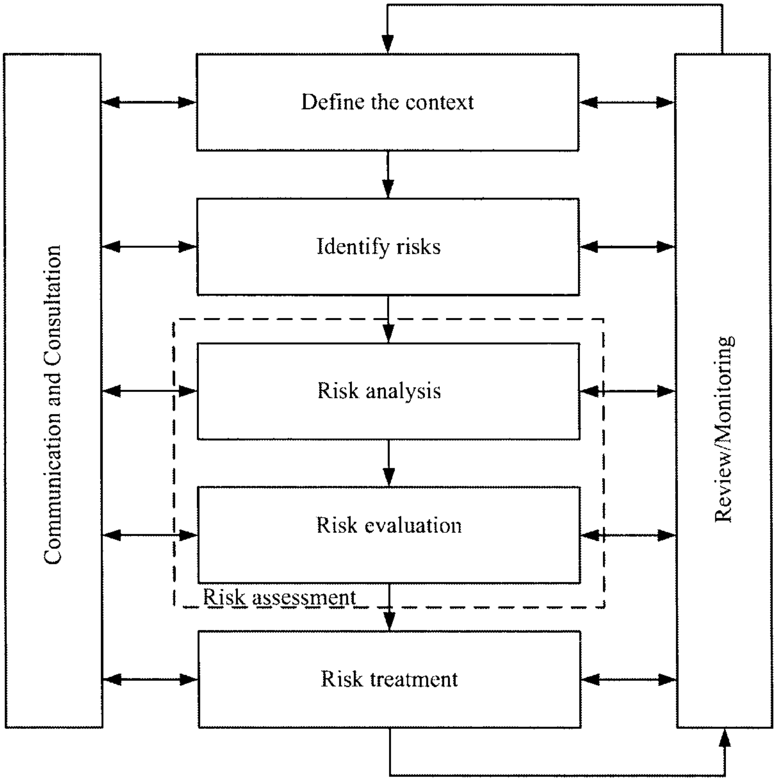
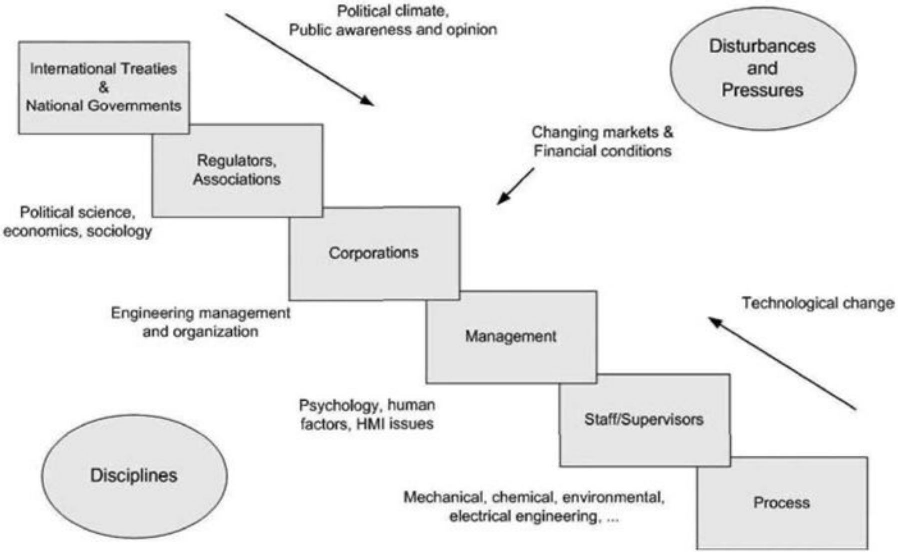


FIGURE 1-1 OVERVIEW OF RISK MANAGEMENT

Figure 1-2, adapted from Rasmussen (1997), shows some of the elements of that dynamic environment in which risk management takes place. This picture, with all its interactions illustrates the challenging nature of modern process risk management.



[redacted] FIGURE 1-2 THE SOCIO-TECHNICAL ENVIRONMENT OF RISK MANAGEMENT

### 1.3.1 The Dimensions of Risk in Process Systems

The term 'process risk' itself is very broad, and encompasses several categories of risk. All categories are essential as they reflect various facets of an organisation's operations. Therefore, for any given situation, it is important to identify which of the categories of risk apply, before undertaking an analysis.

**Risk categories**

The main risk categories in process risks are:

- occupational risks (safety and health of employees)
- plant property loss
- environmental risks (safety and health of public, biosphere, heritage)
- liability risks (public, product, failure to provide service, legal prosecution)
- business interruption risks
- project risks (design, contract, construction, delivery).

Each category has its sub-categories. It should be noted that several of these risks are interlinked and overlapping, and cannot be treated in isolation.

Table 1-1 shows the various categories and sub-categories of risk relevant to engineering and other technology-related situations. These are relevant now considered in more detail.

**TABLE 1-1 OVERVIEW OF RISK TYPES**

| Occupational | Property loss | Environmental | Liability | Business interruption | Project |
|---|---|---|---|---|---|
| • Workplace injury<br>• Workplace fatality<br>• Occupational hygiene<br>Overlaps employee liability risk | Direct:<br>• Industrial accidents<br>• Natural disasters<br>• Breach of security<br>Indirect:<br>• Drop in property value<br>• Drop in share price<br>• Drop in product value<br>Overlaps business interruption risk | People:<br>• Injury to public<br>• Fatality to public<br>• Health impairment to public<br>Biophysical environment:<br>• Air pollution<br>• Water pollution (surface, groundwater, marine environment)<br>• Soil contamination<br>• Hazardous waste storage/ disposal<br>Heritage:<br>• indigenous sites<br>• pristine environs<br>• wilderness regions<br>Overlaps liability risk | • Contract default<br>• Omissions<br>• Legal<br>• Bankruptcy<br>• Employee<br>• Public<br>• Product<br>• Failure to provide services<br>• Defective services<br>Overlaps occupational, environmental risks | • Equipment failure<br>• Property loss<br>• Liability issues<br>• Industrial disputes<br>• Contract default from outsourcing<br>• Significant cost increases<br>• Sabotage<br>Overlaps occupational, property loss and liability risks | • Cost exceeds budget<br>• Completion time exceeds target<br>• Contract default by third party<br>• Political risk<br>• Project financing problems<br>Overlaps environmental, liability and business interruption risks |

### 1.3.1.1 *Occupational risks*

Occupational risks are workplace related, and would affect employees and contractors at the workplace. There are three sub-categories:

- workplace injury
- workplace fatality
- occupational hygiene and health issues in the work environment.

**Workplace injury**

This is the most common form of risk experienced by most employees and employers. Four types of classification of these types of injuries can be made–first aid injury, medically treated injury, lost time injury and disability.

a) First aid injury

This is the simplest type of risk, involving cuts, trips or small bruises due to human error, loss of concentration etc. The injured employee is given first aid treatment on the site, and is back at work within a short period.

b) Medically treated injury, involving slip and fall, or overcome by chemical fumes, requiring examination by a medical practitioner. The injured employee is either treated on the site or at the local medical centre, back at work on the same shift, with effectively no lost time due to the injury. The Medically Treated Injury (MTI) has a higher severity ranking than the First Aid Injury.

c) Lost time injury (LTI)
This sub-category is of a higher severity than MTI, and by far one of the largest costs to the industry. The rehabilitation time may extend from one or two days to several months. The financial risk to the employee is reduced by the Workers Compensation Insurance scheme. However, there is a definite risk in the sense that the employee's position may be taken by another skilled person, and the same position may not be available on return. In some situations the injury sustained may not allow the employee to take up one's former position, or equivalent employment.

The costs to the employer are equally high, if not higher. These include both tangible costs and intangible costs:

- Cost of treatment and rehabilitation, partly covered by insurance
- Cost of incident investigation, and implementation of remedial measures. Sometimes a government agency may be involved in the investigation.
- Loss of skilled worker for a period of time and the need to train a substitute person. This could result in operational inefficiency. This is a significant intangible cost.
- Problems related to reallocation of duties and responsibilities to fill the gap until the return of the injured employee, and additional problems if one cannot be returned to the same duty.

Many employers look upon lost time injury as a risk purely contributed by human error, without considering the fact that in many instances, the risk could be eliminated by proper engineering measures. As a result, not only time and money are wasted in excessive training and re-training, but very often there is no tangible reduction in injury frequency.

d) Disability
This is by far the most serious form of workplace injury, with high cost to the employer and the employee, and should be prevented by all reasonably practicable means.

Disability injuries could occur from accidental deviations in routine industrial processes. Some examples are:

- burn injuries from a process fire
- injuries sustained in a gas explosion from the ignition of leaking flammable gas

- exposure to toxic chemical resulting in irreversible damage to specific organs
- body part caught in moving machinery such as a conveyor
- failure to isolate rotating machinery prior to maintenance work being carried out.

**Workplace fatality**

A much higher order of severity than disability from workplace injury is workplace fatality. A fatal accident affects the morale of other employees, affects a local community, and makes for adverse publicity for the organisation. If there are multiple fatalities, the ramifications for the organisation are far more serious. By far the largest number of fatalities in a work place accident has been the explosion and subsequent loss of the Piper Alpha platform in the North Sea in 1988, with the loss of 167 lives. We shall focus on the prevention of such incidents in organisations and applicable prevention techniques in Chapters 11 and 12.

**Occupational hygiene issues at work**

The risks concerning occupational hygiene include:

- use of chemicals in the workplace and potential for worker exposure, including chemicals which could be confirmed or suspected human carcinogens with potential for long-term health effects
- exposure to excessive noise from rotating machinery or construction equipment
- absence of ergonomic design of equipment resulting in injury, e.g. back strain.

Unlike a workplace injury which is acute, inadequate occupational hygiene at the workplace could result in chronic health problems in the long term, if potential exposure is not properly controlled.

#### 1.3.1.2 *Property and plant loss risks*

Loss of asset from accidental events is a serious risk in process systems. These losses can be divided into two major sub-categories–direct and indirect losses.

**Direct losses**

Direct losses of assets fall under three headings:

a) Industrial accidents
These are the most common form of major asset loss. Examples are fires in warehouses and explosions in industrial processes. The consequences are not only loss of assets, but also injury or fatality to people, employee or public.

EXAMPLE 1-8 POLYETHYLENE PRODUCTION

Following the 1989 vapour cloud explosion at the Phillips 66 polyethylene plant at Pasadena, near Houston (USA), some 23 people died and extensive damage occurred to the plant. The cost of rebuilding parts of the process was in excess of $400 million. The company was also fined $4 million for licence breaches.

b) Natural disasters
These relate to storms, floods and earthquakes. Special precautions are required if the facility is located in flood prone areas, or higher risk earthquake zones.

c) Breach of security
These losses mainly relate to burglary, theft etc., although they could also involve breach of 'intellectual security', such as industrial espionage. It is an important risk to be identified and managed by the organisation. The cost of breach of intellectual security in an Information Technology (IT) company can be very high.

**Indirect losses**

Indirect loss generally results as a secondary effect of a different category of risk. The causes may be internal or external to the organisation. It is not only the direct losses that are important, but the indirect losses as a consequence can far exceed direct losses.

Indirect losses can also be characterised into the following types:

a) Drop in property value
In our current world of rapidly changing technology, an organisation's assets in plant and equipment could be worthless if the technology is completely superseded.

EXAMPLE 1-9 CONTAMINATED SITES

Many companies purchase land for purposes of industrial development. If, during previous uses of the land, the soil and possibly the groundwater table underneath the land had been contaminated with chemicals, and the purchaser does not take this into account, not only the value of the property drops significantly, but there is also the liability risk of clean-up.

It is essential to identify the broader risks to the organisation arising from specific incidents, rather than focus only on the specific events

b) Drop in value of products in the market
The market value of an organisation's products in the market place could drop as a result of the following:

- Defective products endangering consumer safety. If an automobile manufacturer or food/pharmaceutical manufacturer is seen to be issuing recall notices on products frequently, consumer confidence in the company's products would fall, along with the value of the products.

- New products of next generation technology replacing old products. A classic example is the compact disc revolution, making vinyl records almost obsolete.
- A superior product from another company through technological innovation at competitive prices would cause a drop in the product price. The technology and market share competition between IBM and Apple Computers, and the entry of several other smaller manufacturers into the market in the 1980s resulted in the drop in prices of personal computers.

### *1.3.1.3 Environmental risks*

Awareness of environmental risks among organisations became significant in the 1980s. Since 'environment' covers everything around us, including ourselves, the risks are all encompassing. Organisations such as Greenpeace and Friends of the Earth have successfully brought this risk into public awareness and encouraged it to become part of the decision-making and risk-management processes of several companies. There are a number of environmental regulations in nearly every country in the world to protect people and the biophysical environment from industrial processes and industrial accidents.

One of the major problem areas for an organisation in the management of environmental risk is the longer term impact. Unlike loss of property in a fire, which can be quickly replaced, damage to the environment takes a long time to recover, and costs significantly more in clean-up and monitoring. The example of Exxon Valdez has already been mentioned.

Some other examples of environmental risk are:

**EXAMPLE 1-10 EQUIPMENT AND OPERATIONAL FAILURES**

a) Failure of pollution control equipment and release to the environment.

In 2000, there was a major release of cyanide from the tailings dam of a gold mine in Romania, operated by the Romanian Government and the Esmeralda Company. The cyanide found its way into the Tisa River and ultimately into the Danube, affecting aquatic life in Romania, Hungary and Yugoslavia.

b) Breakdown of operating equipment during routine operation, resulting in loss of containment and emission to the atmosphere.

A sulphuric acid plant converts sulphur dioxide to sulphur trioxide in a catalytic reactor. The sulphur trioxide is absorbed in a dilute solution of sulphuric acid in an absorption tower to make concentrated product acid. If the absorption tower circulation pump fails during normal operation, then the sulphur trioxide would not be absorbed, but escape to the atmosphere through the stack. Depending on the quantity of release and prevailing meteorological conditions, the acid mist could disperse hundred or thousands of metres downwind and affect local population centres.

c) Escape of contaminated firewater in a factory/warehouse fire into storm water system.

- In 1986 a fire occurred near Basel in Switzerland in a Sandoz warehouse containing agro-chemicals. Approximately 10,000 tonnes of firewater was used to bring the fire under control, but the contaminated firewater with about 30 tonnes of chemicals escaped through the storm water system into the Rhine and polluted the river several kilometres downstream.
- In 1991 a fire at Diversey Chemicals in Sydney, Australia resulted in escape of contaminated firewater into the nearby Toongabbie Creek, polluting the waterway.

d) Health risk to the public through exposure to soil and groundwater contaminated by industrial pollutants.

Although known, this risk was not taken seriously by regulatory authorities until the late 1970s. The Love Canal and other polluted sites in the USA gave rise to the Superfund for clean-up.

### *1.3.1.4 Liability risks*

This type of risk in some aspects overlaps the previous ones. For example, environmental impairment or public injury from an incident carries a liability for the organisation, either under a regulation or under common law.

**Risk of contract default**

In many process enterprises, part or all of the project work is contracted to external firms. A default in terms of performance guarantee, meeting deadlines, or breach of quality of deliverables carries a liability on the part of the contractor.

The risk is not only for the contractor, but there are significant costs to the organisation as well. These include project delays resulting in increased interest payment on borrowing, depreciation on non-performing assets and loss of market share due to delays, all of which may not be recovered through liability claims alone.

With more and more organisations outsourcing goods and services, the risk of contract default becomes an issue worthy of serious consideration in risk management. In the public sector, risk of contractor default is a significant risk in privatisation, and outsourcing of services.

**Acts and Omissions**

Omissions on the part of a goods or services provider carry liability risks. The omission could be intentional or through negligence. If an organisation designs a bridge, and there are design faults in the project resulting in a failure of the structure, a whole range of liabilities arise. These include financial liability in rebuilding to a correct design, compensations for the injured, and legal costs associated with facing a possible criminal negligence charge, should fatalities occur in the accident.

**Legal**

Legal liability may arise from the following:

- common law claims on the company by a third party
- industrial accidents that requires coronial inquiry or inquest
- prosecution by a government agency for breach of Occupational Health and Safety (OH&S) legislation as a result of a workplace injury
- product defects that threaten the safety of the consumer such as defective toys that could affect child safety)
- third-party damages arising from a firm's industrial activity; these may arise from injury, environmental impairment, loss of amenities and the like.
- breach of environmental licence regulations prescribed by environmental protection authorities.

The major costs of legal liability are legal costs, cost of complying with injunctions and court orders for specific performance, money for settlements, verdicts and fines, and compensatory damages.

**Employee liability**

This could arise from a breach of Occupational Health and Safety Regulations, intentionally or through negligence. Liability could be in terms of payment through the Workers Compensation scheme, or directly being sued by an employee under common law. This risk is part of the legal risk discussed above, but has been listed separately to highlight its importance to the organisation.

#### 1.3.1.5 Business interruption risks

There is considerable overlap between business interruption risk and the other risks discussed above as these could be significant contributors to business interruption. Interruption to business could occur from the following:

- Major breakdown of critical equipment. The facility may not carry the spare parts to carry out repairs, or in the event of a major failure requiring replacement of the equipment item, there may be considerable lead time for delivery/installation.
- Property loss from fires or explosions. There are significant delays due to investigations, insurance loss adjustment and claims processing, as well as the lead time for replacing equipment before production can re-commence.
- Liability issues temporarily halting operations. A product defect could be identified, and there could be product liability issues relating to marketing the product even as 'seconds'. Until the cause of the defect is identified and corrected, production may have to be suspended. The alleged defects in

Firestone Tyres that caused automobile accidents, is one example of the product liability stopping production.

- Inability to cover liability resulting in closure of business. This is part of the bankruptcy risk.
- Industrial disputes.
- Reduction in internal resources of the organisation.
  There has been an increasing trend in organisations in industrialised countries towards reducing internal resources. Reducing the size of the organisation and outsourcing goods and services previously provided from within the organisation have their own intrinsic risks. These risks relate to loss of skills within the organisation and consequent inability to assess the quality of an external service (e.g. design), contract default on the part of the third-party service providers, indirect liability issues arising from the use of non-quality goods and services from external providers etc.
  In smaller organisations, the sudden loss of a few key employees through resignation may seriously upset the operations until a suitable replacement could be found. This may not be so severe for large organisations that they must redeploy resources from other areas of the organisation.
- Significant increase in costs. Loss of market share during the period of business interruption could be made up by a supply through continued manufacturing by a sub-contractor, and/or major advertising and marketing thrust. Either of these would result in an increase in overall costs.

### 1.3.1.6 *Project risks*

In undertaking engineering projects, it is essential to understand clearly at the outset the risks associated with the project and plan for it. Some of the risks discussed above would be present as part of overall project risk.

Key aspects of project risk are:

- Project budget blow out. This can seriously delay the project. If the project is in its early stages, it may cause abandonment of the project by the management as the projected return on the investment on which the project decision was made, could be significantly lowered.
- Project completion delayed. This can result in financial loss due to interest payment on non-performing capital, and any cost penalties for delivery delays in the contract.
- Contract default by third-party services. While this can be partially covered by liability clauses in the contract, the cost and completion time of the project would both exceed budget.
- Political risk. Project delays due to environmental issues associated with the project, raised by external interest groups with political influence, causing delays, abandonment, significant design modification, all result in an increase in overall costs.

It is essential to keep in mind the environmental and political risks for a project. Even if all the economic indicators of the project were positive, the environmental and political risk may force the company to abandon a project, or modify it significantly, with associated costs. Project risk issues are discussed by Grey (1995) and Chapman and Ward (1998), and are not further pursued in this book.

Risk management of process systems can be seen to have a wide range of foci – from employee risks to environmental and corporate reputation. Comprehensive risk management needs to provide the appropriate focus on all relevant aspects that directly or indirectly affect the well-being of the corporation, its employees and related stakeholders.

The following section focuses on the key hazards and risks common to process systems.

### 1.3.2 The Key Players in Risk Management

Process risk management is a stakeholders' paradise. Stakeholders and interested parties are a vital aspect of effective risk management, since it is essential to ensure that all affected groups have the necessary input to the process and that the communication between groups is effective over the life cycle of the process.

Figure 1-3 shows the principal players in process risk management clustered under three general areas of:

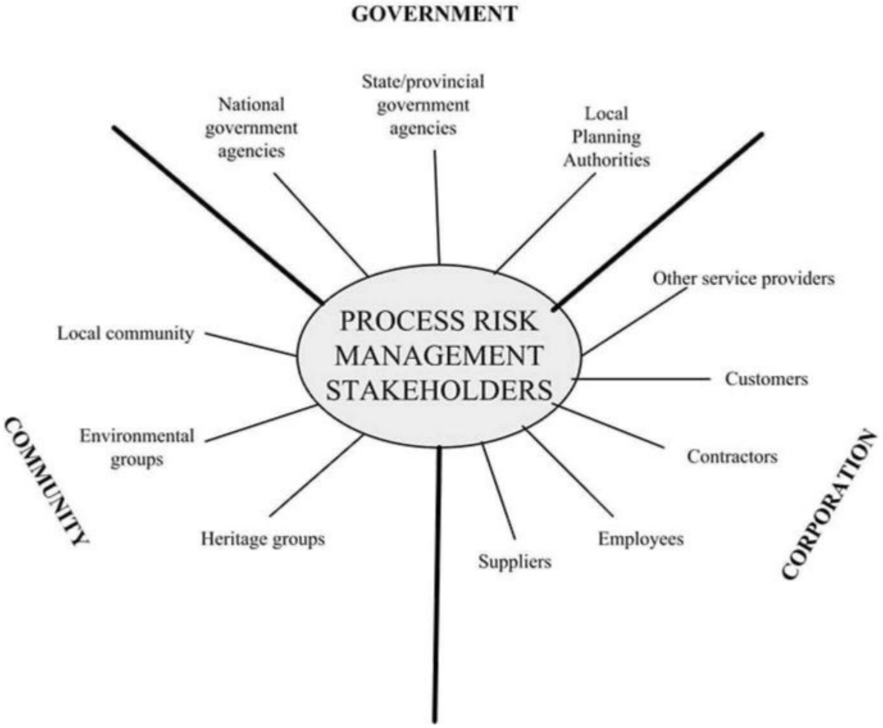
- Corporation
- Government
- Community

The general risk management process in Figure 1-1 shows the necessity for communication to all relevant parties at *each* stage of the process. Major hazard developments will often result in a wide ranging consultation process through the environmental impact assessment (EIA) process, common to many state and national government regulations.

The general issues for the various players can be set out as follows:

National/state governments:

- strategic planning
- regional and economic development
- development control



[redacted] FIGURE 1-3 PROCESS RISK MANAGEMENT STAKEHOLDERS

Local authorities:

- development control plans
- town planning schemes
- potential impacts
- environmental concerns (air, noise, water, waste)
- social concerns (health, safety, consultation)
- infrastructure issues (services, transport, effluent)

Corporation:

- economic viability
- on-site safety
- off-site safety
- communication
- access (markets, raw materials, services)
- operational certainty (nearby land uses)

Public:

- maintenance of amenity
- noise, odour, pollution, lighting
- transport corridors
- natural environment
- refuse and wastewater
- hazards and risks (acute and chronic)
- heritage issues

All these issues play a very important role in the land use planning of major hazard facilities (MHF) and other process related operations. These are addressed in Chapter 13. Risk management provides an accepted framework to help address these concerns in a structured manner. However as we discuss in Chapter 15, the issue of risk perception is vital in the overall effectiveness of risk management practice.

## 1.4 HAZARD AND RISK IN PROCESS SYSTEMS

### 1.4.1 The Incident Spectrum

Section 1.1.1 discussed what constitutes a hazard. What is clear is that hazards arise from a number of areas – the substances used, the types of activities carried out, the way things are done.

Harmful effects flowing from these hazards were also considered and these can cover a wide range of potential impacts–minor injury to death, minor to catastrophic damage. Hence there is a spectrum of potential impacts based on severity.

Coupled with this is the question of 'how often?' these incidents occur. It's clear that in the workplace we might experience a large number of minor effects from hazards. For example, minor cuts, abrasions, strains and the like. However, the incidents at the other end of the spectrum which lead to death or catastrophic damage are usually and thankfully rare. Figure 1-4 shows this spectrum of incidents.

In terms of the control of these incidents, the far left end (low impact, frequent occurrence) is usually associated with occupational health and safety issues. The far right end (high impact, rare occurrence) are those events which require special analysis and which engender particularly strong responses from the public and particular concern to corporations. The whole spectrum is the focus of process systems risk management.

In the following sections events and incidents within the process industries are highlighted.

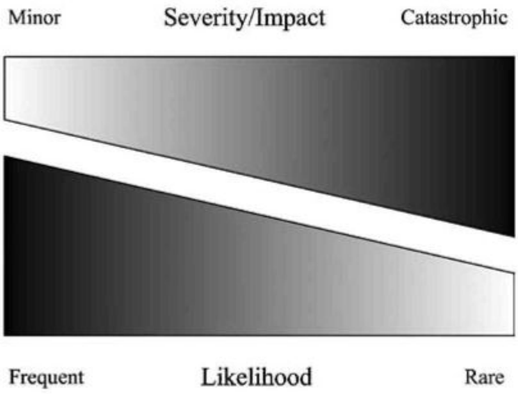


FIGURE 1-4 THE INCIDENT SPECTRUM

## 1.4.2 Events and Incidents in Process Systems

In the context of this book we make specific use of the words 'event', 'incident' and 'accident'.

An 'event' refers to a single happening or occurrence such as a liquid release, evaporation or a fire. A probability or frequency can be assigned to each.

An 'incident' is a sequence of events that could result in adverse impacts or disruption, whereas an 'accident' is a sequence of uncontrolled events producing unintended consequences affecting the on-going functioning of the system.

### *1.4.2.1 Minor incidents*

In the context of the process industries or in the transport of dangerous goods the types of minor events incidents can include:

- Slips, trips and falls
- Nuisance/minor distress from exposure to harmful environments
- Minor burns

### *1.4.2.2 Fires, explosions, toxic release*

There are several events which fall into this category, simply because they have a potential for direct major impact, or impact from incident escalation. These events include:

- Fire (pools, jet, spray, flash)
- BLEVE (Boiling Liquid Expanding Vapour Explosion)
- Vapour cloud explosion (VCE)
- Dust explosions
- Toxic gas releases
- Toxic liquid or solid releases
- Toxic combustion products from fires

All these events have, and can occur in the storage, processing and transport of hazardous materials. Table 1-2 gives a selection of some accidents which have occurred over the last 80 years, showing that these accidents are not confined to a few countries or to a few types of operations but cover a broad range of activities across geographical boundaries.

A quick perusal of the list shows several "classic" accidents such as Flixborough (1974), Seveso (1976), Bhopal (1984) and Piper Alpha (1988) that have led to significant regulatory changes in risk management both nationally and internationally.

### 1.4.3 Contributing Factors to Process Risk

There are many significant contributing factors when considering process risks and the following sections highlight these. They are the subject of further consideration in later chapters.

### *1.4.3.1 Properties of hazardous materials*

Inherent properties of substances or mixtures are important factors in risk assessment. These are the contributing factors to the hazardous nature of the material. We recognise a number of these factors in the case of hazardous substances, including (Lewis 1996):

- Toxicity
  seen as: Lethal dose ($LD_{50}$)
  Threshold Limit Value (TLV)
- Flammability
  seen as: Flash-point
  Auto-ignition point
  Flammability limits (when mixed in air)

TABLE 1-2 SELECTED MAJOR ACCIDENTS

| Date | Location | Substance | Event | Death/ Injury |
|---|---|---|---|---|
| 1921 | Oppau, Germany | ammonium nitrate | explosion | 561d |
| 1942 | Honheiko | coal dust | explosion | 1572d |
| 1944 | Cleveland, USA | LNG | explosion | 131d |
| 1947 | Texas, USA | ammonium nitrate | explosion | 576d |
| 1948 | Ludwigshafen | dimethyl ether | explosion | 207d |
| 1956 | Cali, Colombia | dynamite | explosion | 1100d |
| 1968 | Hull, UK | acetic acid | explosion | 2d, 13i |
| 1969 | Basel, Switzerland | nitro liquid | explosion | 3d, 28i |
| 1969 | Teeside, UK | cyclohexane | fire | 2d, 23i |
| 1970 | Philadelphia, USA | cat. cracker | fire | 1d, 50i |
| 1971 | Houston, USA | VCM | BLEVE | 1d, 50i |
| 1972 | Brazil | butane | explosion | 37d, 53i |
| 1972 | Netherlands | hydrogen | explosion | 4d, 4i |
| 1973 | Potschefstroom | ammonia | toxic | 18d |
| 1974 | Flixborough, UK | cyclohexane | UVCE | 28d, 53i |
| 1975 | Antwerp, Belgium | ethylene | explosion | 6d |
| 1976 | Baton Rouge, USA | chlorine | toxic | 10000 evac |
| 1976 | Houston, USA | ammonia | toxic | 6d, 200i |
| 1976 | Seveso, Italy | dioxin | toxic | 1000+ i |
| 1977 | Columbia | ammonia | toxic | 30d, 22i |
| 1978 | San Carlos de la Rapita, Spain | propylene | fire/explosion | 211d |
| 1978 | Chicago, USA | $H_2S$ | toxic | 8d, 29i |
| 1979 | Bantry Bay, Eire | oil | explosion | 50d |
| 1984 | Bhopal, India | MIC | toxic | 3800d, 250000+i |
| 1984 | Mexico City | LPG | fire/explosion | 450+d |
| 1986 | Rhodes, NSW | oil | explosion | 5d |
| 1987 | Laverton, Vic | hot-metal | explosion | 2d |
| 1987 | Cairns, Qld | LPG | BLEVE | 1d, 5i |
| 1988 | North Sea (Piper Alpha) | gas | fire/explosion | 167d |
| 1989 | Ufa, USSR | LPG | explosion | 500d? |
| 1990 | Sydney, NSW | LPG | BLEVE | - |
| 1992 | Guadalajara, Mexico | Hexane | explosion | 170d, 500+i |
| 1995 | Sao Paulo, Brazil | oil pipeline | fire | 1d, 5i |
| 1997 | Blaye, France | grain | dust explosion | 11d, 1i |
| 1999 | Martinez, California | naphtha | fire | 4d, 1i |
| 2000 | Enschede, Netherlands | fireworks | explosion | 25d, 1000i |
| 2001 | Toulouse, France | ammonium nitrate | explosion | 30d, 2000i |
| 2002 | Al-Rawdatayn, Kuwait | oil | explosion/fire | 4d, 19i |
| 2003 | Amman, Jordan | fuel | tanker fire | 10d, 18i |
| 2004 | Skikda, Algeria | natural gas | explosion/fire | 27d, 72i |

- Explosion
  seen as: Detonation (e.g. TNT)
  Deflagration (e.g. LPG)

Vapour cloud explosion
BLEVE (e.g. LPG)
Dust explosion (e.g. grain, coal, powder, metal)

In attempting to deal with the issue of hazards, classification of certain chemical substances have been internationally accepted under the UN practice (http://www.unece.org/trans/danger/danger.htm), and the International Maritime Dangerous Goods (IMDG) Code. Equivalent national codes have been developed in many countries. These classify a large number of substances into 9 dangerous goods classes. Figure 1-5 shows the classes which are currently used in most dangerous goods codes.

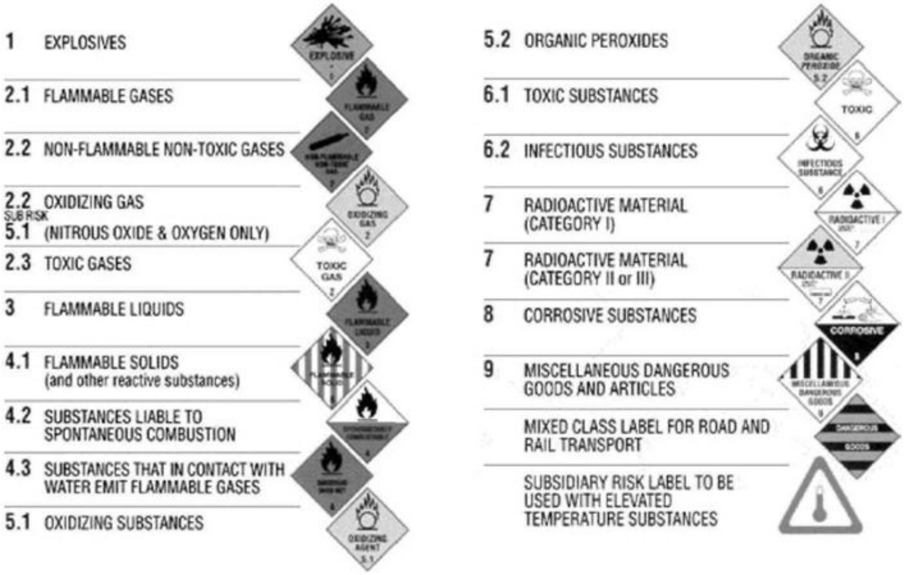

1 EXPLOSIVES
2.1 FLAMMABLE GASES
2.2 NON-FLAMMABLE NON-TOXIC GASES
2.2 OXIDIZING GAS
SUB RISK
5.1 (NITROUS OXIDE & OXYGEN ONLY)
2.3 TOXIC GASES
3 FLAMMABLE LIQUIDS
4.1 FLAMMABLE SOLIDS (and other reactive substances)
4.2 SUBSTANCES LIABLE TO SPONTANEOUS COMBUSTION
4.3 SUBSTANCES THAT IN CONTACT WITH WATER EMIT FLAMMABLE GASES
5.1 OXIDIZING SUBSTANCES
5.2 ORGANIC PEROXIDES
6.1 TOXIC SUBSTANCES
6.2 INFECTIOUS SUBSTANCES
7 RADIOACTIVE MATERIAL (CATEGORY I)
7 RADIOACTIVE MATERIAL (CATEGORY II or III)
8 CORROSIVE SUBSTANCES
9 MISCELLANEOUS DANGEROUS GOODS AND ARTICLES
MIXED CLASS LABEL FOR ROAD AND RAIL TRANSPORT
SUBSIDIARY RISK LABEL TO BE USED WITH ELEVATED TEMPERATURE SUBSTANCES
EXPLOSIVE
TOXIC GAS
TOXIC
CORROSIVE
DANGEROUS GOODS

**FIGURE 1-5 DANGEROUS GOODS CLASSES (CHEM UNIT 2004)**

Once the dangerous goods classification of a substance is known, the appropriate emergency response information can be found in the codes.

A supplementary form of classification is through the use of “risk phrases”. These are typically referred to as R1, R4, R17 etc. and supplement the dangerous goods classifications. The intention is to give further specific hazardous information on the substance. As well as risk phrases there are "safety phrases" which set out details of handling, safe storage and personal protection for a range of substances. Both risk and safety phrases are adopted from European Union initiatives. Again, most substances can be classified under 1 or more of these categories.

A comprehensive list of risk and safety phrases is to be found in Worksafe Australia Code NOHSC: 2012 (1994), as well as the International Labour Organization Convention 170 (http://www.ilo.org).

### *1.4.3.2 Process design, control and operational factors*

Details of hazard identification, design, control and operational factors are described in Chapter 4. Methods of assessing and managing the hazards are described in Chapters 5-14. Only an overview is provided here.

Contributing factors related to the operations might involve deviations from good practice covering,

- Major variables (levels, temperatures, pressures, etc.)
- Time of actions
- Sequence of operations
- Human factors (See Section 1.4.3.3)
- Identification and control of ignition sources
- Operational policies and practices

**Process design**

The underlying design is the fundamental starting point in process risk management considerations. The principal factors which are relevant include:

- Process development philosophy, that seeks to address inherently safer designs
- Processing routes, including process structure and the degree of coupling in the system
- Process complexity in the design including the unit operations and chemical species present
- Process layout, which influences inherent safety such as segregation, separation, maintenance access and emergency response.
- Process design standards, that can be purely compliance based or risk based.

The importance of process design factors is seen in the following examples.

**EXAMPLE 1-11 DESIGN RELATED RISK FACTORS**

a) The historic change in nitroglycerine production from large batch reactors to very small continuous production facilities using nitration injectors led to a huge reduction in risk through improved design and ease of operation.

b) The storage of intermediate chemical products in the process can often be eliminated by immediate use of the intermediate in the next reaction stage. At Bhopal the methyl isocyanate was an intermediate used to produce carbaryl. Some 90 tonnes were held, whereas new process designs have a maximum inventory of only 10 kg. (Willey, 1998).

c) Alternate reaction pathways exist for many chemical products, that lead to routes that are more inherently safer options. The route to carbaryl is one such case where the less hazardous intermediate α-naphthol chloroformate is produced that can then be reacted with methylamine to give carbaryl.

**Process Control**

Process control is an inevitable result of dealing with a system that operates under a range of disturbances.

Contributing risk factors from control include:

- Control feedback structures and increased information complexity
- Failure in control loop components such as sensors, controllers, actuators and valves.
- Multivariable control schemes whose status and root causes of failures are often difficult to interpret when they occur
- Inadequate instruments, alarms, interlocks and maintenance
- Poor human-machine interface (HMI) designs that are difficult to interpret by operators in emergency situations.
- Poor control room layout that creates problems under emergency conditions.

Some examples include:

**EXAMPLE 1-12 CONTROL RELATED RISK FACTORS**

a) Partial failure of a naphtha stripper level control by-pass valve at the Tosco Refinery, California prevented isolation of the line from the process unit contributing to loss of naphtha and subsequent fire that killed 4 workers. (CSB, 2000.)

b) During the Three Mile Island (TMI) nuclear power plant partial meltdown, operators were unaware that a pilot operated relief valve had opened. Multiple alarms and warnings overwhelmed the operators resulting in actions that made conditions worse.
Alarm management and adequate instrumentation were control-related factors contributing to the accident.

### 1.4.3.3 *Human factors*

One can take the view that all incidents are ultimately traceable to human failings. A cursory reading of accounts of major accidents (Chiles, 2001; Hopkins, 2000; Perrow, 1999; Reason, 1990, 1997; Dörner, 1989) emphasizes this point. Human factors are vitally important and Cacciabue (2000) estimates that the human factor contribution to risk is as high as 70-80% and much more visible due to the rapidly increasing reliability of mechanical and electronic components. Working environments for operators have become more demanding on cognitive-reasoning abilities due to increased design and operational complexities.

Identification of human failure modes is described in Chapter 4. Human factors related to reliability are described in Chapter 8, and facility life cycle issues are commented on in Chapter 12.

The literature on the area of human factors in risk management is voluminous (CCPS 1994). It is also a well recognized issue in risk assessment and management as evidenced by major worldwide regulations. These include the European Union through such standards as IEC300-3, Dependability Management which specifically mentions the important role of human factors in risk and the use of human reliability analysis (HRA), task analysis (TA) and human error identification (HEI) as tools to be used in tackling these issues.

In the USA, a number of regulations and codes of practice emphasise similar concerns. The Occupational Safety and Health (OSHA) Process Safety Management (PSM) standard CFR 1910.119 and the EPA Risk Management Plan (RMP) deal with human factor issues. Industry codes such as the American Petroleum Institute (API) Safety Environmental Management Plan (SEMP) RP75 for off-shore operations emphasizes similar human factor concerns.

What is clear from the mass of literature is the increasing focus on human factors in technological systems as well as the difficulties in effectively and comprehensively addressing the issues. It remains one of the most difficult and challenging areas of consideration in process risk management.

Some typical examples where human factors played major roles in accidents are:

**EXAMPLE 1-13 HUMAN FACTORS RELATED TO RISK**

a) The accident at Three Mile Island nuclear power plant had numerous human factors playing a leading role. One was training for incident scenarios that appeared to not consider multiple failures. Another factor was related to design flaws in the control system, making diagnosis extremely difficult and hence affecting decision-making (Perrow 1999).

b) The Piper Alpha offshore platform disaster in the North Sea in 1988 was permeated with many human errors. Maintenance failures to isolate open relief valve flanges, communication failures between operating shifts, superficial inspection regimes, poor decision-making on isolation of emergency fire pumps were all part of the recipe for disaster that killed 167 people.

c) The gas plant explosion at Esso's Longford plant in Victoria Australia in 1999 was strongly linked to organizational failures. Lack of hazard identification, operator training deficiencies, lack of knowledge and corporate responsibility were major human factors that were evident in the post-accident Royal Commission (Hopkins 2000).

■ ■ ■

These few examples illustrate the absolute need to fully address the human risk factors through the complete life cycle of the process to ensure the design, construction and operation are fully considered from this perspective.

### 1.4.4 The Ubiquitous Nature of Uncertainty

Uncertainty pervades all areas of risk management. It is important that due recognition is given to the role that uncertainty plays in each phase of risk management as was outlined in Figure 1-1.

Here the forms of uncertainty and their representation at each phase require careful consideration in any risk analysis and the subsequent decision-making that takes place. We cannot avoid uncertainty, we need to treat it appropriately. It is an inevitable fact due to limited knowledge and assumptions made. In Chapter 10, explicit treatment of uncertainty in the decision-making process is discussed. However, earlier chapters on hazard identification, consequence analysis, causal and frequency analysis highlight uncertainty contributions to overall assessment.

The concept of the precautionary principle is often used to deal with some aspects of uncertainty and sometimes as an excuse to avoid analysing its impact! Whatever the approach adopted it will always play a role in process risk management.

## 1.5 THE REGULATORY ENVIRONMENT OF RISK MANAGEMENT

### 1.5.1 International Conventions

International conventions through such organizations as the International Labor Organization (ILO), the United Nations (UN) or United Nations Environment Program (UNEP) provide umbrella principles under which signatories have established national and regional legislation with accompanying regulations. The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) also develop major standards impacting on worldwide risk management practices.

Within Europe, the European Communities (EC) have been active in establishing directives that address issues of major importance to the member companies. Such directives as the Seveso II directive (EC96) for major hazards and the directive on Classification, Packaging and Labelling of Dangerous Substances (EC99) provide some harmonization framework across community member states. The individual member states adopt directives and express them in national legislation and regulations relevant to the country (Milburn and Cameron, 1992).

### 1.5.2 National and Local Regulatory Frameworks

In all industrialised countries, there is some form of legislation that governs risk management when protecting the health and safety of employees, the environment, and public health.

In Australia as in other jurisdictions this legislation varies from state to state. Instead of providing a list of acts and regulations, the common features of the legislation are provided here to gain an appreciation of the role regulations play in the overall risk management process.

The legislation may be broadly grouped into three classes:

### Group 1: Protection of employees at the workplace

The legislation and regulations that govern this include:

- Acts relating to health and safety at work
- Occupational Health and Safety regulations
- Exposure levels for contaminants in the workplace
- Risk assessment and management in major hazard facilities
- Storage and handling of dangerous goods and hazardous substances
- Fire protection and building regulations

### Group 2: Protection of environment

The regulations in this area have been numerous, with ongoing changes. Major regulations generally cover the following:

- Protection of the environment (air, water, noise control)
- Environmentally hazardous chemicals control
- Contaminated land management
- Waste generation and disposal
- Various other pollution control regulations

### Group 3: Protection of public and public health

Regulations in this area tend to overlap the health and safety at work acts and the environmental protection acts.

Major regulations are:

- Environmental planning regulations
- Siting of hazardous industries in relation to land use safety
- 'Safety Report' requirements from major hazard facility operators addressing public safety issues.
- Health risk regulations from contaminated land and contaminants in surface/groundwater
- Drinking water quality standards
- Surface water quality standards.

Regulatory considerations also include the application of various design Codes, Standards and industry Recommended Practices, many of which have been explicitly and implicitly called for in the regulations.

The number of regulations is vast, and specific references should be made for each country, state or jurisdiction. Some examples follow.

In Australia, there is no federal regulation in the above 3 categories. Each state has its own range of regulations for occupational health and safety, and environmental protection. In the area of control of major hazard facilities, the National Occupational Health and Safety Commission has published a National Standard and Code of Practice, (NOHSC 1014, 2002), but it is advisory only.

Among the states of Australia, Victoria legislated for control of major hazard facilities in 2000, and Queensland in 2001. Other states will follow.

The European Commission has developed community legislation that includes the environment, consumers and health protection. Member countries have developed regulations to address these issues. The main framework for control of major hazards is Directive No. 96/82/EC of December 1996, known as the Seveso II Directive, replacing the previous Directive of 1982.

In the UK, major hazards are controlled by the COMAH (Control of Major Accident Hazards) regulations (1999) administered by the UK Health and Safety Executive. This is in response to the Seveso II Directive of the EC. The Health and Safety at Work Act and its associated Statutory Instruments cover a very wide range of activities.

The COMAH Regulations require an operator to identify the hazards, the impact of the hazard on habitats, species or communities, the severity and likely duration of the effects, and what the operator has in place to prevent major accidents, limit their consequence to persons and environment, assess damage, and/or repair damage after an accident.

The COMAH Regulations also require operators of establishments handling prescribed dangerous substances to prepare on-site emergency plans, and the local authorities to prepare off-site emergency plans.

In the USA, two federal regulations apply to control of hazardous materials:

- USA - OSHA 29 CFR 1910.119
- US EPA Rule 40 CFR Part 68.

In addition, the control of Major Hazard Facilities (MHF) is dealt with by individual state regulations. All relevant laws and regulations appear in the Federal Code of Regulations.

To a large extent, meeting the regulatory requirements would implicitly result in a significant improvement in managing the risks in Major Hazard Facilities. This is further discussed in Chapter 13.

Some useful web sites regarding legislation are:

http://www.austlii.edu.au
- provides a list of legislation in Australia.

http://www.hse.gov.uk
- UK Health and Safety Executive site.

http://europa.eu.int/comm/environment/index-en.htm
- European Commission for the Environment.

http://www.epa.gov
- US Environmental Protection Agency

http://www.osha.gov
- US Occupational Safety and Health Administration

http://www.gpoaccess.gov.cfr
- US Code of Federal Regulations

## 1.6 REVIEW

Hazards and risks are the inevitable result of human activity. The only sure way of eliminating risk - that is the zero chance option is for the activity not to exist. There is no such thing as zero risk for any human activity.

In this chapter we have noted the fundamental difference between hazard and risk. Hazards have the potential to do harm, and arise from the materials or processes associated with the activity. Risk is the likelihood or chance of a nominated level of harm occurring either in a given time or under specified circumstances.

We also saw that there are various contributing factors to hazards, especially when related to activities involving dangerous substances. These must be controlled or eliminated depending on their importance and the viability of doing so. We could call these 'source' oriented factors. As well a popular view of risk which involves the level of outrage is a very real phenomenon and must be dealt with by governments and industry proponents. We all view the risk issue from quite different perspectives, conditioned by our worldview and our experiences.

The task of risk management is to identify risks and treat them accordingly. It is a structured, systems approach that provides the most effective means of achieving risk control.

In summary, the concept of hazard and risk may be put in a few simple words:

- Consider a situation.
- What can go wrong? (Hazard)
- What are the consequences if the hazard were realised? (Severity, one dimension of risk)
- What is the likelihood of the hazard being realised? (Probability, second dimension of risk)
- Have sufficient measures been adopted to prevent an unwanted outcome and/or mitigate its adverse effects? (Risk management)

## 1.7 REFERENCES

Cacciabue, P.C. 2000, 'Human factors impact on risk analysis for complex systems', *Journal of Hazardous Materials*, vol. 71, pp. 101-116.

CCPS, Center for Chemical Process Safety, *Human Factors in Process Safety Management* 1994, AIChE, NY., ISBN 0-81690-6246.

CHEM Unit 2004, Available at: http://www.emergency.qld.gov.au/chem/dangerous/classes.asp .

Chapman, C. and Ward, S. 1997, *Project Risk management - Processes, techniques and insights*, John Wiley.

Chiles, J.R. 2001, *Inviting Disaster - Lessons from the Edge of Technology*, Harper Business, ISBN 0-06-662081-3.

CSB, US Chemical Safety and Hazard Investigation Board 2000, Available at: http://www.csb.gov .

Dörner, D. 1989, *The Logic of Failure*, Perseus Books, USA, ISBN 0-201-47948-6.

EC96 1997, 'Seveso' II Directive (96/82/EC) on the Control of Major Accident Hazards involving dangerous substances, *Official Journal of European Communities*, L10/13-33.

EC99 1999, Directive 1999/45/EC on Classification, Packaging and labelling of dangerous preparations, *Official Journal of European Communities*, L200/1-68.

Grey, S. 1995, *Practical Risk Management for Project Management*, John Wiley.

Hopkins, A. 2000, *Lessons from Longford - The Esso Gas Plant Explosion*, CCH Australia, ISBN 1-86468-422-4.

International Electrotechnical Commission. *Dependability Management Pt3 Application Guide Section 9: Risk Analysis of Technological Systems*, International Electrotechnical Commission, IEC300-3-9:1995.

International Maritime Dangerous Goods (IMDG) Code, Available at: http://www.imo.org .

ISO/IEC, *Risk management -- Vocabulary -- Guidelines for use in standards*, Guide 73:2002.

Jones, D. 1992, *Nomenclature for Hazard and Risk Assessment in the Process Industries*, 2nd edn, The Institution of Chemical Engineers, Rugby, England.

Lewis, R.J. 1996, *Dangerous Properties of Industrial Materials*, 9th edn, Van Nostrand Reinhold, USA.

Milburn, M. and Cameron, I.T. 1992, *Planning for Hazardous Industrial Activities in Queensland,* Australian Institute of Urban Studies, May, ISBN 0-86419-814-0.

NOHSC, National Occupational Health & Safety Commission Australia. *National Code of Practice for the Labelling of Workplace Substance*, NOHSC 2012: 1994.

NOHSC, National Occupational Health & Safety Commission Australia. *Control of Major Hazard Facilities National Standard*, NOHSC 1014:2002 and *National Code of Practice*, NOHCS 2016:1996.

OSHA, Occupational Health and Safety Administration, USA. *Process safety management of highly hazardous chemicals*, Federal Register, Washington DC. OSHA 29 CFR 1910.119:1992.

Perrow, C. 1999, *Normal accidents - Living with High-Risk Technologies,* Princeton University Press, ISBN 0-691-00412-9.

Rasmussen, J. 1997, 'Risk management in a dynamic society: a modelling problem', *Safety Science*, vol. 27, no. 2, pp. 183-213.

Reason, J. 1990, *Human Error*, Cambridge University Press, UK, ISBN 0-521-31419-4.

Reason, J. 1997, *Managing the Risks of Organizational Accidents*, Ashgate, UK, ISBN 1-84014-105-0.

Standards Australia. *Risk Management*, Standards Australia. AS 4360:2004.

US EPA. *Environmental Protection Agency - Risk management programs for chemical accidental release prevention.* Federal Register, Washington D.C., June. Final Rule, 40 CFR Part 68, 1996.

Willey, R.J. 1998, *The Bhopal Disaster*, SACHE Slide Package, Center for Chemical Process Safety, AIChE, New York.

## 1.8 NOTATION

| | |
|---|---|
| ADG | Australian Dangerous Goods Code |
| API | American Petroleum Institute, USA |
| AS | Australian Standards |
| BLEVE | Boiling liquid expanding vapour explosion |
| COMAH | Control of Major Accident Hazards, UK |
| CSB | US Chemical Safety & Hazard Investigation Board |
| DOT | Department of Transport, USA |
| EC | European Communities |
| EIA | Environmental impact assessment |
| EPA | Environmental Protection Agency |
| HEI | Human error identification |
| HMI | Human machine interface |
| HRA | Human Resources Analysis |
| IChemE | Institution of Chemical Engineers, UK |
| IEC | International Electrotechnical Commission |
| ILO | International Labour Organization |
| IMDG | International Maritime Dangerous Goods Code |
| ISO | International Organization for Standardization |
| IT | Information technology |
| $LD_{50}$ | Lethal dose, 50% of population |
| LPG | Liquefied Petroleum Gas |
| LTI | Lost Time Injury |
| LTIR | Lost Time Injury Rate |
| LTIIR | Lost Time Injury Incident Rate |
| MHF | Major hazard facility |
| MTI | Medically treated injury |
| NOHSC | National Occupational Health and Safety Commission, Australia |
| OH&S | Occupational health and safety |
| OSHA | Occupational Safety and Health Agency, USA |
| PSM | Process safety management |
| RMP | Risk Management Plan |
| SEMP | Safety, Environmental Management Plan (USA) |
| TA | Task analysis |
| TLV | Threshold limit value |
| TMI | Three Mile Island, USA |
| TNT | Tri-nitro Toluene |
| UN | United Nations |
| UNEP | United Nations Environmental Program |
| VCE | Vapour Cloud Explosion |

This page is intentionally left blank

# 2

# RISK - ESTIMATION, PRESENTATION AND PERCEPTION

*"Scientists may be able to explain the facts, but the facts rarely speak for themselves. The facts are interpreted by individuals who may behave in quite different ways to those which scientists or public policy makers or the industrialists originally intended."*

*Howard Newby (1997)*

The previous chapter established the need for risk management and some of the important roles that risk management plays in a range of corporate, legal and social contexts. This chapter discusses the principal issues surrounding the measurement of risk, how it is estimated, how it can be presented for appropriate decision making and how it can be perceived by the stakeholders. It provides an overview that will be expanded in subsequent chapters.

## 2.1 MEASURES OF RISK

Here we investigate various risk measures that can be used for a variety of applications. These seek to address the key areas of process related risks given in Table 1-1.

### 2.1.1 Need for Risk Measurement

The discussion so far in Chapter 1 has established the following:

- All activities are associated with some risk.
- In order to make a commercial enterprise successful, it is necessary to identify and manage the risks.
- The two-dimensional nature of risk (likelihood and consequence) has to be recognised for effective risk management.
- Not only the experts' world-view of risk, but that of the non-expert should be given due consideration in the risk management process, if the latter have an input into decision making.
- A decision made based on risk assessment, followed by the implementation of a risk management process would go a long way to ensuring project success.

This raises the question:

'How do we know that a risk is low enough to be acceptable? In other words, how low is low enough?'

To answer this question, we need some measures of risk, so that relative risks can be compared.

### 2.1.2 Qualitative and Quantitative Measures

Risk measures can range from the purely qualitative to fully quantitative, accompanied by uncertainty analysis. In most cases of risk management, measures are applied along a continuum in order to ensure minimum work for the maximum effect. It is important that appropriate measures are used throughout the process life cycle and within a particular project. It is also important that the measures used in a project are commensurate with the stage of analysis and the level of understanding. Figure 2-1 shows the risk measurement continuum with some examples of techniques in each class.

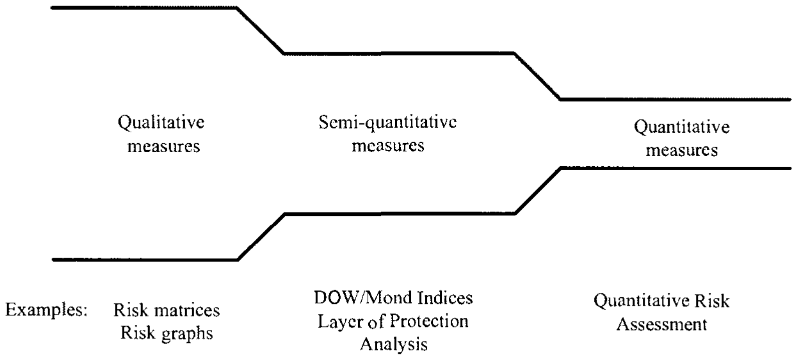


FIGURE 2-1 THE RISK MEASURES SPECTRUM

In Figure 2-1 we can observe a "funnelling" of activity, illustrating that in most cases, events or incidents that are identified can be sorted or ranked and dealt with appropriately across the spectrum. Qualitative analysis can be applied early in the risk management process to sort those events or incidents that need further detailed consideration. As one moves to the right of the risk measurement spectrum the effort expended in analysis and assessment goes up by an order of magnitude at each stage. This is because of the increased complexity and hence time and resources needed to carry out quantitative analyses compared with qualitative analyses. Hence, full quantification of risk is only needed in a minority of process system applications and only for a subset of all identified risks. Quantitative risk assessment (QRA) or probabilistic risk assessment (PRA) studies demand significant time and resources. Hence, only in the case of potentially high impact events are quantitative methods generally justified.

The other issue is to do with insight. By adopting a range of measures that are systematically applied, the analyst or team gains valuable insight into the main risk contributors and those that are low contributors by systematically working through the risk measure stages. This has important implications in the on-going management of these risks. The stage of the process or product life cycle in which the risk management activities take place will also determine the level of analysis possible and justifiable.

### 2.1.2.1 Qualitative measures

These are the simplest to apply. In adopting a two-dimensional view of risk that considers impact and likelihood as the two principal factors we can develop simple tools to firstly rate the impacts or severity as well as the likelihood for each identified event or incident in the system.

The simplest qualitative risk measure is the risk matrix as seen in Figure 2-2.

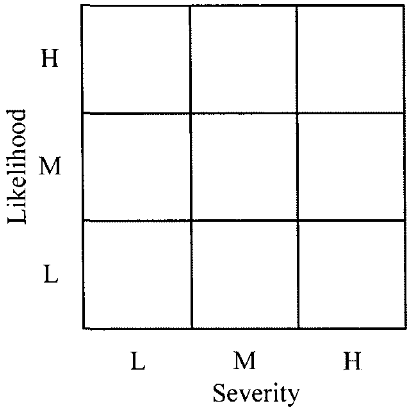


FIGURE 2-2 A RISK MATRIX

Here the two factors of severity and likelihood have 3 classes designated as low (L), medium (M) and high (H). Risk measures need to be allocated so as to place an event in the appropriate cell.

In practice a qualitative risk scale can be set up, such that the risks could be categorized as the product of the severity and the likelihood:

|  |  |  |
|---|---|---|
| H × H | → | Extreme risk (E) |
| H × M | → | High risk (H) |
| M × M or H × L | → | Medium risk (M) |
| M × L | → | Low risk (L) |
| L × L | → | Negligible risk (N) |

Clearly the extreme risks (E), reside in the top right hand corner of the matrix, whilst negligible risks (N) are located in the bottom left cell. Low to high risks are then distributed across the matrix. It is now possible to place events into a particular cell in the risk matrix. Further action can be taken for risk management purposes on those risks that are extreme or high. It allows ranking and prioritization to take place.

In practice a 3 × 3 matrix is too coarse to provide useful information for decision making. More complex versions are defined in Chapters 3 (Section 3.4) and 9.

Risk graphs are an alternative to risk matrices and these are discussed in section 9.2.5. They are simply an alternate representation of the basic severity and likelihood factors, and can also include exposure likelihood.

### 2.1.2.2 Semi-quantitative measures

These measures come in several forms. Risk can be estimated in a semi-quantitative way through the use of indices such as the Dow's Fire and Explosion Index or F&EI (AIChE, 1994a) which allows the estimate of both consequence and likelihood factors in a process unit. This allows a relative ranking of risk to be made for operating units within a process based on total energy content and possible release. Details of this technique are given in Section 4.3.7.1.

Other risk indices of this type include Dow's Chemical Exposure Index or CEI (AIChE, 1994b). Again this provides semi-quantitative analysis of toxic risks for prioritization purposes. (see section 4.3.7.2)

Other variants of these indices exist which attempt to classify risks into various categories. One such is the Safety Weighted Hazard Index (SWeHI) proposed by Khan et al. (2001). Others include insurance based indices such as the Instantaneous Fractional Annual Loss (IFAL) index (Whitehouse 1985).

### 2.1.2.3 Quantitative measures

Risk can be measured and presented in quantitative terms, where both the severity and the likelihood are quantified. Risk quantification is normally undertaken when acceptance or tolerability criteria are available for comparison or acceptance purposes. It can often be used to assess alternate designs and thus used in a relative risk approach. Quantitative criteria are often available for employee and public fatality and injury risk. In this case, the risk values that are computed take a variety of forms which include:

a) Individual fatality risk per year

b) Individual injury risk per year covering such issues as:
   - thermal radiation impacts
   - toxic exposures
   - explosion impacts

c) Societal or group risks that consider the fatality risk to more than 1 person.

Other quantitative risk measures can relate to:

d) Probability of specified levels of environmental impact per year
e) Probability of specific business losses in a year
f) Probability of specific public complaints in a year.

In what follows we introduce the societal risk concept first rather than individual risk, as the latter is a subset of the former.

## 2.2 SOCIETAL RISK

When a hazardous incident can affect a group of people, resulting in potential multiple fatalities, a societal or 'group' risk estimate is the most appropriate measure of impact. The number of fatalities depends on the area of impact, the population density within the area and the vulnerability of the population to the hazard.

Societal risk assesses risk to the exposed population as a whole, without being location specific. It is often expressed as the frequency with which a given number of fatalities may occur from the realisation of a hazard, or alternatively, the product of these two, known as Potential Loss of Life (PLL). This is often termed the expected value of the number of deaths per year.

The uncertainty in the assessment of societal risk is much higher than that for individual risk. The following information is required:

1. Population distribution over the potential impact area of an accident. This may be available only in well established population areas and not in new developments.
2. Probability of fatality given an accident in the area. This value depends on what is impacted - whether the object of impact is clear ground or a building, and the robustness of the building to take the impact.
3. Expected number of fatalities from the incident. The value depends on such factors as the degree of injury sustained and the availability and skills of emergency responders.

In spite of the uncertainties, it is useful to assess societal risk where it is possible, and where relevant data is available with minimal uncertainty. The societal risk is often expressed as a curve of frequency (F) versus number of fatalities (N), for a range of hazards, the F-N curve. A relative evaluation of risk reduction measures can be made by observing the movement of the curve. A typical set of F-N curves for historical accidents is seen in Figure 2-3.

## 2.3 INDIVIDUAL RISK

Individual risk is a measure or estimate based on the exposure of a person to a hazard. However, individual risk can be stated in various ways. These include:

(i) Location specific individual risk (LSIR)
The LSIR relates to an individual at a specific geographic location in the vicinity of a hazard who is exposed continuously to that hazard. No account is taken of evasive action in this case. This is dealt with in section 2.4.3.3. It is commonly used in land use planning criteria for fatality or injury.

(ii) Risk to the most vulnerable person.
This could be related to the young, elderly or an individual with some specific sensitivity to the hazard, such as an asthmatic to gas exposure. This measure is important in land use safety planning in the vicinity of major hazard facilities. However, this measure is difficult to calculate and is not normally used. Instead, the risk tolerability criterion is reduced.

(iii) Risk to most exposed worker per annum (IRPA). In this measure, the risk from each hazardous event on a worker category is calculated based on the area of impact and the probability of a nominated worker group present within the impact area, and summed over all the events. The worker groups include process operators, maintenance personnel and technical professionals. The risk is compared with an internal corporate criteria.

(iv) Averaged risk to exposed individuals
This relates to a risk value averaged across the whole exposed population to a particular hazard, such as the risk of fatality due to train travel. This is discussed in section 2.4.3.2. The average individual risk is the PLL divided by the exposed population, assuming that the risk is equally distributed among the exposed population.

(v) Averaged risk to total population
This is the risk to an individual in a population, whether or not the whole population is exposed to that risk (CCPS 2000). This measure is the equivalent of the PLL divided by the total population. The averaged risk to the total population is less than or equal to the averaged risk to the exposed population, since the total population is less than or equal to the exposed population.

Of the 5 different measures of individual risk described above, the most useful measures are the LSIR (used in land use safety planning decisions), IRPA (corporate criteria for employee risk), and averaged risk to an individual in exposed population (comparison measure for different types of risks).

What is important to remember is that individual risk values can be presented and estimated in different ways. To avoid confusion, the type of individual risk being considered needs to be clearly defined.

## 2.4 RISK ESTIMATIONS

Estimating risk is an important aspect of risk management. In many cases there are good historical data available for a wide range of human activities and for specific risk categories. In this section we review some of the key industry and societal risk estimates. These can be of importance in comparative studies of actual and predicted risks. They often provide a means of target setting which is the subject of section 2.6.24.

### 2.4.1 Units of Risk

Risk is essentially an abstract concept as it involves uncertainty. Risk estimation is largely concerned with the estimation of uncertainty. In the case of quantitative risk analysis (QRA), risk estimation is the quantification of uncertainty. Even though QRA risk results are expressed in numerical terms, the results must be considered in relation to other risks, or relative to risks from other options or activities, in order to make meaningful interpretations.

**EXAMPLE 2-1 RISK UNITS**

The following give some risk expressions:

- 1 chance of fatality per 10,000 per year ($10^{-4}$ per year)
- 4 fatalities per 100 million worked hours in the plant (fatal accident rate of 4)
- Bulk road tanker accident probability of 3.2 per million truck-kilometres ($3.2 \times 10^{-6}$/truck-km)
- 10% chance of an accident event within the lifetime of facility
- 5% chance of production loss for 1 week per year
- 1 in 1000 chance of a 2-tonne environmental spill per year

Depending on the category of risk (risk to people, environment or production loss risk), appropriate units are chosen.

The measure that is often used to define risk is time rate of loss events. For example, if an undesirable event or adverse outcome is chosen as fatality and the time period is taken as one year, then the risk unit is the probability of fatality per year.

Other measures are:

- Frequency of a major accident or incident. In nuclear power generation facilities, this could relate to the frequency with which a radioactive emission might occur that could escape off-site.
- Frequency of loss of defined percentage of production. In an open-cut coal mine, one measure of risk was the frequency with which total production could shut down, say, for two weeks. One cause could be a major failure of the drag line (e.g. drag line tipped over).
- Frequency of loss of defined percentage of assets.

It is clear that risk measurement requires the estimate of probability of occurrence of an event. This can be from historical data or can involve more complex causal analysis as discussed in Chapter 8.

## 2.4.2 Risk of Injury to People

In estimating historical measures of risk to people a number of established approaches for both injury and fatality are used. These relate to occupational risks in various industry sectors or specific activities. They are useful indices.

The measure conventionally used for lost time injuries is expressed as the Lost Time Injury Rate (LTIR). It is also sometimes referred to as Lost time injury frequency rate (LTIFR), even though the frequency and the rate refer to the same thing.

LTIR may be defined as the number of lost time injuries per million hours worked. It is calculated as follows:

$$\mathrm{LTIR} = \frac{\text{Number of LTI} \times 10^6}{\text{Number of hours worked}} \tag{2.1}$$

In some organisations, a basis of 100,000 hours is used instead of a million hours.

Other similar measures for measuring safety performance are:

a) Major injury severity rate:

$$\mathrm{MISR} = \frac{\text{Number of days lost} \times 10^6}{\text{Number of hours worked}} \tag{2.2}$$

(i.e. days lost due to lost time injuries per million hours worked)

b) Lost time injury incidence rate:

$$\mathrm{LTIIR} = \frac{\text{Number of LTI} \times 100}{\text{Average number of employees}} \tag{2.3}$$

Data on lost time injuries, number of days lost for different industries are collected by government agencies responsible for administering the health and safety at work.

## 2.4.3 Risk of Fatality

### *2.4.3.1 Fatal Accident Rate*

For risk of fatality to employees, a commonly used index in the manufacturing industries is the fatal accident rate (FAR). It is used extensively in industry as a measure of risk.

FAR is defined as the number of fatalities per 100 million worked (exposed) hours. Historical FAR is normally calculated using fatality statistics over a defined period and an estimate of the total number of hours worked by all employees over this period:

$$\text{FAR} = \frac{\text{Number of fatalities over M years} \times 10^8}{\text{Total number of hours worked in M years}} \tag{2.4}$$

You can think of this as approximately equivalent to 1000 people each working for 40 years. The FAR provides a common basis for comparing industrial risks.

The fatal accident rates for a few industries in Australia are listed in Table 2-1.

In other contexts, FAR values are quoted in other units such as deaths per 100,000 workers per year (HSE, 2003). Values can be converted to other FAR definitions as well as to individual risk estimates.

TABLE 2-1 FATAL ACCIDENT RATES IN AUSTRALIAN INDUSTRY

| Industry category | FAR |
|---|---|
| Mining (non-coal) | 27 |
| Mining (coal) | 17 |
| Agricultural, forestry | 11 |
| Construction | 9 |
| Chemicals, petroleum | 4 |
| Other manufacturing | 3 |

Source: Calculated from Australian Bureau of Statistics data.

EXAMPLE 2-2 FAR RISK CONVERSIONS

British fatalities in the base metals, coke and extractive industries lie in the range of 6.4 to 8 fatalities per 100,000 workers per year (HSE, 2003). Assuming a 40 hour week and 48 week per year working period, the higher level equates to a FAR of:

$$\text{FAR} = \frac{8}{100{,}000\,\frac{\text{workers}}{\text{year}}} \cdot \frac{1}{\frac{40\,\text{hours}}{\text{worker week}} \cdot \frac{48\,\text{weeks}}{\text{year}}} = 4.1\,\text{per }10^8\,\text{exposed hours}$$

Hence FAR = 4.1.

### 2.4.3.2 Average Individual Risk

Average IR is the risk of fatality to an individual in the exposed population. It is not person specific or location specific.

In the general community, analysis of fatalities for individuals can also be made, these based on historical data. Table 2-2 complied by Higson (1989), shows some average individual fatality rates in chances per million per year for various activities or events.

In these cases, the individual risk is calculated as:

$$\hat{I}_R = \frac{\text{number of deaths per year for event/activity}}{\text{exposed population to the event/activity}} \tag{2.5}$$

### Voluntary and involuntary risks

In order to understand average individual risk, it is necessary to distinguish between voluntary and involuntary risks. A risk is "voluntary" when the person at risk has chosen to be exposed to the hazard. Of course, the real risks might not be truly appreciated. This applies to people who gamble, ride motor bikes, dabble in the stock market, climb mountains etc. The list is almost endless. Risk values to the population exposed to that risk are quoted in Table 2-2.

Most of the risks listed in Table 2-2 are voluntary. The voluntary risk values cannot be applied to a population not exposed to that risk. We all make choices every day which involve some form of risk. We may not consciously think about it but every time you get in your car and drive you are exposed to the hazards of injury or death.

TABLE 2-2 RISKS TO INDIVIDUALS IN NEW SOUTH WALES (Higson, 1989)

| | Chances of Fatality per million person years |
|---|---|
| **Voluntary Risks (average to those who take the risk)** | |
| Smoking (20 cigarettes/day) | |
| • all effects | 5000 |
| • all cancers | 2000 |
| • lung cancers | 1000 |
| Drinking alcohol (average for all drinkers) | |
| • all effects | 380 |
| • alcoholism and alcoholic cirrhosis | 115 |
| Swimming | 50 |
| Playing rugby football | 30 |
| Owning firearms | 30 |
| **Transportation Risks (average to travellers)** | |
| Travelling by motor vehicle | 145 |
| Travelling by train | 30 |
| Travelling by aeroplane | |
| • accidents | 10 |
| **Risks averaged over the Whole Population** | |
| Cancers from all causes | |
| • total | 1800 |
| • lung | 380 |
| Air pollution from burning coal to generate electricity | 0.07-300 |
| Being at home | |
| • accidents in the home | 110 |
| Accidental falls | 60 |
| Pedestrians being struck by motor vehicles | 35 |
| Homicide | 20 |
| Accidental poisoning | |
| • total | 18 |
| • venomous animals and plants | 0.1 |
| Fires and accidental burns | 10 |
| Electrocution (non-industrial) | 3 |
| Falling objects | 3 |
| Therapeutic use of drugs | 2 |
| Cataclysmic storms and storm floods | 0.2 |
| Lightning strikes | 0.1 |
| Meteorite strikes | 0.001 |

There is however another form of risk which is not voluntary. This is termed "involuntary" risk and it refers to a risk imposed on an individual or group of people by activities outside of their choice or control. For example, a local community might be exposed to the risk of injury or death by a rerouting of the transport of dangerous goods through their neighbourhood. It might arise from a new nearby process facility which could impose risks due to fires, explosions or toxic gas releases.

Withers (1988) uses a useful analogy in attempting to illustrate the meaning of a risk level of 1 in a million per year, which is a crucial target in many land use applications. It interprets the levels in terms of life expectancy due to various risks if we were to live for ever but for that single risk. These are given in Table 2-3.

When considering the risk of harm to population exposed to hazards, two measures of risk are used - individual risk and societal risk.

TABLE 2-3 RISK ASSESSMENT CRITERIA - INTERPRETING RISK LEVELS

| Risk (activity) | Life Expectancy (years) |
|---|---|
| Smoking 40 cigarettes per day | 100 |
| Drinking a bottle of wine a day | 1300 |
| Driving a car 10 hours a week | 3500 |
| Struck by lightning | 10,000,000 |
| 1 x $10^{-6}$ p.a. risk level | 1,000,000 |

Source: Withers (1988)

### 2.4.3.3 Location Specific Individual Risk (LSIR)

Individual risk refers to the risk for any individual at a specified location. This is also referred to as Location Specific Individual Risk or LSIR. It refers to a location, and does not refer to any specific person.

The risk criterion assumes that *an* individual (any one, not a specific person) would be at the given location for 24 hours per day, 365 days per year. This is commonly referred to as the "tied to a post", or "peak individual risk" assumption. The basis for the assumption is to address members of the public at the given location who may not be able to escape from the location, when exposed to the hazard. This assumption may be reasonable for residential areas, but not for other land uses, where the location occupancy would be less than 100%, or there are vulnerable members of population who cannot escape without assistance (aged care or child care centres, hospitals etc). In order to accommodate this, the target criterion is increased for locations with lower occupancy, compared to residential areas, and reduced for sensitive land uses. The risk is still calculated as peak individual risk.

Hence the individual risk (LSIR) is the total risk from all (*n*) possible events or incidents that can impact on an individual at a specific location (*x*, *y*) from a particular operation. This can be given by:

$$I_{LSIR}(x,y) = \sum_{i=1}^{n} I_{R_i}(x,y) \qquad (2.6)$$

where:

$I_{R_i}(x,y)$ = risk value for an event/incident *i*. $(yr^{-1})$

In the case of process operations, these events relate to fires, toxic gas releases and explosions. Also, the level of harm can be nominated. It could be fatality but can also be injury in terms of fire radiation or explosion overpressure. Section 9.5.2 discusses these risks.

Different target criteria are set for different land uses. (NSWDOP 1990; Ale 1991). It should be noted that risk criteria are mainly used to determine if the risk is "unacceptable". However, risks that are "not unacceptable" are not always "acceptable". Such risks are still subject to the principle of continual risk reduction to reasonably practicable levels (the ALARP principle).

#### 2.4.3.4 Societal or group risk

Societal risk attempts to address the issue of multiple fatalities or injuries. It is useful in assessing situations where other significant factors not addressed by individual risk are present. These could include:

- multiple fatalities in a process facility
- events which affect many people on and offsite such as a toxic gas cloud
- situations where a community might be exposed for a short period such as shopping complexes or sports fields
- transport situations where exposure time is brief and population densities vary along the route.

We are familiar with multiple road accident fatalities or where a number of people are killed or injured in an incident such as a plane crash, boating disaster or rail accident.

Why use such a risk measure? Recent events show that society is particularly averse to multiple deaths compared with a single, isolated death. An individual shooting death does not generate the same societal outrage as one that leads to many deaths as seen in Columbine (USA), Port Arthur (Australia) and Dunblane (Scotland). In a similar fashion we want to ensure that technology or other activities give rise to an extremely low risk of death for multiple fatalities.

*Societal risk expresses the relationship between the frequency and the number of people suffering from a specified level of harm.*

As seen in section 2.2 it is typically expressed as a frequency-number (F-N) curve. Figure 2-3 shows actual historical data for various categories of hazards (Technica 1987). Looking at these values, it is clear that historically, shipping in Australia has the highest societal risks for large loss of life followed by rail travel. For lower levels of fatality, air travel has the highest societal risk, with these relating to light aircraft operations.

How do we interpret such a graph? The curves on Figure 2-3 show historical data for various accident groups. The x-axis shows the number of fatalities (N) and the y-axis shows the fatality frequency at which N or more people are affected due to that activity. When N = 1 we do not have the same frequency value as average individual risk which is not the same as LSIR.

Estimation of societal risk requires the number of fatalities $N_i$ from event $I$ that occurs with frequency $F_i$. Hence for a value $N$, the frequency $F_N$ is given by:

$$F_N = \sum_i F_i \quad \text{for events } i \text{ where: } N_i \geq N \qquad (2.7)$$

Hence, $F_N$ is the cumulative frequency of all events $i$ where the number of fatalities $N_i$ is greater or equal to a nominated value $N$. Software is readily available to compute F-N curves (TNO 2004) and for smaller studies a simple spreadsheet suffices.

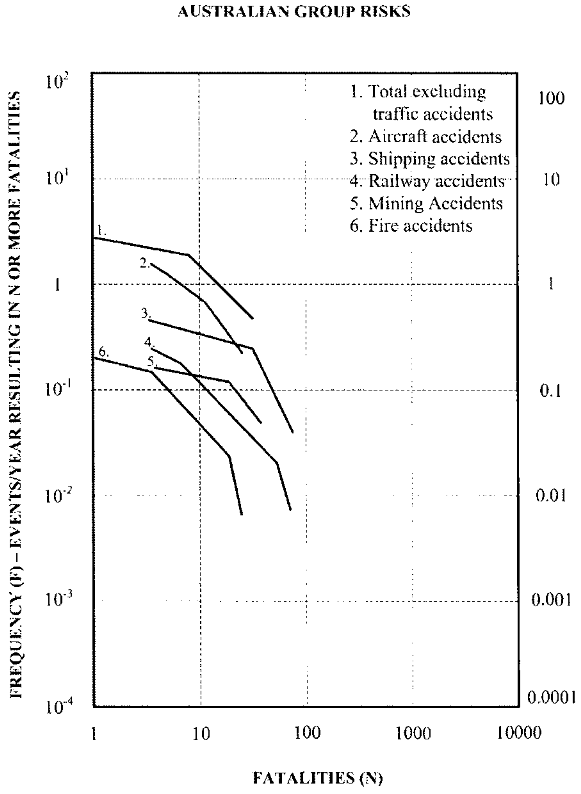


**FIGURE 2-3 HISTORICAL GROUP RISKS FOR AUSTRALIA (SOURCE: TECHNICA 1987).**

### 2.4.4 Corporate Reputation and Public Outrage Risk

Corporate reputation is a vital aspect of any company's risk management strategy. Reputation is a multifaceted concept just like risk assessment. Corporate rankings such as those given by the Fortune Survey involve a wide range of attributes that can include:

- quality of products and services
- social responsibility
- management quality
- innovative character
- employee talent
- use of corporate assets
- honesty and openness

The reputation of a corporation is directly related to the key stakeholders of that company. The shareholders can encompass those that live next to the operations as well as those who deal directly with the business. As such, corporate reputation risk is highly dependent on which attribute is to be highlighted.

**EXAMPLE 2-3 CORPORATE REPUTATION**

a) BHP Ok Tedi copper mine.
The corporate reputation of BHP, a large Australian resource company, was seriously affected by significant environmental damage in the Fly River of Papua New Guinea in the 1990's. It lead to significant opposition to other BHP mining developments in other countries and demands for tighter regulations on future developments.

b) Exxon Valdez
During a March night in 1989 the oil tanker Exxon Valdez struck a reef in Prince William Sound, Alaska. Over 11 million gallons of crude oil was released. The incident caused long term harm to Exxon's corporate reputation and led to the largest ever environmental fine on a US corporation.

c) Union Carbide, Bhopal
The 1984 catastrophe at Bhopal, India which led to massive loss of life and injury, severely damaged Union Carbide's reputation. The company has been vilified ever since by action groups. It continues, even after the Dow Chemical Company takeover in 2001.

Public outrage is clearly closely aligned with corporate reputation. The outrage can be of such a level that in the case of a major accident, government or communities can directly affect corporate liability or planning. Conversely, public outrage can positively contribute to improved risk management as seen for example in the demand for improved motorways that avoid major "blackspots".

Software such as EMSOFT (1989) developed by Sandman (1991) exists to predict outrage risk using well-documented outrage factors.

## 2.5 RISK REPRESENTATION

As seen in Section 2.1.2 risks can be measured in qualitative, semi-quantitative and fully quantitative forms. Qualitative risks are typically presented in risk matrix or tabular form for easy prioritization. With increasing quantification of risk more visual presentations are used.

### 2.5.1 Spatially Distributed Risks

Risks from sources that are geographically fixed, such as warehouses, process plants and storage terminals have spatially distributed risks that reduce as the distance from the hazard increases. This is typically represented in 3 ways.

### 2.5.1.1 Iso-risk contours

Iso-risk contours, that display contours of equal risk estimates projected onto an underlying land use map. This representation shows the spatial distribution of the risk.

Here the map of the facility and surrounding area is divided into a grid. At each point on the grid, individual risk is calculated and then contours joining equal risks are generated in a similar manner to a topographical map.

**EXAMPLE 2-4 LPG STORAGE TERMINAL RISKS**

Figure 2-4 shows the estimated iso-risk contours for an LPG storage facility. The contours relate to individual fatality risks (LSIR) from all hazard sources and show both 1 in a million per year and 10 in a million per year individual risk contours.

### 2.5.1.2 Risk transects

An alternate representation is the risk transect that shows the risk profile for a specified direction away from the source of the risk. This can be a useful alternative to the iso-risk contours in visualizing risk profiles.

Any plane can be proposed to represent a risk transect. Typically the transects are taken in key directions and pass through the centre of the facility being considered.

**EXAMPLE 2-5 RISK TRANSECT, LPG FACILITY**

For the LPG facility shown in Figure 2-4 we can view the individual fatality risk along various transects, in particular those directions which have the largest impact. Individual fatality risk along a NE-SW transect through the centre of the site is seen in Figure 2-5.

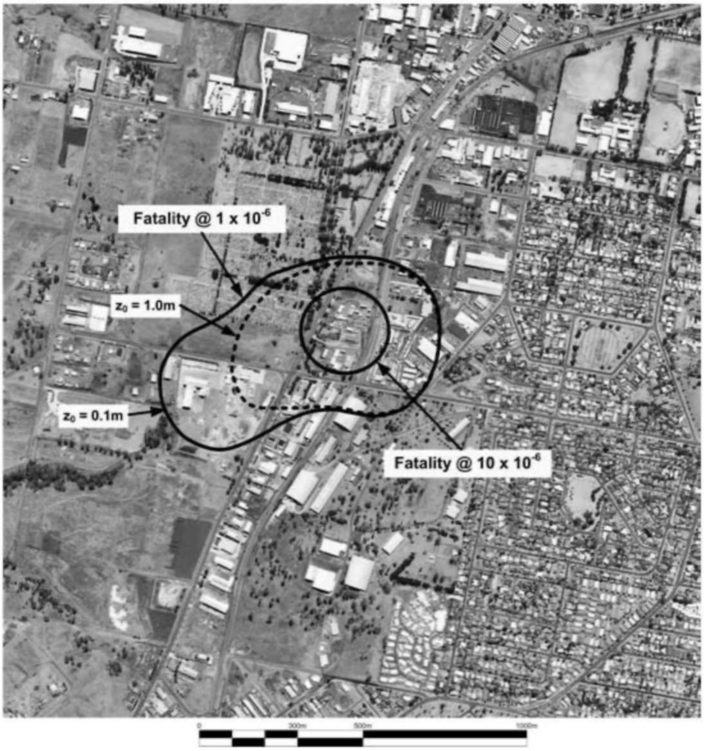


FIGURE 2-4 FATALITY RISK CONTOURS FOR LPG STORAGE FACILITY (ENERGEX 2003)

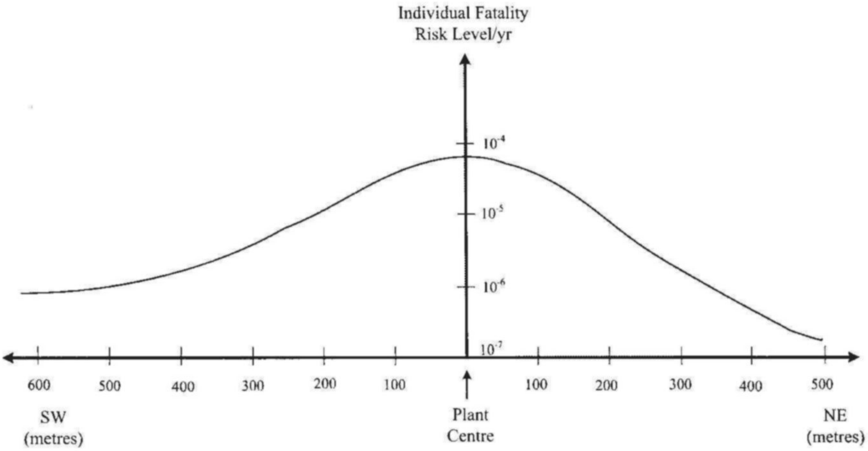


FIGURE 2-5 FATALITY RISK TRANSECT ALONG NE-SW PLANE

### *2.5.1.3 Societal (group) risks*

In the case where multiple fatalities are important, risks can be displayed as a frequency-number or F-N curve displayed on a log-log plot. This displays the frequency of fatality (F) for N or more fatalities. This is seen in Figure 2-6. In this case there is a sharp cut-off in the area of 100 fatalities, illustrating a requirement on the facility design.

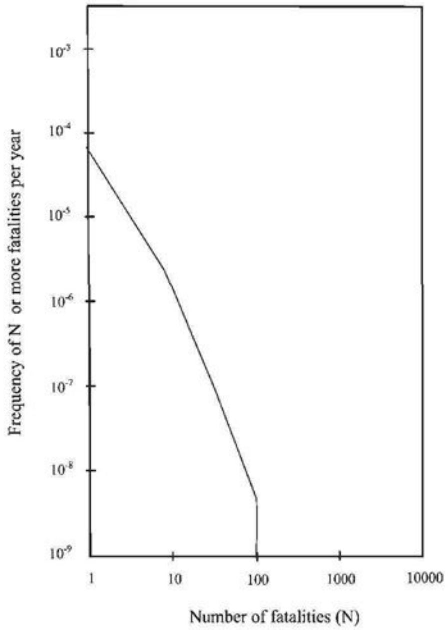


FIGURE 2-6 SOCIETAL RISK ESTIMATE FOR FACILITY

## 2.5.2 Linear Risks

In some cases, such as pipeline and transport risks, the hazard lies within a corridor such as a pipeline, railway easement or a highway. These are commonly called "linear" risks.

In these cases, the risks extend along the length of the corridor and reduce in the direction perpendicular to the corridor. Depending on the terrain, population density and activities along the corridor the risks will extend outwards to a greater or lesser extent. What is often preferable is a presentation of risk transects along the corridor at key locations of interest.

**EXAMPLE 2-6 GAS OR LIQUID PIPELINE RISK TRANSECTS**

Analysis of buried and above ground pipelines for risk management purposes is an important issue, especially where pipelines are near to local populations or sensitive environmental receptors. Figure 2-7 shows the individual fatality risk transects for a major natural gas pipeline of 0.45 m diameter and line pressure of 15.3 MPa. The line was buried to a depth of 1.2 m. The transects are given for both horizontal and vertical flames from the pipeline (Uniquest, 1995).

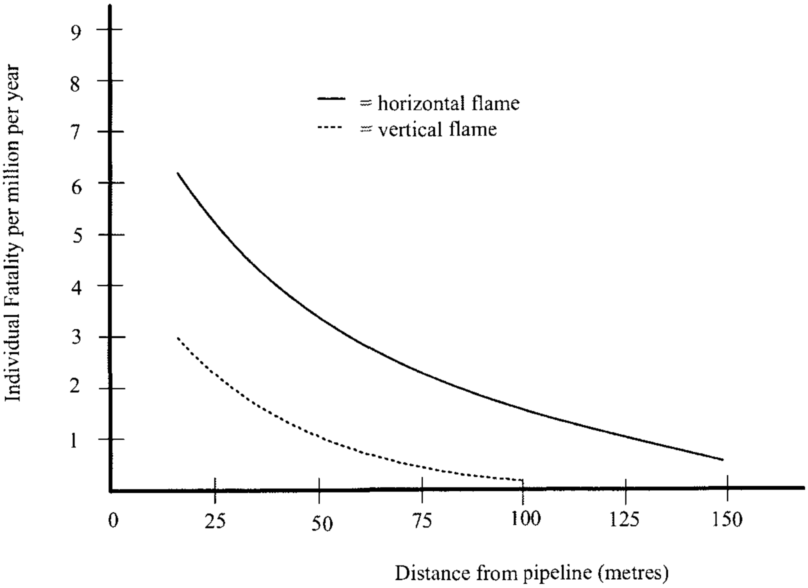


FIGURE 2-7 RISK TRANSECTS FOR GAS PIPELINE (SOURCE: UNIQUEST, 1995)

### EXAMPLE 2-7 MARINE TRANSPORT RISKS

An analysis by the UK Health and Safety Commission (HSC, 1991) of gas carriers at the port of Felixstowe led to the risk contours shown in Figure 2-8. Around the port the risk contours show a typical radial geographic distribution. For the risks along the shipping canal the risks show a typical "linear" characteristic following the path of shipping traffic.

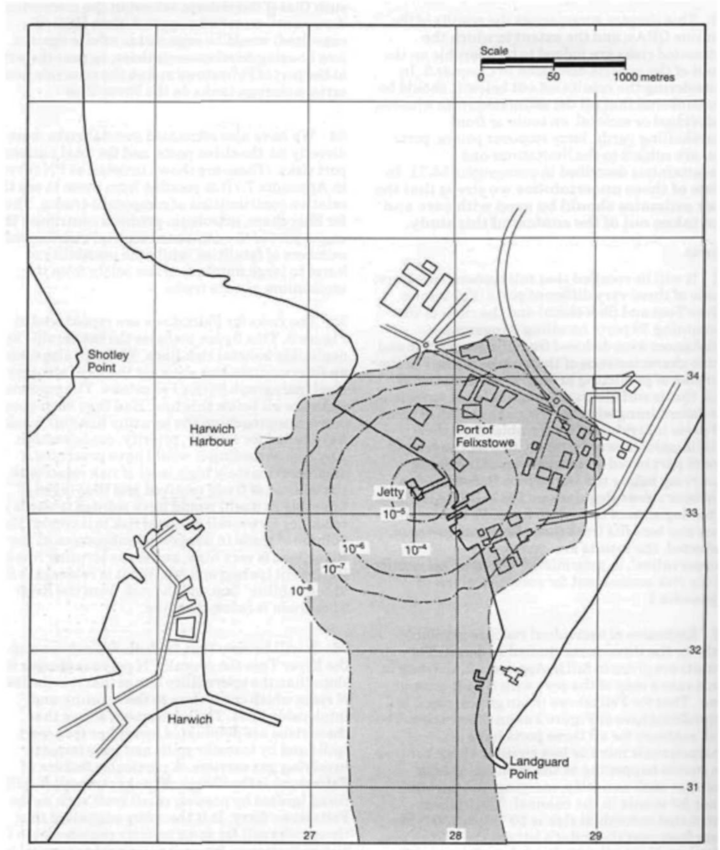


**FIGURE 2-8 FELIXSTOWE (UK) INDIVIDUAL RISK FOR GAS CARRIERS (UK, HEALTH AND SAFETY COMMISSION, 1991)**

## 2.6 RISK TARGETS, TOLERABILITY AND ACCEPTABILITY

### 2.6.1 Tolerability and Acceptability of Risk

A risk might be tolerated but not accepted due to the range of actual or perceived benefits to the individual or corporation that takes the risk. These two risk concepts are quite different.

In dealing with this issue the UK Health and Safety Executive (HSE, 2001) discusses the issues of risk being:

- tolerable
- unacceptable and intolerable
- broadly acceptable.

The HSE (HSE, 2001) comments that:

" 'tolerable' does not mean 'acceptable'. It refers instead to a willingness by society as a whole to live with a risk so as to secure certain benefits in the confidence that the risk is one that is worth taking and that it is properly controlled".

**EXAMPLE 2-8 TOLERABLE AND ACCEPTABLE RISKS**

We tolerate the risks of driving on busy motorways due to the benefits we derive and the general knowledge that controls such as speed restrictions, vehicle design or checks and good road design are in place. However, we might not consider the risk as 'acceptable' because we regard human life as sacrosanct.

In dealing with risk tolerability/acceptability, the concept of 'as low as reasonably practicable' (ALARP) is important. This is a process to reduce risks to a level that is technically feasible without excessive cost.

When determining if a risk is ALARP there are several parameters that should be considered:

1. Benefits versus cost–who gains the benefit and who wears the cost?
2. Is it technically possible to reduce the risk further?
3. Ethical issues come in–the risk may be low but is it right?
4. Do we have enough information to make the decision? – "the precautionary principle".
5. What happens if we do nothing to reduce the risk?
6. What happens if we do not proceed?

In general the decision is made by management or the management committee, or in some instances the regulator. However it must be remembered that risk is an assigned quantity and only gains acceptance by consensus, and therefore it could be soon that the ultimate decision-makers are those that will bear the cost.

What is clear is that application of ALARP is not simply a technical issue of benefit-cost analysis. Other important aspects such as relevant stakeholders, risk bearers and tolerability play their part in the application of ALARP (HSE 1992; Melchers, 2000; HSE, 2001).

Further considerations on the application of ALARP are given in Chapter 10 when discussing decision making under uncertainty.

### 2.6.2 Risk Target Setting

Setting of target risk for an activity has always been a difficult issue since the following factors need to be considered for which there are no ready answers:

- How safe is safe enough?
- How to strike an optimum balance between risk reduction and cost?
- What is an acceptable target?

For hazardous industries such as chemical or petroleum operations the above issues have been addressed in considerable depth during recent years, particularly because of risk to the public in residential areas surrounding installations.

Many countries have legislated for a target risk for LSIR to be achieved during the plant design stage as part of the environmental impact reporting and assessment methods for planning approvals. However, when it comes to societal risk, setting an acceptance criteria poses a problem. For instance, two values of PLL can be the same, one arising from say, a single fatality once in 2 years (PLL = 0.5 year), and the second, 5 fatalities once in 10 years (PLL = 0.5/ year). Numerically the PLL values may be the same, but the societal impact is vastly different, as it includes considerations such as public outrage, and the potential to impact on distinct population groups, such as a family or a business enterprise. In some cases, risk aversion factors can be applied to modify the PLL value by weighting multiple fatalities higher than single fatalities (CCPS 2000; Jonkman et al. 2002).

Because of the uncertainties associated with it, and several factors other than a numerical value of risk influencing decision making, no numerical criteria has been set for societal risk from industrial activities by such agencies as the NSW Department of Infrastructure, Planning and Natural Resources in Australia (DIPNR). This has followed a similar decision by the Health & Safety Executive in the UK (HSE 1990). Nevertheless, some criteria do exist, notably in The Netherlands (Ale, 1991; Jonkman et al. 2003) and in Hong Kong.

In the safety area, risk measures and targets have been well established for public risk from major hazard facilities and set in a regulatory framework, but no legislative target has been set for major risks to employees at the workplace. Many large companies have adopted internal standards consistent with industry average FAR values. The approach is performance-based, rather than prescriptive. Details of available targets are discussed in section 9.5.2.

Almost all organisations have targets for LTIR as this is a measurable quantity against which safety performance can be evaluated. However, it has been well established (Hopkins, 2000) that LTIR reduction does not implicitly mean a high degree of process safety management (PSM) performance.

For risks other than injury or fatality, such as business interruption risk, an organisation would set its goals based on financial considerations.

## 2.7 RISK PERCEPTION

*"I am an expert, You are ignorant, They are irrational"* was a pertinent quotation given by Howard Newby during a lecture entitled "Risk Analysis and Risk Perception: The social limits of technological change" (Newby 1997). The statements capture many common elements in risk perception and communication. The importance of perception is emphasized by the social psychologist W.I. Thomas who was quoted as saying:

> *"Things which are perceived as real will be real in their consequences"*

This is certainly the case with the concept of risk, which has already been described in section 1.2.3 as an *ascribed quantity*. That ascription means risk is a "value-laden" quantity and an individual's risk perception creates a reality that must be appreciated in all risk management activities. This is the concept of the social amplification of risk (Kasperson et al. 1988). The key concepts in risk perception are developed and discussed in this section. Failing to appreciate this in the risk management process, invariably spells disaster to any project.

### 2.7.1 The Importance of Risk Perception

The perception of risk has been a well-studied area over the last 30 years (Marshall 1990; Sandman 1991; Renn 1998; Walker et al. 1998; Pidgeon 1998; Slovic 2000; Renn 2004). Perception relates to the mental processes that take in, deal with and assess data via our many senses. Risk perception includes numerous factors that encompass beliefs, experiences, feelings and attitudes. It reflects wider cultural and social dispositions adopted towards threats to things that are valued (Pidgeon 1998).

Perceptions play important roles in a wide range of risk management areas including:

(i) Risk communication
(ii) Risk tolerability and acceptability, including criteria used for judgement
(iii) Policy making
(iv) Land use planning decisions
(v) Dealing with uncertainties
(vi) Trade-offs between cost and safety including the ALARP concept.

This simply enforces the fact that process risk management practice, although rooted in technical analysis, cannot afford to neglect the broader social perspectives that address such issues as fairness, benefits and loss of amenities to affected individuals or communities.

Everyone perceives risk in different ways as illustrated by Jesper Deleuran in Figure 2-9 (Grønberg & Rasmussen 1992). This is what makes risk presentation and communication such a challenge!

FIGURE 2-9 ATTITUDE TO LIFE'S RISKS (BY PERMISSION OF JESPER DELEURAN)

## 2.7.2 Factors Affecting Risk Perception

In acknowledging that individuals and communities often do not look at risks in the sole light of scientific analysis, Sandman (1991) suggested that an alternate form of risk expression can be given by:

Risk = Hazard + Outrage

The hazard is clearly identified by the individual and the person understands the potential for harm due to the proposed activity. They then respond to the hazard by a specific level of outrage that ranges from indifference to vigorous opposition!. That level of outrage is driven by a number of factors such as:

- The familiarity with the hazard
- Whether a recent incident has occurred elsewhere
- The perception that something is being hidden in the proposal
- The credibility of the proponent.

These factors and more, go to determine the level of 'outrage' produced. Sandman (1991) has given 12 principal outrage components which are listed in

Table 2-4. These components show what is generally regarded as "safe" and "risky". Table 2-5 gives a secondary list of outrage components which are known to be important.

### TABLE 2-4 TWELVE PRINCIPAL OUTRAGE COMPONENTS

| | "Safe" | "Risky" |
|---|---|---|
| 1 | Voluntary | Coerced |
| 2 | Natural | Industrial |
| 3 | Familiar | Exotic |
| 4 | Not memorable | Memorable |
| 5 | Not dreaded | Dreaded |
| 6 | Chronic | Catastrophic |
| 7 | Knowable | Unknowable |
| 8 | Individually controlled | Controlled by others |
| 9 | Fair | Unfair |
| 10 | Morally irrelevant | Morally relevant |
| 11 | Trustworthy sources | Untrustworthy sources |
| 12 | Responsive process | Unresponsive process |

### TABLE 2-5 EIGHT SECONDARY OUTRAGE COMPONENTS

| | "Safe" | "Risky" |
|---|---|---|
| 13 | Affects average populations | Affects vulnerable populations |
| 14 | Immediate effects | Delayed effects |
| 15 | No risk to future generations | Substantial risk to future generations |
| 16 | Victims statistical | Victims identifiable |
| 17 | Preventable | Not preventable (only reducible) |
| 18 | Substantial benefits | Few benefits (foolish risk) |
| 19 | Little media attention | Substantial media attention |
| 20 | Little opportunity for collective action | Much opportunity for collective action |

From these components, Sandman makes the following seven conclusions about hazard and outrage.

1. The public responds more to outrage than to hazard
2. Activists and the media amplify outrage, but they don't create it.
3. Outraged people don't pay much attention to hazard data.
4. Outrage isn't just a distraction from hazard. Both are legitimate and important.
5. When hazard is high, risk communicators try to nurture more outrage.
6. When hazard is low, risk communicators try to reduce the outrage.
7. Companies and agencies usually can't reduce outrage much until they change their own organizations.

This hazard + outrage definition is not necessarily technical but in fact is often the one which can dominate the whole risk management process.

Perceptions about hazards and risks must be taken seriously. No matter what technical advice is offered, people's perception of a risk can dominate the particular issue. And there are good reasons why that is the case. How do we characterise our attitudes to risk?

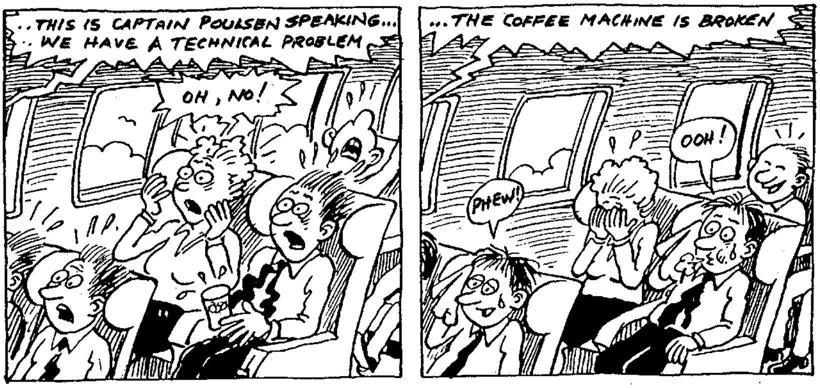

..THIS IS CAPTAIN POULSEN SPEAKING...
..WE HAVE A TECHNICAL PROBLEM
OH, NO!
...THE COFFEE MACHINE IS BROKEN
PHEW!
OOH!

FIGURE 2-10 THE FLIGHT OR FRIGHT? (BY PERMISSION OF JESPER DELEURAN)

Some of the key characteristics are:

The familiarity we have with the risk:
- If we have personal knowledge about the risk then we are often more accepting of it.

Whether we are in control:
- We all think we do better than others etc. in driving a car we believe we have control over the risk of injury or death.

If there has been a recent incident:
- Our perceptions are heightened if there has been a recent incident e.g. a plane crash or multiple deaths in a vehicle accident.

Risk perceptions must be addressed by those proposing activities or by those responsible for planning decisions. Ultimately, the perception of risk, whether it is in line with actual risk values could be the final arbiter in decision making. Hence, perception becomes reality.

In the context of major hazard facilities (MHFs), which are dealt with at length in Chapter 14, risk perceptions play a major role. In particular, the understanding of risk perception is strongly influenced by the local context involving such aspects as (Walker et al. 1998):

(i) local memories of incidents
(ii) first hand experiences of accidents or emergencies at the site
(iii) sensory evidence such as things seen or smelled
(iv) interpretation of company information issued to the public

In contrast to the earlier quote about "They are irrational", a 1998 UK HSE sponsored study (Walker et al. 1998) showed that risk reasoning in local communities was quite complex and was often framed in moral rather than technical terms.

Lack of toleration to risks often stemmed from distrust, worry, a sense of powerlessness and vulnerability. In contrast, those that adopted a more tolerant attitude were characterised by pragmatism, stoicism or resignation. This polarization of views aligns closely with studies done by Allen (1997) where the cost versus safety debate typically produces a bimodal response. This is a key factor in application of ALARP principles considered in Chapter 10. All these factors simply reinforce the value-laden nature of risk management and emphasize the need to take seriously these aspects in risk management practice.

Subsequent chapters will reinforce the influence of values and perception on key areas of risk management.

## 2.8 REVIEW

We need risk measurement within effective risk management practice, be it qualitative or quantitative in character. Risk measures allow decision-making processes to take place in an informed manner. Decisions based on qualitative measures using simple rating systems can prove invaluable in sorting out what needs further attention and potentially more quantification.

As the chapter shows, there is a variety of ways that risks can be presented–most are visual, some need careful interpretation because of the many available risk definitions. This is one of the most difficult areas to grasp and one that can lead to much controversy if not clearly enunciated.

Chapters 9 and 10 expand on the issues of risk estimation and assessment as well as dealing in-depth with issues of risk criteria often used in decision making.

We have also emphasized that risk is an ascribed quantity and the perceptions of individuals or communities can have a major impact on the social amplification of risk. It will impact on risk presentation, decision making and communication. It is a theme that pervades other areas of risk management in the subsequent chapters of the book.

## 2.9 REFERENCES

AIChE 1994a, *DOW's fire and explosion index hazard classification guide*, American Institute of Chemical Engineers, New York, ISBN 0816906238.

AIChE 1994b, *DOW's Chemical Exposure Index Guide*, American Institute of Chemical Engineers, New York, ISBN 0816906475.

Ale, B.J.M. 1991, 'Risk Analysis and Risk Policy in The Netherlands and the EEC', *Journal of Loss Prevention in the Process Industries*, vol. 4, pp. 58-64.

Allen, P.T. 1997, 'Trading Cost Against Safety: The Structure of People's Beliefs', *Process Safety Progress*, vol.16, no. 2, pp. 89-93.

CCPS 2000, *Guidelines for Chemical Process Quantitative Risk Analysis,* 2nd edn, AIChE, ISBN 081690720X.

EMSOFT 1989, *Outrage prediction and management software*, Available at: http://www.emsoft.com.

Higson, D.J. 1989, *Risks to Individuals in NSW and in Australia as a whole*, ANSTO, July.

Hopkins, A. 2000, *Lessons from Longford: The Esso Gas Plant Explosion,* CCH Australia Ltd, ISBN 1864684224.

HSC 1991, *Major hazard aspects of the transport of dangerous substances*, UK-HSC, HMSO, London.

HSE 2003, *Statistics of Fatal Injuries 2001/2002*, UK National Statistics, Health and Safety Executive Report RIDDOR.

HSE 2001, *Reducing risks, protecting people: HSE's decision-making process*, HMSO, Norwich, UK, ISBN 0717621510.

HSE 1992, *The tolerability or risks from nuclear power stations*, HSE Books, UK, ISBN 0118863681.

HSE 1990, *Risk Criteria for Land-Use Planning in the Vicinity of Major Industrial Hazards*, HMSO, London.

Grønberg, C.D. and Rasmussen, B. 1992, *At leve er Risikabelt*, ATV, Denmark, ISBN 87-7783-323-6.

Jonkman, B., van Gelder, P. and Vrijling, H. 2003, 'An overview of quantitative risk measures and their application for calculation of flood risk', *ESREL 2002 European Conference.*

Kasperson, R.E., Renn, O., Slovic, P., Brown, H.S., Emel, J., Goble, R., Kasperson, T.X. and Ratick, S. 1988, 'The Social Amplification of Risk: A Conceptual Framework', *Risk Analysis*, vol. 8, no. 2, pp. 177-187.

Khan, F.I., Husain, T. and Abbasi, S.A. 2001, 'Safety Weighted Hazard Index (SWeHI), A New User-friendly tool for swift yet comprehensive Hazard Identification and Safety Evaluation in Chemical Process Industries', *Transactions of the Institution of Chemical Engineers*, vol. 79, Part B, pp. 65-80.

Marshall, V.C. 1990, 'The social acceptability of the chemical and process industries: A proposal for an integrated approach', *Transactions of the Institution of Chemical Engineers*, vol. 68, Part B, S145-S155, May.

Melchers, R.E. 2000, 'On the ALARP approach to risk management', *Reliability Engineering and System Safety*, vol. 71, pp. 201-208.

Newby, H. 1997, 'Risk analysis and risk perception: the social limits of technological change', Jubilee Lecture IChemE 1997, *Transactions of the Institution of Chemical Engineers*, Part B, vol. 75, pp. 133-137.

NSW Department of Planning, 1990, *Risk Criteria for Landuse Safety Planning, Hazardous Industry Planning Advisory Paper No 4*, ISBN 0-7305-7130-0.

Pidgeon, N. 1998, 'Risk assessment, risk values and the social science programme: why we do need risk perception research', *Reliability Engineering and System Safety*, vol. 59, pp. 5-15.

Renn, O. 2004, 'Perception of Risks', *Toxicology Letters*, vol. 149, pp. 405-413.

Renn, O. 1998, 'The role of risk perception for risk management', *Reliability Engineering and System Safety*, vol. 59, pp. 49-62.

Sandman, P. 1991, Environmental Communication Research Program, Ryders Lane, Rutgers University, New Brunswick, USA.

Slovic, P. 2000, *The Perception of Risk*, Earthscan Publications Ltd., London UK and Sterling, VA, USA.

Technica 1987, *Report on Altona Petrochemical Complex*, Victoria State Government, Australia.

TNO 2004, *RiskCurves, TNO Chemistry*, Apeldoorn, The Netherlands, http://www.chemie.tno.nl.

Uniquest 1995, *Preliminary Risk Assessment SW Queensland Natural Gas Pipeline*, University of Queensland, Brisbane.

Walker, G., Simmons, P., Wynne, B. and Irwin, A. 1998, *Public perception of risks associated with major accident hazards*, HSE Contract Research Report 194/1998, Health & Safety Executive, UK.

Whitehouse, H.B. 1985, 'IFAL - a new risk analysis tool', Assessment and Control of Major Hazards, *IChemE Symposium Series No. 93*, pp. 309-322.

Withers, J. 1988, *Major Industrial Hazards*, Gower Technical Press Ltd, England, ISBN 0-291-39725-5.

## 2.10 NOTATION

| | |
|---|---|
| AIChE | American Institute of Chemical Engineers |
| ALARP | As Low As Reasonably Practicable |
| CCPS | Center For Chemical Process Safety, AIChE |
| CEI | Dow's Chemical Exposure Index |
| DIPNR | Department of Infrastructure, Planning and Natural Resources, NSW, Australia |
| F&EI | Dow's Fire And Explosion Index |
| FAR | Fatal Accident Rate |
| F-N | Frequency-Number of Fatalities (Curve) |
| IFAL | Instantaneous Fractional Annual Loss |
| IR | Individual Risk |
| LPG | Liquefied Petroleum Gas |
| LSIR | Location Specific Individual Risk |
| LTIFR | Lost Time Injury Frequency Rate |
| LTIR | Lost Time Injury Rate |
| LTIIR | Los Time Injury Incident Rate |
| MISR | Major Injury Severity Rate |
| PLL | Potential Loss of Life |
| PRA | Probabilistic Risk Assessment |
| PSM | Process Safety Management |
| QRA | Quantitative Risk Assessment |
| SWeHI | Safety Weighted Hazard Index |

This page is intentionally left blank

# 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 reçognised 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).

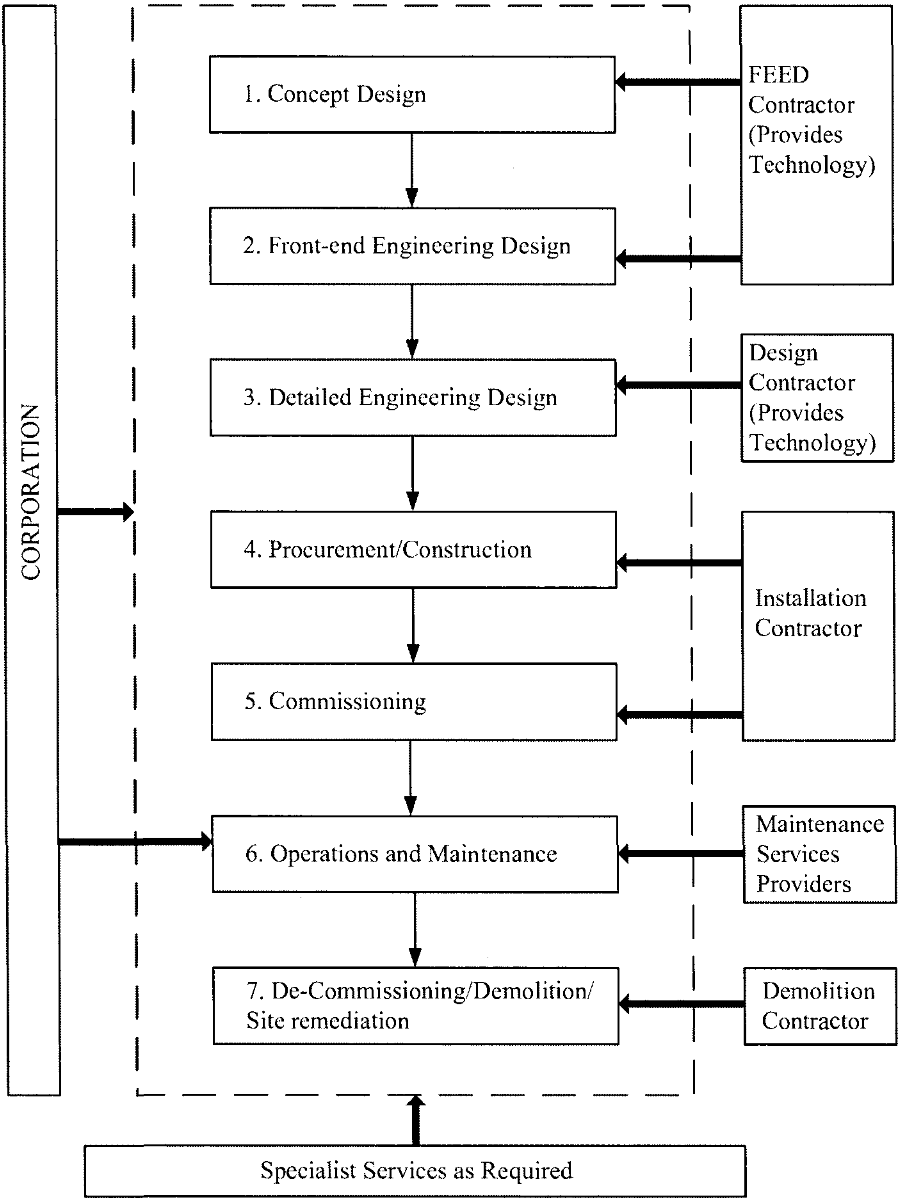

CORPORATION
1. Concept Design
2. Front-end Engineering Design
3. Detailed Engineering Design
4. Procurement/Construction
5. Commissioning
6. Operations and Maintenance
7. De-Commissioning/Demolition/ Site remediation
FEED Contractor (Provides Technology)
Design Contractor (Provides Technology)
Installation Contractor
Maintenance Services Providers
Demolition Contractor
Specialist Services as Required

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.

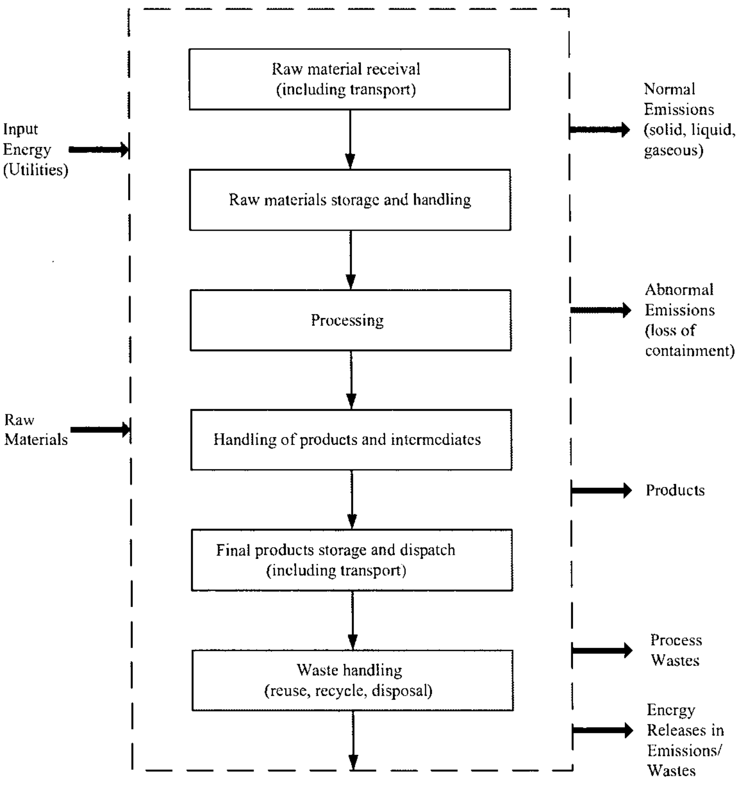


**FIGURE 3-2 PRODUCT ENVIRONMENTAL LIFE CYCLE IN A FACILITY**

## 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).

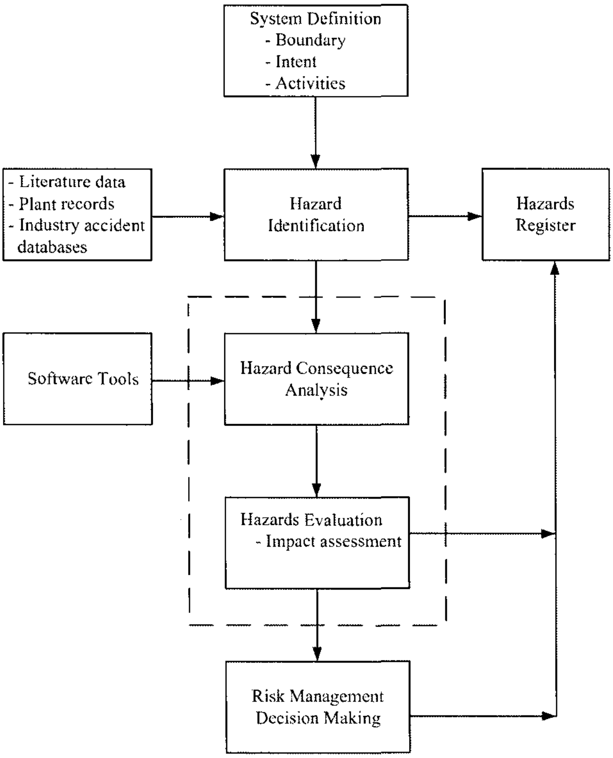


FIGURE 3-3 ONE-DIMENSIONAL MODEL FOR PROCESS RISK MANAGEMENT

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.

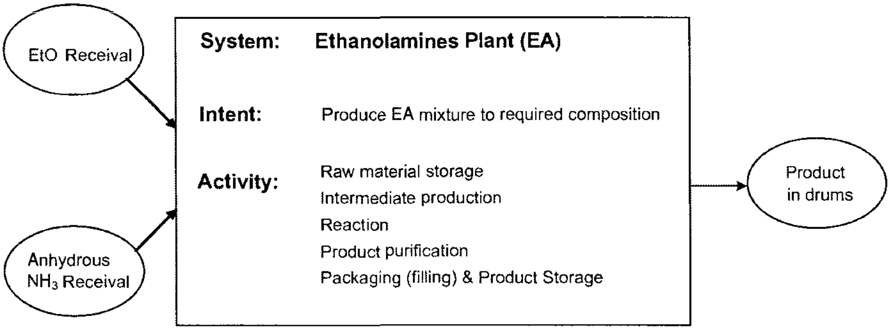
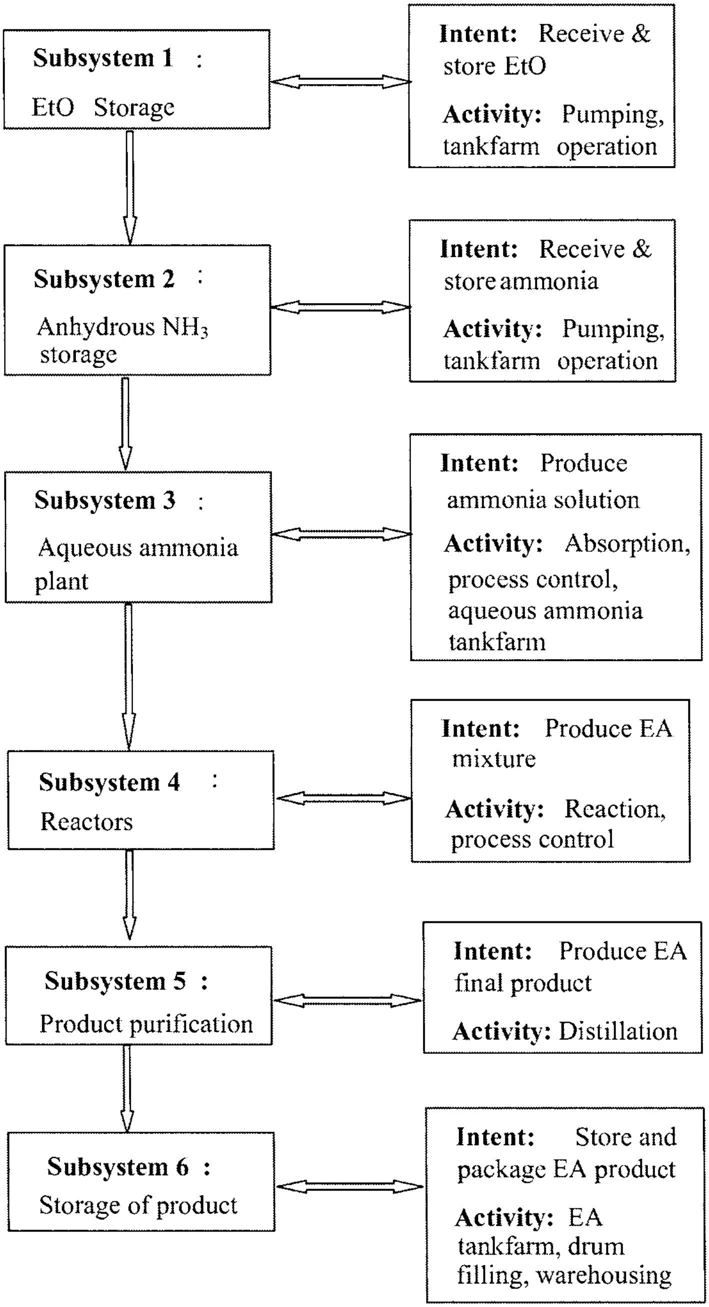

EtO Receival
System: Ethanolamines Plant (EA)
Intent: Produce EA mixture to required composition
Activity: Raw material storage
Intermediate production
Reaction
Product purification
Packaging (filling) & Product Storage
Product in drums
Anhydrous $NH_3$ Receival

**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.


Subsystem 1 :
EtO Storage
Intent: Receive & store EtO
Activity: Pumping, tankfarm operation
Subsystem 2 :
Anhydrous NH$_3$ storage
Intent: Receive & store ammonia
Activity: Pumping, tankfarm operation
Subsystem 3 :
Aqueous ammonia plant
Intent: Produce ammonia solution
Activity: Absorption, process control, aqueous ammonia tankfarm
Subsystem 4 :
Reactors
Intent: Produce EA mixture
Activity: Reaction, process control
Subsystem 5 :
Product purification
Intent: Produce EA final product
Activity: Distillation
Subsystem 6 :
Storage of product
Intent: Store and package EA product
Activity: EA tankfarm, drum filling, warehousing

[redacted] 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<br>• Flange gasket leak<br>• Pipe rupture<br>• Corrosion<br>• Mechanical impact<br>• Failure during transfer from transport vehicle | • Fire<br>• Vapour cloud explosion potential<br>• Incident escalation potential (intermediate consequence)<br>• Toxic impact of ethylene oxide on exposure to personnel | • Storage design integrity<br>• Mechanical integrity inspections<br>• Transfer procedures<br>• Active fire protection<br>• PPE<br>• Protection against mechanical impact |
| 2 | Anhydrous ammonia release | • Stress corrosion of pressure vessel<br>• Flange gasket leak<br>• Pipe rupture<br>• Mechanical impact<br>• Flexible hose failure during transfer from road tanker | • Toxic cloud<br>• Potential for serious injury/ fatality on exposure<br>• Fire potential low compared to toxicity impact | • Storage design integrity<br>• Mechanical integrity inspections<br>• Transfer procedures<br>• Personal protection equipment<br>• Emergency shutdown system (ESD)<br>• Emergency response procedures<br>• Protection against mechanical impact |
| 3 | Runaway reaction | • Loss of cooling water during reaction<br>• Agitator failure<br>• Human error<br>• Temperature control failure<br>• Incorrect reaction mixture | • Rapid temperature/ pressure rise in reactor<br>• Potential for reactor vessel failure<br>• Serious injury/ fatality potential | • Reactant addition control<br>• Temperature monitoring<br>• High pressure protection<br>• High temperature protection<br>• Pressure relief<br>• Operating procedures (batch recipes) |

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

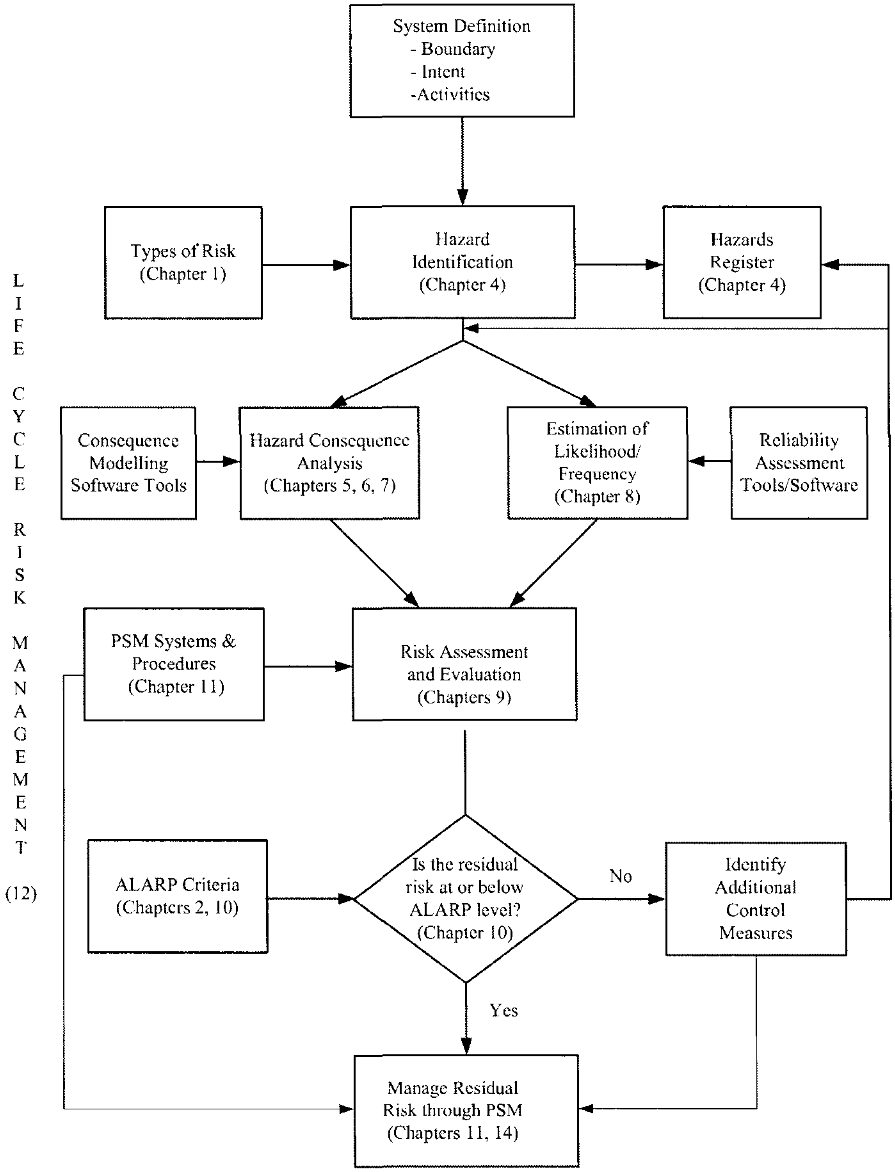

System Definition
- Boundary
- Intent
-Activities
Types of Risk (Chapter 1)
Hazard Identification (Chapter 4)
Hazards Register (Chapter 4)
L I F E C Y C L E R I S K M A N A G E M E N T (12)
Consequence Modelling Software Tools
Hazard Consequence Analysis (Chapters 5, 6, 7)
Estimation of Likelihood/ Frequency (Chapter 8)
Reliability Assessment Tools/Software
PSM Systems & Procedures (Chapter 11)
Risk Assessment and Evaluation (Chapters 9)
ALARP Criteria (Chapters 2, 10)
Is the residual risk at or below ALARP level? (Chapter 10)
No
Identify Additional Control Measures
Yes
Manage Residual Risk through PSM (Chapters 11, 14)

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.

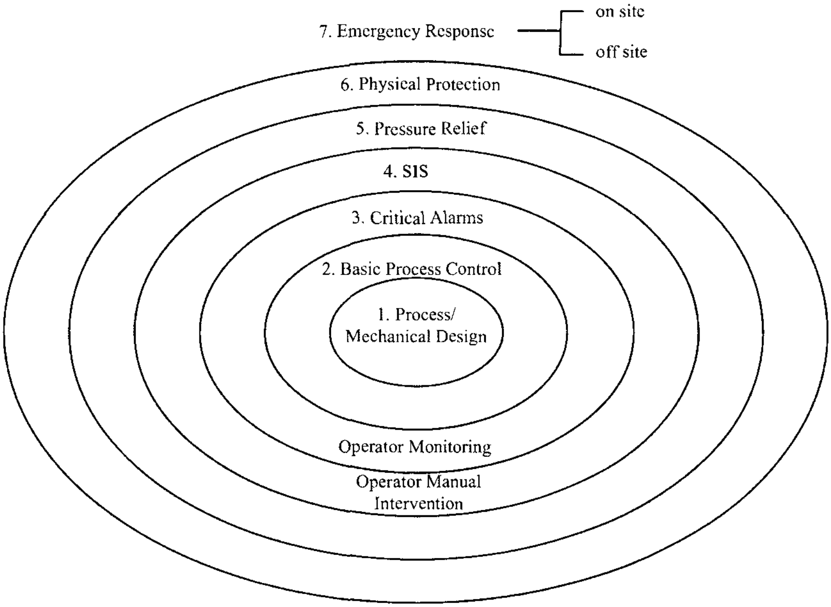


**FIGURE 3-7 OVERVIEW OF LAYERED PROTECTION MODEL**

### *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<br>Definite history of occurrence<br>Frequency between once and ten times a year |
| Likely | Event will probably occur in most circumstances. | Possible history of occurrence<br>Probably occur once per decade and history of near miss<br>Frequency between 1 every 10 years and 1 per year |
| Possible | Event should occur at some time. | May happen once in plant lifetime<br>Possible history of near miss<br>Frequency between 1 every 100 years and 1 every 10 years |
| Unlikely | Event could occur at some time. | Low likelihood of occurrence<br>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<br>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**<br>No observable effect to plants or animals. No requirement to inform authorities. No visible discharges observed offsite | **Minor Pollution**<br>Minor effects on plants & Animals. Required to inform authorities. May involve a cleanup. Visible discharge observed offsite. | **Moderate Pollution**<br>Moderate effects on plants & animals. Physical impact on the public. Required to report to authorities. Extensive cleanup may be required. | **Major Release**<br>Major effects on Plants & Animals. Substantial cleanup costs. Personal & business prosecution possible | **Extreme Event**<br>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.

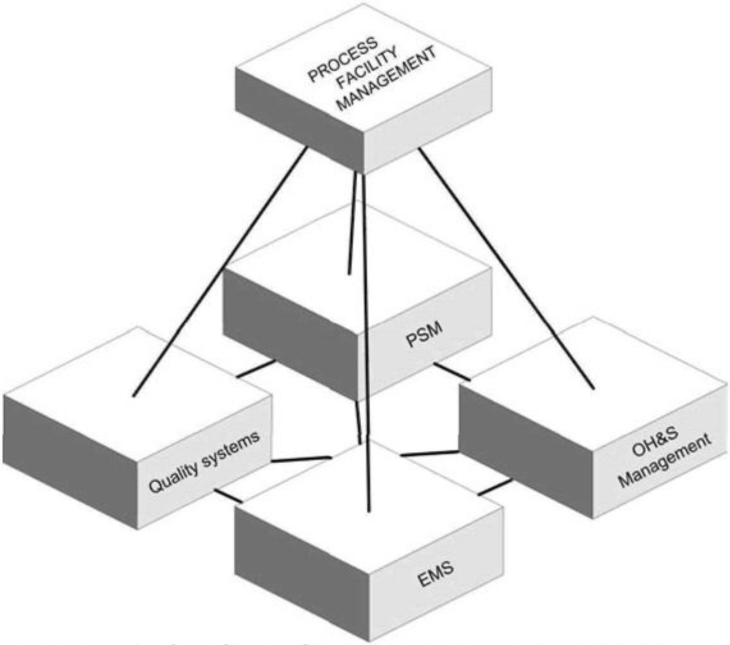


**FIGURE 3-9 INTERFACE MODEL FOR QUALITY, SAFETY AND ENVIRONMENTAL MANAGEMENT**

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.

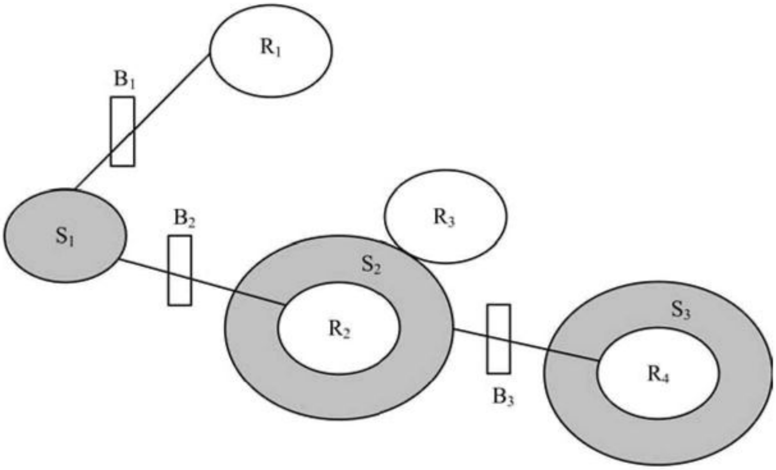


**FIGURE 3-10 GENERALISED HAZARD MODEL FOR GAS SYSTEM**

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 |

This page is intentionally left blank

# 4 IDENTIFYING HAZARDS AND OPERATIONAL PROBLEMS

*"You are amazing Holmes, how were you able to find it (the needle in the carpet) where I failed to find anything?"*
*"That's because my dear Watson, you were not looking for it".*

Hazard identification is the single most important step in the management of process risks. This is one area where, unfortunately, ignorance is not bliss, but a disaster. It has been shown in commissions of inquiry and legal proceedings following major accidents that, not identifying potential accident causes when there are systematic techniques available for such identification, is no defence for the corporation.

The questions often asked after an accident event are:

- Why were these events not identified *a priori* during the design stage, or as a proactive measure in an operating plant?
- Even when a potential event was identified, though remote, why was no action taken by the management? In other words, what is the basis on which 'remoteness' was ascribed to the event, for justifying inaction?

Process systems are complex. Unlike an assembly line, where in most situations material processing occurs sequentially, there is significant coupling of the subsystems that interact on one another. If these couplings and interactions are not identified systematically, the potential accident event can slip through the scrutiny net.

## 4.1 INTRODUCTION

In Chapter 1, we have outlined the difference between hazard and risk. Hazard is not equal to risk and this distinction is critical.

If we focus only on risk analysis, without identifying the underlying causes of the hazards, the questions asked are: "What can go wrong?", "How big?", "How often?" and "So what?" (Kletz 1999). The hazard identification for this level is concerned with the inherent hazard of the material stored or processed, and protection measures in place to prevent a loss of containment. The risk analysis often starts with a loss of containment event (what can go wrong), uses consequence models to estimate severity (how big), uses generic reliability databases for estimating a frequency (how often), and calculates the risk (so what).

In the above approach, the underlying causes of process hazards, especially resulting from abnormal situations and deviations from intended operation may not be identified (Johnson 2000). The 'ignorance factor' arises from failing to identify underlying causes of process hazards.

This chapter is devoted to the systematic hazard identification techniques available for detailed identification of process hazards, and the suitability of each technique for the various life cycle stages.

## 4.2 AN OVERVIEW OF HAZARD IDENTIFICATION

### 4.2.1 The Dimensions of Hazard Identification

There are three major dimensions to hazard identification.

- Time
- Technical
- Management

Figure 4-1 illustrates how these dimensions interact.

**Time:**

Like all good things, systematic hazard identification takes time. It is a multi-disciplinary team effort, in an interactive workshop, often facilitated by an experienced facilitator, with broad experience in process industry hazards.

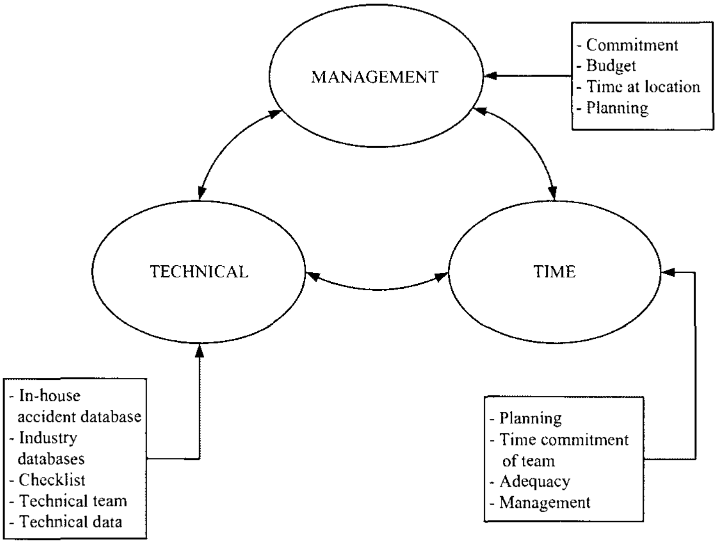


FIGURE 4-1 DIMENSIONS OF HAZARD IDENTIFICATION

Commitment of time required for preparatory work (literature review, database search), and time away from their normal duties for workshop participants, is essential for the success of the effort. Once the project gets started, there is significant time pressure on the entire project team, and personnel are often called away from the hazard identification sessions. Every effort should be made to ensure that this does not occur.

The other key time aspect is the stage of the life cycle. Hazard identification needs to be practicised across the whole life cycle using the most appropriate methods for each stage (see section 4.5.3).

## Technical:

There are no quick formulae or equations that can yield the information sought. It is entirely based on the expertise of the hazard identification team, with input from literature data on past experience.

Important technical inputs are:

- A set of accidents and near misses available from the corporation's own operating history of similar plants world-wide.
- A set of accidents and near misses from literature information and accident database search.
- Incidents not only from similar process plants, but also from processes using similar materials, not necessarily producing the same product as the plant in question.
- A comprehensive checklist of hazard keywords to facilitate the process.
- Experienced personnel from the design contractor, client's project representative, operations and safety personnel from the corporation. The

latter may come from the company's existing operations, as the operations team may not have been recruited during the early stages of a new project.

- Project technical information ready at hand for reference. Detailed requirements are described in Section 4.4.
- Recently expert systems based software has been developed for hazard identification (McCoy et al. 1999a, b; 2000 a, b), which add more to the technical dimension.

**Management:**

Management commitment is vital for the success of hazard identification. Time and technical sources must be committed to this effort.

For new projects, or plant expansion projects, hazard identification should feature as a prominent item in project planning, and time and budget should be allowed for it.

For older plants, built prior to the advent of systematic hazard analysis techniques, there should be commitment to undertake the study, and implement all practicable actions arising out of the study. In some countries, this may be a regulatory requirement. In the case of older plants, this exercise may involve some capital expenditure for upgrading the hazard control measures. This should not deter the management from commissioning such a study.

### 4.2.2 Approaches to Hazard Identification

There are a large number of methods now available for hazard identification. They include:

1. Check-lists
2. "What if?" Analysis
3. Concept Hazard Analysis (CHA)
4. Failure Mode and Effects Analysis (FMEA). This may include a criticality analysis (FMECA).
5. Hazard and Operability Study (HAZOP)
6. Control Hazard and Operability Study (CHAZOP)
7. Scenario based hazard identification
8. Action Error Analysis (AEA)

Only an abridged treatment of these techniques is possible in this book. There is a vast amount of literature on this subject. A detailed list of techniques and extensive bibliography is available in Crawley and Tyler (2003).

Fault tree analysis and event tree analysis are sometimes listed as hazard identification tools (McCoy et al. 1999a). These techniques are more useful in the evaluation of hazards and quantification rather than identification of hazards, but there is an overlap with hazard identification. These have been included as hazard evaluation tool in the CCPS Guideline (1992). Fault tree logic can be of help at the hazard identification stage to understand the combinations of causes and component/system dependencies that could contribute to a major accident. Event trees are of major help in tracing the possible outcomes from the accident event based on various mitigation measures provided. The fault tree and event tree analysis techniques are described in Chapter 8, in relation to quantification of incident probabilities.

## 4.2.3 System Interactions and their Importance

### 4.2.3.1 Linear interactions

Perrow (1999) breaks down an engineering system into a set of sub-systems consisting of the following:

1. Design (philosophy, capacity, applicable codes and standards, integrity of design process)
2. Equipment (procurement, installation, 'fit for purpose')
3. Procedures (covers operations and maintenance)
4. Operators (covers the human factors)
5. Supplies and materials (raw materials, intermediates, products and wastes)
6. Environment (internal – organisational culture and climate, workplace ergonomics, external – regulatory, market driven changes, public perceptions)

The six sub-systems constitute the DEPOSE model (Perrow 1999), and interact on each other.

Each of the elements above depends on the preceding element to some degree in a more or less linear chain. That is, design leading to equipment specification and fabrication, installation and commissioning leading to development of procedures for operations and maintenance, training of operators, ordering of supplies, storage and handling of materials, all operating in a given internal and external environment. For engineering systems, they may be termed 'linear interactions' defined by Perrow (1999) as:

*"Linear interactions are those in expected familiar production and maintenance sequence, and those that are quite visible even if unplanned".*

Examples abound in the literature on incorrect design, equipment not 'fit for purpose', incorrect procedures, human errors and so on (Kletz 1994; Sanders 1999).

Linear interactions are easier to identify when the system boundary is large, and are useful at a higher level of assessment, as given in the following example.

**EXAMPLE 4-1 LINEAR INTERACTIONS**

Manufacture of household detergents consists of three distinct processes:

a) Production of sulphur dioxide ($SO_2$) by burning sulphur and catalytic oxidation to produce sulphur trioxide ($SO_3$)
b) Sulphonation of an alkyl benzene or an ethoxylate with the $SO_3$ and digestion with caustic soda to produce the detergent base

c) Processing the detergent base with additives to produce liquid or powder detergents

d) Packaging and warehousing of the final products for distribution to market

These above four processes as described as linearly coupled. If the $SO_3$ production shuts down, all the other processes are affected in series. However, this dependency can be decoupled by having a detergent base buffer storage, so that production of final products can continue until the detergent base production is back on line.

Similarly, if the detergents plant shuts down, the detergent base can continue to be produced and stored until the product plant can be restarted. The decoupling is achieved by the buffer storage of the intermediate.

### 4.2.3.2 Complex interactions

The linear interaction is easy enough to understand and the required buffer capacity can be planned at the time of design, or further capacity added as the production capacity increases over a period of time due to debottlenecking measures.

If we go into the subsystem in more detail, we find that linear interactions are replaced by a set of complex interactions, not readily visible to superficial scrutiny. Perrow (1999) defines these as:

> *"Complex interactions are those of unfamiliar sequences, or unplanned and unexpected sequences, and either not visible or not immediately comprehensible."*

The more coupled a system is, the more complex the interactions become, as events in one sub-system have a direct effect on all the sub-systems coupled to it.

**EXAMPLE 4-2 COMPLEX INTERACTIONS**

An endothermic reaction is achieved by pyrolytic reaction in a high pressure tubular reactor placed in a furnace fired with gas fired burners. The heat in the flue gases is used to generate steam in the upper part of the furnace, before discharging to stack. A separate boiler feed water (BFW) pump supplies the pipes in the convection bank of the furnace, and the steam is separated in a steam drum.

The process stream from the reactor is quenched by circulating liquid, which also reduces the system pressure. The stream is then fed to a downstream distillation train.

The quench liquid circulation pump has two pumps, one electric motor driven pump used for plant startup, and one steam turbine driven pump, that uses the steam generated in the furnace during normal operation. This arrangement gives significant energy efficiency in plant operation. A schematic drawing is shown in Figure 4-2.

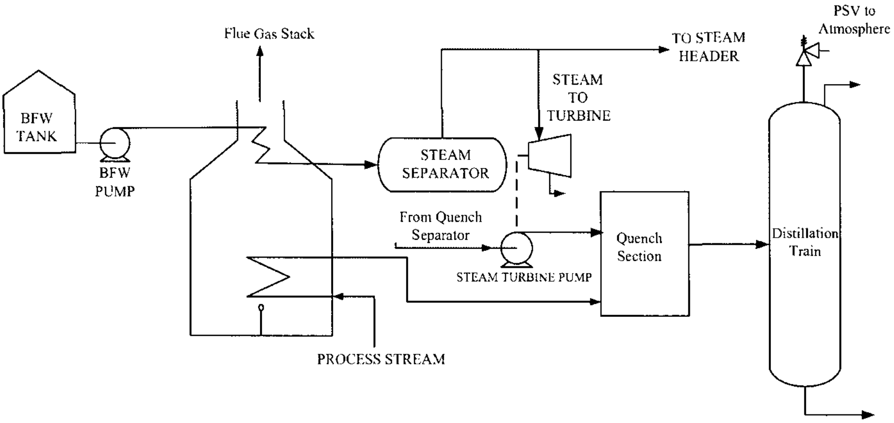


**FIGURE 4-2 COUPLED SYSTEM WITH COMPLEX INTERACTIONS**

If the boiler feed water pump fails, there are a number of simultaneous problems:

- Flue gas heat is not removed and the convection bank tube temperature would exceed design limit, resulting in tube failure.
- There is no steam to drive the turbine pump, no quench circulation and a hot, high pressure gas stream enters the distillation train.
- The operating procedure calls for the operator to start the electric pump for quench liquid circulation on failure of the turbine pump, but this requires local field start and may not be accomplished quickly.

The consequence is not only exceeding the design temperature of the distillation equipment, but exceeding the design pressure, and discharge of process fluids to atmosphere through the pressure safety valve (PSV).

There can be extensive damage to the furnace steam tubes and distillation equipment, causing extended downtime and production loss. There would also be an investigation from environmental regulators on the discharge of a large quantity of chemical to atmosphere.

It is evident that nearly all chemical process systems have complex interactions. These need to be identified and properly considered in the design process.

There are three main characteristics of complex interactions:

- Common mode failures or failures due to sub-system dependencies. A failure in one sub-system can affect sub-systems upstream and downstream beyond the contiguent ones.
- Hidden interactions.
- Human reliability issues such as the ability to diagnose a fault in the control of process and take appropriate corrective action within a reasonable time before the process gets out of control. Process industry surveys in Japan, Europe and North America have shown that about 40% of abnormal operations were caused by human errors (Nimmo 1995) and in the UK, in

about 80% of the accidents, human error was present as one of the contributing factors (Lardner and Fleming 1999).

All of the above issues need to be addressed in a systematic manner using one or more of the hazard identification methods.

## 4.3 COMPARATIVE HAZARD IDENTIFICATION METHODS

### 4.3.1 Past Experience

It is often said that those who do not learn from history are destined to repeat it. It is very much applicable in the case of 'learning from accidents' in the process industries.

One of the first steps in hazard identification is to ask the following questions:

a) What hazardous events have occurred in the past, within the organisation or in the industry as a whole, in facilities producing the same or similar product using the same or similar process?
b) What lessons have been learnt?
c) Can these events or similar events occur in the process under consideration?
d) If the answer to (c) is 'yes', what needs to be done to eliminate or prevent the occurrence of those events?

Organisations tend to have poor memory, compounded by a corporate mindset that does not actively promote information sharing on process safety across all of its facilities.

Fortunately, there has been an increasing awareness since the accidents in Flixborough in 1974 and in Seveso in 1976 that there is much to be learnt by systematically capturing the information in the investigation reports of accidents and near-misses. In many countries, accidents and near misses are reportable to the safety regulators, who maintain a database of accident information.

Learning the lessons from available literature data on past accidents, and using them to identify what could happen in the future is referred to by Bond (2002) as the Janus approach to safety. "Janus was a god of the ancient Romans who is depicted as having two faces, one looking backwards and the other to the front. He was a guardian of the beginnings and the month of January is named after him because he looked back to the past year and forward to the year to come" (Bond 2002).

### 4.3.2 Incident Databases

A number of industry databases are available. Some of the information in the databases is taken from the media, which focuses more on the event itself, rather than its causes. The most reliable are those maintained by regulatory agencies, as the causes of the accident are often identified, in official investigations following an accident. Relevant databases include:

1. Major Hazard Incident Data System (MHIDAS). This database is maintained by AEA Technology in the U.K. for the Health & Safety Executive (UK HSE).
2. FACTS (TNO in the Netherlands)
3. IChemE Accident Database (The Institution of Chemical Engineers, UK). This is based on information published in the Loss Prevention Bulletin, journal articles, official reports of investigations from regulatory agencies, and confidential reports from organisations.
4. Major Accident Reporting System (MARS). This database contains information reported by the member states of the European Union (EU), in accordance with the EU Council Directive 96/82/EC (Seveso II). MARS is operated and maintained by the Major Accident Hazards Bureau (MAHB) of the EU's Joint Research Centre in Ispra, Italy (Drogaris 1993, Balasubramanian and Louvar 2002).
5. Accident Release Information Program (ARIP). This database was developed by the US Environmental Protection Agency (US EPA) using the reportable release incidents of chemicals, and a screening criteria based on the severity of the incident (injury or fatality), listed chemical, and quantity released. This database covers only incident from facilities based in the USA.
6. FIRE - This is a database on chemical warehouse fires (Koivisto and Nielsen 1994).
7. Offshore hydrocarbon releases (HCR) database maintained by UK HSE (2001). This is a statistical database, useful for probability analysis (see Chapter 8), but the types of release scenarios are useful at the hazard identification stage as well.
8. Safety Alert Database and Information Exchange (SADIE) – This database is maintained by the Steel Construction Institute in the UK to enable the offshore oil and gas industry to share information on important safety issues, and information gained from accidents and near misses. This database and information format is reported to exceed the standards of databases for onshore process industries (Selby, 2003).
9. Process Safety Beacon - One-page safety awareness messages based on case history, produced by the Center for Chemical Process Safety of the AIChE. These can be found on the internet website – http://www.aiche.org/ccps/safetybeacon.htm
10. WOAD - World Offshore Accident Database (annual) for offshore oil and gas installation accidents
11. Database of accidents reported to and investigated by the US Chemical Safety & Hazard Investigation Board can be found in the website http://www.csb.gov and select 'completed investigations'.
12. Database of inspection details of accidents recorded by the US Department of Labor under the Occupational Health & Safety Administration (OSHA) at http://www.osha.gov/oshstats/index.html.

### 4.3.3 Analysis of Incident Statistics

Khan and Abbasi (1999) have conducted an extensive analysis of process industry accidents covering 70 years (1926 to 1997). A total of 3222 accidents have been reported in the literature, on average one a week. Figure 4-3 shows the distribution of these accidents. Approximately 41% of the accidents occurred in transportation, indicating that in life cycle risk management, it is necessary to pay attention to transportation of hazardous materials, in addition to the fixed installation hazards.

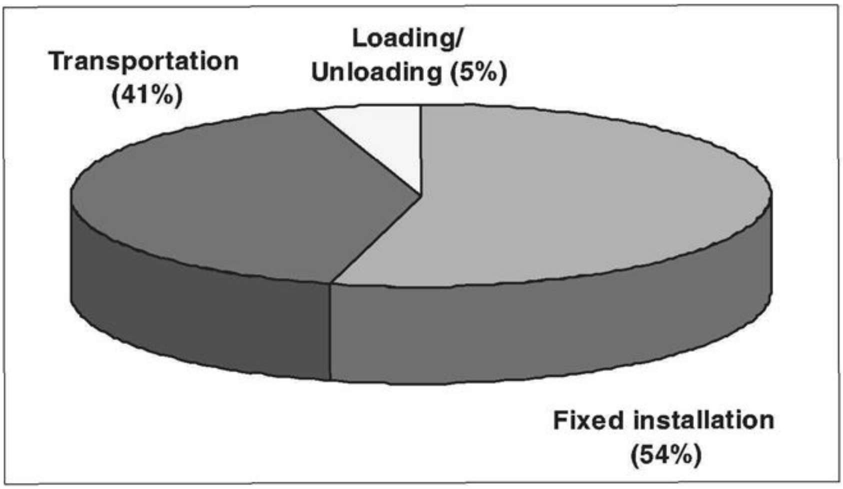


FIGURE 4-3 CLASSIFICATION OF HISTORICAL PROCESS INDUSTRY ACCIDENT DATA

Historical data also provide the relative contributions of causes to failures of equipment and components in the process industries. While specific failure causes are not listed, Figures 4-4 and 4-5 give a good indication of the type and range of failures over a 40-year history (Source: Balasubramanian and Louvar 2002).

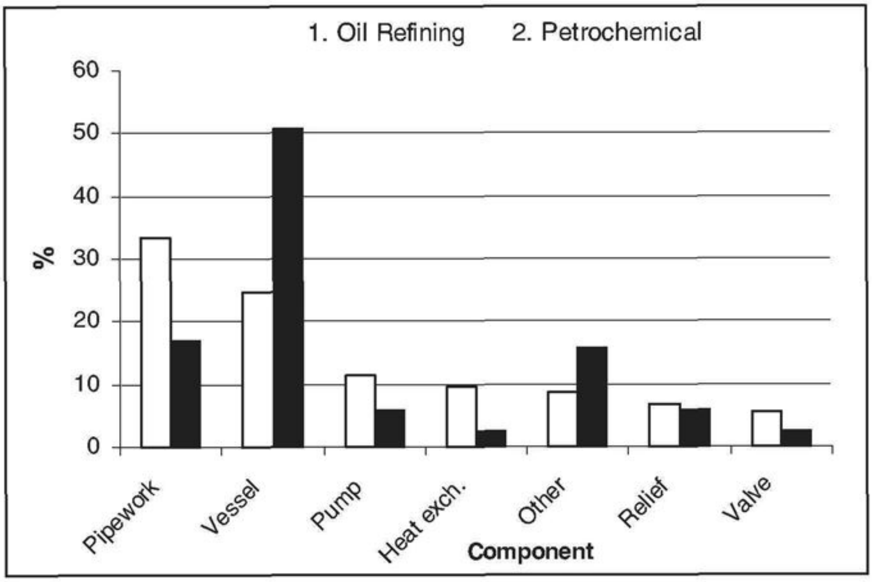


FIGURE 4-4 ANALYSIS OF PROCESS INDUSTRY ACCIDENTS BY COMPONENT

It is seen that there has been a larger contribution to failures from vessels in the petrochemical industry, compared to pipework in the petroleum refining industry. Pumps and heat exchangers failures are higher in oil refining.

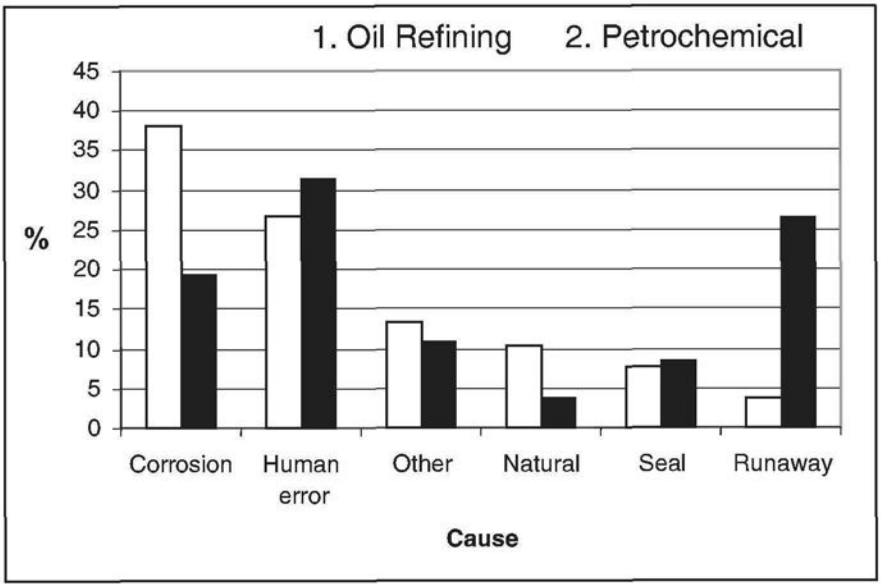


FIGURE 4-5 ANALYSIS OF PROCESS INDUSTRY ACCIDENTS BY CAUSE

The results are reasonably consistent with expectations. Human error contributions are about the same, indicating that it is a process industry-wide issue rather than the type of facility. Corrosion contribution is higher in refining compared to petrochemical industry, which is to be expected, given the sulphur compounds and water in crude oil refining. Chemical reaction hazards contribute more in the petrochemical industry compared with refining.

A number of case studies are provided by Kletz (1994, 2001), Sanders (1999, 2002), Khan and Abbasi (1999), and Guoshun (2000). Statistical data on process accidents are reported by Planas-Cuchi et al. (1999), Fowler and Baxter (2000), Bradley and Baxter (2002).

It is necessary to refer to past experience of recorded incidents to ensure that the failure causes have been taken into account for the context in question, but this alone is not sufficient for full hazard identification, due to hidden interactions in complex systems. There are other limitations in relying on past experience only.

a) Not all accidents or incidents are reported and this makes the database restricted. The level of documentation and information vary considerably.
b) The combination of complex cause–consequence relationships is not always well established after an accident, as any evidence is sometimes destroyed in the accident. Therefore, any hazard identification should

develop the logical sequences leading to a potential accident rather than just record the final event.

### 4.3.4 Checklists, Standards and Codes of Practice

The use of established engineering codes and standards are vital for a robust design. In many areas, compliance with specified codes is a regulatory requirement. These codes are based on hundreds of man-years of industry experience, and to a major extent, have incorporated into the design requirements, the lessons learnt from major accidents.

Checklists are most useful for compliance checks with engineering standards, procedures, and regulations. Non-conformances are identified, and corrective actions are taken to rectify the problem. Checklists can cover any aspect of the facility life cycle. Each item can be examined or verified, noting the appropriate status on the checklist. “Checklists represent the simplest method used for hazard identification” (Hessian and Rubin 1991).

Compliance with codes and standards alone for hazard identification and control has a number of limitations:

- Codes and standards may not be available in all situations in the country where the facility would be installed. Some international code may have to be used, but the applicability of the code from one country to another varies. For example, the design code may call for a material specification to cope with severe winter conditions in northern Europe, and is obviously not required in the tropics.
- A code may not be fully applicable to the particular situation in question, or may be capable of more than one interpretation.
- Codes and standards are generic requirements, and often cover 'minimum requirements'. Depending on the type of project, its location, and the sensitivity of the surrounding environment, design standards may have to be applied which go far beyond code requirements. For example, the separation distances specified in some codes for storage of flammable liquids or liquefied flammable gases are more for protecting the storage from surrounding activity within or outside the site boundary, than for protecting the environment surrounding the facility from the subject activity.

Many hazards can be identified by the use of a checklist. The following procedure is adopted for checklist development.

1. Define the objectives of the checklist. What is its purpose, where will it be used, and what is the expected outcome? More importantly, what are the items that the checklist *will not deliver*, and what other methods are necessary? Know your limitations before you start.
2. Identify areas of expertise that need to be included in the checklist, and select competent personnel in each specialist area. For hazard identification checklist development, the project safety representative would prepare the checklist, with input from the designers, operations

representatives, and project personnel. Input from prior knowledge of the system or plant is essential. In new processes, design contractor input would be required.

3. Develop the checklist. Divide the project into subsystems for easy analysis. Not all the checklist questions would apply to all systems.
4. Undertake an independent review of the checklist by an experienced manager or project engineer. This step is crucial for identifying possible omissions or oversights.
5. Update the checklist where appropriate, as new information is gathered, subject to relevant approvals.

It should always be remembered that checklists have a number of limitations.

- Other than codes and standards, checklist items tend to depend largely on the knowledge and expertise of the preparer(s) and the reviewer(s). Selection of the right personnel is therefore critical. Sometimes specialist help may be required.
- Checklist has a simple “yes” or “no” answer to questions, and merely provides the status of the item in question. It provides very little insight into system interactions or interdependencies. For example, a checklist attribute may be 'Will actuated valve close on instrument air failure?' Answer: 'Yes' or 'No'. The checklist indicates whether the design is correct. Even in the event of a 'yes' answer, it does not state the ramifications of non-closure of the valve.
- Checklists do not rank hazards in order of priority.
- If checklists are prepared by inexperienced persons and/or are not independently verified by an expert, any items omitted from the list may go undetected.

Sample checklists developed by Hessian & Rubin (1991) provide a good basis and understanding for checklist development. These checklists are designed for verification of compliance against codes and standards, regulations and procedures, more in the form of an audit.

The checklist method may be appropriate for low hazard, simple process plants. As the systems become complex this method alone is not sufficient for comprehensive hazard identification.

### 4.3.5 Process Hazard Identification Matrix

One of the simplest, yet very effective methods of hazard identification is the development of hazard matrices. Clark (1997) describes the process matrix approach for hazard identification. This technique provides a first pass list of hazards, which can be screened and ranked for more detailed evaluation at the next step in hazard management.

Process hazards can arise from:

1. Uncontrolled mixing of incompatible substances (chemical-chemical interactions)

2. Interactions between chemical and materials of construction
3. Interactions between chemicals and materials with energy sources (kinetic: rotating equipment; electrical: junction boxes, static electricity; chemical: reaction energy; radioactive; potential: elevated sources; thermodynamic: pressure, thermal)
4. Interaction between process and utilities (cooling water, demineralised water, steam, instrument air, plant air, power, hydraulic systems, fuel-gas, diesel etc).
5. Interaction between chemicals, materials of construction, or utilities with the environment (people: personnel and public, air, water: surface water and groundwater, land: onsite and offsite).

We can now construct a triangular matrix, with the upper triangular shown, as in Figure 4-6.

| | Chemicals | Materials of construction | Energy sources | Utilities | Environment |
|---|---|---|---|---|---|
| Chemicals | | | | | |
| Materials of construction | | | | | |
| Energy sources | | | | | |
| Utilities | | | | | |
| Environment | | | | | |

FIGURE 4-6 PROCESS HAZARDS IDENTIFICATION MATRIX

The matrix appears simple on the face of it, but it is enormously large. Let us take a simple example.

- Let us say there are 12 chemicals that include raw materials, intermediates and products, reagents, catalyst, solvents, lubricants etc.
- There are 6 materials of construction, carbon steel, stainless steel, special alloy steel, and plastics. In practice, one has to list all the materials that will be used for all equipment, piping, flanges and gaskets, valves, and instrument connections. There can be several of them depending on the nature of materials handled.
- There are 6 types of energy sources as listed in Item 3 above. Each energy source in each category can be separately listed, e.g. compressor, fan, centrifuge for kinetic energy.
- There are say 6 utilities (there may be some overlaps of utilities with chemicals and energy sources).
- The environment consists of 8 categories (operators, maintenance personnel, public, air, surface water, groundwater, onsite land, offsite land). There can be more if one includes flora and fauna, and the marine environment.

All of the above add up to 42 items. The process hazards identification matrix shown in Figure 4-6 is actually a 42 x 42 matrix, and even larger once individual energy sources are listed. This can be readily built into a large spreadsheet.

The following sequence of steps applies for building the process hazard identification matrix.

**Step 1:** Construct the matrix by listing the following.

- List all chemicals. These include raw materials, intermediates, products, lubricants (there may be incompatible chemicals in lubricants), reagents, catalysts, cleaning chemicals, solvents, radioactive materials used in nucleonic measuring instruments. Do not exclude anything. If the same material is used at different temperatures and pressures, list them separately. For example, propane may be used as a feedstock in the petrochemical process, but it may also be used a cryogenic in the refrigeration plant.
- List all existing or intended materials of construction for the plant (metals, alloys, plastics and composites used in process and electrical equipment and utilities, rigid and flexible piping, gaskets, seals, gland packing, instruments, instrument impulse lines, cables and insulation)
- List all energy sources.
  - Kinetic energy sources can be identified by the specific individual equipment, e.g. feed pump, circulation pump, centrifuge, recycle gas compressor etc.
  - Electrical energy can be listed as electric drives, junction or terminal boxes, and static electricity. List static electricity as a separate entry.
  - Radioactive energy is implicitly included in the chemicals list, but worth specifying as a separate energy source.
  - Chemical energy – reactivity, reaction heat (endothermic, endothermic)
  - Potential energy – elevated sources of inventory, materials handling at heights during maintenance, personnel working at heights
  - Thermodynamic energy – Pressure energy. List pressurised process systems, compressed air, steam, high pressure boiler feed water, hydraulic oil etc. Thermal energy – these can be materials at high temperatures and hot surfaces, or conversely cryogenic materials.

- List all utilities on site. These include cooling water, demineralised water, steam, instrument air, plant air, nitrogen, fixed gaseous fire suppressants, hydraulic oil, natural gas as fuel, diesel as backup fuel.
- List the environmental receptors (operator, maintenance personnel, public offsite, air, surface water, groundwater, land onsite, land offsite, and the marine environment)

**Step 2:** Populate the process hazard identification matrix.

Initially a qualitative assessment is made. Take the first chemical (top left hand side). Work along the row and ask the question – "Is there is a reaction hazard of this chemical with any of the items appearing in the columns, once these two come into contact?" If the answer is 'yes', then place an "X" or "✓" in that cell. Once the row is complete, fill in the next row and so on until the matrix is completed. If more information is known on the specific interactions, this can be used to populate the cells in the matrix.

The process may appear tedious, but there will be many empty cells towards which no future attention needs to be given. Despite the tedium, it is highly useful, when the process is complex and not sufficiently known.

When the matrix is populated fully, hazard identification may stop. All the marked boxes are collated, and scenarios developed out of them for more detailed analysis in the next step of the risk management framework.

**Step 3:** Conduct semi-quantitative assessment.

The process hazard identification matrix developed in Step 2 is qualitative. Because of the large number of entries that need to be processed, one may choose to apply some form of risk quantification and ranking to the entries, so that the items can be ranked in the order of priority. In this way, only the higher risk items would be carried forward to more detailed analysis, and the rest would be covered by applying standards and codes of practice, and procedures.

In order to make the matrix quantitative, a scale of risk needs to be established. As we have seen in Chapter 2, risk is the product of consequence severity and the likelihood. Therefore, it is necessary to establish scales for both the severity and the likelihood, from which the risk scale can be calculated.

There can be 3 severity categories, to represent each category of risk.

- Risk to people
- Risk to plant and property (asset loss, production loss)
- Risk to the environment (the extent of potential impairment and cleanup/remediation required)

Risk scales for semi-quantification and ranking have been discussed in Chapter 3.

### 4.3.6 What-If Analysis

The "What-If" procedure is not as structured as FMEA or HAZOP procedures. It requires significant skill on the part of a facilitator to stimulate discussion among a multi-disciplinary team.

The purpose of "What-If" analysis is to consider the result of unexpected events that have the potential to produce adverse consequences. The method consists of examining potential deviations from design, construction, modification or operating intent.

The "What-If" method uses questions that begin with "What if ....?". Examples are:

- What if the pressure rises rapidly?
- What if a control valve sticks or fails?
- What if an operator opens a wrong valve?

The process system is divided into a number of subsystems and the "What-If" technique is applied to each subsystem. A checklist of issues of concern may be used to stimulate the discussion. Additional items may be added to the list during the course of the discussion.

The analysis is too unstructured for use in new designs, or even for evaluation of operating plants. Considerable time needs to be spent on formulating the "What-If" questions.

One of the significant uses of the "What-If" analysis is in plant modifications, as part of the change management procedure.

A simplified checklist for "What-If" analysis provided by Burk (1992) is reproduced in Table 4-1, with some additions and modifications. The guidewords in this checklist can be used to stimulate discussion in a brainstorming session, and should not be treated as exhaustive.

**TABLE 4-1 SIMPLIFIED CHECKLIST FOR MATERIAL STORAGE**

| Equipment | Issues for Consideration |
|---|---|
| STORAGE OF RAW MATERIALS, PRODUCTS AND INTERMEDIATES | |
| Storage tanks | Design separation, inerting, materials of construction, design code, isolation provisions |
| Dikes/Bunds | Capacity, drainage, integrity, erosion protection for earthen bunds |
| Emergency valves | Remote control, hazardous materials, closure times of valves, fail-safe |
| Inspections | Flash arresters, relief devices, pressure/vacuum valve, access |
| Procedures | Contamination prevention, sampling, water draining (in the case of some petroleum products) |
| Specifications | Chemical, physical, quality, stability (e.g. inhibitor for monomers) |
| Instrumentation | Level control/monitoring, temperature monitoring, pressure sensors for pressurised storage |
| Limitations | Temperature, time, quantity, vacuum arising from steam cleaning during maintenance |
| MATERIALS HANDLING | |
| Pumps | Relief, reverse rotation, identification, materials of construction, seals integrity, suction protection, protection against closed head operation |
| Ducts | Explosion relief, fire protection, support, access |
| Conveyors, mills | Stop devices, coasting, guards, access, fire protection |
| Procedures | Spills, leaks, drainage, decontamination |
| Piping | Rating, codes, cross-connections, materials of construction, isolation (provision of valves, spades or spectacle blinds), provision for draining, purging, low points, access |
| Instrumentation | Flow metering, pressure/temperature monitoring |
| PROCESS EQUIPMENT, FACILITIES AND PROCEDURES | |
| Procedures | Startup, normal operation and maintenance, shutdown, emergency |
| Conformance | Job audits, short cuts, suggestions |
| Loss of utilities | Electricity, heating, coolant air, inerts, agitation, cooling water, instrument air, plant air, hydraulics, gaseous/liquid fuel, demineralised water, steam |
| Vessels | Design, materials, codes, access, materials of construction, provision for spades/spectacle blind for isolation |
| Identification | Vessels, piping, switches, valves, instruments |
| Relief devices | Reactors, exchangers, glassware (lined vessels), pressure vessels, relief location, design codes (single phase, two-phase) |

| Equipment | Issues for Consideration |
|---|---|
| Review of incidents | Plant, company, industry |
| Inspections, tests | Vessels, relief devices, corrosion, piping, access |
| Hazards | Loss of containment, reactivity hazards, fires, vapour cloud explosions, explosion inside equipment, dust explosions, toxic effects, domino effects |
| Electrical | Hazardous area classification schedule and drawings, conformance, purging, earthing or grounding |
| Process | Description, up to date P&IDs, test authorisations, problem diagnosis, troubleshooting |
| Operating ranges | Flow, level, pressure, temperature, ratios, composition, concentration, density, time, sequence. normal operating limits, safe operating limits |
| Ignition sources | Rotating equipment, hot surfaces, hot work, self-ignition (peroxides etc), friction, fouling, pyrophoric substances, heaters, static electricity, lightning, terminal boxes, missing intrinsically safe barriers |
| Compatibility | Heating/cooling media, lubricants, packing, materials of construction, chemical reactivity, reagents, solvents |
| Safety margins | Design limits, test limits, excursions |
| Flare | Location, height, capacity, flare radiation, codes, prevention of liquid carryover, monitoring |
| PERSONNEL PROTECTION | |
| Protection | Barricades, personal protection equipment (PPE), safety shower, escape aids |
| Ventilation | General, local, air intakes, rate |
| Exposures | Workplace, other processes, public environment, exposure limits |
| Utilities | Compressed air, pressurised water, inert gases, steam, radioactive substances |
| Hazards manual | Material safety datasheets (MSDS), toxicity, flammability, reactivity, corrosion, symptoms, first aid |
| Environment | Discharges, sampling, vapours, dusts, noise, radiation |
| CONTROLS AND EMERGENCY DEVICES | |
| Controls | Ranges, redundancy, fail-safe |
| Calibration, inspection | Frequency, adequacy, access |
| Alarms | Adequacy, limits, fire & gas (flammable, toxic) detection system |
| Interlocks | Tests, bypass procedures, software controlled interlocks, hard-wired interlocks |
| Emergency shutdown system | Logic solver, system separate to the process control system, reliability |
| Relief devices | Adequacy, vent size (single-phase, two-phase discharges), discharge location, drain, support, material of construction, can it relieve to atmosphere (hazardous materials)? |
| Emergencies | Prevention, depressuring, dumping, water deluge, dilution |
| Process isolation | Block valves, fire-safe valves, purging, valve closure times for actuated valves |
| Instruments | Adequacy, redundancy, reset philosophy (automatic after time delay, manual), materials of construction, specification for classified hazardous area |
| WASTE DISPOSAL | |
| Ditches and drains | Flame traps, reactions, exposure, solids |
| Vents | Discharge, dispersion, radiation, mists |
| Characteristics | Sludges, residues, fouling materials, toxicity |
| Disposal methods | Regulatory requirements, approvals |

| Equipment | Issues for Consideration |
|---|---|
| SAMPLING FACILITIES | |
| Sampling points | Accessibility, ventilation, valving |
| Procedures | Plugging, purging |
| Samples | Containers, storage, disposal |
| Analysis | Procedures, records, feedback |
| MAINTENANCE | |
| Isolation | Selection of isolation requirement - single block valve, double block valves, double block & bleed valves, spades for positive isolation. |
| Access | Accessibility, ergonomics |
| Decontamination | Solutions, equipment, procedures |
| Vessel openings | Size, obstructions, access |
| Procedures | Vessel entry, hot work, lockout and tagging |
| FIRE PROTECTION | |
| Passive protection | Passive protection coating on vessels, support structures |
| Fire barriers | Fire wall, fire and blast wall |
| Active fixed protection | Fire areas, water demand, firewater pump and distribution system, sprinklers, deluge, monitors, hydrants and hoses, location, accessibility, inspection, testing, procedures, adequacy |
| Extinguishers | Type, location, training |
| Drainage | Slope, drain rate and adequacy, prevention of contaminated firewater runoff to stormwater system |
| Emergency response | Emergency response team, equipment, training, preparedness |

The questions raised using the checklist in Table 4-1 should be in the form of full sentences, along with their answers, and actions arising, with responsibility allocated for follow up and closeout.

### 4.3.7 Semi-quantitative Methods

A number of empirical methods have been developed to estimate the area of impact surrounding a process unit when energy is released from flammable materials in the process. The most popular index that has survived the test of time is the Dow fire and explosion index (AIChE 1994a), and its companion the Dow chemical exposure index (AIChE 1994b). The Mond Index (Tyler et al. 1994) is sometimes used as an alternative.

Refinement to these indices have been suggested by Tyler et al. (1994) for toxicity and Khan et al. (2001) which takes into account management factors in assessing the fire and explosion index. These methods have not been tested as widely as the Dow indices.

#### *4.3.7.1 Dow Fire and Explosion Index*

The Dow Fire and Explosion Index (F&EI) is based on the hazardous properties of the materials inventory in the process unit as well as the operating conditions. The methodology consists of the following:

1. Select a process unit
2. Calculate the material factor (flammable and explosive property of the process material)
3. Calculate general and special process hazards (based on the pressure and temperature of operation, reaction systems etc)
4. Calculate the F&EI using the above information
5. Estimate the area of impact around the process unit, for a given F&EI
6. From the area, calculate the radius of impact.

Data sheets are provided in the manual (AIChE 1994a), for steps 2 to 4, and a graph or correlation is provided for step 5.

The radius of impact provides the extent of loss surrounding the unit under consideration, and is used in the layout design for separation distances between units.

### EXAMPLE 4-3 DOW F&EI FOR NATURAL GAS-STEAM REFORMER

| | | | | |
|---|---|---|---|---|
| **Date:**<br>March 2004 | | **Location:**<br>Australia | **Plant:** Synthesis gas | **Process Unit:**<br>Reformer |
| **Basic Material:**<br>Reformer gas (CO, $H_2$) | | **Operating Mode:** Normal | **Evaluated By:**<br>R.Raman | **Reviewed By:**<br>I.Cameron |
| **MATERIAL FACTOR (from table 1 of Dow F&EI Manual)** | | | | 21 |
| **1. GENERAL PROCESS HAZARDS** | | **Penalty** | **Penalty Used** | **Comments** |
| Base Factor | | 1.00 | 1.00 | |
| A | Exothermic Chemical Reactions (factor .30 to 1.25) | | | Reaction not exothermic |
| B | Endothermic Process (factor .20 to .40) | | 0.40 | Reaction endothermic |
| C | Material handling & Transfer (factor .25 to 1.05) | | | Gaseous system |
| D | Enclosed or Indoor Process Units (factor .25 to .90) | | | Outdoor plant |
| E | Access | 0.35 | 0.20 | Open area |
| F | Drainage and Spill Control (factor .25 to .50) ____ Gals | | | No liquids |
| General Process Hazards Factor ($F_1$) (sum A to F) | | | **1.60** | |
| **2. SPECIAL PROCESS HAZARDS** | | | | |
| Base Factor | | 1.00 | 1.00 | |
| A | Toxic Materials (factor .20 to .80) | | 0.20 | Sulphur removed |
| B | Sub Atmospheric pressure (500mmHg) | 0.50 | | No vacuum |
| C | Operation in or near Flammable Range | | | |
| | 1. Tank farms storage flammable liquids | 0.50 | | No liquids |
| | 2. Process upset of purge failure | 0.30 | | No purges |
| | 3. Always in flammable range | 0.80 | 0.80 | Upon leak to atmosphere |

| | | | | |
|---|---|---|---|---|
| **Date:**<br>March 2004 | **Location:**<br>Australia | | **Plant:** Synthesis gas | **Process Unit:**<br>Reformer |
| D | Dust Explosion (factor .25 to .30) | | | No dust |
| E | Pressure (Dow F&E I) Op Press ___ Relief Setting __ | | 0.94 | |
| F | Low Temperature (factor .20 to .30) | | | Reaction at high temperature |
| G | Qty of Flammable/unstable Material ___lbs Hc= __ BTU/lb | | | |
| | 1. Liquids, gases and reactive materials (Dow F&E Index) | | 0.15 | |
| | 2. Liquids or gases in storage (Dow F&E Index) | | | Not in storage |
| | 3. Combustible solids in storage, dust in process (F&E) | | | No solids |
| H | Corrosion and erosion (factor .1 to .75) | | 0.20 | Some $CO_2$ corrosion |
| I | Leakage – Joints and Packing (factor .10 to 1.50) | | 0.30 | Ring joints, spiral wound gaskets |
| J | Use of Fired Heaters (see Down F&E Index) | | 0.10 | Yes |
| K | Hot Oil Heat Exchange System (factor .15 to 1.15) | | | Not used |
| L | Rotating Equipment | 0.50 | | |
| Special Process Hazards Factor ($F_2$) | | **3.69** | | |
| Unit Hazard Factor ($F_1$ x $F_2$ = $F_3$) | | **5.90** | | |
| Fire and Explosion Index ($F_3$ x MF = F&E Index) | | | | **124** |
| Exposure radius (from graph in manual) | | | | **32 m** |

The F&EI can be applied across all units of a design to obtain a relative hazard ranking for prioritization purposes of risk management. The effect of design aspects, fire detection and prevention systems allows credit factors to be estimated that reduce the "raw" index value.

### 4.3.7.2 Dow Chemical Exposure Index

The Dow Chemical Exposure Index (CEI) is a measure of the relative acute toxicity impact (AIChE 1994b). It may be used for ranking of chemical hazards in the initial stages of hazard evaluation. The methodology consists of the following steps:

1. For the toxic chemical being considered, determine the concentrations to emergency response planning guideline, ERPG, various levels (ERPG-1, 2 or 3). The units are in mg/m$^3$. These can be found in CEI (AIChE 1994b) or American Industrial Hygiene Association (AIHA) (2004). Definitions of ERPG levels are provided in Section 7.4.1.
2. Define a release incident (based on a postulated hole size for release). These are described by Marshall and Mundt (1995).

a) Process pipes - full bore rupture for pipes < 50mm in diameter

b) For pipes up to 100mm in diameter, rupture equivalent to that of a 50mm pipe
c) For pipes > 100mm, rupture area equal to 20% of cross sectional area of pipe
d) For hoses – full bore rupture
e) For pressure relief devices to atmosphere, total release rate at set pressure
f) Vessels – based on largest diameter process pipe attached to vessel, using the piping criteria in (a) to (c)
g) Tank overflow and spills
h) Others (facility specific)

3. Calculate the release rate (kg/s) for gas, liquid or two-phase release using the relevant equations in Chapter 6.
4. Calculate the air borne quantity (AQ) as follows:
   - For gases, AQ = release rate
   - For non-flashing liquids, AQ = evaporation rate from a pool, after determining pool size
   - For flashing liquids, AQ = release rate x min(flash fraction x 5, 1) + evaporation from residual pool (if any)

   Details are given in the CEI manual.
5. Calculate the CEI as CEI = $\min\{655.1\ (AQ/ERPG\text{-}2)^{\frac{1}{2}}, 1000\}$
6. Calculate the hazard distance to a given ERPG concentration, HD = $\min\{6551\ (AQ/ERPG)^{\frac{1}{2}}, 10{,}000\}$, where ERPG can be for Levels 1, 2 or 3.

Dow uses the CEI as the guide for the level of audit required for a facility. CEI of 100 or less receives local review whereas CEI > 300 receives regional and corporate review. It is used as a risk screening tool and for developing measures to reduce the CEI, and not as a risk assessment tool as the index is based on consequences only.

## 4.4 FUNDAMENTAL HAZARD IDENTIFICATION METHODS

### 4.4.1 Concept Hazard Analysis

In 1991, the Commission for the EU initiated a project to develop ‘an overall knowledge-based methodology for hazard identification’. A methodology was developed by the University of Sheffield in the UK and Risø National Laboratory in Denmark (Rasmussen and Whetton 1993), based on functional modelling of the system. This functional approach has been found to be very useful for Concept Hazard Analysis (CHA) . The CHA methodology has also been described by Wells et al. (1993).

The CHA is a high-level hazard identification tool, and its output can be used for more detailed analysis of specific areas, as identified.

#### *4.4.1.1 Functional description*

In the plant functional model, a function is an object comprising an 'intent', a list of more than one 'methods', which are used to satisfy the intent, and a list of zero or more 'constraints', which impose restrictions upon the Intent. Each element of the lists of methods and constraints can itself be treated as an object defining a new Intent with its associated methods and constraints. A simple schematic model is shown in Figure 4-7.

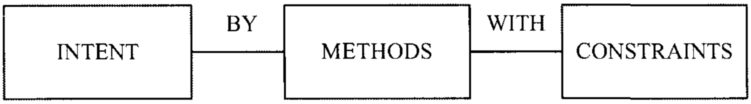


FIGURE 4-7 FUNCTIONAL MODEL FOR CONCEPT HAZARD ANALYSIS

Hence, a plant model contains objects whose elements can be classified as follows:

- Intents representing the functional goals of the specific plant activities in question
- Methods representing items such as hardware, procedures and software that are used to carry out the Intent or operations that are carried out using those items.
- Constraints describe items (physical laws, work organisation, control systems, regulatory requirements etc.) that exist to supervise or restrict the Intent; constraints can contain information about the organisational context in which the Intents are fulfilled.

A schematic model is shown in Figure 4-8, which shows the possibility of including inputs and outputs linking together the Intents in the functional plant model.

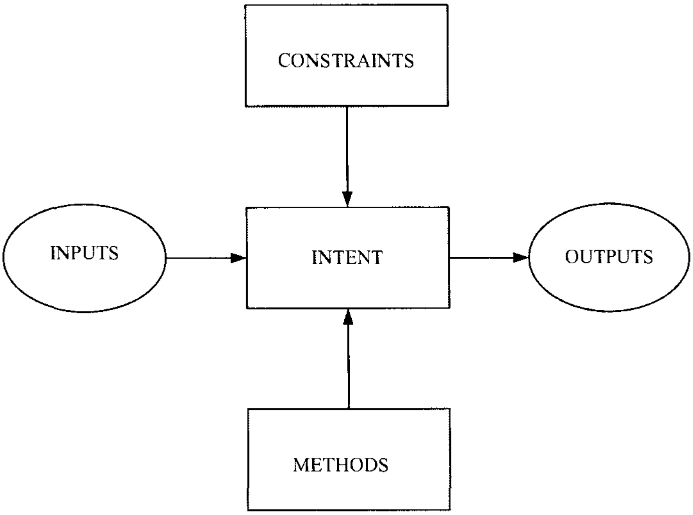


FIGURE 4-8 INTERRELATIONSHIPS BETWEEN OBJECTS AT THE SAME FUNCTIONAL LEVEL

Inputs show the necessary conditions to perform the intent and the link to the previous intent. Outputs show the outcome produced by the intent and the link to subsequent intent.

Rasmussen and Whetton (1993) have stressed the need for careful judgement in defining the Intent, in order to make sure that it is not mixed with Methods and Constraints. The following example is given.

**EXAMPLE 4-4 EXAMPLES OF INTENT**

Intent: *Produce liquid oxygen.*
This is clearly an Intent and nothing else.

Intent: *Produce liquid oxygen by air liquefaction.*
Here the Intent has been mixed with the Method "by air liquefaction".

Intent: *Produce liquid oxygen at a cost less than $X/tonne.*
Here the Intent is mixed up with a cost constraint.

Intent: *Produce liquid oxygen with noble gases as by-products.*
This is a valid Intent. This can be split into two Methods – "Produce liquid oxygen" and "extract noble gases as by-products".

■ ■ ■

#### 4.4.1.2 Concept hazard analysis procedure

The procedure for CHA is as follows:

**Step 1:** Define the overall intent of the plant.

Once the sentence for the Intent is written down, examine each clause of the sentence to see if it is a Method or a Constraint. If it is either, then remove the clause and place it in the category it belongs.

**Step 2:** Subdivide the plant to produce the following hierarchy.

(i) Plant
(ii) System (plant section or unit)
(iii) Subsystems (for each system)
(iv) Equipment (aggregate, in each subsystem)
(v) Component (in each equipment)

Depending on the level of analysis, the whole hierarchy or part of the hierarchy may be selected. The higher the level of analysis, the fewer the levels in the hierarchy.

**Step 3:** For each sub-system, write the Intents.

Separate the Intents from Methods and Constraints, as described in Step 1. A subsystem may have more than one Intent. If this is the case, it may be necessary to subdivide the subsystem again. One subsystem, one Intent is easier to analyse.

**Step 4:** For each Intent in each subsystem, identify Methods and Constraints.

This is the tricky part of the analysis. Use the equipment level to generate the Methods, e.g. use equipment A and B to achieve the Intent. A good knowledge of the process is required to complete this step.

A set of CHA keywords can help to identify the constraints. A set of generic keywords is provided in Table 4-2. (Wells et al. 1993). These can be generic, but are best generated from the intent, methods and constraints for the system/subsystems. For instance, for a reaction system, the keyword "Temperature" can be used to generate a constraint "Maintain reaction temperature within a specified range".

Not all the keywords may apply to the subsystem being analysed.

TABLE 4-2 KEYWORDS FOR CONCEPT HAZARD ANALYSIS (SOURCE: WELLS ET AL. 1993)

| Keyword | Undesired Event | Consequences/Problems |
|---|---|---|
| *Flammables* | | |
| Ignition | Release on loss of containment | Fire – flash, torch, pool |
| Fire | Release by discharge | Chemical explosion |
| Explosion | Release during handling | Physical explosion |
| | Vessel entry | Vapour cloud explosion |
| | | Electrical explosion |
| *Chemicals* | | |
| Toxicity | Release on loss of containment | Inhalation, ingestion, skin absorption |
| Corrosion | Release by discharge | |
| Reactivity | Vessel entry | Environmental impact |
| | | Waste disposal, cleanup, remediation |
| *Pollutants* | | |
| Emissions | Handling | Asphyxiation |
| Effluents | Fugitive emissions | Toxic, corrosive, exposure effects |
| Waste | Periodic emissions | Accumulation after discharge |
| | Emergency emissions | |
| *Health Hazards* | Exposure to chemicals | Toxicity effects, systemic effects |
| | Exposure to heat or cold | Exposure to thermal radiation, hot surfaces, cryogenic materials, toxic combustion products |
| | Noise exposure | |
| | Exposure to smoke plume | |
| | Radiation | Effects of radioactive materials |
| *External Threats* | Impact, vibration | Equipment damage |
| | Extreme weather | Exposure of personnel, structural failure |
| | Seismic effects | |
| | Release from neighbouring hazardous facilities | Damage, loss of containment, loss of services, loss of supply. |

| Keyword | Undesired Event | Consequences/Problems |
|---|---|---|
| | Breach of security | Exposure of personnel<br>Damage, asset loss, loss of containment |
| *Reactions* | Runaway reactions<br>Unintended reactions<br>Flammable/toxic materials | Explosion, loss of containment, impact on personnel, release of reaction energy<br>Off-specification material<br>Fire, explosion, toxic exposure |
| *Thermodynamic hazards* | | |
| Overpressure<br>Underpressure<br>Overtemperature<br>Under-temperature<br>Abnormal opening to atmosphere | Overpressure<br>Underpressure<br>Overtemperature<br>Under-temperature<br>Overheating/cooling<br>Corrosion<br>Degraded mechanical integrity<br>Wrong status of equipment, valves, relief devices | Equipment rupture, impact<br>Equipment outside safe operating limits – material weakened<br>Cold embrittlement failure<br>Loss of containment<br>Abnormal operation or failure of emergency relief devices |
| *Mechanical hazards* | | |
| Structural hazards<br>Dropped objects<br>Collapse | Overload, stress, tension<br>Loss of structural integrity<br>Mechanical energy release | Rupture of equipment, loss of containment<br>Change in material properties<br>Failures from impact of dropped objects<br>Structural failure |
| *Electrical hazards* | Charge, current, electromagnetic radiation, high voltage | Explosion, spark, shock, heat transfer, ionisation, shock to personnel |
| *Equipment problems* | Failure<br>Incorrect operation<br>Incident initiators | Loss of containment<br>Off-specification material |
| *Mode of Operation* | | |
| Startup<br>Shutdown<br>Maintenance<br>Abnormal<br>Emergency | Notable disturbances<br>Incident initiators | Loss of containment<br>Common cause failures<br>Off-specification material |
| Human factors | | |
| Training<br>Human error/reliability<br>Emergency preparedness | Adequacy of training<br>Diagnostic error, incorrect response to process deviations<br>Inadequate emergency response<br>Incident initiators | Incident escalation<br>Loss of containment<br>Major emergency |

**Step 5:** Systematically work through each subsystem and each Intent with its Methods and Constraints to consider:

- main variance (i.e. deviation from Methods or Constraints)
- consequences of the variance (including complex interactions discussed before)
- prevention/mitigation measures provided

- any additional control measures required
- notes and comments

The CHA information is documented in the form of a table.

The process in Step 5 is similar to HAZOP, but not the same, as HAZOP also focuses on the impact on other systems/subsystems, caused by a deviation in the subsystem under consideration.

**Step 6:** Summarise the findings and prioritise key areas for further in-depth study.

We shall illustrate the CHA methodology by using the ethanolamine production in Example 3-1 of Chapter 3.

### EXAMPLE 4-5 CONCEPT HAZARD ANALYSIS

For simplicity, let us assume that aqueous ammonia is imported in tankers and stored, and anhydrous ammonia is not used (inherently safer design). The hierarchical structure is shown in Figure 4-9. Some of the boxes (product packaging) have not been filled, but the diagram shown is sufficient to illustrate the method.

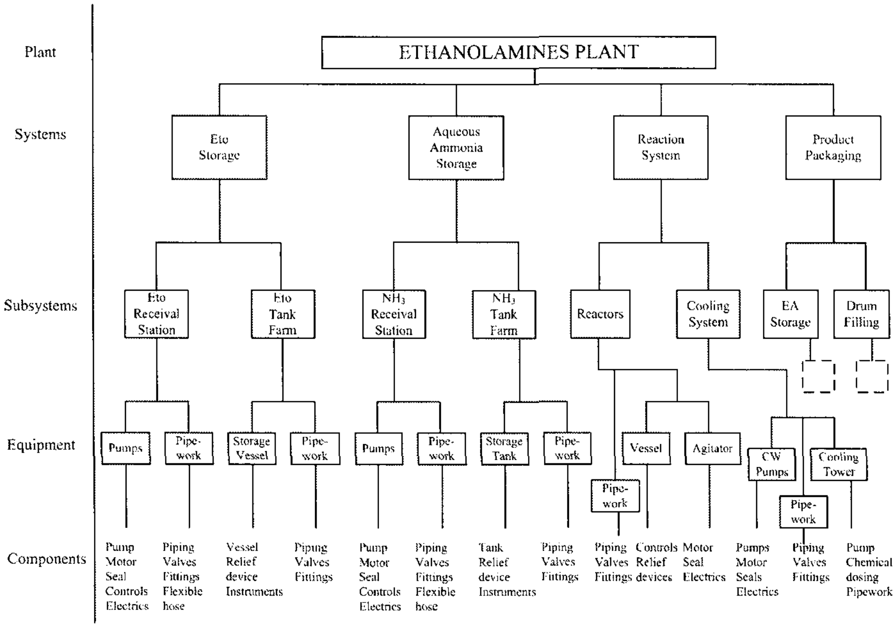


FIGURE 4-9 EXAMPLE OF STRUCTURAL DECOMPOSITION OF PLANT

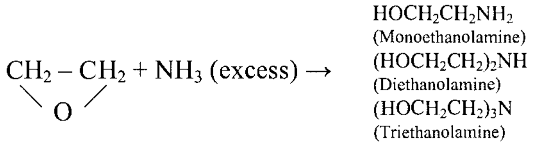
Plant Level – Overall Intent: Produce ethanolamines mixture

System Level:

Intent 1: Receive ethylene oxide
Intent 2: Store ethylene oxide
Intent 3: Receive aqueous ammonia
Intent 4: Store aqueous ammonia
Intent 5: Carry out reaction
Intent 6: Maintain reactor cooling system during reaction (This can also be a Method for Intent 5. It is the analyst's choice).
Intent 7: Store product ethanolamines
Intent 8: Package product

Note: If we write Intents at system level, then the sub-systems would become Methods, and the analysis gets to a higher level. For achieving a reasonable depth, it is advisable to choose the subsystem and write the Intent for each subsystem, as we have done above. In this case, the equipment and components become the Methods for achieving the Intent.

The chemical reaction is:



Information required to conduct the analysis involves:

- List of chemicals and their inventories
- Hazardous properties of materials
- Reactivity of chemicals
- Process flow diagram and mass balances
- Piping & Instrumentation diagrams
- Operating conditions (level, temperature, pressure, composition)
- Activity sequence for semi-batch operation
- Equipment register and specifications (may not be available in the early stages of new projects)
- Operating manual (for analysis on existing plant)

Basic information includes:

Ethylene oxide:

- Atmospheric boiling point 10.4°C
- Flash point -20°C
- Toxic – Suspected human carcinogen
- Threshold limit value (TLV) 1 ppm
- Short term exposure limit (15 minutes) 5 ppm
- Flammability limits: 3% (lower) – 100% (upper)
- Highly reactive with contaminants and a wide range of chemicals

- Acute systemic effects for exposure to low concentrations, and potentially fatal at high concentrations.
- Vessel impinged on by external fire can explode from exothermic decomposition

Aqueous ammonia:

- Concentration 28%
- Toxic fumes on release
- Corrosive liquid
- Non-flammable

Part of the CHA table is shown in Table 4-3 for Intent 1. Note how the keywords in Table 4-2 have been used in Table 4-3 to generate the constraints and the variances.

The table is not exhaustive, and highlights major issues, but is sufficient to illustrate the application of the CHA technique. It provides a high level basis for a reasonably safe design. Where the consequences are high (e.g. explosion, potential fatality), further analysis would be required.

## TABLE 4-3 CONCEPT HAZARD ANALYSIS TABLE FOR ETHANOLAMINES PLANT

| Description | I/M/C | Keyword | Variance | Consequence | Safeguard | Action |
|---|---|---|---|---|---|---|
| | I | Receive Ethylene Oxide | | | | |
| Unload from shipping container | M | Flammables: Explosion | Release and delayed ignition | Vapour cloud explosion (VCE) potential | Unloading procedures<br>Mechanical integrity<br>Emergency procedures and response | Ensure written procedures<br>Provide operator training |
| | | Flammables: Ignition | Ignition of release | Fire, smoke effects | Unloading procedures<br>Control of ignition sources<br>Emergency procedures and response | Relevant signposting<br>Ensure hazardous area classification carried out<br>Check compliance of all electrical equipment with area classification |
| | | Chemicals: Toxicity | Release, evaporation | Personnel exposure, adverse health impact | Unloading procedures<br>PPE<br>Emergency response procedures | Ensure PPE is worn<br>Prepare pre-incident plan<br>Carryout emergency drills |
| No leaks | C | Mode of operation – abnormal | Pump seal failure<br>Flexible pipe failure<br>Gasket leak | Release, VCE, fire, personnel exposure to toxic chemical | Scheduled preventive maintenance<br>Pressure testing of flexible hoses | Consider spiral wound gaskets to minimise leaks |
| Unload into dedicated vessel | M | Human factors: Error | Incorrect valve line-up<br>Unload into wrong vessel | Reactive chemical – explosion<br>Rupture<br>Serious injury, fatality potential | Unloading procedures<br>Signposting<br>Valves clearly marked<br>Dedicated line from unloading area to vessel | |
| Use $N_2$ for shipping container-storage vessel transfer | M | Thermodynamic hazards: Overpressure | Nitrogen supply pressure exceeds container design pressure. | Container rupture.<br>Release, VCE, fire, personnel exposure to toxic chemical | Nitrogen supply pressure regulated.<br>PSV on container | Design to ensure that maximum supply pressure of nitrogen will not exceed container design pressure. |

#### 4.4.1.3 Comments on concept hazard analysis

The strength of CHA arises from the functional description and modelling. Therefore, this methodology is suitable for all types of processes, and all activities associated with the life cycle. CHA is particularly useful for the following:

- processes requiring sequential activity (e.g. batch processing, chemical or petroleum products storage terminals)
- man-machine interfaces
- installation hazards identification (onshore plants and offshore oil and gas facilities – topsides and subsea)
- commissioning hazards identification
- maintenance hazards identification
- offshore drilling and well operations

Hazards that are repetitive within the same function and across different functions tend to get duplicate actions in the CHA table. In smaller studies, such duplication can be readily identified and cross referenced. For larger studies, unless dedicated software is used (Rasmussen and Whetton, 1993), poring over the table to identify duplicated entries can be tedious.

### 4.4.2 Failure Mode and Effects Analysis (FMEA)

Failure Mode and Effects Analysis (FMEA) is a qualitative analysis of hazard identification, universally applicable in a wide variety of industries. FMEA is a tabulation of each piece of equipment, noting the various modes by which the equipment can fail, and the corresponding consequences (effects) of the failures. The effects can be on the subsystem to which the equipment belongs, or on another subsystem within the same system, or another system, depending on interdependencies.

FMEA is a powerful tool as it is capable of delving into the depths of failure modes of every single component, and for this reason, is being used extensively in the electronic, nuclear, aerospace and defence industries. Its use in the process industries has been more limited compared with the above mentioned industries, with HAZOP as one of the main contenders for the preferred hazard identification tool. When the FMEA is extended to include a criticality analysis, we get Failure Mode and Effects Criticality Analysis (FMECA), which can be used for screening and ranking of identified hazards.

Human failure modes are not generally included in FMEA, but can be readily incorporated for functional analysis. Wells et al. (1992), describe FMEA with human failure modes, and incorporated within a Task Analysis, as "arguably the most complete hazard identification system in current use".

A failure mode is one of a number of ways a piece of equipment or operation can fail. Some examples are given in Table 4-4.

TABLE 4-4 EXAMPLES OF FAILURE MODES

| Subsystem | Failure mode |
|---|---|
| Pressure control system | Fails high |
| | Fails low |
| | Degraded (high noise signal) |
| | Erratic |
| Actuator block valve | Fails to open |
| | Fails to close |
| | Internal leakage |
| | External leakage |
| Operator response to process alarm | Incorrect response |
| | Delayed response |
| | No response |
| | Recoverable error |
| | Non-recoverable error |

The advantages of listing the failure modes are that the effects on the system for different failure modes can be quite different. For instance, a block valve failing on demand can create a serious safety issue, but failure to open would have no safety effect, but can impact on operability/production loss. Similarly, if an operator's delayed response creates a non-recoverable error (i.e. incident has escalated), then an alarm and operator response is insufficient. In automatic action/interlock may be necessary.

FMEA is excellent for identifying single failure modes that can result in an adverse effect on safety or operations. However, it is not so efficient in identifying combinations of failure modes, and common mode failures that can result in a major accident event. For this, a fault tree analysis is necessary, with FMEA providing the input for the base events.

### 4.4.2.1 *Generic failure modes*

In conducting an FMEA, it is useful to have a checklist of generic failure modes that can be applied to each piece of equipment. A list of significant failure modes is shown in Table 4-5.

TABLE 4-5 SIGNIFICANT FAILURE MODES

- Failure to open/close
- Failure to start/stop or continue operation
- Spurious failure (fails when it should not)
- Degradation (equipment, signal)
- Erratic behaviour (fluctuations)
- Internal leakage (isolation failure)
- External leakage (containment failure)
- Premature operation
- Intermittent operation
- Mechanical failure (wear and tear)
- Input/output failure
- Logic solver failure (programmable electronic system)
- Open or short circuit/sparking/overheating (electrical equipment)

Most components would fall into one of the above categories.

#### 4.4.2.2 *Criticality assessment*

In criticality assessment, a measure of significance (severity scale) and a failure frequency (likelihood scale) are ascribed for each failure mode. Once the scales are ascribed, the risk matrix technique can be used to assess criticality.

Table 3-3 in Chapter 3 can still be used to assess severity ranking, for the relevant risk category. Table 3-2 provides an estimate of frequency ranking. If the failure data is available in failure rate per hour, which is often the case, it can be expressed in the format in Table 3-2 to assess the likelihood scale.

It was mentioned above that human error modes can be analysed using FMEA. If a criticality needs to be assessed for human error failure modes, then a qualitative likelihood scale is more useful, as quantitative scales for human error have not been well established. The Health and Safety Commission study in the UK provides some guidance on human error probabilities (HSC 1991).

Using the severity and likelihood scale for the failure mode, a risk ranking can be arrived at. If the risk is "High" or "Extreme" in the risk matrix, the failure mode can be categorised as critical.

The application of FMECA: in the human error context is also referred to as Action Error Analysis (AEA). AEA was developed in Scandinavia to analyze operators and their interaction with control systems. There have been some efforts in developing techniques for automatic diagnosis of abnormal operations and simultaneous capture and performance assessment of operators and the process, using fuzzy logic (Sebzali and Wang 2002). Additional discussion on human error and reliability may be found in Chapters 8 and 10.

#### 4.4.2.3 *FMEA methodology*

The methodology consists of the following steps:

1. Define the complete functional boundaries of the system to be analysed. Decide *a priori* if a criticality assessment is required.
2. Decide whether the study will be conducted at component level, or at sub-component level. For example, if a centrifugal pump is one component in the system, a component level analysis might include the failure modes of the pump (stopped, racing, low output, cavitating, seal leakage etc.). A sub-component level analysis will have to look at each of the elements that make up the pump (casing, impeller, shaft, seal, drive motor etc). Sub-component level of detail is required mainly for sensitive applications, such as the nuclear or aerospace industry. For the process industries, major sub-components may be included where relevant.
3. Populate the FMEA data sheet. A typical data sheet format is shown in Table 4-6.
   a) The component identifier may be a functional identifier, (e.g. boiler feed water pump), or an identification tag that can be tied to a

drawing. The failure mode must be concise and realistic. Table 4-5 may be used for guidance.

b) Determine the effect of failure mode on the system. This is the most critical aspect of the study. The effect can be considered in terms of safety to personnel, financial loss due to production interruption or environmental damage. Multi-disciplinary input is often required.

c) Ascribe a severity and likelihood scale as described above, if a criticality assessment is undertaken.

d) Method of failure detection. For high severity consequences, it may be necessary to provide some form of failure detection, to detect incipient failures before they become critical. If no detection exists, the study may develop one and include it in the documentation. The detection method could be procedural such as regular inspection, testing and calibration. For rotating equipment, it can be a high vibration alarm or bearing high temperature alarm.

e) System and operator response. The response may include: (a) automatic control to absorb the effects of failure, e.g. high vibration and automatic shutdown of compressor or (b) ability of the operator to respond to the failure in time. This should be realistic and not too optimistic. Allow for the fact that the operator can be busy elsewhere and hence may not respond immediately, or may not even hear the alarm.

f) Document any resolution on any additional detection/protection, or changes to procedures required, for consideration after the study.

4. The worksheets produced in the analysis should be critically reviewed to ensure that the judgments are appropriate. Independent review by a senior person from outside the team may be required.

The following documents are required as a minimum, for FMECA.

- Design basis
- P&I Diagrams
- List of system functions and functional description
- System operating procedure manual (for existing plants). This may not be available for new plants during the design stage
- Equipment register with design specifications
- Manuals for vendor supplied equipment

An FMEA is normally conducted by a single person but more frequently by a team. The right experience is necessary for the team members. For example:

- ability to apply the FMEA technique effectively;
- prior experience with equipment involving broad exposure to the causes and effects of transients and equipment failures;
- knowledge of system engineering involving controls and mechanical or electrical design.
- familiarity with the design and operation of the system.

TABLE 4-6 TYPICAL FMECA DATA SHEET

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **FMECA Data Sheet** | | | | | | | | | | |
| **System: Gas Compressor (Centrifugal)** | | | | | **Drawing reference:** | | | | | |
| **Subsystem:** | | | **Date:** | | **Team members:** | | | | | |
| **No** | **Component** | **Failure Mode** | **Possible Causes** | **Effect** | **Severity Scale** | **Likelihood Scale** | **Criticality** | **Detection Method** | **Response** | **Action** |
| 1 | Flammable gas detector | Fails to detect | Sensor fails short circuit power supply<br>Calibration fault | Gas leak not detected. Potential for fire/explosion if ignited. | Major | Likely | Critical (Extreme risk) | Regular scheduled calibration and testing | Immediate repair. | Carry adequate spares.<br>Regular testing schedule. |
| 2 | Compressor bearing | Over-heating | Lubrication fails<br>Maintenance fault | Compressor damage. Loss of production. | Moderate | Possible | Critical (High risk) | Bearing high temperature alarm | Operator check and compressor shutdown | Consider bearing high high temperature trip<br>Check procedures |
| 3 | Labyrinth seal | Seal gas failure | Maintenance fault<br>Incorrect type | Gas leak to atmosphere. Potential for fire/explosion | Major | Possible | Critical (Extreme risk) | Seal gas low flow/low pressure. | Automatic trip of compressor on loss of seal gas | Function testing of interlock for reliability |

It is not uncommon that the team leader may not have all the requirements in one person. Any gap can be supplemented by the skills of a team member, or specialist input on a needs basis.

#### 4.4.2.4 *Advantages of FMEA*

The major advantages of the FMEA technique are:

- ease of construction at component level
- quick identification of critical failures
- ability to identify criticality of failures for setting priorities in risk management
- provides input to other hazard evaluation tools such as fault tree analysis and event tree analysis
- ability to apply for any system (flow and non-flow processes, batch operation, materials handling, sequential operation, man-machine interactions, mechanical, electrical, pneumatic and hydraulic systems)
- ability to incorporate human error failure modes to determine the level of automatic response required. This is highly useful in the design of control systems and layered protection systems.
- Does not require large amount of resources

#### 4.4.2.5 *Limitations of FMEA*

There are limitations on the range of applicability of FMEA that one should be aware of.

- FMEA addresses only one component at a time, and may not reveal the complex and hidden interactions in the subsystem and between subsystems in the system. In some cases, this coupling can be identified by extending the question 'What is the effect of failure on the system? What other system/component is affected?'
- It does not provide sufficient detail for quantification of system consequences.
- FMEA often focuses more on the failure modes rather than the causes of the failure modes. The main reason why the causes of failures are often not analysed in depth in the FMEA is because, for failures to which a criticality is assigned, the causes would be explored in detail outside the FMEA framework, as part of an in-depth assessment.

### 4.4.3 Hazard and Operability Study

The Hazard and Operability (HAZOP) study is perhaps the most widely used structured tool for identification of hazards and operability problems the process industries. The philosophy of HAZOP enables this technique to be extended to all types of operational situations, even outside the process industries. It is normally applied at a sub-system level.

The study is generally undertaken before the construction of new plant or equipment, or before making major modifications to existing plant, in order to facilitate recognition of a large number of hazards or potential operating problems which can be avoided by redesign or adoption of suitable operating procedures. The earlier a potential problem is found, the less expensive it is to rectify the problem, and the more likely it is that the solution will in fact be implemented.

The study is undertaken by a multi-disciplinary group, and facilitated by an experienced facilitator.

#### 4.4.3.1 HAZOP philosophy

The underlying philosophy of HAZOP is to identify potential deviations from intended operation of a system or subsystem, the consequences of the deviations, and develop design/procedural requirements to prevent the adverse consequences of the deviation from occurring.

In the process industry, this philosophy translates into a systematic examination of the design or operation of an installation, as represented by the layout, general arrangement and P&I diagrams with all control and instrumentation and sequence of operations shown. Deviations from the design value of key process parameters (physical and thermodynamic) are studied, using guidewords to stimulate the examination evaluation, and assisted by design documents and operations manuals.

Since the pioneering work of Lawley (1974), and the early work of the Chemical Industry Association in the UK (1977), the HAZOP technique has continued to enjoy extensive coverage in the process safety literature (Kletz 1999, Lees 2001, Knowlton 1992, Tweeddale 2003, Crawley and Tyler 2000, 2003).

#### 4.4.3.2 HAZOP methodology

The team formally reviews each part on the P&I diagram, selecting a process pipeline or equipment item, one at a time, using a set of deviation guidewords to consider what could happen to the process, equipment and personnel in an abnormal situation and how that situation could arise.

It is essential to make the guidewords as specific as possible and appropriate to the type of process or operation studied, in order to make the HAZOP technique most effective. For instance, slightly different guidewords are required for batch processing, compared with continuous processing. The approach combines the FMEA and the HAZOP techniques and applies to batch processing (Collins 1995, Mushtaq and Chung 2000).

Typical guidewords for fluid systems and non-fluid systems are listed in Tables 4-7 and 4-8 respectively.

TABLE 4-7 HAZOP GUIDEWORDS FOR FLUID SYSTEMS

| | |
|---|---|
| **For continuous and batch processes** | |
| **For each line/equipment or subsystem:** | |
| **Guideword** | **Deviations** |
| Changes in quantity – Flow | High flow/Low flow/No flow/Reverse flow |
| Changes in quantity – Level | High level/Low level/No level |
| Changes in physical condition – Pressure | High pressure/Low pressure/surge (hammer effect) |
| Changes in physical condition – Temperature | High temperature/Low temperature |
| Changes in physical condition – Viscosity | High viscosity/Low viscosity |
| Change in composition | Contaminants (gaseous, liquid and solid)<br>Concentration changes, reactions, multi-phase flow<br>Foaming, scum formation |
| Monitoring and control | Instruments, Control systems (interlocks, redundancies, location, effectiveness, adequacy, function testing etc.), sampling |
| **Additional guidewords for batch reaction systems** | |
| For each step in the operational sequence: | |
| Timing | Too late, too early, duration too short, duration too long, incorrect sequence |
| Reaction | Too fast, too slow, incomplete<br>More, less, incorrect charge<br>Runaway<br>Incorrect recipe<br>Catalyst<br>Contaminants |
| Valve position | Open, closed, modulating |
| Agitation | On, off, overspeed, underspeed |

TABLE 4-8 HAZOP GUIDEWORDS FOR NON-FLUID SYSTEMS

| | |
|---|---|
| **For non-fluid systems (solids, material handling)** | |
| **Guideword** | **Deviations** |
| Position | Too high, too low, too far, misaligned, wrong position |
| Movement | High speed, low speed, no movement, reverse movement, vibration, friction, slip, obstacles |
| Load | High load, low load, high flow, low flow, loss of containment |
| Energy | (Electrical, pneumatic, hydraulic, steam, etc.) low energy, high energy, energy failure |
| Timing | Too late, too early, too short, too long, incorrect sequence |
| Contamination | Water, oil, dust, flammables, corrosives, incompatible materials |
| Size | Too large, too small, too long, too short, too wide, too narrow |
| Process control | Adequate, automatic versus manual, interlocks, limits, trips, critical variable monitoring, location |
| Maintenance | Isolation, access, cleaning/purging, inspection/testing. |

The HAZOP procedure is shown in Figure 4-10.

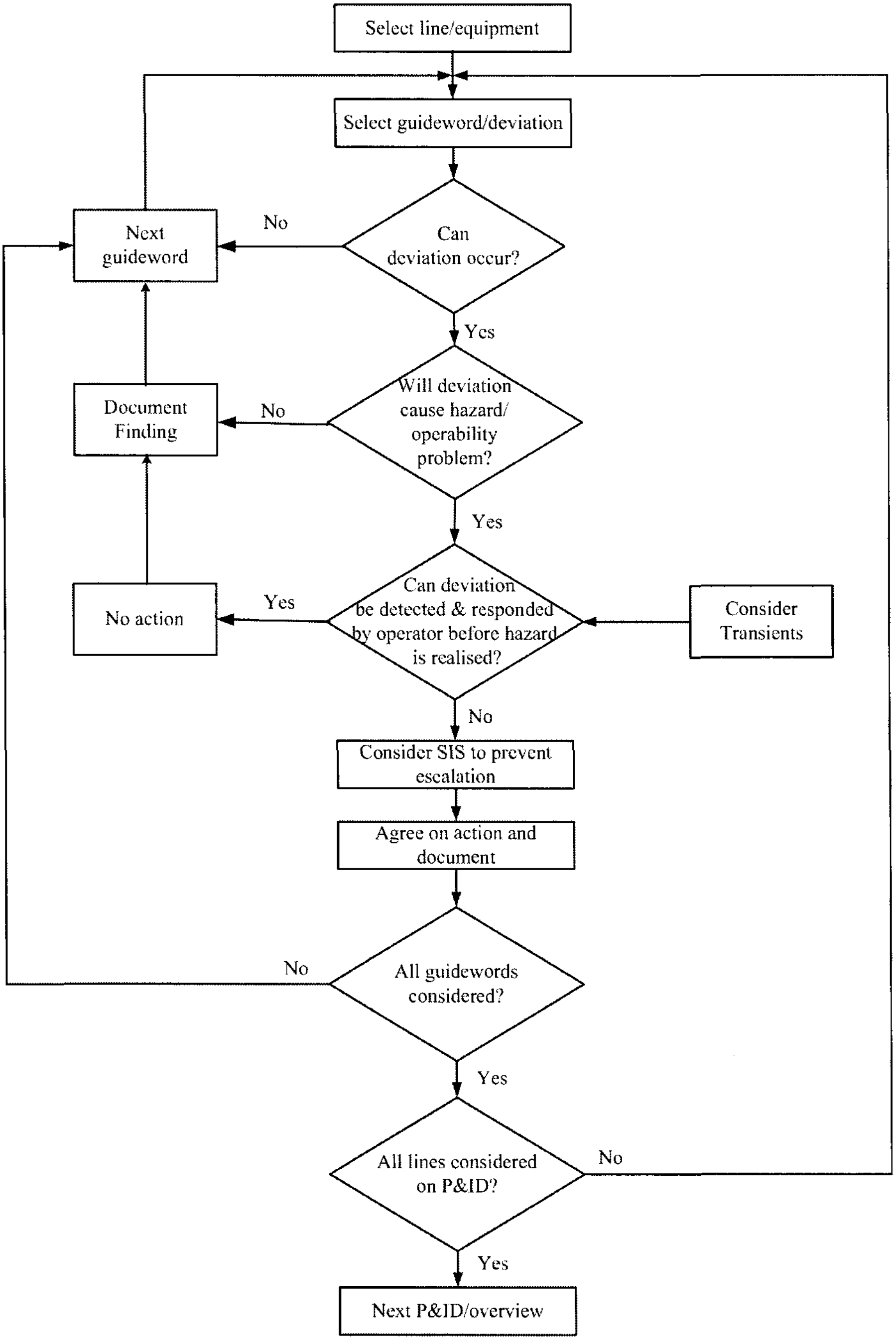

Select line/equipment
Select guideword/deviation
Can deviation occur?
No
Next guideword
Yes
Will deviation cause hazard/ operability problem?
No
Document Finding
Yes
Can deviation be detected & responded by operator before hazard is realised?
Yes
No action
Consider Transients
No
Consider SIS to prevent escalation
Agree on action and document
All guidewords considered?
No
Yes
All lines considered on P&ID?
No
Yes
Next P&ID/overview

FIGURE 4-10 HAZOP PROCEDURE SCHEMATIC

In what follows we outline the steps in a HAZOP study, along with special hints in making the HAZOP effective.

1. Select a P&ID for review.
2. Conduct preliminary review.
   Select a process line or a plant section (node) in the P&ID for review. The line/plant section may spread over more than one P&ID. Wherever possible, ensure that the line originates from an equipment (e.g. vessel, pump) and terminates at an equipment.
3. Select a guideword. The guideword can be a combination of a parameter and a deviation (e.g. Level Low), or a single guideword where the parameter and the deviation are already concatenated.
4. Identify possible causes of the deviation. If no causes can be identified, the deviation is deemed infeasible, and the study moves on to the next deviation. It is important to record all causes because different causes may have different consequences. Causes should only be grouped together when the team agrees the consequences are the same for each cause. Ahmed and Khan (1992) outline a number of causes of deviations for operating parameters such as flow, level, temperature and pressure.
5. Identify the consequences of the deviations. It is important to identify delayed consequences as well as immediate, and consequences both within and external to the node under examination. It helps to consider the transients in the development of consequences, noting the time at which an alarm or an interlock may operate. This allows a realistic judgement on the likelihood and influence of operator intervention.
   The effectiveness of the HAZOP depends on the extent to which the impact of the transients following the deviation is considered. For instance, the question to ask is: *If the operator becomes aware of the deviation through a detection system, will there be incident escalation before the operator can take corrective action?* If the answer to this is 'yes', then either an inherently safer design option or a safety instrumented layer of protection may need to be considered.
6. Identify the relevant safeguards and determine their adequacy. The team should identify the existing safeguards that control the risk arising from the identified deviation. The safeguards may help prevent the cause, reduce the consequences, or both. Both hardware such as alarms and interlocks, and administrative controls such as operating procedures/operator response to alarms should be considered.
   The team then uses its experience and judgement to assess whether the specified safeguards are adequate to control the risk. In making this assessment, the team takes account of the likelihood of the event, the seriousness of the consequences, and the probability that one or more of the safeguards fail.
   Some general guidelines are:
   - Control systems and protection systems should be separated. That is, a component which is part of a control loop should not be used to carry out a protection function.
   - If the consequences of a deviation are severe, generally a single protection system is inadequate. A layered system would be required.
7. Document the proceedings in a standard template. A sample is shown in Example 4-6 below.

8. Repeat steps 3 to 7 until all guidewords are exhausted, and then repeat the whole procedure for other lines/plant sections.
9. When the P&IDs relating to a defined plant section are completed, conduct a HAZOP overview to identify global hazards.

Table 4-9 lists a set of guidewords for line by line review, and a set of overview guidewords.

TABLE 4-9 OVERVIEW GUIDEWORDS FOR HAZOP

| Guideword | Issues |
|---|---|
| Hazardous materials | Hazardous substances storage and handling (toxicity, handling procedures, precautions, exposure limits, exposure monitoring, escape routes, regulatory requirements, licensing), radioactive materials, pyrophoric substances |
| Electrical systems | Hazardous area classification, electrical isolation, earthing, high voltage systems |
| Equipment integrity | Materials of construction (vessels, piping/valves/gaskets/pumps/seals, others), codes and standards |
| Breakdown/Loss of supply | Utilities and services (instrument air, plant air, nitrogen, cooling water, process water, demineralised water, steam, electricity, natural gas, auxiliary fuel), Computer control, hydraulic system |
| Commissioning and start-up | Commissioning (sequence, procedures)<br>Start-up (first time start-up, routine start-up) |
| Shutdown | Planned, unplanned, emergency |
| Waste | Effluent (gaseous, liquid, solid), treatment, disposal |
| System maintenance and inspection | Preparation for inspection/maintenance (isolation, draining, purging, maintenance access, vessel entry, recommissioning) |
| Loss of containment hazards | Loss of containment (fugitive emissions, minor leaks, major leaks, isolation, bunding or diking, etc.) |
| Occupational safety & health | Noise (sources, exposure limits, regulatory requirements, control measures)<br>Safety equipment (personal protection, respirator, breathing apparatus, access, training, location of safety showers etc.) |
| Fire protection | Fire/explosion (detection systems, separation distances, blast proofing, passive and active fire protection, access etc.) |
| Quality | Output and efficiency (reliability, conversion, product quality, product testing) |
| Environmental impact | Emissions (normal, abnormal), impact on air quality, water quality, soil contamination, marine environment |
| Sampling | Materials, location, frequency, handling safety |
| Erosion/Corrosion | Internal, external, corrosion underneath insulation, monitoring, prevention, protection |
| Static electricity buildup | Sources of static electricity, prevention |
| Lifting | Crane operations, impact, dropped load |
| Collision | Vehicle movements in plant, forklift operations |
| Vibration | High vibration, monitoring |

It can be seen that most of the overview guidewords are focused towards hazard identification rather than operability, which is covered by the parametric deviation guidewords. Static electricity impacts are discussed by Pratt and Atharton (1995) and Astbury and Harper (2001), and Pavey (2004).

### 4.4.3.3 How to make a HAZOP study effective?

The HAZOP study is considered the single most important safety study in a process plant's life. Things missed in a HAZOP or a HAZOP not performed, often come back to haunt in the form of incidents and near misses. A number of case studies have been cited (Ender and Laird 2003, Kletz 1994, Sanders and Spier 1996, Riezel 2002, Gustin 2002). The HAZOP report is also difficult to audit in terms of completeness, unless there have been blatant errors of omission, which are not expected of a competent team.

A workshop conducted by the IChemE Safety and Loss Prevention Group (Turner 1996) found the following:

- 71% said that an industry HAZOP standard for defining hazard study quality was necessary.
- 68% said that they would use a 'lessons learned' database as part of the HAZOP, if one was available.
- An audit trail of the HAZOP process was considered essential in the documentation.
- Computerised recording of HAZOP and follow-up of actions was very much preferred.

McKelvey (1988) has identified six problem areas for failure of a HAZOP.

a) Lack of experience (leader and/or team)
b) Failure to communicate (loss of organisational memory)
c) Management of shortcomings (key people availability, lack of continuity, lack of commitment)
d) Complacency and poor loss prevention practices ("we have operated this way for several years without incidents" syndrome)
e) Shortage of technical information (e.g. you cannot conduct an effective HAZOP of a reaction system without information on reaction kinetics and reactivity hazards)
f) The ultimate limitation: tired human beings with brains stretched and loss of concentration.

A number of hints are offered below in ensuring that the HAZOP process is effective, and reasonably complete. One can never state with absolute certainty that all hazards have been identified.

1. Ideally, select an experienced facilitator, with an understanding of the process in question, process design experience, familiarity with layers of protection assessment, and operational experience. Not all persons who have merely attended a training course as a HAZOP facilitator can actually lead a HAZOP effectively.
2. Select the correct and compact team composition. For new facilities, minimum full time presence of the process designer, project engineer, instruments/control system engineer, operations representative, and safety representative is necessary. Personnel from other disciplines and vendor

representatives may be called into the session on an as needed basis. For an existing facility, it is also necessary to have a maintenance representative, and experienced operator or plant supervisor. The HAZOP minutes secretary (scribe) must be a technical person, and be under the direct guidance of the facilitator.

3. Have the right support documentation. Minimum data requirements are: design basis, process description, layout and general arrangement drawings, P&IDs, equipment register with design specifications, instruments register with alarm and trip settings, relief valve capacity and settings, instruments cause & effects diagrams, hazardous area classification drawings, manuals of vendor packages, and operations/maintenance manuals (for operating plants), hazardous properties of materials and information on reactivity hazards.
4. Prior to commencement of HAZOP sessions, conduct a search of accident databases (see Chapter 3 for a list of databases available) and compile a 'lessons learnt' dossier relevant to the process being examined. Its value has been stressed by Mannken (2001) and also recognised in the survey by IChemE (Turner 1996).
5. The leader should explain at the outset that there will be questions to stimulate the thinking, that the design and operating practices may be challenged, and that there is no need for a defensive response from the process design or operations representative. No incompetence on their part was implied, but the discussion would result in better understanding of the design and operation by all concerned.
6. If an issue is not resolved within 5–10 minutes of discussion, document an action for review outside the HAZOP session. If additional protection is required, record the intent. *Do not design.*
7. Make sure that the consequence of the deviation is pushed to the stage of operator response and examine the transients to determine if another layer of protection would be required. Once again, do not design.
8. Do not skip a guideword on the grounds of familiarity. Remember that HAZOP always has hidden surprises. Conversely, additional guidewords may be used, if found necessary, for a given situation.
9. In the early days of HAZOP, the documentation was by exception, meaning that if there is no hazard identified for a deviation, it was not recorded. In recent times, the importance of an audit trail has been recognised, especially when the HAZOP report becomes a document in evidence in legal proceedings. Therefore, make sure that all guidewords are documented, and in the case of no hazards, add a comment that 'no hazard identified' for the sake of completeness.
10. The general principles of group dynamics, managing a brainstorming team, having regular breaks to keep the brain cool apply. They are not elaborated here.

### EXAMPLE 4-6 HAZOP METHOD ILLUSTRATED

A large petrochemical facility has an ammonia plant and other downstream plants that use the anhydrous ammonia as the intermediate for other products. One of the downstream plants is located 800m from the main ammonia storage spheres.

An ammonia storage bullet at the downstream plant is used for receiving, storing and distributing ammonia. The day tank is fitted with a local level gauge, a level transmitter indicating the level at the central control room 800m away, with level alarm high, and an independent high high level alarm, to sound in the control room.

The transfer procedure is for the field operator to inform the control room operator, open a manual isolation valve to transfer ammonia to the day tank (the pump at the ammonia sphere is always on as ammonia is also supplied to other users on the site), watch the local level gauge, and close the valve when the desired level is reached. Should the high level alarm sound in the control room, the control room operator is to contact the field operator by radio and ask that the transfer be stopped.

A schematic of the P&I diagram is shown in Figure 4-11.

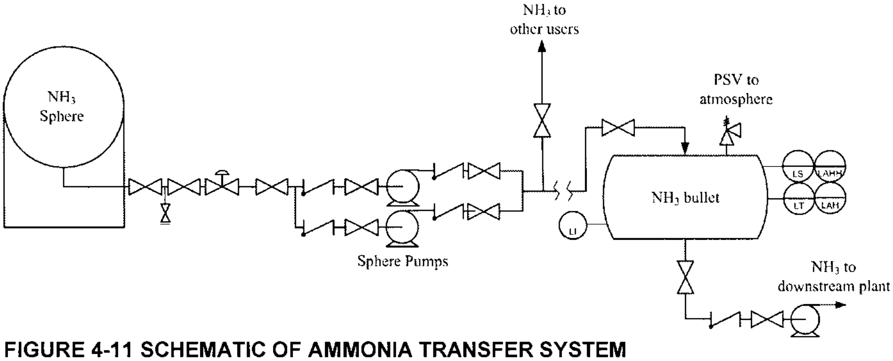


**FIGURE 4-11 SCHEMATIC OF AMMONIA TRANSFER SYSTEM**

The HAZOP documentation for the main transfer line is shown in Table 4-10. Only a partial list is shown, illustrating the technique.

Entries 7 and 8 indicate that there is clearly a problem. There is no mechanism to resolve the conflict between local gauge indication and control room level indication. There is no clear operating instruction for the field operator that he cannot ignore a request from the control room, regardless of which instrument is faulty, as this is a fail safe action.

If we view this from a layer of protection analysis point of view, the existing procedure covers up to Level 3 (Chapter 3, Section 3.3). The action arising in Entry 8 is necessary because of the severity of the consequences, taking it to Layer 4 (safety instrumented system).

TABLE 4-10 HAZOP DOCUMENTATION FOR AMMONIA TRANSFER

| HAZOP STUDY | | | |
|---|---|---|---|
| **ct No:** | Ammonia system upgrade | **System:** | Ammonia transfer to day tank |
| | | **Present:** | List attendees, Leader and Scribe |
| **No:** | | **Line No:** | |
| **No:** | | **Line description:** | Transfer line from $NH_3$ sphere to day tank |

| Guideword | Causes | Consequences | Safeguards | Action | Responsible |
|---|---|---|---|---|---|
| High Flow | Pump overspeed<br>Changes in hydraulics with less flow to other users | Faster filling of day tank | Operator present during transfer<br>Level gauge watched continually | – | |
| Low Flow | Pump cavitation<br>More draw off from other users | Longer duration to fill day tank | Operator present during transfer<br>Level gauge watched continually<br>Radio communication with control room | – | |
| Low Flow | Leak from transfer line | Ammonia release to atmosphere, toxic impact | Underground line, protected from impact<br>Line corrosion protected<br>Manual detection by personnel on site<br>Emergency response procedures | Review the mechanical integrity program for transfer pipeline | Engineering |

| Guideword | Causes | Consequences | Safeguards | Action | Responsible |
|---|---|---|---|---|---|
| No flow | Pump failure | No product transfer.<br>Downstream plant affected due to lack of feed. | Preventive maintenance.<br>Standby pump installed.<br>Procedure ensures sufficient inventory in day tank to supply downstream plant when transfer commences | Consider LAL on day tank | |
| No flow | Blocked isolation valve | Pump may operate against closed valve if other users not taking product. Seal damage and ammonia release. | Valve line up checked by operator as part of transfer procedure.<br>Operator in attendance during transfer and communicates with control room if no increase in level noted. | – | |
| No flow | Line rupture | Ammonia release to atmosphere, toxic impact | See "Low Flow" – Entry No.3. | | |
| High Level | Faulty level gauge.<br>Operator fails to shut valve. | Vessel overfill and overpressurised.<br>Atmospheric release of ammonia through PSV.<br>Toxic cloud impact onsite and offsite. | LAH in control room<br>Control room operator in radio contact with field operator asking to shut transfer valve. | Review maintenance and calibration check on local level gauge. | Maintenance |

| Guideword | Causes | Consequences | Safeguards | Action | Responsible |
|---|---|---|---|---|---|
| Instruments and controls | Level gauge reads low. Conflict between local level gauge and level transmitter. Field operator trusts local indication (Human error of over-riding control room instruction) | Vessel overfill and overpressurised. Atmospheric release of ammonia through PSV. Toxic cloud impact onsite and offsite. | Independent LAHH in control room.<br>Control room operator in radio contact with field operator (which may not occur, as control room operator has already done so when LAH was raised) | Install actuated valve on transfer line and automatic shutoff initiated by LAHH.<br>Include the interlock in function testing schedule<br>Update transfer procedure and re-train operator | Engineering<br>Maintenance<br>Operations |

*Note:* This example was taken from a real life incident. The level gauge was faulty, there was tank overfill, control room operator radioed the field or, who ignored it, deciding to trust the local instrument, independent high high alarm was raised, but control room operator did not call the field or again on the belief that this has been done already, and action would be taken (human error, misunderstanding, communication failure). PSV rge occurred, and emergency response was activated. It was interesting to note that the television crew from the local TV network was the first on the ahead of the external emergency services! Fortunately no one was hurt.

#### 4.4.3.4 Benefits of HAZOP

The HAZOP technique offers a number of benefits and it is hardly surprising that it is the most widely used tool for identification of hazards and operability problems in the process industry.

1. The multidisciplinary approach helps identify a whole range of issues (safety, operations, maintenance, design, construction)
2. It is a powerful medium of communication of the designer's intent to the operations personnel, and helps to accommodate operational requirements at design stage
3. It identifies both linear and complex interactions between various subsystems in the system, and between systems, and functions
4. It highlights hazardous events that could occur from a combination of causes (complex interactions) and provides input for detailed hazard analysis.
5. For new projects and extensions to existing plants, the review is conducted on paper before the design is complete and hence offers the flexibility to make the necessary design changes.
6. It provides for smooth commissioning of the plant and equipment, and continued smooth operation thereafter, avoiding costly shutdowns and modifications at a later stage.
7. When a HAZOP study is conducted on an operating plant, it reveals not only the appropriate action to be taken to prevent a recurrence of previous incidents that may have occurred, but also a whole range of other actions to prevent potential incidents that may not have occurred.
8. The HAZOP study can be used to define operating limits and safety limits (upper and lower bounds) on critical operating parameters such as temperature and pressure (De la Cruz-Guerra and Cruz-Gomez 2002). Defining the operating and safety limits is a specific requirement of process safety management in many regulations (e.g. OSHA 1992, Queensland Government 2001).

The CHA technique, properly used, can address loss of containment issues and issues related to failures of utilities better than the overview guidewords in HAZOP, as causes of these are also investigated. In some instances, the combination of HAZOP for P&ID line by line review, and CHA for the overview provides a powerful hazard identification tool. If this approach is used, one should make sure that the CHA keywords incorporate all the HAZOP overview guidewords.

It should be appreciated that some process information related to abnormal situations may not be known and may not be spotted during the HAZOP, despite the skills of the HAZOP team, if the abnormal situation had not been experienced before, and was not within the skill set of the team. In these cases the Process Hazards Matrix is a good tool, as it covers all possible interactions between chemicals, materials of construction, utilities and the environment.

### 4.4.4 Computer Hazard and Operability Study

When the HAZOP technique was developed and found application in the chemical process industry, plant control system designs were relatively simple and consisted of mainly analog devices, with limited logic capabilities. The HAZOP study did not address the root cause of deviations, some of which are attributable to malfunction or failure of programmable electronic systems (PES).

This inadequacy of HAZOP became apparent when the failure of one of the computers controlling a polymerisation reaction failed, resulting in a total uncontrolled plant shutdown, and loss of containment of 3 tonnes of molten polymer at 300°C, under nitrogen pressure of 27 bar. An investigation led to the need for a HAZOP type study of PES (Nimmo et al. 1987). Literature on safety awareness and hazard identification of PES have been sparse (Andow 1991; Jones 1989,1991; Burns and Pitblado 1993; Broomfield and Chung 1994). With an increasing trend in the knowledge based systems approach, the identification of hazards from PES failures is becoming critical, especially in the processes handling hazardous chemicals, and in nuclear and defence systems applications.

The term computer HAZOP or CHAZOP was given to application of the HAZOP method for PES. CHAZOP may be viewed as an extension of HAZOP to root cause level in that, in HAZOP we stop with the deviation being a control loop failure (high, low or none), whereas in CHAZOP, we extend this failure to its causes in the PES.

There are two basic approaches to CHAZOP, the traditional checklist/guideword method of HAZOP and task analysis method (Raman and Sylvester, 2001).

#### *4.4.4.1 Checklist guideword method*

This method is the logical evolution of the traditional HAZOP method, where the review is by a multi-disciplinary team, but the focus is on PES. The scope of the study covers both hardware and software aspects of the computer control system.

Typical guidewords are NO, MORE, PART OF, OTHER THAN, EARLY, LATE, BEFORE and AFTER (Ministry of Defence UK 2000a,b). Variations of these guidewords are implicitly included.

These guidewords are applied to the following:

- Communications (data signals)
- Digital hardware (processor, I/O)
- Mechanical items (mainly origin and destination items in the control loop – e.g. sensors and interlock valves).

The Ministry of Defence standard (2000b) clearly states that the study focus is on interactions only. Components in detail may be considered only if an understanding of their failure modes is essential to the assessment of deviations from design intent or interconnections. It is necessary to develop specific guideword lists for each study.

The main information required for CHAZOP are:

- SIS loop diagrams or block diagrams or flow charts
- Electrical circuit diagrams where relevant
- Instrument cause and effect charts and
- P&I diagrams for identifying the process consequences of deviations in PES.

A set of suggested guidewords is shown in Table 4-11.

TABLE 4-11 SUGGESTED GUIDEWORDS FOR CHAZOP STUDY

| **Deviation Guideword** | **Interacting subsystem** |
|---|---|
| | *Communication* |
| No | Signal (zero read, full scale read) |
| More | More current. Erratic signal. |
| Part of | Incomplete signal |
| Other than | Excessive noise. Corrupt signal. |
| Early | Signal generated too early (timer problems) |
| Late | Signal generated too late |
| Before/After | Incorrect signal sequence |
| | *Digital hardware* |
| No | I/O failure |
| More | Multiple failure (control card, processor rack, processor) |
| Part of | Partial failure of card, failure of counters |
| Other than | Abnormal temperature, dust |
| | *Software* |
| No | Program corruption |
| More | Memory overflow |
| Part of | Addressing errors/data failure |
| Other than | Endless loops, data validation problems, operator override |
| Early/Late | Timeout failure, sequence control problems, sequence interpretation error |

Mechanical items such as sensors and end devices in SIS are often covered in the HAZOP itself, as these are integral to the P&ID.

### 4.4.4.2 Task analysis method

In contrast to the checklist/guideword method, the task analysis method (Broomfield and Chung 1994) is at system component level. The focus is on the function of the hardware/software interface.

There are four functional levels: intervention, input/output (I/O), communication, control and processing. Associated with each level are system components, and corresponding tasks for each component. It also accounts for human error in the analysis.

The method is different to HAZOP and has more similarities with FMEA, where the failure of the components and/or associated tasks is examined by turn, with its impact on the system/process and identification of prevention/remedial measures.

CHAZOP has been successfully applied in highly automated and normally unmanned facilities where reliability and online time is critical, e.g. water and wastewater treatment, gas compression and transmission pipelines, processes requiring complex sequence control, interconnected process plants, and plants with complex startup/shutdown systems and interlocks.

### 4.4.5 Identification of Chemical Reactivity Hazards

The CHA and HAZOP methods refer to chemical reactivity and reactions in the checklist of guidewords, but do not offer a systematic procedure for identifying chemical reactivity hazards. Where the process hazard identification matrix identifies that there is a potential for chemical interactions, as part of a comprehensive hazard identification, the reactivity hazards need to be identified.

A chemical reactivity hazard is a situation with the *potential* for an *uncontrolled chemical reaction* that can result directly or indirectly in serious harm to people, property or the environment (Johnson et al. 2003; Johnson and Lodal 2003). The authors provide a simple screening method to determine if chemical reactivity hazards exist in a process facility. The reactive hazard exists if:

- chemical reactions are intentionally carried out (other than fuel combustion in air)
- there is heat generation in mixing or other physical processing of different substances
- any substance stored or handled is
    - spontaneously combustible (pyrophoric, UN Hazard Class 4.2 material for shipping purposes)
    - peroxide forming
    - reacts with water (UN Hazard Class 4.3 material)
    - oxidising agent (UN Hazard Class 2.2 – compressed oxygen, Class 2.3, Class 5 materials)
    - self-reactive (polymerising, decomposing, rearranging). These include UN Hazard Class 1 (explosives), Class 5.2 (organic peroxides), a range of monomers
- there is potential for incompatible materials coming into contact causing undesired consequences

The classical work of Bretherick (Urben 1999) provides the most extensive compilation of reactive chemical hazards. The reactivity matrix described is similar to the process hazard identification matrix described above. A worksheet for constructing the chemical reactivity hazard matrix can be found in the website http://response.restoration.noaa.gov/chemaids/react.html.

Once a reactive hazard is identified, it is included as a potential hazardous event in the compilation of hazards.

### 4.4.6 Scenario Based Hazard Identification

We have seen that techniques like FMECA and the HAZOP study are useful in identifying deviations from intended operation. Many deviations would result in only operability problems and not hazards. In fact, it is not easy to address major hazards using the HAZOP/FMEA techniques alone. It is possible to miss hazardous scenarios because the possibility of adverse consequences is not always apparent in the deviation (Baybutt 2003).

If the objective is to identify only *major hazards*, then scenario based hazard identification offers a cost and resource effective tool, especially for loss of containment scenarios as initiating events.

The following steps are adopted.

1. Divide the plant into isolatable inventories. By "isolatable" we mean, one inventory can be separated from another by actuated shutdown valves.
2. Consider one inventory at a time, and brainstorm and list all issues associated with safety, operations and related-environmental impact. A checklist, similar to the one for 'what if' analysis may be used, but this is essentially for prompting the brainstorming, and should not be considered exhaustive. The focus is largely on loss of containment hazards. Process deviations are not generally considered here as this would be addressed in a HAZOP study separately.
   Some of the issues may be causes (e.g. a gasket failure and leak), some may be consequences (e.g. gas jet fire), some may be detection systems (e.g. fire and gas detectors), and some may be protection systems (e.g. deluge system, ESD). At the brainstorming stage, no distinction is made.
3. An issue is selected and a major hazard scenario is constructed out of it. If a scenario cannot be constructed, the issue is not considered relevant for safety. In constructing a scenario, others issues are implicitly absorbed. For example if the issue is small bore pipework failure, the associated listings could be vibration, impact, corrosion, jet fire, impingement/engulfment etc. In other words, in constructing a hazardous scenario, the initiating events, intermediate events, other enabling events and consequences are picked out of the generated list.
4. Construct a table to include the following record, one for each scenario:
   - scenario description;
   - causes (initiating, intermediate, enabling)
   - consequences; and
   - existing control measures (prevention and mitigation measures, hardware and procedural).
5. Repeat steps 3 and 4 until all issues are exhausted.
6. Repeat steps 2 to 5 until all isolatable inventories are covered.

It is also possible to allocate severity and likelihood scores for the event and assess the risk using the risk matrix.

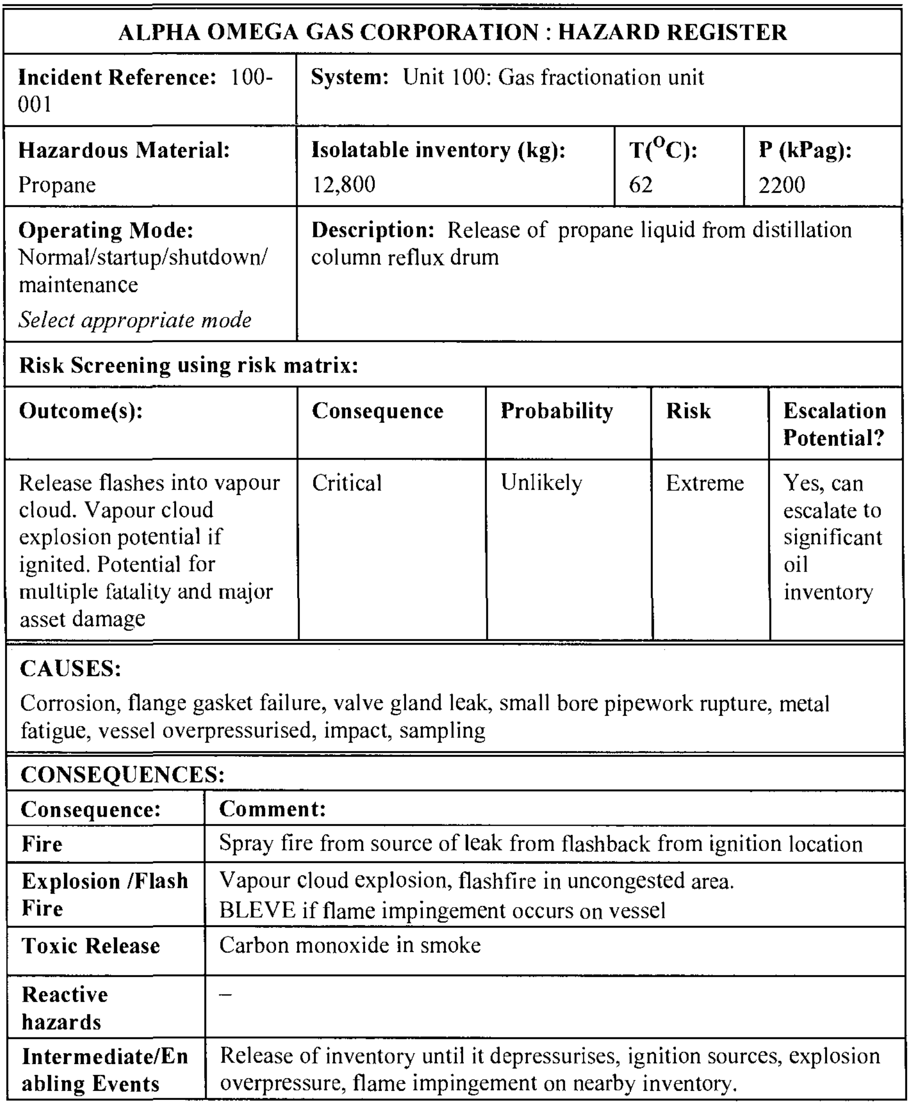
Similar to HAZOP, the study is conducted in a multi-disciplinary workshop. A review of previous incidents from accident databases is necessary to make this process effective. As always, the knowledge and experience of the facilitator is crucial to the success of this method.

It has been our experience that a combination of scenario based hazard identification (which feeds into safety analysis studies), and the HAZOP study for process deviations and reliability management provide a very effective approach in hazard identification. This can be supplemented by AEA for human error aspects.

### 4.4.7 Development of the Hazard Register

All incident scenarios developed using any of the hazard identification techniques above may be entered into hazard register sheets, which are compiled into an electronic hazard register. The hazard register forms the basis of all subsequent hazard evaluations and safety assessments, and is continually updated during the facility life cycle, starting from the risk reduction measure incorporated into the design to changes in the plant, processes and procedures during the plant life.

A pro forma example of a hazard register sheet is shown in Figure 4-12. Instructions on how to complete the register in the safety hardware column and references section are given in italics. Many companies have intranet based hazard registers accessible to personnel across the corporation.



| ALPHA OMEGA GAS CORPORATION : HAZARD REGISTER | | | |
|---|---|---|---|
| **Incident Reference:** 100-001 | **System:** Unit 100: Gas fractionation unit | | |
| **Hazardous Material:**<br>Propane | **Isolatable inventory (kg):**<br>12,800 | **T($^{o}$C):**<br>62 | **P (kPag):**<br>2200 |
| **Operating Mode:**<br>Normal/startup/shutdown/ maintenance<br>*Select appropriate mode* | **Description:** Release of propane liquid from distillation column reflux drum | | |

| Risk Screening using risk matrix: | | | | |
|---|---|---|---|---|
| **Outcome(s):** | **Consequence** | **Probability** | **Risk** | **Escalation Potential?** |
| Release flashes into vapour cloud. Vapour cloud explosion potential if ignited. Potential for multiple fatality and major asset damage | Critical | Unlikely | Extreme | Yes, can escalate to significant oil inventory |

| CAUSES: |
|---|
| Corrosion, flange gasket failure, valve gland leak, small bore pipework rupture, metal fatigue, vessel overpressurised, impact, sampling |

| CONSEQUENCES: | |
|---|---|
| **Consequence:** | **Comment:** |
| **Fire** | Spray fire from source of leak from flashback from ignition location |
| **Explosion /Flash Fire** | Vapour cloud explosion, flashfire in uncongested area.<br>BLEVE if flame impingement occurs on vessel |
| **Toxic Release** | Carbon monoxide in smoke |
| **Reactive hazards** | – |
| **Intermediate/Enabling Events** | Release of inventory until it depressurises, ignition sources, explosion overpressure, flame impingement on nearby inventory. |

| **PREVENTION/MITIGATION SYSTEMS:** | |
|---|---|
| **System:** | **Comment:** |
| **Hardware** | Gas detection and alarm, emergency shutdown valves (isolates inventory), PSV to flare, depressuring valve to flare manually actuated from control room, automatic deluge on reflux drum, control of ignition sources (classified hazardous area and electrical equipment/instruments to conform).<br>*List tag numbers, identify if hardware safety critical.* |
| **Procedures** | Mechanical integrity inspections, PSV service, gas detector calibration, function testing of shutdown/depressuring valves |
| **REFERENCES:** *Make reference all SMS procedures that maintain the integrity of the safety critical systems in the hardware.* | |

FIGURE 4-12 EXAMPLE OF HAZARD REGISTER SHEET

### 4.4.8 Documentation and Software Systems

There are a number of software systems for documentation and reporting of workshop sessions on FMEA, HAZOP or hazard identification. These are useful in processing the minutes of the workshops and report compilation. Action sheets can be generated and distributed to those responsible for implementation. These software are essentially database tools, and do not perform any expert function.

There have been recent attempts to develop expert systems for hazard identification and HAZOP. Freeman et al. (1992) describe the expert application for HAZOP planning that has resulted in significant saving in manpower resources.

Vaidhyanathan et al. (1996) and McCoy et al. (1999 a,b,c; 2000,a,b) have described ambitious software systems, designed to perform at least 60% of the HAZOP and hazard identification (HAZlD) study functions. There is no commercially available expert system software for conducting hazard identification studies. None of these systems claim to replace the role of an experienced team in effective hazard identification, but facilitate this role.

## 4.5 QUALITY AND COMPLETENESS OF STUDIES

### 4.5.1 Comparison of Capabilities of Hazard Identification Models

The questions often asked by consulting practitioners and corporations alike are:

1. How do we know that a hazard identification study is complete and that we have identified all hazards (or have we)?
2. What is the most appropriate hazard identification tool for a given application?

The answer to the first question is – we don't (Taylor 1981). We can never state with certainty that *all* hazards have been identified. However, given the right hazard identification technique, and an experienced team, and effective use of literature data, we can say that almost all major hazards, and more than 90% of minor hazards have been identified. The state of the art has been evolving continually, especially the use of accident analysis information and lessons learnt.

This brings us to the second question. Almost all techniques use incident scenarios as their primary model. However, none of them cover all incident scenarios in their entirety, but cover only one part at any time (Wells et al. 1992).

An overview summary of the hazard identification models and their capabilities are given in Table 4-12.

TABLE 4-12 SUMMARY OF HAZARD IDENTIFICATION MODEL CAPABILITIES

| Identification method | Capability and limitations |
|---|---|
| Checklists | Best suited for compliance review of design with codes and standards, and in auditing.<br>Best suited for simple processes<br>Provides a basis for other hazard identification techniques, but in itself cannot identify hazards fully except in small systems with predominantly linear interactions.<br>Quality and completeness of the checklist is critical for success. |
| Process hazard identification matrix | This simple tool goes a long way in giving a preliminary outline of all the hazards and related issues. Identifies all the potential interactions between materials, processes, people and the environment.<br>Very useful in small systems, but can become tedious in large systems due to the size of the matrix, especially with no entry in many cells when there are no interactions. Necessary even for large systems if the process details are not adequately known.<br>Useful first pass technique, especially at the early stage of a new project. Since it is not scenario based, the output should be used for next level of analysis where scenario based techniques can be used for developing specific prevention/protection measures.<br>This method is not suitable for all life-cycle stages of a facility, but mainly at design stage, with some application to operating facility that had not been subjected to formal hazard identification procedure.<br>Useful for identifying chemical reactivity hazards. |
| "What-if" analysis | Check list based. Success of the method depends on how good the checklist is. Items not in the checklist could be missed.<br>Takes the checklist one level further to scenario development. Not as structured as CHA, FMEA or HAZOP. Suitable for small systems. Difficult to identify dependent failures and complex interactions using this technique. Can be used to examine the effectiveness of a HAZOP search. |
| CHA | Versatile because of functional modelling approach. Can be used for all types of processes, operations, and industries.<br>Can be used at the flowsheet stage of a project to identify principal hazards, and use the information for selection of optimum solution and P&ID development.<br>Better suited to task oriented operations and man-machine interactions, and non-flow processes where classical HAZOP technique is not suitable. |

| Identification method | Capability and limitations |
|---|---|
| FMEA/FMECA | Similar to the CHA, this technique can be applied universally in every situation, as it follows the sequence "Physical object –> Failure modes –> Event scenario chain".<br>The focus is on physical systems, and therefore this technique needs to be combined with a task analysis (human factors) technique such as Action Error Analysis, to be complete.<br>Identification of failure modes implicitly leads to root cause failures, which are not identified in a HAZOP. It is a time-consuming process, but not as resource-intensive as HAZOP. Needs specialist input from outside the analysis team.<br>The assignment of criticality, though time consuming, can eliminate trivial failure modes, so that attention can be focused on critical failures.<br>FMEA is more suitable for non-reactive systems. Different methods are required for identification of chemical reaction hazards.<br>FMEA is highly suited to hazard identification of programmable electronic systems, where none of the other techniques are capable. The CHAZOP technique is an adaptation of both HAZOP and FMEA techniques. |
| HAZOP | Excellent for identifying process deviations, immediate causes and immediate consequences. Needs to be used in conjunction with another method for identification of major hazards, focused on loss of containment. Significantly team experience dependent, resource-intensive.<br>Highly suitable for flow processes.<br>Capable of handling large systems as it uses discretisation and a physical model of the process, along with simple guidewords.<br>Problems in applying classical method for task oriented operations and man-machine interactions. Does not identify root causes of deviations, and all the consequences in the chain of events. |
| CHAZOP | Complements the HAZOP study by evaluating programmable electronic systems. Highly useful for sequence control systems involving reactive chemical hazards, normally unmanned operations where high reliability and online time is required, and where complex interlocks and their sequence is critical for safety. |
| Scenario based hazard identification | Highly useful for identification of major hazards, and works well as a complement to HAZOP/FMEA. By itself, is not suitable for identification of process deviations.<br>Can be used for large systems, as the system is discretised into isolatable inventories.<br>This method is also useful in hazard identification of sequential manual operations, e.g. construction and installation, drilling, maintenance. |
| Action Error Analysis | Useful tool for human error analysis. Task oriented. Uses FMEA principles, but applies to task analysis. Forms a useful adjunct to any of the above hazard identification tools, which do not effectively consider human factors. Output can be directly used for deciding level of automation required, development of procedures, and operator training. |

The main points to note are:

- No single technique is capable of covering all the life cycle stages. Different techniques would be required for different stages.
- No single technique is capable of covering the design and operational stages fully. More than one technique would need to be used for comprehensive hazard identification.

All the techniques require a knowledge base, plant-specific experience, and depend on the skill and experience of the hazard identification team, which is crucial for a successful outcome.

### 4.5.2 Socio-Technical Factors in Identification of Root Causes

If a hazard identification study is undertaken not as part of a design, but as part of an accident investigation, an interesting question arises: How do we know we have identified the root causes, and how far along the causal chain should one go? When a human error is cited as a contributory factor, shall we stop with general management system failure, gaps in supervisory or maintenance procedures (Reason 1997)?

According to Rasmussen (1990), we need *stop* rules, to lead us along the causal path towards root causes. A review of past accident investigation reports reveals that the stop rule has been applied when an error or an unsafe act on the part of an operator or maintenance personnel has been identified. In some instances, the reasons for the error were not investigated, which can be linked to socio-technical factors in the organisation such as organisational culture and climate, level of training received at ground level, effectiveness of internal auditing of the safety management system (SMS), feedback and control by management (Hopkins 2000).

Figure 4-13 summarises the underlying socio-technical causes of accidents.

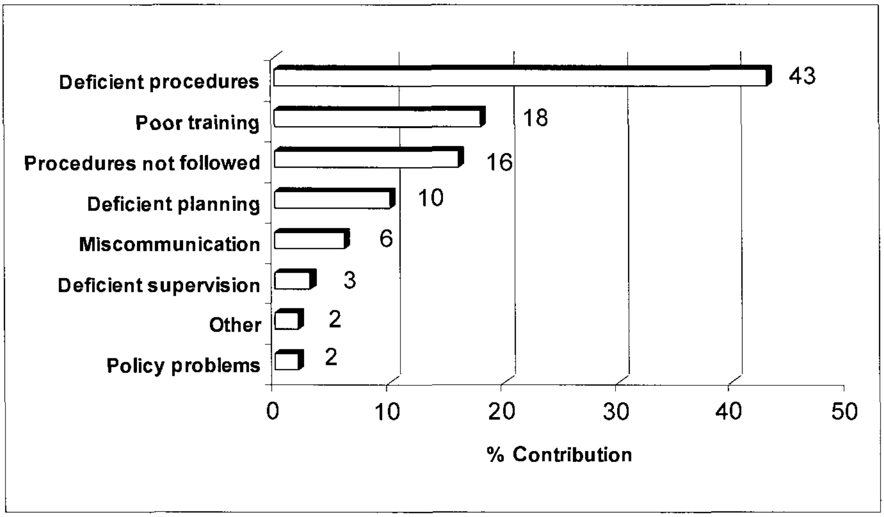


FIGURE 4-13 SOCIO-TECHNICAL FACTORS CONTRIBUTION TO ACCIDENTS (DATA SOURCE: LARDNER AND FLEMING 1999).

Wells et al. (1994) identified the need for evaluation of socio-technical factors as part of overall process safety reviews. The analysis is similar to the CHA (see Section 4.4.1), but uses a different set of keywords under the following main headings:

- External systems (Government and industrial bodies, contractors/consultants, external emergency facilities, general public)
- Organisational climate, corporate safety culture, local culture
- Organisation and management control
- Communications and information
- Procedures and practices
- Working environment
- Operator performance (recruitment, training, capability, morale, attitude, aptitude)

There are a number of elements within each of the factors. Some are given by Wells et al. (1994) and others can be brainstormed. One or more of the above factors can form the root causes. To apply the stop rule to the last of those (operator performance) could mean missing out on tackling root causes, which could resurface again.

### 4.5.3 Hazard Identification for Facility Life Cycle

Much of the discussion in the preceding sections had focused on the design and operational stages of the facility life cycle. However hazard identification does not stop with the design and operational stages. It needs to be continued into all phases of life cycle if process risks have to be effectively managed.

The following sections cover the other stages of facility life cycle, not discussed hitherto.

#### *4.5.3.1 Construction/installation stage*

Three techniques are useful for this stage.

a) Concept hazard analysis
b) Scenario based hazard identification of construction sequence
c) FMEA of the construction sequence, including action error analysis

It has been our experience that the combination of (a) and (b) provides a better outcome, especially if an incorrect installation (e.g. structural alignment) in one step in the sequence could carry forward the problem to subsequent steps.

The process safety focus is directed towards the mechanical integrity of the installation, and quality assurance (QA) of onsite fabrication and inspection plays a major role (e.g. correctness of welding rods, qualification of welder). The items of importance in installation are the lifting capability of cranes, prevention of dropped load, structural alignment in modular construction, identification and rectification of damage to skid mounted modular assembly during transport etc. A team brainstorming of issues by the project representatives and construction contractor is necessary, using an initial checklist as a thought stimulating guide.

If the construction is related to an extension to the operating plant, and operation continues until the newly constructed extension is ready for tie-in, there are interaction hazards relating to simultaneous operations like production and construction that need to be considered.

To the above should be added the issues related to management of contractor safety (Whitaker 1993).

### 4.5.3.2 Commissioning stage

Modern projects tend to follow the fast-tracking process. There is significant time pressure to reduce the duration of design and construction, so that commissioning and operations can commence. There are also penalty clauses in the contact, which places additional burden on the part of the contractor.

If the design stage had been managed properly with respect to process safety, one can expect commissioning to the smooth. Unfortunately, the same mistakes are repeated, and many problems get pushed to the commissioning stage.

The main problems at commissioning are:

- Unlike process plant operation, which is a steady state process in continuous operating mode, commissioning is a transient process. The process conditions change with time until steady state is established. They can be unpredictable if new technology is involved.
- Different process modules may be designed and commissioned by different vendors. The operating modules interfaces must be synchronised to achieve smooth commissioning.
- If the process is new, operators are unfamiliar with the operation, though they may have had previous experience in the process industry.
- Sufficient thought is to be given at design stage as to how the pressure testing of the plant will be carried out in situ (medium of pressure testing, provision for pressurisation, venting and draining, structural overload potential in the case of full load hydraulic test.
- It is not uncommon to see one plant section commissioned and operating, storing or flaring the intermediate, while a second plant section is being commissioned, and construction is still incomplete on a third plant section.
- There is significant potential for human error during this stage, diagnostic error in an unfamiliar process, operator/control system interfaces, communication failures, incorrect process isolation resulting exposure of personnel in other plant areas to process materials, spurious trips, aborted start up, and so on.

There have been suggestions that a multilevel HAZOP study could be applied at commissioning stage, the operator level, the control system level and the plant/process level. Variations to the deviation guidewords are used (Cagno et al. 2002).

The HAZOP approach or a concept hazard analysis for each step of the commissioning sequence, integrated with a FMEA/task analysis of operator roles would be useful. This can be supplemented by a scenario based hazard identification for identification of major hazards during commissioning.

Brainstorming by the project and operations team from the client and commissioning representatives from the contractor, facilitated by an experienced facilitator with commissioning experience (similar to a HAZOP facilitator) produces good results.

It is necessary to undertake this work at the early stages of construction and installation, so that preparation for commissioning can proceed concurrently. The documentation is similar to the scenario based hazard identification table (Item 4 in Section 4.4.6).

### 4.5.3.3 Decommissioning stage

Decommissioning is normally defined as the shutdown of a facility in order to prepare for complete demolition. Part of the equipment recovered may be reused elsewhere after refurbishment, depending on the condition. The term 'decommissioning' is normally used for onshore process facilities. The same activity is referred to as 'abandonment' in the offshore oil and gas industry, and 'closure' in the mining industry.

The hazard identification is conducted on a developed decommissioning plan, with sequence of steps well defined. The initial review is on the correctness of the sequence. For example, if the decommissioning is for the whole site, utilities such as steam and power would be required till the decommissioning is complete and the equipment is ready for demolition. Therefore, utilities are the last systems to be decommissioned on the site.

The CHA technique or the scenario based hazard identification are suitable, and are applied to each of the decommissioning steps. Some keywords are listed in Table 4-13 as a guide. Additional keywords should be brainstormed for the occasion. Some useful tips are provided by Phillips (2002).

**TABLE 4-13 KEYWORDS FOR DECOMMISSIONING HAZARD IDENTIFICATION**

| Keyword | Possible problems |
|---|---|
| Draining/Purging | Pressurised medium, vacuum from steam cleaning, drain/purge discharge location, exposure, permit to work, isolation, communication |
| Chemicals | Residual chemicals left in equipment and pipework – flammable, toxic, pyrophoric residues, corrosion products |
| Sampling | Means of sampling for completeness of decontamination |
| Simultaneous operations | Impact on other operating plants when one plant on the site is decommissioned. Potential for re-contamination of decontaminated areas. |
| Electrical hazards | Excavation of cables, live equipment, isolation |
| Human factors | Training, communication, emergency preparedness, labelling and signposting, preventing demolition access to live areas |
| Third party management | Contractors on site (can be several), coordination, consistency of procedures |
| Waste disposal | Temporary storage, means of disposal, transport |

| Keyword | Possible problems |
|---|---|
| Mechanical handling | Crane operations, access, lifting, dropped loads, impact, communications, prevention of access to operating areas. |
| Underground tanks and pipes | Excavation and removal. Dust exposure, interference with live cables and utilities. |
| Environmental | Environmental impacts, runoff to surface water or marine environment, contaminated land. |
| Regulatory | Approvals, compliance |

Hicks et al (2000) describe the need for accounting for decommissioning at the design stage from several points view, chief among which are:

- sustainability and ecological integrity
- regulatory requirements (full life cycle to be considered at design stage)
- business and financial dimension (life cycle costs, business risk). Between 4 and 8% of the asset value is allocated for capital cost of decommissioning for the petroleum and mining industries, and up to 25% for the nuclear industry.

### 4.5.4 Quality Control Procedures

It is essential that a quality control process be in place to ensure the integrity of hazard identification (Rouhiainen, 1990). Main features are:

- Selection criteria for workshop team members. It should be multi-disciplinary and must have an experienced representative from client operations.
- Selection criteria for hazard identification workshop facilitator, depending on the identification method chosen. The HAZOP facilitator is to be independent of the design team, especially for new facilities and major extensions to existing facilities.
- Agreed documentation. This is ensured by online minute taking and projecting the computer screen on a larger screen for viewing by team members.
- Traceability of documentation. Cross-referencing of equipment and instrument tag numbers, P&ID number and line number, and the minute number that gave rise to an action.
- It is not uncommon to have a representative from the regulator as observer for part of the workshop duration, especially in environmentally sensitive projects under the public gaze. Sometimes the regulator may require an independent observer, or insist on approving the credentials of the nominated facilitator.

### 4.5.5 Uncertainty in Hazard Identification

The uncertainty in hazard identification arises from the fact that all the techniques described in this chapter are dependent on the experience of the team. Two different teams conducting the same HAZOP may produce a report where each team may identify some hazards that the other team has not.

In Australia, following the gas explosion in Longford, Victoria in 1998, the HAZOP technique has received legal status. Both the Royal Commission into the explosion (Dawson and Brooks 1999) and subsequent legal proceedings singled out that the hazard could have been identified had a HAZOP study of the plant been undertaken. This finding places an extra burden on the corporation and the HAZOP team, in terms of the due diligence required in hazard identification. This point is also emphasized by Kletz (1994).

In order to minimise uncertainty in hazard identification, the following approach is suggested for a process plant:

- Selection of appropriate hazard identification methods. Indicative selections are given in Table 4-14.
- Use of more than one method complementing one another at each stage of the life cycle assessment.
- Adoption of quality control procedures as described in Section 4.5.4.
- Allowing for sufficient time to complete the studies

TABLE 4-14 MINIMISING UNCERTAINTY IN HAZARD IDENTIFICATION

| Life Cycle Stage | Suggested Hazard Identification Model |
|---|---|
| Concept design (New Facility) | CHA (high level) or Checklist or 'What if' analysis<br>Process hazard identification matrix<br>Chemical reactivity hazard screening<br>Dow F&EI and CEI<br>Literature review - lessons learnt |
| FEED (New facility) | Process hazard identification matrix<br>Scenario based hazard identification<br>Dow F&EI and CEI<br>Chemical reactivity hazard |
| Detailed design (New facility) | HAZOP of design and subsequent modifications<br>CHAZOP of specific safety/operability critical systems<br>FMEA (if root cause failures/human error identification is required) |
| Commissioning | Scenario based hazard identification<br>HAZOP (time dependent processes)<br>FMEA (human error identification/task analysis)<br>CHA |
| Operations (Existing facility if no hazard evaluation done before) | Scenario based hazard identification<br>Chemical reactivity hazard<br>HAZOP of design and subsequent modifications<br>CHAZOP of specific safety/operability critical systems<br>FMEA (if root cause failures/human error identification is required) |
| Maintenance | CHA (manual operations)<br>FMEA (human error identification/task analysis) |
| Decommissioning | CHA<br>Scenario based hazard identification |

Fault tree and event tree analysis would generally follow the hazard identification, once the scenario is developed. They can also be used for quantification of likelihood of events and hence are covered in Chapter 8.

## 4.6 REVIEW

In Chapter 4, we have focused attention on the various hazard identification (HAZID) tools available. This is the largest chapter in this book, as hazard identification forms the foundation of risk management.

A number of hazard identification techniques have been introduced. Some are suitable directly for continuous flow processes (e.g. HAZOP), and others are more suited to sequential processes, man-machine interfaces, and non-process operations such as maintenance and mechanical handing. Methods, by which human factors can be accounted for in hazard identification, have been described.

The advantages and limitations of the various HAZID tools are described, with suggestions on the choice of technique for various applications through the facility life cycle. Fault tree and event tree analysis form the border line between hazard identification and hazard analysis, with a stronger foothold in the latter camp. Therefore, they only get a mention in Chapter 4, with more details in Chapter 8.

Illustrative examples are provided to describe the technique. Simple processes have been used in the examples to ensure that the reader is not lost in the processes used for illustration, but understands the techniques.

We have emphasized the fact that no single HAZID tool can by itself assist in identification of the full range of hazards in the process, covering all the operations. A judicious combination of different techniques must be used for any given facility. Suggestions on the choice of techniques have been made for the various stages of the facility life cycle.

A large number of references are included for further reading, for the interested reader.

## 4.7 REFERENCES

Ahmed, N. and Khan, A.A. 1992, 'Common telltales can identify safety hazards', *Chemical Engineering Progress,* July pp.73-78.

AIChE 1994a, *Dow's Fire and Explosion Index,* American Institute of Chemical Engineers, New York.

AIChE 1994b, *Dow's Chemical Exposure Index*, American Institute of Chemical Engineers, New York.

Andow, P.K. 1991, *Guidance on HAZOP Procedures for Computer Controlled Plants*, HMSO, London.

Astbury, G.R. and Harper, A.J. 2001, 'Large scale chemical plants: Eliminating the electrostatic hazards', *Journal of Loss Prevention in the Process Industries*, vol. 14, pp. 135-137.

Balasubramanian, S.G. and Louvar, J.F. 2002, 'Study of major accidents and lessons learned', *Process Safety Progress*, vol. 21, no. 3, September, pp. 237-244.

Baybutt, P. 2003, 'Major hazards analysis: An improved method for process hazards analysis', *Process Safety Progress*, vol. 22, no. 1, March, pp. 21-26.

Bond, J. 2002, 'A Janus approach to safety', *Transactions of Institution of Chemical Engineers*, Part B, Process Safety and Environmental Protection, vol. 80, pp. 9-15.

Bradley, P.L. and Baxter, A. 2002, 'Fires, explosions and related incidents in Great Britain in 1998/1999 and 1999/2000', *Journal of Loss Prevention in the Process Industries,* vol. 15, pp. 365-372.

Broomfield, E.J. and Chung, P.W.H. 1994, 'Hazard identification in programmable systems: a methodology and case study', *Association for Computing Machinery Computing Reviews*, vol. 2, no. 1, p. 7.

Burk, A.F. 1992, 'Strengthen process hazard reviews', *Chemical Engineering Progress*, June, pp. 90-94.

Burns, D.J. and Pitblado, R.M. 1993, 'HAZOP Methodology for Safety Critical System Assessment' in *Directions in Safety Critical Systems*, eds. F.S. Redmill and T. Anderson, Springer, London.

Cagno, E., Caron, F. and Mancini, M. 2002, 'Risk Analysis in plant commissioning: the multilevel Hazop', *Reliability Engineering and System Safety*, vol. 77, pp. 309-323.

CCPS 1992, *Guidelines for Hazard Evaluation Procedures,* 2nd edn, Center for Chemical Process Safety, American Institute of Chemical Engineers, New York.

Chemical Industry Association (UK) 1977, *Hazard and Operability Studies.*

Clark, D.G. 1997, 'Apply these matrices to help ensure plant safety', *Chemical Engineering Progress*, December, pp. 69-73.

Collins, R.L. 1995, 'Apply the Hazop method to batch operations', *Chemical Engineering Progress*, April, pp. 48-51.

Crawley, F. and Tyler, B. 2000, *HAZOP: Guide to best practice*, The Institution of Chemical Engineers, Rugby, U.K.

Crawley, F. and Tyler, B. 2003, *Hazard identification methods*, The Institution of Chemical Engineers, Rugby, U.K.

Dawson, D. and Brooks, B. 1999, *Report of the Longford Royal Commission: The Esso Longford gas plant accident*, Government Printer for the State of Victoria, Melbourne, Australia.

De la Cruz-Guerra, C. and Cruz-Gomez, J.M. 2002, 'Using Operating and Safety Limits to Create Safety procedures', *Process Safety Progress*, vol. 21, no. 2, pp. 115-118, June.

Drogaris, G. 1993, *Major Accident Reporting System - Lessons learned from accidents notified*, EUR 15060 EN, Elsevier, Amsterdam.

Ender, C. and Laird, D. 2003, 'Minimise the risk of fire during column maintenance', *Chemical Engineering Progress*, September, pp. 54-56.

Fowler, A.H.K. and Baxter, A. 2000, 'Fires, explosions and related incidents in Great Britain in 1996/97 and 1997/98', *Journal of Loss Prevention in the Process Industries*, vol. 13, pp. 547-554.

Freeman, R.A., Lee, R. and McNamara, T.P. 1992, 'Plan HAZOP studies with an expert system', *Chemical Engineering Progress*, August, pp. 28-32.

Guoshun, Z. 2000, 'Causes and lessons of five explosion accidents', *Journal of Loss Prevention in the Process Industries*, vol. 13, pp. 439-442.

Gustin, J.-L. 2002, 'How the study of accident case studies can prevent runaway reaction accidents from recurring', *Transactions of Institution of Chemical Engineers*, Part B, Process Safety and Environmental Protection, vol. 80, pp. 16-24.

Health and Safety Commission (HSC) 1991, *Study group on human factors*, 2nd report, Human reliability assessment - a critical overview. HMSO, London.

Health and Safety Executive (HSE) 2001, *Offshore Hydrocarbon Releases Statistics 2001 for the Period 1-10-92 to 31-3-01,* Hazardous Installations Directorate, UK HSE.

Hessian, R.T. Jr and Rubin, J.N. 1991, 'Checklist reviews' in *Risk Assessment and Risk Management for the Chemical Process Industry*, eds. H.R. Greenberg and J.J. Cramer, van Nostrand Reinhold, New York, pp. 30–47.

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.

Hopkins, A. 2000, *Lessons from Longford: The Esso gas plant explosion*, CCH Australia Limited, Sydney.

Johnson, R.W. 2000, 'Analyse hazards, not risks', *Chemical Engineering Progress*, July, pp. 31-40.

Johnson, R.W., Rudy, S.W. and S.D. Unwin, 2003, *Essential practices for managing chemical reactivity hazards*, Center for Chemical Process Safety, AIChE, New York.

Johnson, R.W. and Lodal, P.N. 2003, 'Screen your facilities for chemical reactivity hazards', *Chemical Engineering Progress*, August, pp. 50-58.

Jones, P.G. 1989, 'Safety overview of computer control for chemical plant' in *Hazards X: Process safety in fire and speciality chemical plants including developments in computer control of plants*, Institution of Chemical Engineers Symposium Series No.115, 281-290.

Jones, P.G. 1991, 'Computers in chemical plant - a need for safety awareness', *Transactions of IChemE*, Part B, Process Safety and Environmental Protection, vol. 69, pp. 135-138.

Khan, R.I. and Abbasi, S.A. 1999, 'Major accidents in process industries and an analysis of causes and consequences', *Journal of Loss Prevention in the Process Industries*, vol. 12, pp. 361-378.

Khan, F.I., Husain, T. and Abbasi, S.A. 2001, 'Safety weighted hazard index (SWeHI): A new, user friendly tool for swift yet comprehensive hazard identification and safety evaluation in chemical process industries', *Transactions of Institution of Chemical Engineers*, Part B, Process Safety and Environmental Protection, vol. 79, pp. 65-80.

Kletz, T.A. 1994, *What went wrong? Case histories of process plant disasters*, 3rd edn, Gulf Publishing Company.

Kletz, T.A. 1999, *Hazop and Hazan - Identifying and assessing process industry hazard*, 4th edn, The Institution of Chemical Engineers, Rugby, U.K.

Kletz, T.A. 2001, *Learning from Accident*, 3rd edn, Butterworth-Heinemann, Oxford.

Knowlton, R.E. 1992, *A manual of hazard and operability studies*, Chemetics International, Vancouver, Canada.

Koivisto, R. and Nielsen, D. 1994, 'FIRE - a database on chemical warehouse fires', *Journal of Loss Prevention in the Process Industries*, vol. 7, pp. 209.

Lardner, R. and Fleming, 1999, M. 'To err is human ....', *The Chemical Engineer*, Oct 7, pp. 18-20.

Lawley, H.G. 1974, 'Operability studies and hazard analysis', *Chemical Engineering Progress*, vol. 70, no. 4, pp. 45-56.

Lees, F.P. 2001, *Loss Prevention in the Process Industries*, 3rd edn, Chapter 8, Butterworths-Heinemann, Oxford, UK.

Mannken, G.E. 2001, 'Use case histories to energise your HAZOP', *Chemical Engineering Progress*, March, pp. 73-78.

McCoy, S.A., Wakeman, S.J., Larkin, F.D., Jefferson, M.L., Chung, P.W.H., Rushton, A.G., Lees, F.P. and Heino, M.P. 1999a, 'HAZID, a computer aid for hazard identification. 1. The STOPHAZ package and the HAZID code: An overview, the issues and the structure', *Transactions of Institution of Chemical Engineers*, Part B, Process Safety and Environmental Protection, vol. 77, pp. 317-327.

McCoy, S.A., Wakeman, S.J., Larkin, F.D., Chung, P.W.H., Rushton, A.G. and Lees, F.P. 1999b, 'HAZID, a computer aid for hazard identification. 2. Unit model system', *Transactions of Institution of Chemical Engineers*, Part B, Process Safety and Environmental Protection, vol. 77, pp. 328-334.

McCoy, S.A., Wakeman, S.J., Larkin, F.D., Jefferson, M.L., Chung, P.W.H., Rushton, A.G., Lees, F.P. and Heino, M.P. 1999c, 'HAZID, a computer aid for hazard identification. 3. The fluid model and consequence evaluation systems', *Transactions of Institution of Chemical Engineers*, Part B, Process Safety and Environmental Protection, vol. 77, pp. 335-353.

McCoy, S.A., Wakeman, S.J., Larkin, F.D., Jefferson, M.L., Chung, P.W.H., Rushton, A.G. and Lees, F.P. 2000a, 'HAZID, a computer aid for hazard identification. 4. Learning set, main study system, output quality and validation trials', *Transactions of Institution of Chemical Engineers*, Part B, Process Safety and Environmental Protection, vol. 78, pp. 91-119.

McCoy, S.A., Wakeman, S.J., Larkin, F.D., Jefferson, M.L., Chung, P.W.H., A.G. Rushton, Lees, F.P. and Heino, M.P. 2000b, 'HAZID, a computer aid for hazard identification. 5. Future development topics and conclusions', *Transactions of Institution of Chemical Engineers*, Part B, Process Safety and Environmental Protection, vol. 78, pp. 120-142.

McKelvey, T.C. 1988, 'How to improve the effectiveness of hazard and operability analysis', *IEEE Transactions on Reliability*, vol. 37, no. 2, June, pp. 167-170.

Ministry of Defence. *Hazop studies on systems containing programmable electronics - Part I, Requirements*, Ministry of Defence, Glasgow, UK, Defence Standard 00-58:2000a.

Ministry of Defence. *Hazop studies on systems containing programmable electronics - Part II, General application guidance*, Ministry of Defence, Glasgow, UK, Defence Standard 00-58:2000b.

Mushtaq, F. and Chung, P.W.H. 2000, 'A systematic Hazop procedure for batch processes, and its application to pipeless plants', *Journal of Loss Prevention in the Process Industries*, vol. 13, pp. 41-48.

Nimmo, I., Nunn, S.R. and Eddershaw, B.W. 1987, 'Lessons learned from the failure of a computer system controlling a nylon polymer plant' in *Achieving*

*Safety & Reliability with Computer Systems*, ed. B.K. Daniels, Elsevier Applied Science, London, pp.189-206.

Nimmo, I. 1995, 'Adequately address abnormal operations', *Chemical Engineering Progress*, September, pp. 36-45.

OSHA, Occupational Safety and Health Administration, USA. *Process safety management of highly hazardous chemicals*, Federal Register, Washington DC. OSHA 29 CFR 1910.119:1992.

Perrow, C. 1999, *Normal accidents living with high risk technologies,* Princeton University Press, USA.

Phillips, L.T. 2002, 'Decommissioning process plant facilities', *Chemical Engineering Progress*, December, pp. 68-73.

Plans-Cuchi, E., Vilchez, J.A. and Casal, J. 1999, 'Fire and explosion hazards during filling/emptying of tanks', *Journal of Loss Prevention in the Process Industries*, vol. 12, pp. 479-483.

Pratt, T.H. and Atharton, J.G. 1995, 'Some electrostatic considerations in the transportation of flammable liquids', *Process Safety Progress*, vol 15, no. 3, pp. 173-177.

Queensland Government 2001, *Dangerous Goods Safety Management (DGSM) Act and the DGSM Regulations*, Queensland Government Printer, Brisbane, Australia.

Raman, R. and Sylvester, S. 2001, 'Computer hazard and operability study or 'CHAZOP': Benefits and applications', *2001 Spring National Meeting,* Houston, Texas, April, Paper 37e.

Rasmussen, J. 1990, 'Human error and the problem of causality in analysis of accidents', *Philosophical Transactions of the Royal Society London*, B327, pp. 449-462.

Ramussen, B. and Whetton, C. 1993, *Hazard Identification Based on Plant Functional Modelling,* The University of Sheffield, UK and Riso National Laboratory, Roskilde, Denmark, Report Riso-R-712 (EN), October.

Reason, J. 1997, *Managing the risks of organisational accidents,* Aldershot: Ashgate.

Reizel, Y. 2002, 'Explosion and fire in a gas-oil fixed roof storage tank: Case study and lessons learned', *Process Safety Progress*, vol 21, no. 1, pp. 67-73.

Rouhiainen, V. 1990, *The quality assessment of safety analysis*, Publication 61, VTT Finland, ISBN 9513835693.

Sanders, R.E. and Spiers, W.L. 1996, 'Monday morning quarterbacking: Applying PSM methods to case histories of yesteryear', *Process Safety Progress*, vol. 15, no. 4, pp. 189-193.

Sanders, R.E. 1999, *Chemical process safety - Learning from case histories,* Butterworth-Heinemann, Oxford.

Sanders, R.E. 2002, 'Picture this! Incidents that could happen in your plant', *Process Safety Progress*, vol. 21, no. 2, June, pp. 130-135.

Sebzali, Y.M. and Wang, X.Z. 2002, 'Joint Analysis of process and operator performance in chemical process operational safety', *Journal of Loss Prevention in the Process Industries*, vol. 15, pp. 555-564.

Selby, C. 2003, 'Steeling a march on offshore safety', *The Chemical Engineer*, pp. 34-35, June.

Taylor, J. 1981, *Completeness and discrimination of hazard analyses*, Risø-M-2306, Denmark.

Turner, S. 1996, 'Are your Hazops up to scratch?', *The Chemical Engineer*, 22 February, pp. 13-15.

Tyler, B.J., Thomas, A.R., Doran, P. and Greig, T.R. 1994, 'A toxicity hazard index' in *Hazards XII, European Advances in Process Safety,* IChemE Symposium Series, no. 134, pp. 351-366.

Tweeddale, M. 2003, *Managing risk and reliability in process plants,* Gulf Professional Publishing.

Urben, P.G. (ed) 1999, *Bretherick's handbook of reactive chemical hazards,* 6th edn, Vols.1 and 2, Butterworths-Heinemann, Oxford.

Vaidhyanathan, R., Venkatasubramanian, V. and Dyke, F.T. 1996, 'HAZOP*Expert*: An expert system for automatic HAZOP', *Process Safety Progress*, vol. 15, no. 2, pp. 80-88.

Wells, G., Phang, C., Wardman, M. and Whetton, C. 1992, 'Incident scenarios: Their identification and evaluation', *Transactions of Institution of Chemical Engineers*, Part B, Process Safety and Environmental Protection, vol. 70, pp. 179-188.

Wells, G., Wardman, M. and Whetton, C. 1993, 'Preliminary safety analysis', *Journal of Loss Prevention in the Process Industries*, vol. 6, no. 1, pp. 47-60.

Wells, G., Phang, C. and Wardman, M. 1994, 'Improvements in process safety reviews prior to HAZOP' in *Hazards XII, European Advances in Process Safety,* IChemE Symposium Series, no. 134, pp. 301-314.

Whitaker, G.W. 1993, 'Contractor Hazard Identification and Control', *Process Safety Progress*, vol. 12, no. 3, pp. 133-136.

## 4.8 NOTATION

| | |
|---|---|
| AEA | Action Error Analysis |
| AIChE | American Institute of Chemical Engineers |
| AIHA | American Industrial Hygiene Association |
| AQ | Airborne Quantity kg/s |
| ARIP | Accident Release Information Program |
| BLEVE | Boiling Liquid Expanding Vapour Explosion |
| CCPS | Center for Chemical Process Safety (AIChE) |
| CEI | Dow Chemical Exposure Index |
| CHA | Concept Hazard Analysis |
| CHAZOP | Computer Hazard and Operability Study |
| CO | Carbon monoxide |
| ERPG | Emergency Response Planning Guideline, mg/m$^3$ |
| ESD | Emergency Shutdown |
| EtO | Ethylene Oxide |
| EU | European Union |
| F&EI | Dow Fire and Explosion Index |
| FMEA | Failure Mode and Effects Analysis |
| FMECA | Failure Mode Effects and Criticality Analysis |
| $H_2$ | Hydrogen |
| HAZID | Hazard Identification |
| HAZOP | Hazard and Operability study |
| HCR | Hydrocarbon Releases |

| | |
|---|---|
| I/O | Input/Output (digital hardware) |
| IChemE | Institution of Chemical Engineers (UK) |
| kg | kilogram |
| kPag | kilo Pascals gauge |
| LAH | Level Alarm High |
| LAHH | Level Alarm High High |
| LI | Level Indicator (gauge) |
| LS | Level Switch |
| MAHB | Major Accident Hazards Bureau |
| MARS | Major Accident Reporting System |
| MHIDAS | Major Hazard Incident data System |
| MSDS | Material Safety Data Sheet |
| $NH_3$ | Anhydrous ammonia |
| OSHA | Occupational Health and Safety Administration (USA) |
| P&ID | Piping & Instrumentation Diagram |
| PES | Programmable Electronic System |
| PPE | Personal Protection System |
| ppm | Parts per million |
| PSV | Pressure Safety Valve |
| QA | Quality Assurance |
| SADIE | Safety Alert Database and Information Exchange |
| SIS | Safety Instrumented System |
| SMS | Safety Management System |
| $SO_3$ | Sulphur trioxide |
| TLV | Threshold Limit Value |
| UK | United Kingdom |
| UK HSE | UK Health and Safety Executive |
| UN | United Nations |
| US EPA | United States Environment Protection Agency |
| VCE | Vapour Cloud Explosion |

This page is intentionally left blank

# 5 ANALYSING THE CONSEQUENCES OF INCIDENTS

*"It is easy to dodge our responsibilities but we cannot dodge the consequences of dodging our responsibilities."*

*Lord Stamp of Shortlands*

An important aspect of risk management following hazard identification is the task of consequence analysis. Hazards and operational problems often lead to the release of energy and hazardous materials. What is of importance is the knowledge of "how big?" or "what impact?" will flow from hazardous events. This is the area of consequence analysis and there are several key issues that are discussed in this chapter as a prelude to the more detailed discussion in Chapters 6 and 7. What will be evident from these discussions is that current practice relies heavily on the use of mathematical models to predict a range of physical effects as well as potential impacts on vulnerable receptors.

## 5.1 EVENTS, INCIDENTS AND SCENARIOS

In discussing consequence analysis it is helpful to clearly distinguish between individual events, incidents and scenarios. We adopt the following conventions in this book:

event: a single action or outcome from a system failure

incident: a chain of related events with an initiating event and a termination event.

scenario: a collection of one or more incidents related to a risk analysis investigation.

### 5.1.1 Events

This is a single action or outcome which characterizes a failure and potentially its subsequent propagation. What is important is the view that each event is a system with its own inputs, outputs, states and parameters as seen in Figure 5-1.

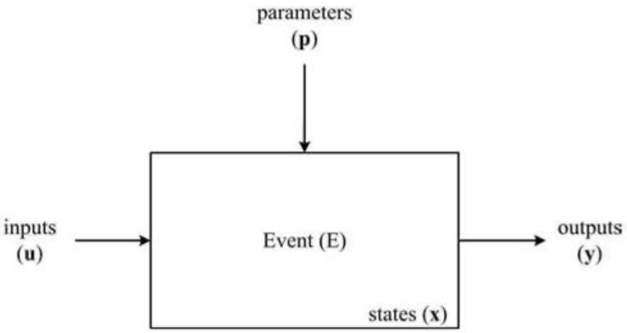


**FIGURE 5-1 EVENT SYSTEM**

**EXAMPLE 5-1 FIRE EVENTS IN CONSEQUENCE ANALYSIS**

It is possible to categorize fire events into several classes such as:

- pool fire, where burning liquid is in the form of a contained or uncontained pool
- torch or jet fire, where high pressure gas or flashing liquids form a jet fire of varying shape and dimension
- flash fire, where a flammable gas cloud is ignited and burns rapidly.

These are all common events analyzed for industrial and transport operations.

There are many classes of events that could occur in the process industry, ranging from release of material from the process, through to intermediate material behaviour (pool formation, vapour dispersion) and then impacts on people, property and the environment. Due to the systems nature of events, these are amenable to representation in the form of mathematical models that relate outputs ($y$) or predictions to given inputs ($u$), parameters ($p$) and model form ($M$).

For the event $E$, we can write simply that the outputs are a function of inputs and parameters:

$$y = E(u, p) \tag{5.1}$$

The event states ($x$) are implicitly included in the event $E$.

For the model ($M$) that seeks to represent the event behaviour we have in simple terms

$$y^M = M(u, p) \tag{5.2}$$

where $y^M$ are the predicted outputs, and $M$ is the model used to predict the outputs. Clearly, model predictive quality is related to the difference.

$$|\ y^M - y\ | \tag{5.3}$$

which can vary significantly depending on the complexity of the actual situation and the sophistication of the model used to predict its behaviour. Typical values of $y^M$ can be a factor of 2 to 5 from the real value $y$. Outputs from the model are typically physical effects such as release flowrates, thermal radiation levels, gas concentrations and explosion overpressures. The inputs and parameters for each event are specific to that event. For a gas release the inputs could involve system pressure, aperture size and material being released. Parameters could include material properties such as specific heat capacities and specific volumes. There are uncertainties in both the inputs, parameters and the model form. Hence there are output or prediction uncertainties. This is discussed more fully in Chapter 10.

To illustrate the potential events, Figure 5-2 gives an overview of possible events associated with hazardous substances and other operational and natural events. The left half of Figure 5-2 traces a number of key events after a substance is released from either fixed sites or transport operations. This includes both "safety" related events with impacts on people and plant as well as "environmental" impacts on air, water resources and the like. The right-hand side deals with other key events, common to process systems, including the influence of operational failures, structural failures and natural hazards such as earthquake and storm.

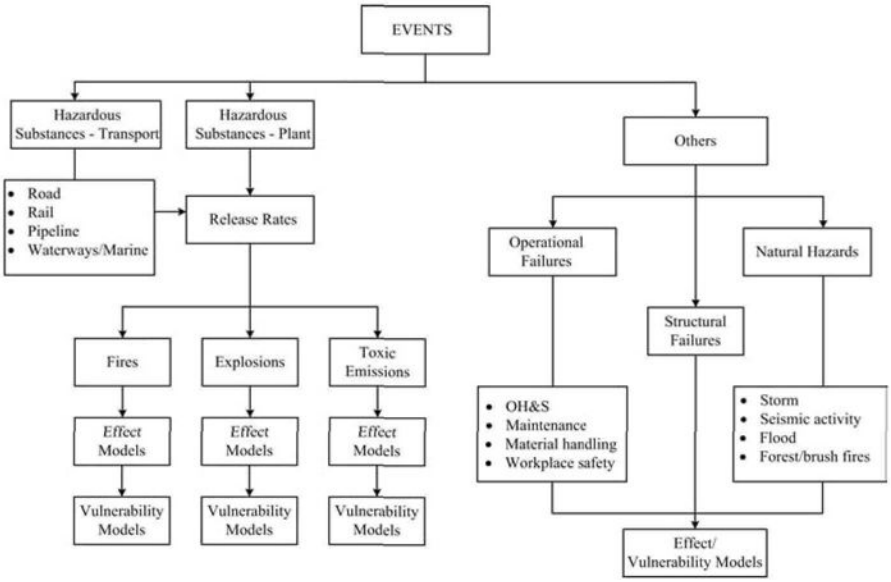


FIGURE 5-2 CONSEQUENCE ANALYSIS OVERVIEW

## 5.1.2 Incidents

An incident ($I$) is a chain of events with an initiator and a terminator event. Figure 5-3 shows a simple toxic gas incident ($I_1$) whereas Figure 5-4 shows a more complex liquefied gas incident ($I_2$). Individual events are denoted by a single circle whilst the double circle denotes an impact event for the vulnerable receptor under consideration.

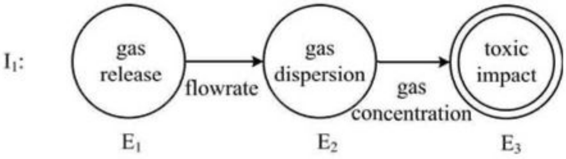


FIGURE 5-3 SIMPLE GAS INCIDENT

As seen in Figures 5-3 and 5-4, incidents can be simple to very complex. The events $E_i$ $(i = 1, \ldots, n)$ are also linked by edges or arcs in specific ways depending on various environmental and processing conditions such as ignition sources. Hence, these edges can represent probabilities dependent on many contributing factors. In Chapter 8 formal methods of event tree and fault tree analysis are used to understand the causal relationships that could exist. It is also clear that propagation of event chains depends on the presence and probabilities of the edges or arcs.

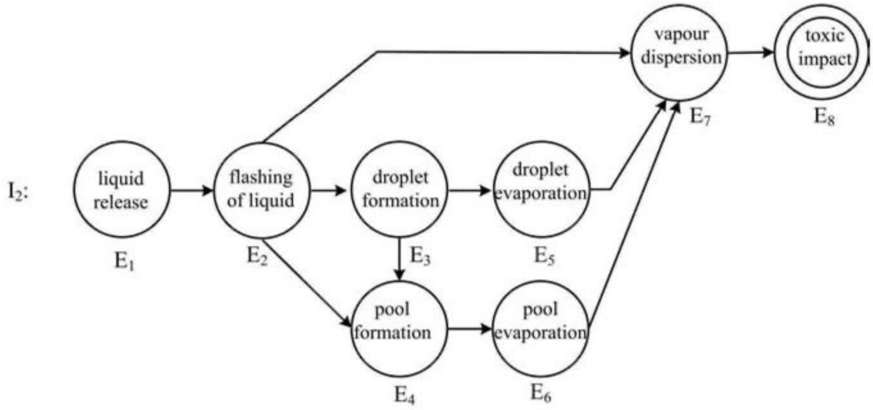


FIGURE 5-4 COMPLEX LIQUEFIED GAS INCIDENT

**EXAMPLE 5-2 COKEMAKING ENVIRONMENTAL INCIDENT**

Contamination of flushing liquor, used to cool coke ovens gas in a cokemaking battery led to massive blockages of the spray system with carryover of tar products. The use of copious amounts of fresh water eventually led to an environmental accident through release of contaminated water into a local creek. The simplified incident consisted of the following events (Figure 5-5).

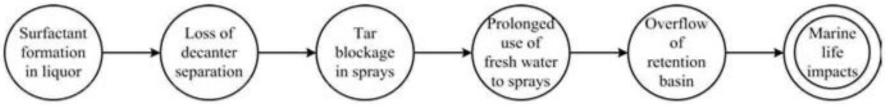

Surfactant formation in liquor
Loss of decanter separation
Tar blockage in sprays
Prolonged use of fresh water to sprays
Overflow of retention basin
Marine life impacts

FIGURE 5-5 ENVIRONMENTAL INCIDENT

### 5.1.3 Scenarios

These relate to a set of incidents that could be used to assess overall impact from system failures. Scenarios are commonly used in quantitative risk assessment where impacts from all potential incidents are used to assess individual, societal or other nominated risks.

For example, a set of incidents $I_i$ ($i$=1, … , $n$) might be defined for a particular situation that have the potential for individual fatality impacts. Another scenario could relate to a set of incidents $I_j$ ($j$ = 1, … , $m$) that could have purely environmental impacts on air or water resources. In some cases, incidents can have multiple impacts such as the release of a toxic, flammable substance that causes injury or death through fire or toxic dose impacts.

## 5.2 EFFECT AND VULNERABILITY MODELS

One of the key issues arising from the identification of hazards is to estimate the magnitude of the effects that might flow from them. This could be related to a release of material from a rupture or leak, the effects of a fire on people or structures, or the effect of gases which disperse in the surrounding area.

When considering this issue there are two distinct parts which must be addressed. These are:

- the magnitude of the physical effects,
- the damage caused by these effects.

The first considers the effects arising from the actual release and subsequent events. These are quantified in terms of measurements like: concentrations of toxic gases, radiation levels from fires or over-pressures from explosions. There is a plethora of models available in the literature of varying degrees of fidelity and sophistication (CCPS 2000, TNO 1997, Lees 2001). Major journals such as:

- Journal of Hazardous Materials
- Journal of Loss Prevention in the Process Industries
- Reliability Engineering and System Safety
- Transactions of the Institution of Chemical Engineers (UK), Part B.
- Process Safety Progress
- Chemical Engineering Progress
- American Institute of Chemical Engineers Journal

provide useful sources for recent information in model development and application. Chapter 6 discusses some of the key effect models often used in quantification of physical effects.

The second aspect considers what impact these effects have on the receptors we are considering. The receptor might be a plant structure or people or an eco-system. Mathematical models are normally used for these estimates.

The first type of model is an "effect" model whereas the second is known as a "vulnerability" model.

Figure 5-6 illustrates the relationship between these types of models and how they are applied. In Figure 5-6 the "effect" models help to predict the magnitude of the phenomenon associated with the event such as heat radiation levels from a fire. These effects then impact on the environment or the vulnerable receptors. The role of the "vulnerability" models is to take the magnitude of the phenomenon and estimate the damage to people, structures or eco-systems. The overall concept of consequence analysis is given in Figure 5-6 which shows how the incidents are used to obtain a damage quantification.

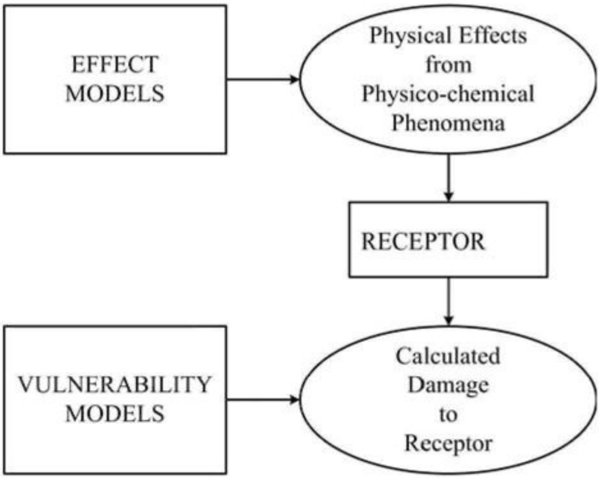

EFFECT MODELS
Physical Effects from Physico-chemical Phenomena
RECEPTOR
VULNERABILITY MODELS
Calculated Damage to Receptor

FIGURE 5-6 EFFECT AND VULNERABILITY MODELS

Consequence analysis provides:

- information to industries on effects of events.
- details for designers as to what consequences could occur and should be minimised.
- details to competent authorities on possible effects of events and then aids in appropriate planning decisions.
- workers with details of their personal situation in the event of an incident.
- a basis for emergency planning and emergency response.

In section 5.2.2 we briefly consider the types of events which commonly arise from accidental releases of materials and the consequences that can flow from these events. In Chapter 6, details are given of the models frequently used in estimating those effects. Vulnerability assessments are described in Chapter 7. Of particular importance in consequence analysis is eco-system impact and this is now considered.

### 5.2.1 Consequence Analysis for Eco-Systems

Process systems can have significant impacts on eco-systems over a range of time scales. Acute, short term impacts from accidents can have a range of consequences depending on the release mode, quantity and toxicity. Longer term, chronic impacts are also possible and should be considered under environmental risk assessment (ERA) methodologies (DOE 1995; Benjamin and Belluck 2001; Standards Australia 2000).

Eco-system impacts can be extremely complex to analyse and often more difficult to quantify. Figure 5-7 shows the key aspects for consideration in ERA. This is a particular instance of the general effect-vulnerability framework given in Figure 5-6. The principal issues in Figure 5-7 that require comment are:

(i) Sources

- For ERA, sources of chemicals of concern (COC) or chemicals of potential concern (COPC) derive from loss of containment through system failures, handling of wastes, storage failures of raw materials or spent materials. The sources can be both acute and chronic and the COC is delivered into the environment in many ways.

(ii) Fate and transport

- Once in the environment, COCs can migrate between various media. The interaction of the COC with the environment can be complex and specialised models for air, water and soil pathways are needed to track transport and the fate of chemical species. Typical of these models are many available through government agencies such as the US EPA (www.epa.gov/epahome/models.htm).

(iii) Impact

- An organism or receptor will encounter the COC by means of a medium (soil, air, water, ...). Ecological receptors include fish, birds, insects and the like. Human receptors include children, adolescents and adults. Models for COC uptake into the receptor are needed in this phase as well as the definition of the ecological endpoints. These endpoints are specific characteristics of a receptor affected by the COC. They could be mortality in a fish population or cancers in humans.

In all these cases, models and data are necessary to provide risk estimates for a given source, transport pathways and final impacts. Specialist advice is nearly always needed for such ERA studies.

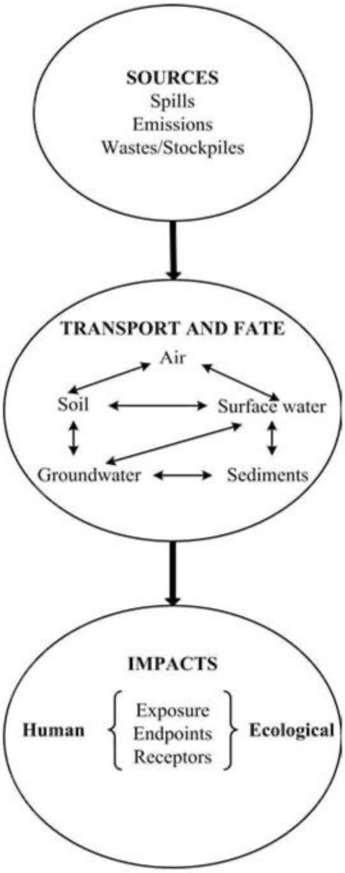


FIGURE 5-7 KEY CONCEPTS IN ENVIRONMENTAL RISK ASSESSMENT

## 5.2.2 Major Effects in Consequence Analysis

There are several classes of events which are important to consider. The first category we consider are the releases of material into the environment.

### *5.2.2.1 Release, fire, toxic emissions and explosion*

Releases can be in the form of:

- Vapour/gases
- Liquid (normal and superheated)
- Solids

These releases can be from systems which operate at high pressure such as a storage vessel or reactor. They can be spillages from trucks, specialised transport vehicles or conveying systems. In some cases, like LPG, the release is a liquefied gas under pressure (superheated) which rapidly vaporises once it is released. These "flashing" materials can be particularly difficult to analyze.

These foregoing events are typically the initiators for a range of incidents and their rate of release and form are the key aspects in consequence analysis. They are commonly referred to as "source terms".

Fires of various types can occur, related to the way flammable materials are released or the nature of the material itself. We can identify a number of events including:

- flames on pools
- flash fires
- jet fires (also known as torch fires)
- Boiling Liquid Expanding Vapour Explosions (BLEVE)

Each of these events produces different impacts on the surrounding vulnerable receptors, which should be considered.

Of importance here is the level of thermal radiation produced by flames and the duration of the radiation. The directional aspects of the flame are crucial to impact analysis.

**EXAMPLE 5-3 BLEVE–CAIRNS, QUEENSLAND**

In 1987 at a LPG storage terminal in Cairns, Australia, a mechanical failure in the transfer line from a 40 tonne LPG rail tanker led to a BLEVE event that resulted in significant building damage and the death of 1 person.

(Source: Queensland Fire Service, 1987)

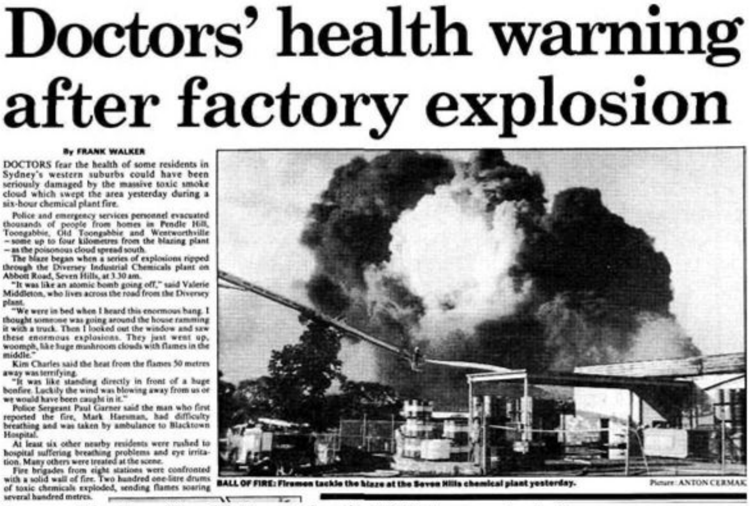
Toxic gas emissions to the atmosphere are important although equally, releases of liquids and solids to watercourses are also important. The types of emissions that could be considered include:

- toxic gases
- flammable substances
- toxic products of combustion

In many cases, these releases are complicated by obstructions or confinement as well as the physical nature of the material released. In the case of solid releases complicated dissolution mechanisms come into play. Clearly, toxic emissions with subsequent dispersion into the environment lead to concentration levels which can have catastrophic impacts such as those seen at Bhopal, India.

**EXAMPLE 5-4 CHEMICAL WAREHOUSE FIRE**

In 1989 a fire at a chemical storage warehouse led to an explosion and subsequent dispersion of toxic fire combustion products with impacts on the local community.



# Doctors' health warning after factory explosion

By FRANK WALKER

DOCTORS fear the health of some residents in Sydney's western suburbs could have been seriously damaged by the massive toxic smoke cloud which swept the area yesterday during a six-hour chemical plant fire.

Police and emergency services personnel evacuated thousands of people from homes in Pendle Hill, Toongabbie, Old Toongabbie and Wentworthville – some up to four kilometres from the blazing plant – as the poisonous cloud spread south.

The blaze began when a series of explosions ripped through the Diversey Industrial Chemicals plant on Abbott Road, Seven Hills, at 3.30 am.

"It was like an atomic bomb going off," said Valerie Middleton, who lives across the road from the Diversey plant.

"We were in bed when I heard this enormous bang. I thought someone was going around the house ramming it with a truck. Then I looked out the window and saw these enormous explosions. They just went up, woomph, like huge mushroom clouds with flames in the middle."

Kim Charles said the heat from the flames 50 metres away was terrifying.

"It was like standing directly in front of a huge bonfire. Luckily the wind was blowing away from us or we would have been caught in it."

Police Sergeant Paul Garner said the man who first reported the fire, Mark Haesman, had difficulty breathing and was taken by ambulance to Blacktown Hospital.

At least six other nearby residents were rushed to hospital suffering breathing problems and eye irritation. Many others were treated at the scene.

Fire brigades from eight stations were confronted with a solid wall of fire. Two hundred one-litre drums of toxic chemicals exploded, sending flames soaring several hundred metres.

**BALL OF FIRE: Firemen tackle the blaze at the Seven Hills chemical plant yesterday.** Picture: ANTON CERMAK

(Source: The Sun-Herald, December 3, 1989, by permission)

Explosion events can be particularly devastating and blast effects need to be considered when designing and planning operations that could potentially generate these impacts.

In particular, we can categorize explosions under the following headings:

- vapour cloud explosions (eg. deflagration or detonation)
- dust explosions (eg. flour, coal, powders)
- condensed phase explosions (eg. TNT, RDX)

The estimation of explosion effects is quite complex. First, it is necessary in the case of vapour cloud explosions to realise that the degree to which the flammable vapour cloud is confined by process equipment, buildings and trees or determines the type of explosion (detonation or deflagration). Detonations are sonic events and result in very fast (2km - 10km per second) pressure waves. Condensed phase explosions often result in detonations. On the other hand, deflagrations are sub-sonic events, resulting from much slower burning processes (less than 300 metres per second). The damage resulting from these explosion types is quite different, with detonations producing significantly more damage than deflagrations.

Second, the damage pattern can be quite varied where there are many obstructions, buildings or vegetation. One area might receive very high damage, another almost nothing. Hence the need to be wary about results from simplistic models. For some complex cases there are sophisticated tools to predict these effects and this is discussed in Chapter 6.

Finally, of importance are incidents that lead to environmental damage. In some cases this can be due to direct release of toxic substances to ground or watercourses. Another important case is when secondary material such as contaminated fire water from fire fighting operations escapes site containment and enters water courses or causes ground contamination.

**EXAMPLE 5-5 FIRE WATER CONTAMINATION OF THE RHINE RIVER**

In November 1986 a fire occurred in the Sandoz chemical manufacturing plant in Basel, Switzerland. There were over 90 different chemicals, including 20 pesticides stored on the site. These included substances such as parathion, thiometon, captafol and endosulfan. Up to 15,000 m$^3$ of contaminated fire water was discharged into the river during this incident. Marine life in the river was greatly affected for over 170 km downstream.

### 5.2.2.2 *Effect models for consequence analysis*

As seen in section 5.1, effect models that help predict outputs of events are of the general mathematical form:

$$y^M = M(u,p) \tag{5.4}$$

The model $M$ transforms or maps the given inputs ($u$) and model parameters ($p$) to the outputs $(y^M)$. It is clear that the form of $M$ and its internal structure are very important in generating the predictions. Some models are completely empirical such as BLEVE size and duration predictions, whilst release models are normally mechanistic being based on mass and energy conservation principles. Many effect models are a mixture of mechanistic and empirical - the so-called "grey box" model.

There is a plethora of effect models in the literature (Lees, 2001) with many being implemented into software tools. Some are extremely simple, easily implemented on standard spreadsheet tools, others such as computational fluid dynamics (CFD) models can require significant computation time for complex 3D situations.

The principal considerations in using models for any event type are:

- The inputs $u$:
  - what are they and how easy are they to obtain?
  - what uncertainty is associated with those inputs?
  - what effect does input uncertainty have on the predictions?
  - what is the range of uncertainty or its distribution?
- The parameters $p$:
  - are these well known or easily obtained?
  - what uncertainty is associated with these values?

- how is the parameter uncertainty reflected in the model predictions?
- what is the range of parameter uncertainty?

- The model form $M$:
  - what fidelity of model is really needed for the purpose of the study?
  - is the model empirical, mechanistic or "grey box" in nature?
  - what validation has been made on the model?
  - what is the application range of the model?

There are important formal means of addressing issues such as parametric and model structure uncertainty. One of the key aspects in using mathematical models is an assessment of input and parametric uncertainties. For changes in $p$ and $u$, it is important to assess the corresponding changes in $y^M$. Hence we can define at least two sensitivity measures for event models:

Parameter sensitivity:
$$\frac{\partial y_i^M}{\partial p_j} \cong \frac{y_i^M(u, p_j + \Delta p_j) - y_i^M(u, p_j)}{\Delta p_j} \tag{5.5}$$

Input sensitivity:
$$\frac{\partial y_i^M}{\partial u_j} \cong \frac{y_i^M(u_j + \Delta u_j, p) - y_i^M(u_j, p)}{\Delta u_j} \tag{5.6}$$

By perturbing $p_j$ by an amount $\Delta p_j$ the parameter sensitivity on output $y_i^M$: $\frac{\partial y_i^M}{\partial p_j}$ can be estimated as seen in equation (5.5). A similar sensitivity study for inputs $u_j$ can be made.

Sensitivity estimates can be ranked and then attention given to the most critical inputs and parameters. This can be a vital step in carrying out consequence analysis in order to show the effect of prediction uncertainties due to inputs and parameters. It is an area that is often poorly addressed in risk management practice.

### 5.2.2.3 Vulnerability models for consequence analysis

Vulnerability models are representations of dose-response situations, where a vulnerable target receives a "dose" or impact in various forms that include:

(i) thermal radiation dose (radiation level for a specified duration)
(ii) toxic dose (toxic gas concentration for a specific duration)
(iii) explosion impulse (overpressure and duration)

There are a number of ways that impacts can be assessed that include:

a) Dose-response curves that represent the mean value response of a human or animal to toxic doses. Doses are typically in terms of mg substance/kg body weight.

If the response is plotted against the logarithm of the dose a typical sigmoidal or 'S' shaped curve is obtained, as seen in Figure 5-8.

b) Use of probit or probability unit functions that fit dose-response data to the mathematical form (CRC, 1968):

$$P = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{Y-5} \exp\left(-\frac{1}{2}w^2\right) dw \qquad (5.7)$$

where $P$ = percentage or fraction of resource affected
$Y$ = probit variable (related to the dose)
$w$ = independent variable in the integral

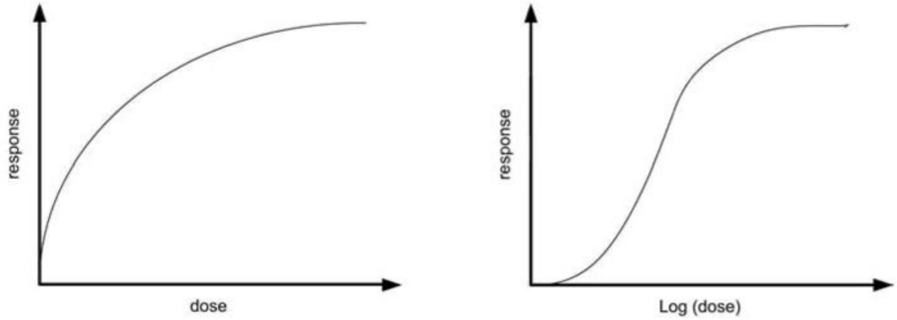


**FIGURE 5-8 DOSE RESPONSE RELATIONSHIPS**

Probit equations provide a useful mathematical function to compute impacts on vulnerable receptors. Probits are available for a limited number of impacts of toxic gases as well as thermal radiation and explosion impacts. Further details are given in Chapter 7.

c) There are several toxic gas exposure indices for injury effects:

TLV = Threshold limit value for occupational exposure to gases and vapours, defined as "the average airborne concentration of a particular substance when calculated over a normal eight-hour working day, for a five-day working week". The TLV is also referred to as the Time Weighted Average (TWA).

STEL = Short term exposure limit for occupational exposure, defined as "a 15 minute TWA exposure that should not be exceeded at any time during a working day even if the eight-hour TWA average is within the TWA exposure standard. Exposures at the STEL should not be longer than 15 minutes and should not be repeated more than four times per day. There should be at least 60 minutes between successive exposures at the STEL".

IDLH = Immediately dangerous to life and health gas concentrations levels at which, if exposure occurs for more than 30 minutes, irreversible injury may occur.

ERPG = Emergency response planning guidelines defined at 3 levels of concentrations, used for possible civil evacuation purposes.

The above toxicological indices are useful in assessing injury potential and emergency planning for evacuation purposes, but not applicable when estimating lethal effects on individuals or groups from accidental releases.

Care must be exercised in using the probit methods for toxic impact assessment as significant extrapolation from animal studies is often used in arriving at specific toxic index values. An example of this is given in Chapter 7.

Table 5-1 summarizes the initiating events, the physical effects and the type of damage on different receptors. Some details are given in TNO (1992). Chapter 7 gives more detail on the specific vulnerability models that can be used within process risk management applications.

TABLE 5-1 VULNERABILITY MODELS

| Damage Causing Event | Physical Effects | Resource Affected | Type of Damage |
|---|---|---|---|
| FLASH FIRE | Thermal radiation | People | Death<br>Injury |
| POOL BURNING | Thermal radiation | People | Death<br>Burns |
| | | Structures | Failure |
| JET FIRE | Flame impingement | Structures | Failure |
| | Thermal radiation | People | Death<br>Injury |
| EXPLOSION | Blast overpressure<br>Blast impulse<br>Thermal radiation<br>Flying fragments | People | Death<br>Injury<br>Ear/lung damage<br>Fractures<br>Punctures |
| | | Structures | Structural damage<br>Glass breakage |
| TOXIC RELEASE | Toxic vapour concentration dose | People | Death<br>Injury<br>Irritation<br>Distress |
| | | Biosphere | Death<br>Damage |

## 5.3 LIMITATIONS AND UNCERTAINTIES IN CONSEQUENCE ANALYSIS

There are some significant limitations on the use of effect models. This is simply because:

- most of the mathematical models are based on idealized systems. That is, they often do not take into account irregularities. In the case of ideal dispersion models, no account is taken of the effect of buildings in breaking up or concentrating gases flowing around them. The same is true of most fire models and explosion models. Sophisticated models are needed in circumstances where fidelity is desired. Even then limitations must be recognized. Sophistication should not be equated to fidelity.

- most models are empirical or semi-empirical, being based on a limited set of experimental data. Predictions outside the validation range is often dangerous.
- many models have only been verified by small scale tests and as such have significant uncertainties attached to them when applied to new situations where the physical size of the event is much larger. An example is the prediction of evaporation rates from very large spills using models based on 1 metre diameter experimental pools.

The result of these issues is that there can be significant uncertainty in the results from such model predictions. Also much of the input data to these models has uncertainty associated with it. For example the size of the hole leading to the release or the windspeed for dispersion calculations. Typically we can expect predictions to vary by a factor of 2 to 5.

This is not to say that the predictions are useless. It just means that we need to appreciate the variability of the predictions and carry out sensitivity checks to see how the model output varies with our assumptions on the input data. In that way we get a "feel" for what is important and what is not. This is considered in Chapter 10.

### 5.3.1 Need for Assumptions

Like any area of analysis, it is vital to either explicitly state the assumptions underlying the methods used or refer to modelling and analysis assumptions that are implicit in the work.

Stated assumptions allow both the analyst and the reader to assess the appropriateness of the methods used in consequence analysis as well as the input data and model parameters. The assumptions should include:

(i) The event sequences (incidents) used.
(ii) The effect models used for each event in the incident.
(iii) The input data assumed for the models and an estimate of the uncertainty for those inputs.
(iv) The parameters for the models with estimates of their uncertainty in terms of parameter ranges or specific distributions eg. (Gaussian or log-normal etc.).
(v) Assumptions relating to excluded events or incidents and their justification for their exclusion in the analysis.

### 5.3.2 Quality of Assumptions

The quality of the assumptions is vital. In some cases, lack of insight and understanding can lead to inappropriate assumptions being made and applied in a risk assessment study. The underlying assumptions can be improved by:

(i) Ensuring a clear physico-chemical understanding of the phenomena relating to release scenarios (see Example 5-6a).

(ii) Appreciating the limitations of the effect models and their applicability in specific circumstances (see 5-6b).

(iii) Improving the knowledge concerning the sensitivity of outputs to inputs and parameters for a specific model. This can force the user to improve initial estimates of key inputs and parameters for an application.

(iv) Over-simplification in the case of mixtures that have been released. In some circumstances, mixtures of substances are approximated by the dominant component. This might be due to limitations within software systems such as the inability to handle physical properties or phase equilibria predictions of mixtures. These assumptions should be scrutinized carefully for adequacy and the appropriate model used when initial assumptions are inadequate.

(v) In the case of vulnerability models, particular care must be taken when assuming the legitimacy of dose-response or probit functions. In particular, the extrapolation or modification of animal toxicological data for human response predictions can be wildly amiss. "Hidden" conditions such as partial clothing in certain probit functions affects thermal impact assessments.

(vi) Assessing assumptions concerning escape and shelter from various effects such as gas concentrations or thermal radiation impact. Where appropriate these assumptions can make major differences in impact outcomes if they are not adopted.

The message is simply, check sources and the basis on which the models were established. Use the model "fit for purpose", meaning that it must be no simpler or complex than needed. The concept of parsimony applies. Overly complex models can give the appearance of sophistication, an illusion of accuracy and a false sense of security. They can be totally inadequate if applied incorrectly.

**EXAMPLE 5-6 HF CHEMISTRY**

a) Release of HF gas-liquid mixtures requires special consideration because of the complex behaviour of hydrogen fluoride. In particular, HF forms higher molecular weight oligomers $(-HF)_n$ that make HF releases behave as a dense gas. Reaction with ambient moisture generates heat whilst dilution with air cools the mixture. Using simple models for such releases can lead to significant errors.

b) Fire radiation models that assume a "point source" for energy transmission grossly underestimate nearfield effects when more appropriate "view factor" methods that consider flame shape and flame luminosity should be applied.

## 5.4 ASSESSMENT OF EVENT PROPAGATION

Section 5.1.2 considered the definition of an incident as being a sequence of interconnected events. Event propagation occurs due to a number of characteristics including:

(i) The form of the initial release (gas, liquid, solid)
(ii) Presence of contributing factors (ignition sources)
(iii) Absence of mitigation systems (bunds/dikes, drainage systems, emergency shutdown devices)
(iv) Human intervention/lack of action (failure to isolate, inability to diagnose in time or correctly)
(v) Meteorological conditions (windspeed, direction, atmospheric stability)
(vi) Presence of personnel or the public in the vicinity.

Some or all of these factors can play important roles in performing credible consequence analysis.

### 5.4.1 Domino Effects

When certain events propagate into other systems then there is the likelihood of "domino" effects taking place. Typical events that can spawn domino events include:

(i) Explosion (missiles, overpressure effects)
(ii) Fire (pool, jet, fireball or flash fire events)
(iii) Toxic releases (gases and liquids)

Domino effects have become increasingly significant in process risk management due to tighter process integration, tighter spatial designs such as offshore facilities and the establishment of large scale integrated production sites consisting of many adjacent production units. Domino effects have been the subject of several recent studies (Khan and Abbasi, 2001; Cozzani and Salzano, 2004a,b). They are also the subject of major regulatory frameworks such as Seveso II.

Domino effects can be seen as a cross-linking of an event sequence (incident) into another incident through effects generated at any event in the original incident. In Figure 5-4 schematic illustration of this cross-linking or event propagation is given, where the original incident, $I_1$ potentially spawns incident $I_2$ and so on.

Key factors that contribute to the potential for domino effects can include:

(i) The form of effect associated with a particular event $E_i$ in an incident $I_j$. This includes thermal radiation, overpressure, impulse or missiles (vessel fragments)
(ii) The magnitude of the physical effect as predicted by effect models.
(iii) The vulnerability of primary receptor to the physical effects from the incident $I_i$ that leads to the initiation of a new incident $I_k$. This relates to the probabilities $P_{12}$, $P_{23}$, $P_{1x}$, ... that the incident $I_i$ is successful in initiating incident $I_k$.

For example, in assessing missile effects, Hauptmanns (2001), provides a modelling and estimation approach to obtain fragment ranges and trajectories for a variety of scenarios.

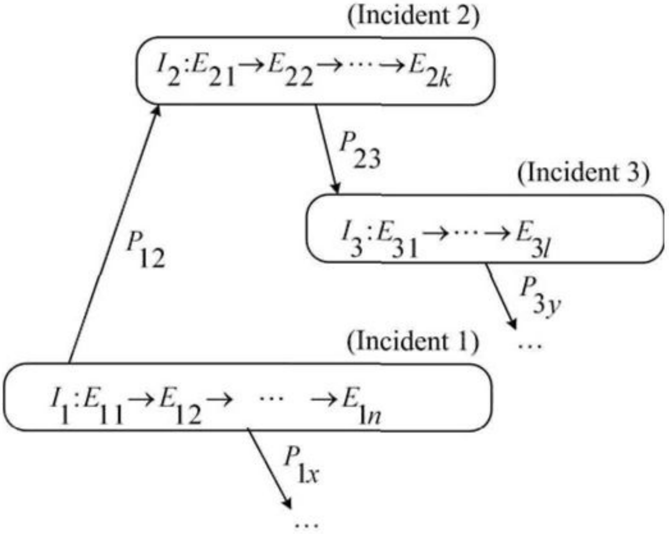

(Incident 2)
$I_2:E_{21}\rightarrow E_{22}\rightarrow\cdots\rightarrow E_{2k}$
$P_{23}$
(Incident 3)
$I_3:E_{31}\rightarrow\cdots\rightarrow E_{3l}$
$P_{12}$
$P_{3y}$
(Incident 1)
...
$I_1:E_{11}\rightarrow E_{12}\rightarrow\ \cdots\ \rightarrow E_{1n}$
$P_{1x}$
...

FIGURE 5-9 DOMINO EFFECT REPRESENTATION

It is clear that effect and vulnerability models play an important role in assessing domino effects. Their consideration is of growing importance in contemporary risk management especially in circumstances of tight spatial integration within a plant and across sites.

### EXAMPLE 5-7 DOMINO INCIDENTS

a) Failure in internal vessel integrity of an acid droplet separator in an ammonia absorption unit led to carry over of an acidic solution to a decanter. The acid reacted with decanter contents, emulsifying the decanter and losing separation of tar components that eventually recycled to a coke making operation causing massive blockages. As a result of the blockages large amounts of fresh water were needed to cool hot coke ovens gas. The contaminated water eventually overflowed a retention basin causing an environmental accident in the local waterway.

b) The initial LPG fire and explosion at Pemex, Mexico in 1984 propagated through the complete facility over a period of 8 hours leaving over 500 people dead, the majority of the site destroyed and major damage to surrounding housing areas. Over 200,000 people were evacuated.
A major factor in domino effects was the extremely close layout of vessels on the site and the amount of flammable materials that were stored. Inappropriate housing development was a major contributing factor to the high number of deaths off-site. In this instance domino effects were extreme (TNO 1985).

### 5.4.2 Models to Represent Propagations

There are two primary cases to consider where propagation is important. These are:

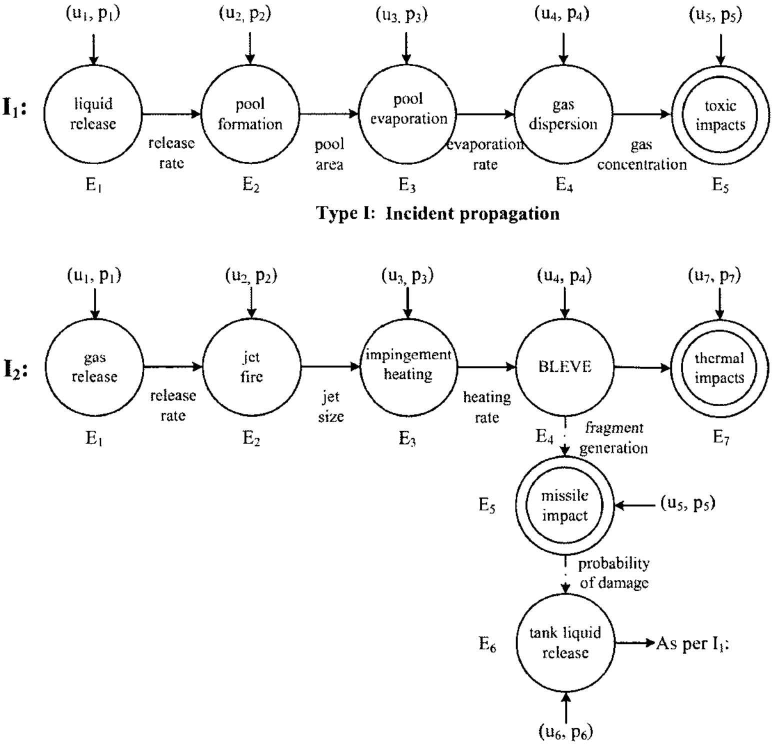
a) Event to event propagations via effect models (Type I) .
b) Event to event propagations via vulnerability models (Type II) .

In case a) the incident is formed from an initiating event $E_1$ whose physical effect is used as a partial input to event $E_2$ and so on until reaching the terminating event, normally represented by a vulnerability model.

In case b) one or more events in an incident sequence spawn other incidents. This is the domino issue where new incidents are generated from a single initiating incident. In this case the linking across incidents is done through a vulnerability model.

In both cases it is necessary to effectively link the submodels together in the incident so that event propagations are established. One key issue in doing this is that outputs from one model must be within validity limits of the inputs to another model. Otherwise it is possible to generate invalid or nonsense results. This is reinforced by Cozzani and Salano (2004a) where the use of inappropriate vulnerability models can lead to errors of up to 500%. This was in the context of vessel response to explosion overpressures.

Figure 5-8 illustrates the two key propagation types that have been discussed showing the use of specific models, their inputs ($u_i$), parameters ($p_i$) and linkages. Again, models "fit for purpose" is the principal requirement in obtaining credible outcomes from such analyses. Some of these modelling issues are addressed in Chapters 6 and 7 where consideration is given to effect models and then vulnerability models.



Type I: Incident propagation

Type II: Incident to incident propagation (Domino)

FIGURE 5-10 EVENT PROPAGATION MODELS

## 5.5 REVIEW

This chapter has introduced a number of key concepts in consequence analysis. In particular, the two principal models of effect and vulnerability were discussed. Both play an important role in process systems risk analysis.

Events, incidents and scenarios were introduced and the accompanying models that allow quantitative estimates to be made were discussed in general terms. Each model has its application area and its own limitations and validity ranges. This must be appreciated. A knowledge of these factors is vital in generating credible results from the use of such models.

It was emphasizcd that considerable uncertainty can be associated with various models particularly when they are used outside their validation limits. The use of input and parameter sensitivity studies should be carried out in order to gauge the importance of these inputs. Efforts in tying down key inputs and parameters to better estimates can be then made. For all model use we must appreciate the parametric and structural uncertainties present in the models and address them effectively.

## 5.6 REFERENCES

Benjamin, S.L. and Belluck, D.A. 2001, *A Practical Guide to Understanding, Managing and Reviewing Environmental Risk Assessment Reports*, Lewis Publishers, Boca Raton, USA.

CCPS 2000, *Guidelines for Chemical Process Quantitative Risk Analysis*, 2nd edn, AIChE, New York

Cozzani, V. and Salzano, E. 2004a, 'The quantitative assessment of domino effects caused by overpressure Part I Probit models', *Journal of Hazardous Materials*, vol. A107, pp. 67-80.

Cozzani, V. and Salzano, E. 2004b, 'The quantitative assessment of domino effects caused by overpressure Part II Case studies', *Journal of Hazardous Materials*, vol. A107, pp. 81-94.

CRC 1968, *CRC Handbook of Tables for Probability and Statistics*, (ed.) W.H. Beyer, Chemical Rubber Company, Cleveland, USA.

DOE 1995, *A Guide to Risk Assessment and Risk Management for Environmental Protection*, Dept. of the Environment, UK Government, HMSO, London.

Hauptmanns, U. 2001, 'A Monte-Carlo based procedure for treating the flight of missiles from tank explosions', *Probabilistic Engineering Mechanics*, vol. 16, pp. 307-312.

Khan, F.I. and Abbasi, S.A. 2001, 'An assessment of the likelihood of occurrence and the damage potential of domino effect in a typical cluster of industries', *Journal of Loss Prevention in the Process Industries*, vol. 14, pp. 283-306.

Lees, F.P. 2001, *Loss Prevention in the Process Industries*, 3 volumes, Butterworth-Heinemann, UK, ISBN 0 750615478.

Queensland Fire Service 1987, *Gas Explosion - Cairns, Australia*, Queensland Fire Service, Queensland State Government Report.

Standards Australia. *Environmental Risk Management: Principles and Process*, , Standards Australia, Canberra, HB203:2000.

TNO 1985, *Analysis of the LPG incident in San Juan Ixhuatepec, Mexico City, 19 November 1984*, Report 85-0222, Netherlands Organisation for Applied Scientific Research, Division of Technology for Society, Apeldoorn, The Netherlands.

TNO 1992, *Methods for the determination of possible damage*, (CPR 16E, the TNO Green Book), The Director General of Labour, The Netherlands, Vooburg, ISBN 9053070524.

TNO 1997, *Methods for the Calculation of Physical Effects,* CPR14E, Director General of Labour, The Netherlands (the TNO Yellow Book, volumes 1 & 2.

## 5.7 NOTATION

| | |
|---|---|
| AS | Australian Standards |
| BLEVE | Boiling Liquid Expanding Vapour Explosion |
| CCPS | Center for Chemical Process Safety, AIChE, USA |
| CFD | Computational Fluid Dynamics |
| COC | Chemical of Concern |
| COPC | Chemical of Potential Concern |
| DOE | Department of Environment |

| | |
|---|---|
| ERA | Environmental Risk Assessment |
| ERPG | Emergency Response Planning Guidelines |
| HF | Hydrogen Fluoride |
| IDLH | Immediately Dangerous to Life and Health |
| km | kilometre |
| LPG | Liquefied Petroleum Gas |
| $m^3$ | Cubic metres |
| RDX | Cyclo-trimethylene-trinitramine explosive |
| Sdu | Director-General for Social Affairs, the Netherlands |
| STEL | Short Term Exposure Limit |
| TLV | Threshold Limit Value |
| TNT | Trinitro Toluene |

This page is intentionally left blank

# 6 EFFECT MODELS FOR CONSEQUENCE ANALYSIS

*"Every cause must produce an effect and every effect must have a cause"*
*Law of Universal Causation in Logic*

We discussed in Chapter 5 that there are two components to consequence modelling–effects models and vulnerability models. This chapter deals with the physical effects of releases of hazardous materials and the subsequent events that generate thermal radiation, toxic gas concentrations or explosion overpressures. Vulnerability of receptors is dealt with in Chapter 7. Wells (1980) has described a number of issues of how to incorporate the effects and vulnerability modelling in process plant design.

It is not the purpose of this chapter to give a complete coverage of effect models. The chapter provides an overview of the key issues and approaches, providing references for more detailed modelling information. What is given are insights and suggestions for the use of such models in hazard analysis. A number of well established software tools are available for these predictions.

## 6.1 RELEASE OF HAZARDOUS SUBSTANCES

### 6.1.1 Factors Affecting Release Modelling

The first category of events is the release of a hazardous material from containment such as a pipe, tank and vessel or transport tanker.

Table 6-1 gives a summary of the types and location of releases (Lees, 2001) which could be encountered. Each release has a specific characteristic which is dependent on

(i) the physical state of the material (solid, liquid, gas)
(ii) the physical situation (pipe, pump, vessel)
(iii) physico-chemical properties (density, viscosity, vapour pressure, reactivity)
(iv) operating conditions (pressure, temperature, concentration)

Variations in factors such as aperture size, type of plant, material state lead to quite different release cases. Taking one item from each parameter in Table 6-1, a large number of combinations is possible.

Some simple models can help quantify the release rates. What follows is a summary of some simple models and examples of their application.

TABLE 6-1 RELEASE CASES

FLUID:
- gas/vapour
- liquid
- two-phase

PLANT:
- vessel
- other equipment
- pipework

APERTURE:
- complete rupture
- limited rupture

ENCLOSURE:
- inside building
- in open air

HEIGHT:
- below ground level
- at ground level
- above ground level

FLUID MOMENTUM:
- low
- high

### 6.1.2 Key Points in Release Modelling

It cannot be over-emphasized that release modelling or "source" modelling is one of the most important aspects of consequence analysis. It is the first event in any incident and as such plays a dominant role in the outcomes. Key issues in dealing with releases include:

(i) **Material state**:

A single component or mixture can, under appropriate conditions, exist in several states such as vapour, liquid or solid. It is vital that the storage conditions (temperature and pressure) are considered, so as to determine the form of release.

In storage vessels containing liquids, material can escape from either the vapour space or in the liquid region, having significantly different release rates and subsequent behaviour.

(ii) **System dynamics**:

Most releases are dynamic (time variant) in nature, since temperatures and pressures within a containment system change as inventory changes or as the release continues.

Pressurized gas storage vessels drop in pressure as gas is released. This rate of pressure decrease is dependent on the size of the failure. This in turn reduces the driving force (pressure difference) and hence the flowrates over time. Basing the discharge rates only on initial system conditions can lead to massive conservatism in consequence analysis.

Similar comments can be made when considering releases from major gas transmission lines, where rapid depressurization can occur depending on the aperture size of the failure. Here the initial gas "burst" rate can rapidly diminish in seconds as the depressurization takes place.

(iii) **Isolatable Inventory**:

In process plants, a frequently encountered situation is where safety instrumented systems (SIS) activate in order to isolate an inventory.

In such a case, the maximum release quantity is restricted to the inventory isolated from other process units. The time-variant release rate and the duration of the release need to be evaluated for effects modelling.

(iv) **Flow systems**:

In many cases, release events occur in piping systems where the flow is maintained by a pump or a gas compressor. In these instances, if the motive device continues to operate, then the sustained flow is ultimately controlled by the following:

(a) Aperture size controlling. The leak rate is much smaller than the process flow rate, and the release rate is controlled by the aperture size of the leak.

(b) Process flow rate controlling. The line or vessel failure is substantial, and after an initial high rate of release, the release rate would settle down to the process flow rate until the motive device is shut down.

(v) **Physico-chemical phenomena**:

Substances and mixtures can often display unexpected behaviour due to the phase equilibria properties. Substances such as acetic acid can form dimers (double molecules) in the vapour phase. Hydrogen fluoride (HF) forms oligomers (multiple molecules). This type of chemical and phase behaviour directly affects estimates of release rates.

Some materials such as gases compressed into liquid form, such as LPG, butane or butadiene produce vapour-liquid mixtures on release from containment. The subsequent behaviour of the release then needs to be handled correctly to estimate vapour and liquid source terms from such "flashing" releases. "Rain-out" of liquid droplets can also occur.

(vi) **Release location**:

The release behaviour depends on the location in the system and the presence of nearby obstacles or equipment. Key issues to consider are:

- Direct discharge impingement altering the ultimate release orientation. For example, to ground or onto nearby structures.
- Release on suction or discharge side of pumps or compressors.
- Release inside, outside or over bunded/diked areas.
- Release from vessel wall, nozzle or along connecting pipework in the case of "flashing" liquids, can give different release rates, based on the length of the leak path.

### EXAMPLE 6-1 GAS TRANSMISSION LINE RELEASE

Figure 6-1 shows gas release estimates for the full-bore discharge from a natural gas pipeline of 457 mm diameter operating at 15.3 MPa. Rapid depressurization leads to a significant drop in gas discharge rate over the first 10 seconds.

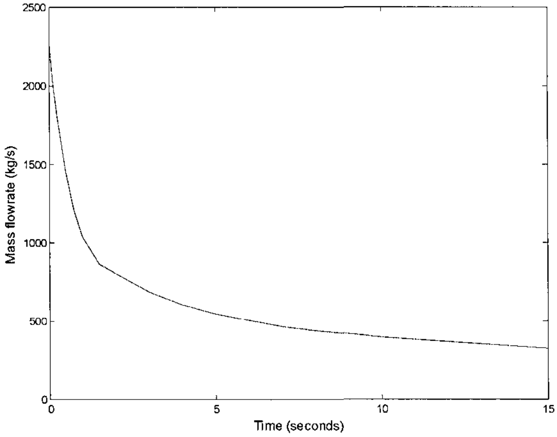


FIGURE 6-1 GAS RELEASE FLOW TRANSIENT FOR PIPELINE

## 6.2 GAS RELEASES

Figure 6-2 gives an overview of gas release types and potential consequences. Both short-term and continuous releases are covered as well as subsequent impacts. In considering gas releases, there are two situations which need to be addressed. The first is when the pressure driving force ($P_1$ - $P_2$) is small and the gas flowrate is below sonic velocity (speed of sound). The other is when the pressure difference is large when there is sonic flow. There is a critical pressure ratio $\left(\frac{P_2}{P_1}\right)$ which determines the type of release, where $P_1$ is the upstream (higher) pressure and $P_2$ refers to the downstream (lower) pressure. Sonic flows occur when this ratio is less than about 0.5.

In some cases, the flowrate switches from sonic to subsonic flow as $P_1$ decreases and the critical pressure ratio is reached.

Table 6-2 gives the common models for pressurized gas releases.

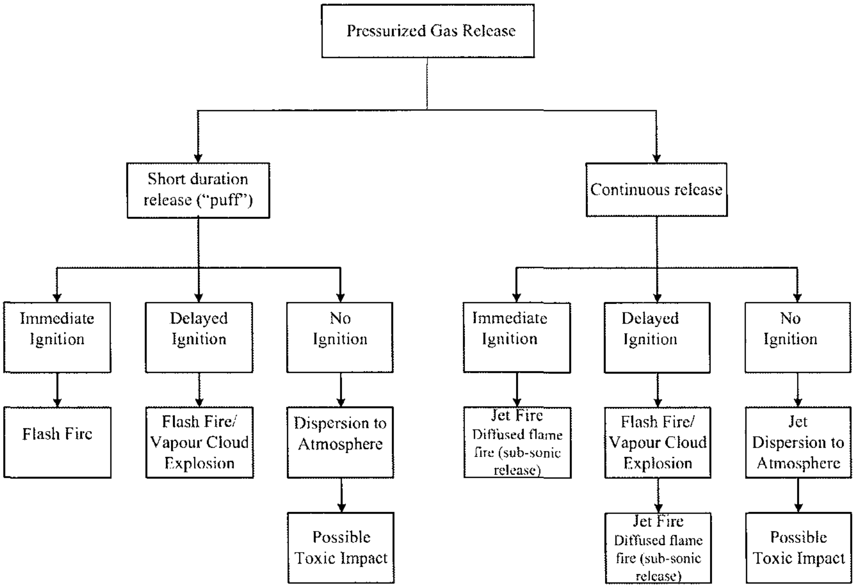

Pressurized Gas Release
Short duration release ("puff")
Continuous release
Immediate Ignition
Delayed Ignition
No Ignition
Immediate Ignition
Delayed Ignition
No Ignition
Flash Fire
Flash Fire/ Vapour Cloud Explosion
Dispersion to Atmosphere
Jet Fire Diffused flame fire (sub-sonic release)
Flash Fire/ Vapour Cloud Explosion
Jet Dispersion to Atmosphere
Possible Toxic Impact
Jet Fire Diffused flame fire (sub-sonic release)
Possible Toxic Impact

FIGURE 6-2 PRESSURIZED GAS RELEASE CONSEQUENCES

## TABLE 6-2 GAS DISCHARGE MODELS

The specific discharge rates for gases are given by the following models, where the high pressure is condition 1, the low pressure is condition 2.

Subsonic Flow

$$W = \frac{C_d}{V_2}\left[2P_1V_1\frac{k}{k-1}\left(1-\left(\frac{P_2}{P_1}\right)^{\frac{k-1}{k}}\right)\right]^{\frac{1}{2}} \qquad (6.1)$$

Sonic Flow

$$W = C_d\left[\frac{P_1}{V_1}k\left(\frac{2}{k+1}\right)^{\frac{k+1}{k-1}}\right]^{\frac{1}{2}} \qquad (6.2)$$

where:

$W$ = specific mass flowrate (kg/m$^2$s)

$k$ = ratio of specific heats $C_p/C_v$)
$\approx$1.67 for monotomic gases (argon, helium)
$\approx$1.41 for diatomic gases ($O_2$, $N_2$, $H_2$)
$\approx$1.3 for complex gases ($CH_4$, $CO_2$)

$V_1$, $V_2$ = specific volumes of gases at conditions 1 and 2 (m$^3$/kg)

$P_1$ = upstream (high) pressure (Pa)

$P_2$ = downstream (low) pressure (Pa)

$C_d$ = discharge coefficient
~ 0.61 for sharp discharge hole
~ 0.80 for smooth discharge hole

The critical pressure ratio for sonic conditions is given by:

$$\frac{P_2}{P_1} \langle \left(\frac{2}{k+1}\right)^{\frac{k}{k-1}} \qquad (6.3)$$

### EXAMPLE 6-2 DISCHARGE OF ETHYLAMINE VAPOUR

The gas release from a broken 25mm nozzle in the vapour space of a storage tank is required. Storage temperature is 65°C giving a 500 kPa vapour pressure. Specific volume of gas is 0.125 $m^3/kg$.

From equation (6.3) the critical pressure ratio is:

$$\frac{P_2}{P_1} = \left(\frac{2}{k+1}\right)^{\frac{k}{k-1}} \simeq \left(\frac{2}{1.3+1}\right)^{\frac{1.3}{0.3}} = 0.55$$

Since $P_2/P_1 < 0.55$ sonic flow occurs. Equation (6.2) gives:

$$W = 0.6\left[\frac{5\times10^5}{0.125}(1.3)\left(\frac{2}{2.3}\right)^{\frac{2.3}{0.3}}\right]^{\frac{1}{2}} = 800\,\text{kg/m}^2\text{s}$$

Mass flowrate G = W*Area of flow = 800 (4.91 x $10^{-4}$) = 0.4 kg/s

Figure 6-3 summarises the sequence of effects following a gas release.

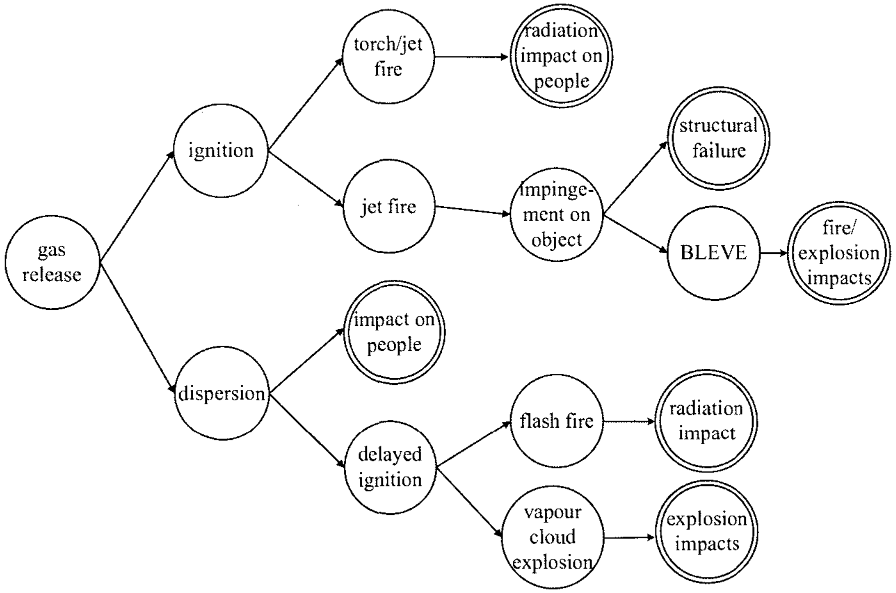


FIGURE 6-3 LIKELY GAS RELEASE INCIDENTS

## 6.3 LIQUID RELEASES

### 6.3.1 Atmospheric Storage

Many liquids are stored in tanks vented to atmosphere. Leaks from such storage facilities are driven by the available head of liquid, which generates the internal pressure at the leak aperture. The rate is a function of the pressure and the aperture size as well as fluid density. Leaks from bunded/diked storage can end up in the containment area. For atmospheric storage, bund/dike design and distance of bund wall to tank is specified by codes (e.g. NFPA30-2000, AS1940-1993) to ensure that jets of liquid cannot project over bunds or dikes.

### 6.3.2 Pressurized Storage

When a liquid is released under pressure it flows at a rate which is dependent on the pressure difference across the hole (aperture) and the size of the hole. Figure 6-4 shows the various incidents that can take place on the release of liquids from containment.

When release is from pressurized storage there are two contributions to the pressure driving the liquid from the hole. The first is the pressure in the tank due to pressurized storage. The second is the liquid head generated by the height of liquid above the hole. In pipelines we are normally given an operating pressure and hence the second term is not relevant to the flowrate calculation.

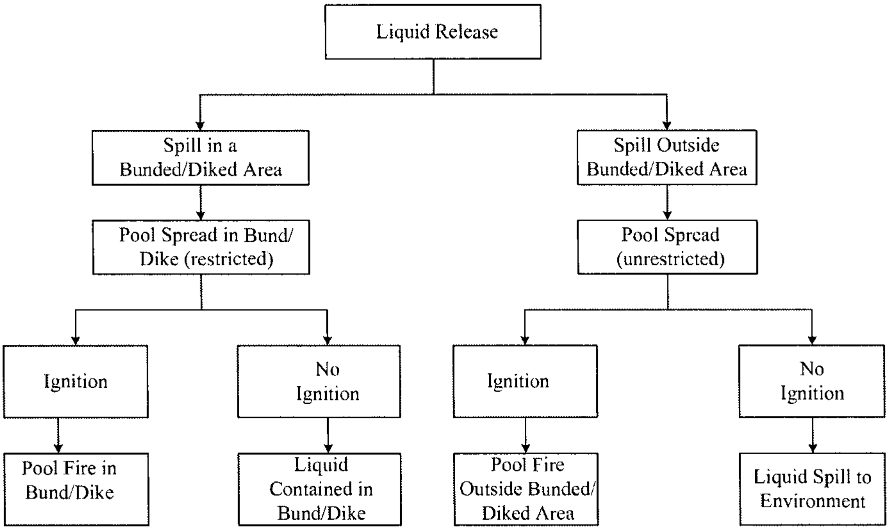

Liquid Release
Spill in a Bunded/Diked Area
Spill Outside Bunded/Diked Area
Pool Spread in Bund/ Dike (restricted)
Pool Spread (unrestricted)
Ignition
No Ignition
Ignition
No Ignition
Pool Fire in Bund/Dike
Liquid Contained in Bund/Dike
Pool Fire Outside Bunded/ Diked Area
Liquid Spill to Environment

FIGURE 6-4 CONSEQUENCES OF LIQUID RELEASE FROM STORAGE

Table 6-3 gives the model used for estimating liquid releases, based on the Bernoulli equation.

### TABLE 6-3 LIQUID DISCHARGE MODEL

The discharge rate is given by:

$$W = C_d\sqrt{2\rho_L(P_1 - P_2)} + C_d\rho_L\sqrt{2gh} \tag{6.4}$$

where:

| | |
|---|---|
| $W$ | = specific mass flowrate (kg/m$^2$s) |
| $\rho_L$ | = liquid density (kg/m$^3$) |
| $C_d$ | = discharge coefficient<br>0.61 sharp edged orifice<br>0.80 short piece of pipe |
| $P_1$ | = upstream absolute pressure (Pa) |
| $P_2$ | = downstream absolute pressure (Pa) |
| $h$ | = head of liquid (m) |
| $g$ | = gravitational constant (9.81 m/s$^2$) |

We calculate the mass flowrate per unit area ($W$) then multiply by the area of the opening to get the final mass flowrate.

### EXAMPLE 6-3 DISCHARGE OF ETHYLAMINE FROM A FUEL STORAGE VESSEL

A 3.0 m high tank has a leak via a broken 25mm nozzle on its base. Storage temperature is 65°C and the vapour pressure of the liquid is 5 × 10$^5$ Pa. Liquid density is 680 kg/m$^3$, and atmospheric pressure is 1 × 10$^5$ Pa.

Using equation (6.4) we have:

$$W = 0.61\sqrt{2(680)(5\times10^5 - 1\times10^5)} + 0.61(680)\sqrt{2(9.81)3.0} = 17409\,\text{kg/m}^2\text{s}$$

Area of aperture = $\pi D^2/4$, hence $A = \frac{\pi}{4}(0.025)^2 = 4.91\times10^{-4}\ \text{m}^2$

Mass flow $G = W.A = 8.5$ kg/s

Figure 6-5 is a summary of the sequence of effects following a liquid release.

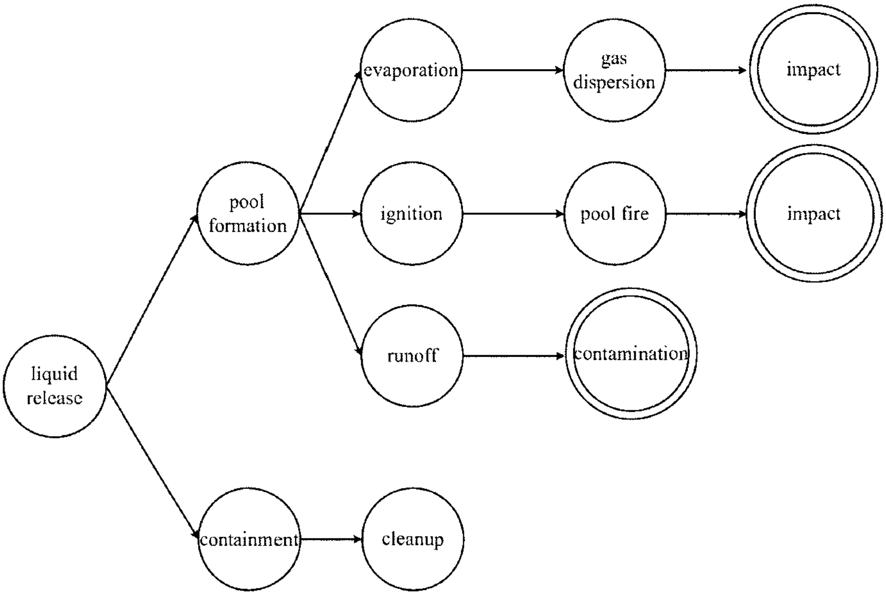


FIGURE 6-5 LIKELY LIQUID RELEASE SCENARIOS

## 6.4 FLASHING LIQUID RELEASES

### 6.4.1 Liquefied Gases

Liquefied gases are common substances. Many gases are liquefied by two mechanisms:

(i) Liquefaction by pressure, such as propane or butane (LPG)
(ii) Liquefaction by cooling, such as ethylene

Liquefaction reduces the volume of the material and aids in storage and handling. It does however generate significant effects when loss of containment occurs. The following sections outline the important issues.

### 6.4.2 Liquids above their Atmospheric Boiling Point

Liquefied gas releases are common and pose particular problems due to the "flashing" nature of the liquid as the pressure is reduced. Figure 6-6 shows the potential incidents associated with liquefied gas releases. In some cases, like the storage of LPG under pressure, when the liquid LPG starts to flow down a pipe which has a hole in it, there is a significant pressure gradient along the leak path, from storage pressure to the "choke" pressure (i.e. pressure at the hole at the point of discharge to atmosphere). This causes part of the LPG to vaporize, and a two-phase mixture exists at the choke. . Thus the discharge is a mixture of both liquid and vapour.

The release rate for such a flow is given in Table 6-4.

### TABLE 6-4 TWO PHASE FLOW RELEASE MODEL

The specific mass flowrate is given by:

$$W = C_d \sqrt{2\hat{\rho}(P_1 - P_c)} \tag{6.5}$$

where:

$C_d$ $\cong$ 0.61
$\hat{\rho}$ = mean density of the vapour-liquid mixture (kg/m$^3$)
$P_I$ = upstream pressure (Pa)
$P_c$ = choke pressure (Pa)

We calculate the mass flowrate per unit area ($W$) then multiply by the area of the opening to get the final mass flowrate.

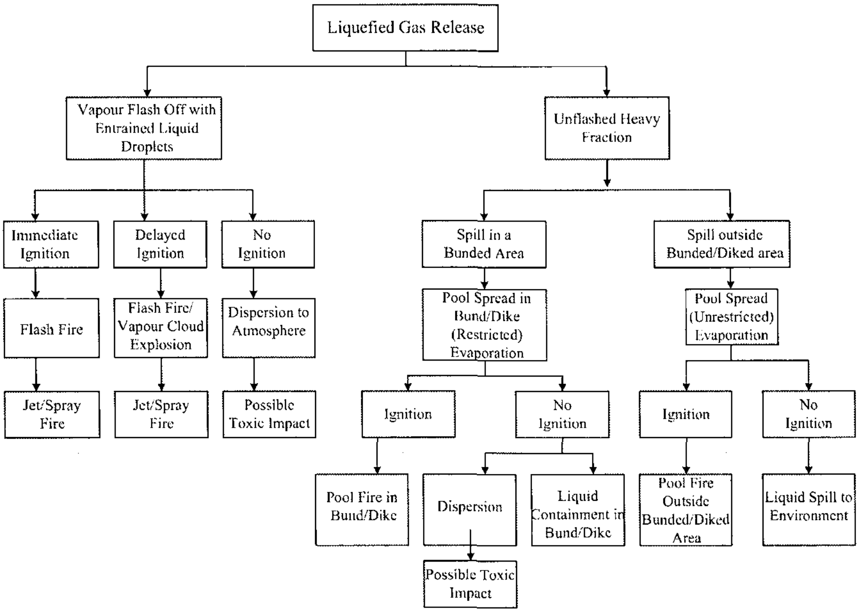

Liquefied Gas Release
Vapour Flash Off with Entrained Liquid Droplets
Unflashed Heavy Fraction
Immediate Ignition
Delayed Ignition
No Ignition
Spill in a Bunded Area
Spill outside Bunded/Diked area
Flash Fire
Flash Fire/ Vapour Cloud Explosion
Dispersion to Atmosphere
Pool Spread in Bund/Dike (Restricted) Evaporation
Pool Spread (Unrestricted) Evaporation
Jet/Spray Fire
Jet/Spray Fire
Possible Toxic Impact
Ignition
No Ignition
Ignition
No Ignition
Pool Fire in Bund/Dike
Dispersion
Liquid Containment in Bund/Dike
Pool Fire Outside Bunded/Diked Area
Liquid Spill to Environment
Possible Toxic Impact

**FIGURE 6-6 CONSEQUENCE OF RELEASE OF LIQUEFIED GASES**

In equation (6.5) the choke pressure $P_c$ is difficult to estimate and is clearly critical in determining the specific mass flowrate $W$. This is because the temperature and hence fluid properties change along the pipe thus making the calculation non-trivial. Techniques are available to handle this situation in a thermodynamically rigorous manner (TNO 1997).

An alternate approach suggested by Fletcher and Johnson (1984) uses a simpler expression:

$$W = C_d f(l)\sqrt{P_1} \tag{6.6}$$

where:

| | |
|---|---|
| $W$ | = specific mass flowrate (kg/m$^2$.s) |
| $f(l)$ | = flow correction function, based on length |
| $C_d$ | $\cong 0.61$ |
| $P_l$ | = upstream pressure (Pa) |

The function $f(l)$ is derived from experiments with 2-phase water flows and varies with length of pipe ($l$) to the break. The following table presents values of $f(l)$ as a function of distance to the break.

**TABLE 6-5 FLOW CORRECTION FACTORS FOR 2-PHASE FLOW**

| Length to aperture l(mm) | $f(l)$ |
|---|---|
| 0 | 44.72 |
| 25 | 31.62 |
| 50 | 22.36 |
| 75 | 18.71 |
| 100 | 17.32 |
| 150 | 16.12 |
| 200 | 15.81 |
| 300 | 15.49 |
| 500 | 15.33 |
| 700 | 14.14 |

It should be remembered that this is an approximate method, which nevertheless gives a reasonable first estimate of the flow. Use of this method should be restricted to pipe lengths no greater than 750 mm, e.g. pipework close to storage vessels. Other techniques are needed for long pipes such as LPG transmission systems.

**EXAMPLE 6-4 ESCAPE OF ETHYLAMINE IN CONNECTING PIPE**

Consider a release of ethylamine from a 25 mm diameter pipe connected to the base of a storage tank, where ethylamine is stored at 65°C and a vapour pressure of $5 \times 10^5$ Pa. Liquid density is 680 kg/m$^3$.

The pipe is broken 500 mm from where it joins the tank. The height of liquid in the tank is 3 metres.

The pressure at the tank base ($P_l$), is the vapour pressure plus the liquid head:

$$P_1 = 5\times10^5 + \rho_L gh = 5\times10^5 + 680(9.81)(3) = 5.2\times10^5 \text{ Pa}$$

Using the simplified equation (6.6) and the flow correction from Table 6-5:

$$W = 0.61(15.3)\sqrt{5.2 \times 10^5} = 6743\ \text{kg/m}^2\text{s}$$

The mass flowrate is then

$$G \quad = \quad W.(Area) = 6743\ (4.91\ \text{x}\ 10^{-4}) = 3.3\ \text{kg/s}$$

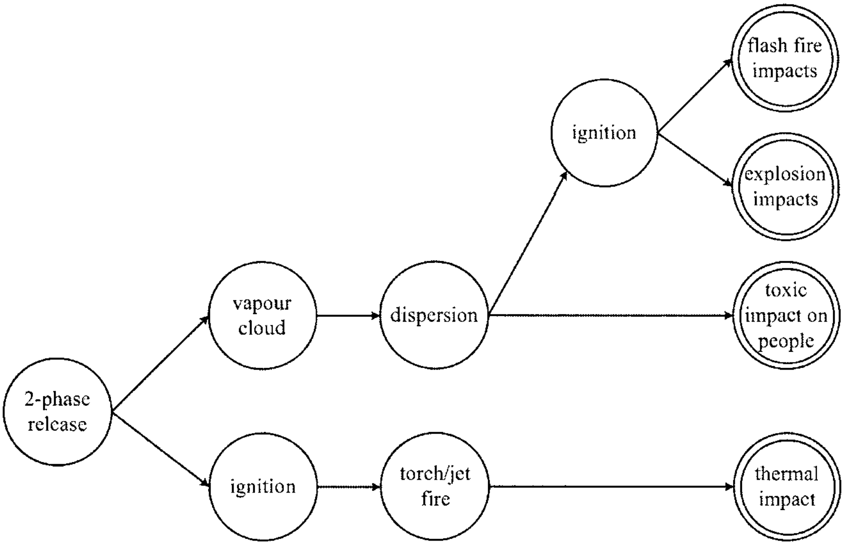


FIGURE 6-7 TWO-PHASE RELEASE INCIDENTS

### 6.4.3 Flash-off and Rainout

When a liquid held under pressure and at a temperature above its normal boiling point is released, some of the liquid "flashes" to form vapour. In these cases it is important to know how much vapour is formed. Not only is vapour formed but droplets of liquid are entrained in the vapour. Drops of very small size (aerosol) subsequently form part of the vapour cloud. Larger droplets may "rain out" and drop back to ground. This mechanism needs to be considered in effects modelling. Table 6-6 gives the model for computing the flashed amount from pressurized release. This is derived form an energy balance on the liquid.

### TABLE 6-6 FLASH MODEL FOR LIQUEFIED GASES

The mass fraction of liquid flashed ($\phi$) is:

$$\phi = 1 - \exp\left[-\frac{C_p}{\Delta H_v}\left(\theta_1 - \theta_2\right)\right] \quad ; \quad \theta_1 > \theta_2 \tag{6.7}$$

where:

$C_p$ = specific heat of liquid (kJ/kgK)
$\Delta H_v$ = latent heat at boiling point (kJ/kg)
$\theta_1$ = storage temperature (K)
$\theta_2$ = normal boiling point (K)

Typically the fraction entrained (e) is: $e = \phi$ (if $\phi < 0.5$) or $e = 1 - \phi$ (if $\phi > 0.5$)

Total mass of cloud is: $W = (e + \phi)\, W_o$ (6.8)

Volume of cloud is: $V = \dfrac{WM_a}{\rho_a M}$ (6.9)

where:

$\rho_a$ = density of air (kg/m$^3$)
$M_a$ = molecular weight of air (29 kg/kgmole)
$M$ = molecular weight of fluid (kg/kgmole)
$V$ = volume of cloud (m$^3$)
$W$ = cloud mass (kg)
$W_o$ = initial mass of liquid (kg)

### EXAMPLE 6-5 PRESSURE RELEASE OF STORAGE TANK

Pressure is suddenly reduced on a tank of ethylamine via a significant structural failure which leads to release of the contents. The basic data are:

$C_p$ = 2.92 kJ/kgK
$\theta_1$ = initial temperature = 65 + 273 = 338K
$\theta_2$ = boiling point = 290K
$\Delta H_v$ = 623 kJ/kg

Using equation (6.7) the flashed fraction is

$$\phi = 1 - \exp\left[-\frac{2.92}{623}\left(338 - 290\right)\right] = 0.20$$

Spray fraction: $e \cong \phi = 0.2$ (since $\phi < 0.5$)

Fraction of vapour is $\phi + e \cong 0.4$

If the tank contained 20,000 kg of ethylamine then the mass of material in the cloud is approximately:

$$W = 0.4\ (20{,}000) = 8000\ \text{kg}.$$

## 6.5 EVAPORATION OF LIQUID POOLS

When a liquid is spilled and there is air movement over the surface, the substance will evaporate and travel downwind. It is necessary to know the rate at which material evaporates as this can then be used with a dispersion model to calculate downwind distances to flammability limits or specified toxic gas concentrations.

The principal factors requiring consideration in treating evaporation from liquid pools are given in Table 6-7.

TABLE 6-7 KEY FACTORS IN EVAPORATION MODELS

- Pool extent: contained or unrestrained spread
- Ground conditions: porous, non-porous, …
- Ambient conditions: windspeed, temperature, cloud cover
- Evaporation regime: non-boiling, boiling pools
- Heat transfer: solar, ground effects, ambient, …
- Physico-chemical properties: vapour pressure, boiling point, …
- Mass transfer: convective, stagnant film (no wind)
- Time effects: transient, steady state

Figure 6-8 shows a typical scenario for contained spills and the various heat and mass transfer mechanisms that can be important. Table 6-8 develops a generic pool evaporation model.

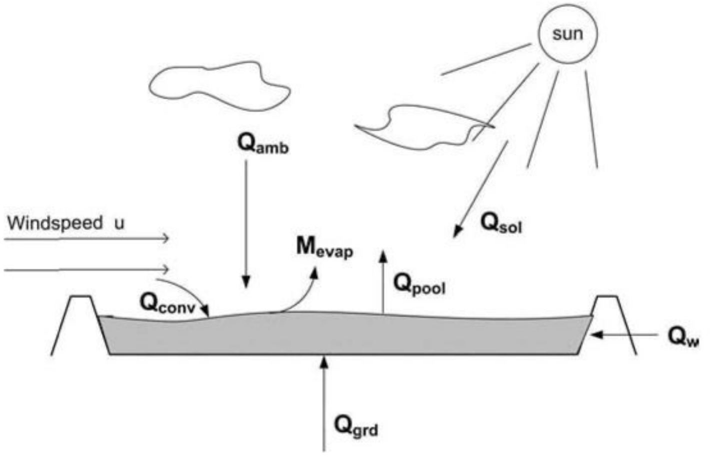


FIGURE 6-8 POOL EVAPORATION - KEY MECHANISMS

## TABLE 6-8 GENERIC POOL EVAPORATION MODEL

A general dynamic model can be developed which accounts for these controlling factors (Kawamura and Mackay 1987).
This is an energy balance that can be written as:

$$\frac{dE_P}{dt} = \frac{d(M_P T_P C_P)}{dt} = Q_{amb} + Q_{conv} + Q_{grd} + Q_w + Q_{sol} - Q_{pool} - \dot{m}A\Delta H_v \quad (6.10)$$

where:

| | |
|---|---|
| $E_p$ | = total pool energy (kW) |
| $M_p$ | = mass of liquid in the pool (kg) |
| $T_p$ | = pool temperature (K) |
| $C_p$ | = liquid heat capacity (kJ/kgK) |
| $Q_{amb}$ | = longwave radiation from atmosphere (kW) |
| $Q_{conv}$ | = convective heat flux from wind (kW) |
| $Q_{grd}$ | = conductive heat flow from ground (kW) |
| $Q_w$ | = conductive heat flow from walls (kW) |
| $Q_{sol}$ | = shortwave solar radiation (kW) |
| $Q_{pool}$ | = longwave radiation from the pool (kW) |
| $\dot{m}$ | = evaporation rate (kg/s.m$^2$) |
| $A$ | = pool surface area (m$^2$) |
| $\Delta H_v$ | = latent heat at boiling point (kJ/kg) |

Correlations for the $Q$ terms can be obtained in standard references (TNO 1997) whilst mass transfer coefficients from pools are also available (Kawamura and Mackay 1987). The Kawamura correlation is:

$$k_m = 4.786 \times 10^{-3} u_w^{\ 0.78} d_p^{\ -0.11} Sc^{-0.67} \quad (6.11)$$

Here the Schmidt number ($Sc$) = $\upsilon_a/D_a$ (~ 0.8 for vapours)

and

| | |
|---|---|
| $\upsilon_a$ | = vapour kinematic viscosity (m$^2$/s) |
| $D_a$ | = diffusivity of vapour in air (m$^2$/s) |
| $d_p$ | = pool diameter (m) |
| $u_w$ | = wind velocity (m/s) |
| $k_m$ | = mass transfer coefficient (m/s) |

Other issues that often need addressing in pool evaporation events are:

(i) The prediction of pool spread if the release is outside bunded/diked areas. This is typically in the form of:

$$r(t) \cong ct^b \quad (6.12)$$

where $C$ and $b$ are constants relevant to particular release and ground conditions.

(ii) Ground cooling under the pool. Here a hot ground surface may cool rapidly on contact with the liquid and thus $Q_{grd}$ might reduce rapidly, especially for cryogenic liquid spills.

(iii) Boiling pools. In the case where liquefied gas is released to ground the evaporative mechanism is controlled by boiling. This requires an estimate of critical heat fluxes. Models such as LPOOL (Cavanaugh et al. 1994) consider this mechanism. In the case of LPOOL, initial flash and aerosol entrainment models are also available.

In most models, the evaporation rate for non-boiling pools is a function of $u_w^{0.78}$, reflecting the 0.78 power dependence within the mass transfer correlation. In many cases, initial evaporation estimates based on steady state conditions can be given by rather simple correlations. The evaporation rate models by Lees (1980) and Peress (2003) are given in Table 6-9.

**TABLE 6-9 SIMPLE EVAPORATION MODELS**

The evaporation rate from small rectangular and circular pools is given by (Lees, 1980) as:

Rectangular Pools:

$$E_R = 2.625\times10^{-7}\left(\frac{M.P^\circ}{T}\right)u_w^{0.78}x^{0.89}y \tag{6.13}$$

Circular Pools:

$$E_C = 7.876\times10^{-7}\left(\frac{M.P^\circ}{T}\right)u_w^{0.78}r^{1.89} \tag{6.14}$$

where:

$E_R, E_c$ = evaporation rate (kg/s)
$x$ = downwind pool dimension (m)
y = crosswind pool dimension (m)
$M$ = molecular weight of liquid (kg/kgmole)
$P^o$ = vapour pressure of the liquid (Pa)
$T$ = absolute temperature of liquid (K)
$u_w$ = mean wind speed (m/s)
$r$ = radius of pool (m)

The model by Peress (2003) in SI units is given by:

$$E_p = 2.117\times10^{-6}u^{0.78}M^{\frac{2}{3}}\cdot\frac{AP^\circ}{T} \tag{6.15}$$

where A = pool area (m$^2$)

Where actual experimental data exists for pool evaporation rate, this should be used in preference to the models. Shaw and Briscoe (1978) describe the pool evaporation rates for specific substances including LNG.

**EXAMPLE 6-6 EVAPORATION OF ETHYLAMINE**

A rectangular pool of ethylamine is formed which has dimensions 2m wide and 4m long in the direction of the wind which is blowing at 2 m/s. What is the evaporation rate if the liquid is at an ambient temperature of 15°C?

Data: Molecular weight = 45.085 kg/kgmol
Antoine vapour pressure equation for ethylamine is:

$$\ln(P^{\circ}) = 17.0073 - \frac{2616.73}{(\mathrm{T} - 37.3)}$$

where $P^{\circ}$ = mmHg, T = Kelvin

Now at 15°C, T = 273.15 + 15 = 288K so that,

$$\ln(P^{\circ}) = 17.0073 - \frac{2616.73}{(288 - 37.3)} = 717.6\,\text{mmHg} \equiv 95664\,\text{Pa}$$

Using the evaporation equation (6.13) for $E_R$

$$E_R = 2.625 \times 10^{-7}\left[\frac{45.085(95664)}{288}\right](2)^{0.78}(4)^{0.89}(2) = 0.046\,\text{kg/s}$$

Using the Peress equation (6.15) we obtain:

$$E_P = 2.117 \times 10^{-6}(2)^{0.78}\,(45.09)^{\frac{2}{3}}\,\frac{8(95664)}{288} = 0.112\,\text{kg/s}$$

Hence there is a variability factor of 3 in the results from the 2 methods. If critical then more sophisticated methods such as the LPOOL model should be used.

## 6.5.1 Estimation of Release Duration

The duration of a release is critical in determining the ultimate effects from many release events. In many cases, release duration is not continuous and steady, so that assumptions need to be incorporated into the release events. Such issues include:

(i) The short term release of materials from relief devices such as pressure relief valves.

(ii) The varying release of liquids and gases from pipelines and vessels that are being depressurized by the release.

(iii) The limitation of release amounts due to inventories in the system.

(iv) The limitation of release duration by the activation of emergency isolation systems such as emergency shutdown (ESD) devices.

(v) The intervention of operational personnel in limiting release durations through manual isolation or other controls.

In many cases, where the release rate and duration are critical factors, dynamic models can be employed to obtain time varying estimates that are closer to reality. Continuous, maximum flow assumptions can lead to significant conservatism.

## 6.6 EFFECTS MODELLING OF FIRE

The key physical parameter associated with fires is the thermal radiation intensity. This is normally stated in kilowatts per square metre (kW/m$^2$). Various levels of radiation intensity can have differing effects. On humans the effects range from skin burns to fatality. On structures fire impact can result in loss of mechanical integrity and load bearing capacity. A summary of radiation intensity values and their effects is provided in Chapter 7 (Table 7-1).

In planning and design of activities where flammable substances are present, it is required to evaluate potential radiation intensities from various fire incidents such as flash fires, jet or torch fires, pool fires and BLEVEs. Each fire event has particular characteristics which need to be appreciated in order to evaluate fire radiation intensities. The following sections deal with the key fire scenarios often encountered in the process industries. Much research has been conducted into fires and reported in the literature (Crowley and Johnson 1992, 1992a, 1992b) and the Fire and Blast Information Group (FABIG) of the Steel Construction Institute (1998) for offshore topside structures.

The following sections outline simple approaches to estimating radiation intensities for each of these events.

### 6.6.1 Fires on Pools

In the following sections the key characteristics of pool fires that affect potential impacts are discussed. In many cases, uncertainties in regard to parameters such as emissive power, wind effects and burning rates can be investigated using sensitivity studies (see section 5.2.2.2).

#### *6.6.1.1 Characteristics of pool fires*

Pool fires are one of the most common occurrences in the process industries. Many occur because of accidental releases of flammable material from storage or in transport situations. The spilled material can be contained in diked or bunded areas or some cases flows unimpeded across land or into drainage areas.

Pool fires are primarily characterized by the heat of combustion and how that is distributed into radiative, convective and reflective components. Convection leads to high heat releases in the plume whilst radiant energy impacts nearby structures or people. The reflective or feedback heat aids liquid vaporization (Hamins et al. 1995).

Pool fires are characterized by varying levels of thermal radiation that are dependent on the flammable material. The surface emissive radiation flux (kW/m$^2$) is highly dependent on the flammable material, the size of the fire, which determines the effectiveness of combustion air ingress, and the prevailing wind conditions. The most prominent factor is the area of the fire which determines flame size. The ratio of carbon to hydrogen (C:H) in the flammable substance determines the surface emissive power of the flame. High C:H ratio substances typically burn with smoky flames compared with low C:H ratio materials.

It is important to recognize that there are 3 main zones in a pool fire (Hamins et al. 1995):

(i) Fuel rich zone:
located just above the liquid pool, this is roughly 20% of the flame height. Here, little air (oxygen) has penetrated. The flame is usually quite bright with little smoky component.

(ii) Intermittent zone:
where the majority of the combustion takes place as air mixes with the hydrocarbons. Here combustion products such as carbon monoxide (CO), carbon dioxide ($CO_2$), water vapour and soot particles form. Soot plays a vital role in radiant energy levels. Soot that is being oxidized emits significant radiant energy, more than other combustion products. However, in very smoky flames where soot production is high it acts to block radiant energy as the soot is not being oxidised. Methanol and LNG fires have light coloured flames and hydrogen fires are invisible due to the lack of soot. Their radiant energy fraction is low compared with heavier hydrocarbons like gasoline or solvents.

(iii) Fire plume zone:
where the residual combustion takes place, ambient air is entrained and the temperature in the plume decreases rapidly with height.

#### *6.6.1.2 Parameters affecting pool fires*

The key parameters are:

- burning rate of flammable material
- shape of the flame
- direction or orientation of the flame
- amount of soot produced
- effect of wind drag on the flame
- carbon to hydrogen ratio
- oxygenation level of substance

### 6.6.1.3 Evaluation of heat radiation on targets

The intensity of the radiation is dependent on the rate of burning, the form of the combustion products (lots of smoke or clean flame) and the atmospheric conditions (e.g. dry or humid day). It is also clearly dependent on the distance of the receptor from the flame.

From a modelling perspective there are two basic approaches to represent the heat radiation intensity at a specified distance from the fire. These are:

- point source model
- view factor model.

The first idealises the fire as emanating from a single point, whilst the second sees the shape of the flame and the view which the receiver has of it as being important. Figure 6-9 shows the conceptual differences. Clearly the point source approach is simple and very idealised. However for distances far from the fire it provides a useful prediction. For distances close to the flame it tends to over-estimate the heat radiation. The view factor approach is more complicated since we need to calculate the "view-factor" which represents a measure of how much of the flame shape is "seen" by the receptor (the solid angle subtended on the flame within the view of the target).

In many cases the view-factor can be quite small, thus reducing the incident radiation on the receptor. This is a very important factor in obtaining credible thermal radiation impacts.

### 6.6.1.4 The point source model

The point source model depends on

(i) The total energy release via combustion
(ii) The fraction of total energy radiated (*f*)
(iii) The amount of energy transmitted to the receptor (transmissivity)
(iv) The distance to the target

Table 6-10 gives the point source model.

**TABLE 6-10 POINT SOURCE FIRE RADIATION MODEL**

The heat flux, $Q$ at a distance $x$ from the fire centre is given by:

$$Q = \frac{MH_c f\tau}{4\pi x^2} \tag{6.16}$$

where:

$Q$ = heat flux (kW/m$^2$)
$M$ = rate of combustion (kg/s)
$H_c$ = heat of combustion (kJ/kg)
$f$ = fraction of thermal energy radiated (0.15 - 0.35)
$x$ = distance from flame centre to observer (m)
$\tau$ = atmospheric transmissivity (0.5 - 0.8)

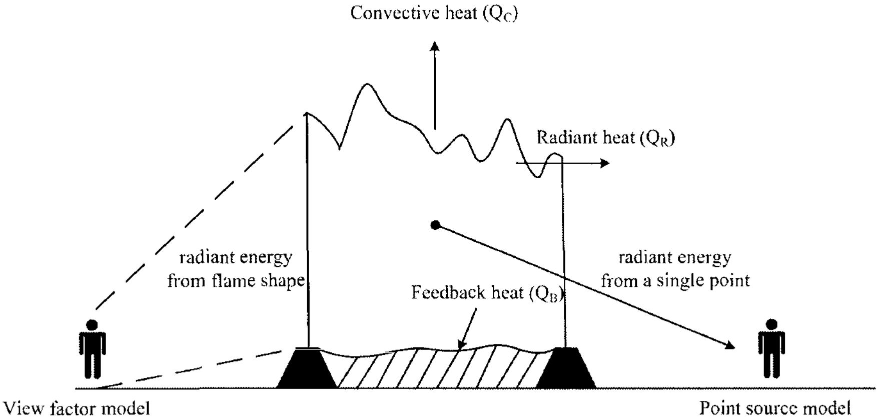


FIGURE 6-9 POOL FIRE MODEL CONCEPTS

The radiant fraction (*f*) is that fraction of the heat of combustion which goes into radiant energy. Typical values over a range of fire diameters are:

| | |
|---|---|
| methanol | = 0.16 - 0.18 |
| butane | = 0.20 - 0.27 |
| benzene | = 0.34 - 0.36 |
| LNG | = 0.20 - 0.27 |
| gasoline | = 0.14 - 0.30 |

Typically as the pool diameter increases for high sooting materials, the radiant fraction (*f*) reduces. Heptane for example has a radiant fraction of 0.35 for pool sizes up to 3m, then reduces to 0.2 for pool diameters of around 10m.

The transmissivity, $\tau$ depends strongly on the amount of moisture in the air and this is measured by relative humidity (RH). It is also a function of distance. An approximation can be used, given by

$$\tau = \log_{10}\left[14.1(RH)^{-0.108}r^{-0.13}\right] \qquad (6.17)$$

where:

| | |
|---|---|
| *RH* | = percent relative humidity |
| *r* | = distance (m) |

A rough guide is also given by Table 6-11.

TABLE 6-11 APPROXIMATE VALUES FOR TRANSMISSIVITY AT 40% RH

| r(m) | $\tau$ |
|---|---|
| 50 | 0.75 |
| 100 | 0.70 |
| 500 | 0.60 |
| 1000 | 0.58 |

A maximum burning rate ($M$) can be estimated from the size of the pool and the burning rate per unit area ( $\dot{m}$ ) given by:

$$\dot{m} = \frac{1 \times 10^{-3} H_C}{(H_V + C_p \Delta T)} \tag{6.18}$$

where:

$H_C$ = heat of combustion (kJ/kg)
$H_V$ = heat of vaporization (kJ/kg)
$C_p$ = heat capacity of the material (kJ/kgK)
$\Delta T$ = ($T_{boiling}$ - $T_{ambient}$ )(K)

Typical values of $\dot{m}$ are around 0.05-0.10 kg/m$^2$.s. The burning rate ($M$) is then simply $M = \dot{m} A$, where $A$ is the pool area (m$^2$). This is a conservative estimate.

The flame height ($h_f$) can be predicted by the Thomas correlation (Thomas 1963).

$$h_f = 42\, d_p \left[ \frac{\dot{m}}{\rho_a \sqrt{g d_p}} \right]^{0.61} \tag{6.19}$$

where:

$d_p$ = pool diameter (m)
$\rho_a$ = density of air (kg/m$^3$) $\simeq$ 1.2 kg/m$^3$ at 20°C
$\dot{m}$ = burning rate per unit area (kg/m$^2$.s)
$g$ = 9.81 m/s$^2$

**EXAMPLE 6-7 BURNING POOL OF GASOLINE**

Consider a 4m diameter pool of gasoline which radiates to an observer 10 metres away from the pool edge. What is the heat flux at the observer? Relative humidity is 50% with ambient temperature of 20°C.

For gasoline we have:

| | |
|---|---|
| $H_C$ = 42400 kJ/kg | $T_a$ = 20°C = 293K |
| $H_V$ = 330 kJ/kg | $C_p$ = 2 kJ/kgK |
| $T_b$ = 415 K | $f \cong 0.25$ |

Using (6.18) the burning rate is:

$$M = \dot{m}A = \frac{1 \times 10^{-3}(42400)}{(330 + 2(415 - 293))} \cdot (12.56\,\mathrm{m}^2) = 0.93\ \mathrm{kg/s}$$

The transmissivity from equation (6.17) is:

$$\tau = \log_{10}[14.1(50)^{-0.018}(12)^{-0.13}] = 0.83$$

Note: distance from pool centre = 10m from pool edge + 2m pool radius, giving 12m.

The flame height from equation (6.19) is:

$$h_f = 42(4)\left[\frac{0.074}{1.2\sqrt{9.81(4)}}\right]^{0.61} = 10\,\text{m}$$

Distance from the flame centre to the observer is

$$\sqrt{(10+2)^2+(5)^2} = 13\,\text{m}$$

$$Q = \frac{0.93(42400)(0.25)(0.83)}{4\pi(13)^2} = 3.9\,\text{kW/m}^2$$

### 6.6.1.5 The view factor model

The view factor model is given in Table 6-12.

TABLE 6-12 VIEW FACTOR MODEL

The heat flux $Q$ for the viewpoint model is given by

$$Q = \tau EF \tag{6.20}$$

where

$Q$ = heat flux (kW/m$^2$)
$E$ = surface emissive power of the flame (kW/m$^2$)
$F$ = geometric view factor.
$\tau$ = transmissivity

Emissive power ($E$) is the amount of radiation flux which emanates from the surface of the flame. It is often difficult to calculate because many flames burn with a lot of smoke. Hence the bright and smoky parts emit different amounts of radiation. It is also very dependent on the degree to which air can be mixed with the fuel, and the size of the fire. It is the most uncertain of all the data used in the view factor model.

For pool fires of various hydrocarbons, we can estimate the emissive power as the composite of clear flame and smoky flame emissive powers:

$$E = E_{smoke}.\psi + E_{flame}(1-\psi) \tag{6.21}$$

where:

$E_{smoke}$ = emissive power of smoky flame (~ 20 kW/m$^2$)

$E_{flame}$ = emissive power of clear flame (~130 kW/m$^2$)
$\psi$ = fraction of smoky surface in fire

Values of $\psi$ vary significantly, typically up to 0.8 (80%) of the flame surface. Typical maximum emissive powers of clear flames are around 130 kW/m$^2$. Average values of $E$ are around 40 kW/m$^2$.

Alternately, measurements on pool fires give emissive powers ($E$) (TNO 1992) as seen in Table 6-13.

TABLE 6-13 EMISSIVE POWER OF VARIOUS POOL FIRES

| Substance | Emissive Power ($E$: kW/m$^2$) |
|---|---|
| aviation fuel | 60-130 |
| kerosene: | |
| (small pools ≤ 10m) | 120 |
| (large pools > 30m) | 10-25 |
| methanol | 70 |
| LNG | 150-220 |
| LPG | 60 - 130 |

If in doubt it is best to use a range of $E$ values to assess the sensitivity of thermal radiation impact to the change in $E$.

Wind tilt of flames is often important, especially when the target is close to the flame. Caution is needed when applying flame tilt models. The most widely used model is of the general form (Johnson 1992; Pritchard and Binding 1992).

$$\frac{\tan\theta}{\cos\theta} = c(Fr)^a(\mathrm{Re})^b \tag{6.22}$$

where $Fr$ = Froude number ($u^2/gd_p$)
$\theta$ = angle of flame tilt, radians
$Re$ = Reynolds number ($ud_p/v$)
$v$ = kinematic viscosity of air (m$^2$/s) (~ 1.5x10$^{-5}$ @ 20°C)

Rew and Hulbert (1996), suggest that the simplest model, with the best data fit, is given by:

$$\frac{\tan\theta}{\cos\theta} = 3.13Fr^{0.431} \tag{6.23}$$

There was virtually no dependence on $Re$ from the data fitting.

View factors are calculated based on the geometry of the flame and the receiver. These are typically much less than 1.0. For a pool fire we can idealise the situation in two ways:

- consider the flame as a cylinder or tilted cylinder
- consider the flame as a flat surface

### Tilted cylinder view factors

Consider the flame as a tilted cylinder of radius *r*, flame length *L* and tilt of *θ*. The receiver is located a distance *x* from the centre of the flame as shown in Figure 6-10.

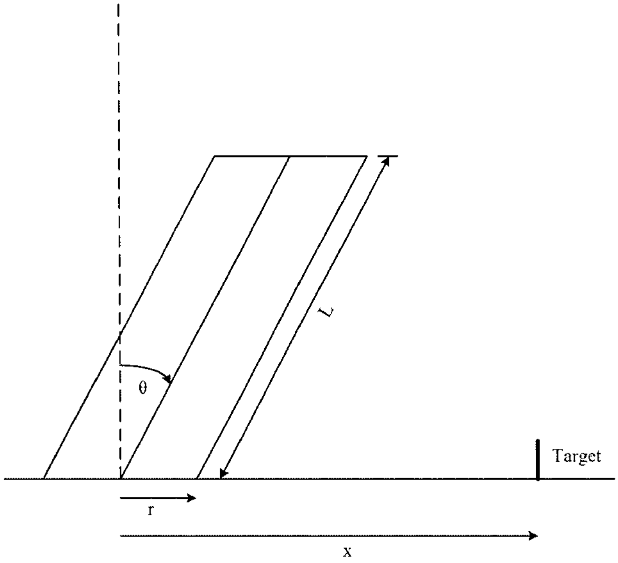


FIGURE 6-10 CYLINDRICAL FLAME VIEW FACTOR

For an event we need to estimate two key measurements

$$L_r = \frac{L}{r}; \quad x_r = \frac{x}{r} \tag{6.24}$$

The maximum view factor ($F_{max}$) is the root mean square of horizontal ($F_h$) and vertical ($F_v$) factors.

For a vertical flame ($\theta$ = 0 radians), the maximum view factor $F_{max}$ is given in Figure 6-11 (TNO 1997). View factor expressions for $F_v$ and $F_h$ are available for tilted flames (TNO 1997; Lees 2001). These are best computed from the mathematical expressions. For values of $x_r$ = 10 and $L_r$ = 5 and a tilt of 30°, the view factor increases by about 25%.

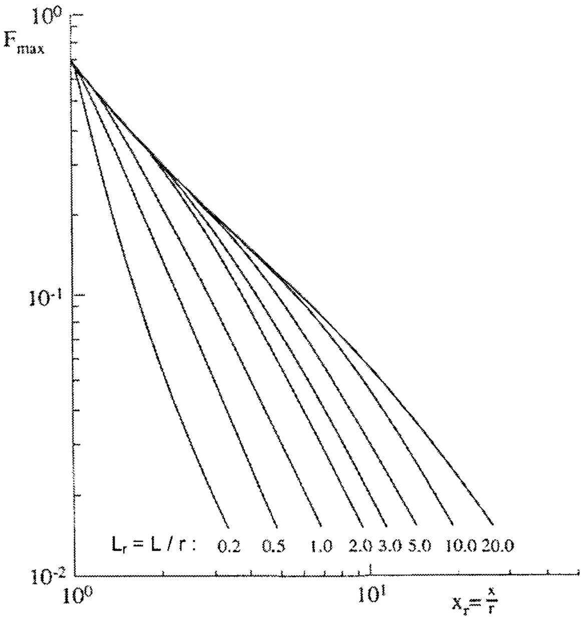


FIGURE 6-11 CYLINDRICAL FLAME MAXIMUM VIEW FACTOR ($\theta$ = 0 RADS) (TNO 1997)

### Vertical flat surface view factors

This is a useful idealisation for cases where the pool is large or confined to a rectangular, bunded area. The situation is shown in Figure 6-12 where the flame is the vertical surface of height $L$ and length $2b$ with receiver located centrally and at a distance $x$. Again it is necessary to define two dimensionless parameters,

$$L_r = \frac{L}{b}; \quad x_r = \frac{x}{b} \tag{6.25}$$

The values of the maximum view factor are shown in Figure 6-13. (TNO 1997)

If the pool is rectangular with length/width <2 then an equivalent diameter can be used, given by

$$d_p = d_{eq} = \frac{4 \times pool\ area}{pool\ perimeter} \tag{6.26}$$

and this can be used with the tilted cylinder view factor to estimate the value of $F_{max}$.

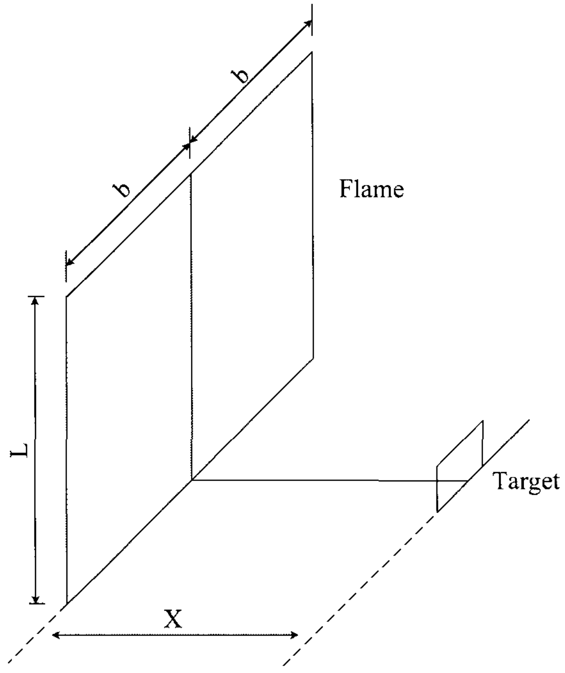


FIGURE 6-12 VERTICAL FLAME GEOMETRY VIEW FACTOR GEOMETRY

**EXAMPLE 6-8 BURNING GASOLINE**

Consider Example 6-5 of a 4m diameter pool of gasoline and an observer at 10m from the pool. Windspeed $u = 0$ m/s.

Previously: $\dot{m} = 0.074$ kg/m$^2$ s and flame height = 10m

From equation 6.21, emissive power of flame is given by

$$E = 0.8(20) + 0.2(140) = 44 \text{ kW/m}^2$$

and transmissivity $\tau = 0.83$.

The view factor (as a cylinder) with $L_r = \frac{10}{2} = 5$; $x_r = \frac{12}{2} = 6$ gives

$F_{\max} = 0.075$ (Figure 6-11).

Heat flux at target, $Q = \tau EF = 0.83(44)(0.075) = 2.7 \text{ kW/m}^2$.

This is smaller than that predicted by the point source method.

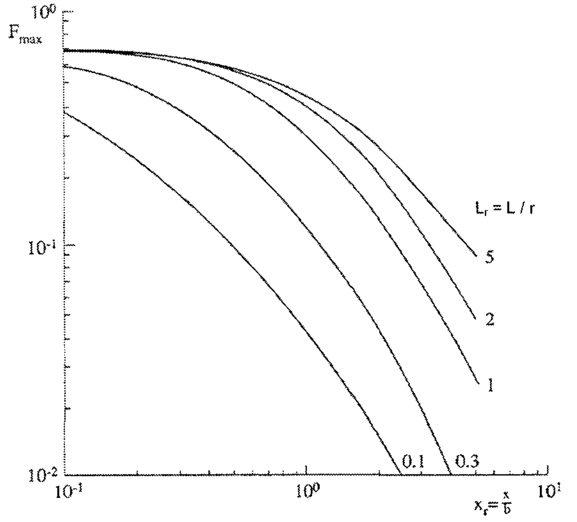


FIGURE 6-13 VERTICAL FLAME MAXIMUM VIEW FACTOR (TNO 1997)

The previous model based on the view factor method and given by equation 6.20, can be improved by considering separately the clear flame and smoky flame portions to arrive at:

$$Q = \tau E_{cf} F_{cf} + \tau E_{sf} F_{sf} \tag{6.27}$$

where:

$E_{cf}$ = clear flame emissive power (kW/m$^2$)
$F_{cf}$ = clear flame view factor
$E_{sf}$ = smoky flame emissive power (kW/m$^2$)
$F_{sf}$ = smoky flame view factor

This is the model advocated by Rew and Hulbert (1996), based on earlier work by Pritchard and Binding (1992). It gives superior results to the more simplistic models but relies on predicting clear flame length, which is given by Pritchard and Binding (1992) as:

$$\frac{L_{cf}}{D} = 11.404(\dot{m}_*)^{1.13}(u_9^*)^{0.179}\left(\frac{C}{H}\right)^{-2.49} \tag{6.28}$$

where:

$\dot{m}_* = \dot{m} / [\rho_a (g d_p)]^{\frac{1}{2}}$ (scaled burning rate)

$\overset{*}{u_9} = u_9 / [(g\dot{m}d_p / \rho_a)]^{\frac{1}{3}}$ (scaled burning rate)

$\dfrac{C}{H}$ = carbon to hydrogen ratio of the burning material

$u_9$ = windspeed at height of 9m (m/s)

$\rho_a$ = air density (kg/m$^3$) $\simeq$ 1.2 kg/m$^3$ at 20° C

### 6.6.1.6 Limitations

It should be remembered that uncertainties in radiation level predictions arise at each substep of the estimation process. The most crucial aspects are the emissive powers used in the estimate. If field data, such as LNG or LPG emissive powers are available then they should be used rather than correlations. It is important to perform sensitivity studies to check the effect of assumed values of $E_{cf}$and $E_{sf}$.

## 6.6.2 Boiling Liquid Expanding Vapour Explosions (BLEVEs)

In the case of a BLEVE, we can idealise the fire situation as a large fire ball suspended above the ground. Emissive power is usually high since fuel-air mixing is good. Typically the emissive power at the surface is in the range of 200-350 kW/m$^2$.

Of importance is the size of the fire ball and the duration of burning. Extensive work by TNO after the PEMEX disaster in Mexico City in 1984 led to correlations for these basic parameters as shown in Table 6-14 (TNO 1985).

TABLE 6-14 BLEVE CORRELATION MODEL

The TNO BLEVE correlations are:

$$D = 6.48\ W^{0.325} \qquad (6.29)$$
$$t = 0.852\ W^{0.260} \qquad (6.30)$$

where:

| | |
|---|---|
| $D$ | = diameter of fireball (m) |
| $t$ | = duration (s) |
| $W$ | = weight of fuel (kg) |
| $H$ | = bottom height = 0.5 D (m) |

The idealised situation is seen in Figure 6-14.

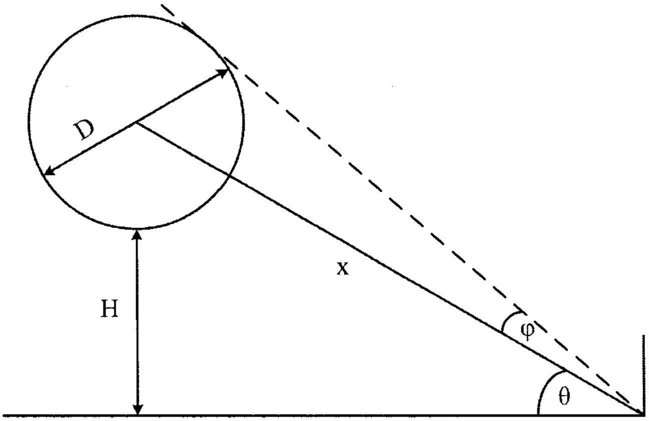


FIGURE 6-14 IDEALISED BLEVE MODEL

The view factor method is used to estimate the radiation intensity at the receiver. This is given by:

$$Q = \tau E F$$

with

$Q$ = received flux (kW/m$^2$)
$F$ = view factor $= D^2 \cos\theta / 4x^2 \quad (\theta \leq 90° - \phi)$
$E$ = emitted flux $\cong \varepsilon\, \sigma\, T_s^4$

where

$\varepsilon$ = emissivity (~1.0)
$\sigma$ = Stefan-Boltzmann constant = $5.67 \times 10^{-11} \dfrac{\text{kW}}{\text{m}^2\text{K}^4}$
$T_s$ = flame surface temperature (K)
$\tau$ = transmissivity

The above view factor is applicable when the fire ball is in full sight of the receiver. In cases where $\theta > 90° - \phi$ not all of the fireball is seen by the receiver and the view factor becomes more complex. (see TNO 1997; Lees 2001).

**EXAMPLE 6-9 BLEVE INCIDENT**

A storage tank releases 20,000 kg of LPG which ignites and forms a fireball. What is the radiation intensity 200m from the incident?

TNO correlations give (6.29) and (6.30):

$D$ $= 6.48\,(20{,}000)^{0.325} = 162$ metres
$t$ $= 0.852\,(20{,}000)^{0.260} = 11$ seconds

Heat flux at 200m from fireball centre

If $E$ = 250 kW/m$^2$ with the view factor at maximum ($\theta = 0°$)

$$Q = \tau EF \cong 0.7(250)\frac{D^2}{4x^2} = 0.7(250)\frac{(162)^2}{4(200)^2} = 29\ \text{kW/m}^2$$

At this radiation level there would be significant injuries and some fatalities for exposure over the duration of the fireball.

### 6.6.3 Jet Fires and Spray Fires

Here we are concerned about fires which result from the ignition of a high velocity jet of gas and/or liquid escaping from a pipe or vessel.

This type of fire can occur when there are discharges from safety valves such as in the case of LPG storage or from holes in pipes, or vessel walls, or gasket leaks

### 6.6.3.1 Characteristics of jet fires

Jet fires are high momentum releases of burning hydrocarbon or combustible substances, either in liquid or gaseous form. Their burning characteristics depend strongly on the flammable material, the release pressure and the state of the substance. For release of liquefied gases, there is the phenomenon of flashing and droplet formation that affects the subsequent fire. Jet fires burn with considerably more emissive power than pool fires. The flames are affected by buoyancy such that horizontally released jets often have significant "turn up" along the jet fire due to buoyancy of the hot combustion gases. Wind can also have significant impacts in cooling and shortening vertical and angled jet fires.

For high velocity jets, there is often a significant "lift off" distance where a region of no flame is seen near the release point. Here the liquid or gas is rapidly expanding, mixing with air and travelling at very high velocity such that the flame cannot burn back to the discharge point. These characteristics have been well documented and in some cases captured in current models (Chamberlain 1987; Johnson et al. 1994; Crowley et al. 1992).

A particularly difficult situation is dealing with the directionality of the jet fire, especially where ground or nearby vessel impingement changes the "natural" flame shape. Here, specialized models are needed based on computational fluid dynamics (Johnson et al. 1999).

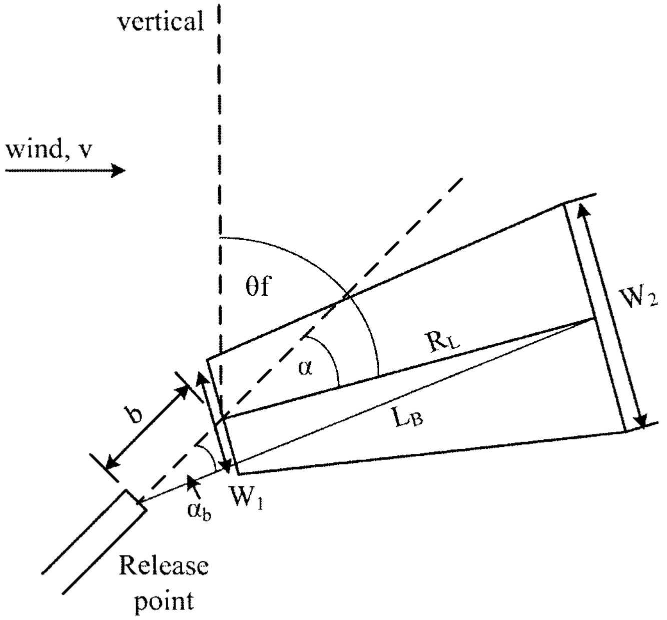


FIGURE 6-15 JET FIRE IDEALISATION (Chamberlain 1987)

### 6.6.3.2 Models for jet fires

Simplistic approaches to jet fire modelling have existed in a number of engineering standards (API RP521, 1997). These represent flares as a single point source radiating to a target. Modified approaches that divide the flame into multiple point source segments are also used. These approaches can be useful for initial, rough estimates.

The most widely used jet fire model is that developed by Chamberlain (1987), commonly known as the "Thornton" model due to the work of Shell Research Ltd at their Thornton facility. Further developments by Johnson et al. (1994) addressed the issue of horizontally oriented jet fires. The conceptualization of the fire as the frustum of a cone is seen in Figure 6-15. Here the jet fire has a discharge angle of ($\theta_f$ - $\alpha$) from the vertical with a flame tilt due to wind of $\alpha$. The flame lift off is given by the distance, *b*. The flame length ($L_b$), base and tip dimensions of the cone frustum ($W_1$, $W_2$) are given by correlations (Chamberlain 1987).

Once these key dimensions are estimated it is then possible to consider thermal radiation impacts on targets in the vicinity of the jet fire. These estimates are based on the view factor method as given in equation (6.20). The surface emissive power (*E*) can be estimated as:

$$E = \frac{F_s Q}{A} \tag{6.31}$$

where:

$F_s$ = fraction of heat radiated = $0.21e^{-0.00323u_j}+0.11$
$u_j$ = gas velocity at the exit (m/s)
$Q$ = net combustion energy (kW)
$A$ = surface area of the frustum ($m^2$)

Values of $F_s$ are in the range of 0.15 to 0.30. The view factor can be obtained by assuming an equivalent tilted cylinder geometry (TNO 1997) or by integration of the standard view factor formula (Holman 1981).

Simple semi-empirical models, based on experiments with vertical flares were developed by Cook et al. (1987). These correlations, as well as the Chamberlain model (1987) are applicable for vertical and angle flames, where wind momentum dominates over buoyancy. These are not suitable for horizontal jet fires. An extension of the Chamberlain model was developed by Johnson et al. (1994) from tests with horizontal jet flames. It includes the effect of buoyancy lifting the flame above the horizontal, and the effect of wind momentum.

**EXAMPLE 6-10 NATURAL GAS JET FIRE IMPACTS**

Figure 6-16 shows the thermal radiation levels for a 10 MPa natural gas jet fire released at 5° from the vertical, subject to windspeeds of 0, 5 and 10 m/s. The gas release rate is 25.0 kg/s. The release height was at ground level and the target is downwind of the release point (Daesim 2004). The model is based on the work of Chamberlain (1987).

It can be seen that in the far field (> 60 m) the incident radiation is essentially the same for all windspeeds. However, in the near field, there are substantial differences in thermal radiation levels due to the flame tilt and shortening under different windspeeds.

### *6.6.3.3 Limitations*

The current models for jet fires provide good, validated approaches to fire radiation estimates that are based on a wide range of field experiments. The most significant limitation of these models is when impingement of the flame occurs. In these cases special approaches are required that use computational fluid dynamics (CFD) methods (Johnson et al. 1999).

Also nearly all the field work on jet fires has used natural gas or propane. When other substances are involved it is important that a range of emissive powers are investigated to check the predicted range of radiation levels on the target.

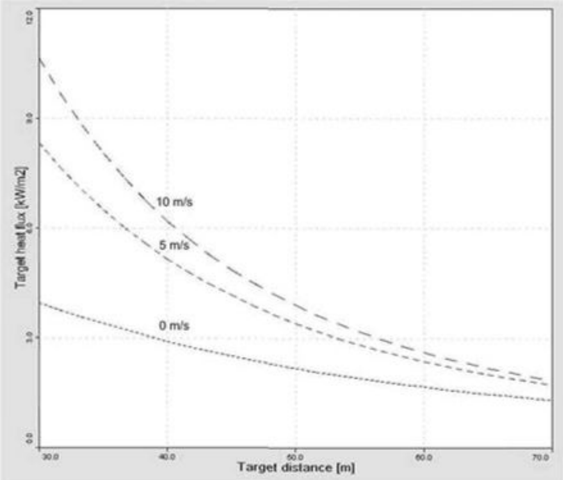


FIGURE 6-16 METHANE JET FIRE THERMAL RADIATION IMPACTS (DAESIM 2004)

## 6.7 EFFECTS MODELLING OF EXPLOSIONS

### 6.7.1 Characteristics of Gas Explosions

Explosions are one of the most devastating events which occur in the process industries and also in transport situations. In most cases we are dealing with flammable vapour-air mixtures or solid-air mixtures which are ignited in some way by flame, friction, sparks or heated surfaces. These mixtures could be hydrocarbons like LPG (propane or butane) or dusts such as sugar or coal (Guilbert and Jones 1996). In many cases very little energy is needed to initiate the combustion processes which lead to the explosive event.

The types of structural damage effects resulting from a range of explosion overpressures are given in Chapter 7, Table 7-4. In mining applications dense phase explosions often need to be addressed.

These effects are the result of the enormous amounts of energy released over a short period of time when the explosion occurs. The important factors and principal approaches to predicting these events are given in Table 6-15.

TABLE 6-15 EXPLOSION CHARACTERISTICS AND PREDICTION METHODS

| Important Factors | Methods of Prediction |
|---|---|
| • Peak overpressure | • TNT Equivalent models |
| • Positive phase duration | • TNO Multi-Energy model |
| • Degree of confinement | • 3D Mechanistic models |
| • Pressure impulse | |

Explosions in process systems can be related to a number of events which include:

(i) The escape of flammable liquid or gas that subsequently forms a combustible fuel-air mixture and is subsequently ignited. In this case there is a vapour cloud explosion of varying effects depending on the degree of confinement of the explosive mixture.

(ii) The ignition of a flammable mixture in the vapour space of storage tanks. The ignition can be due to static electricity, direct flame or sparks from maintenance operations. In this case, roof design and venting should relief pressures but explosions can result in major structural damage.

(iii) The ignition of flammable materials in process vessels due to autoignition or other direct causes such as static discharges or explosive reactions that can propagate through adjoining pipework or lead to vessel disintegration. Blast waves and blast fragments are major results of such incidents.

(iv) The ignition of fine particulates such as coal dust, sulphur, aluminium and combustible grains that can lead to devastating explosions that destroy storage and handling facilities as well as generate significant blast waves and fragments.

### EXAMPLE 6-11 EXPLOSION INCIDENTS

a) A 15,000 m$^3$ ethanol storage tank was destroyed in January 2004, at a storage facility in NSW, Australia when the vapour space was ignited during maintenance work on the tank. The roof was blown onto the foam generation station and a nearby tanker loadout facility and the subsequent fire burned for many hours before being extinguished.

b) The release of large amounts of cyclohexane in the Nypro works at Flixborough in 1974 lead to a massive vapour cloud explosion that destroyed the control room killing 28 personnel. It caused significant damage at the nearby village. The explosion varied in its intensity due to significant areas of confinement within the cloud.

In relating the key explosion factors to ultimate damage we need to know both values of peak overpressure $p_o$ and the positive phase duration $t_p$. In Section 7.3 an approach based on probit functions utilising information on pressure-time profiles provides estimates of impacts on people and structures. Figure 6-17 shows typical incidents related to vapour cloud explosions.

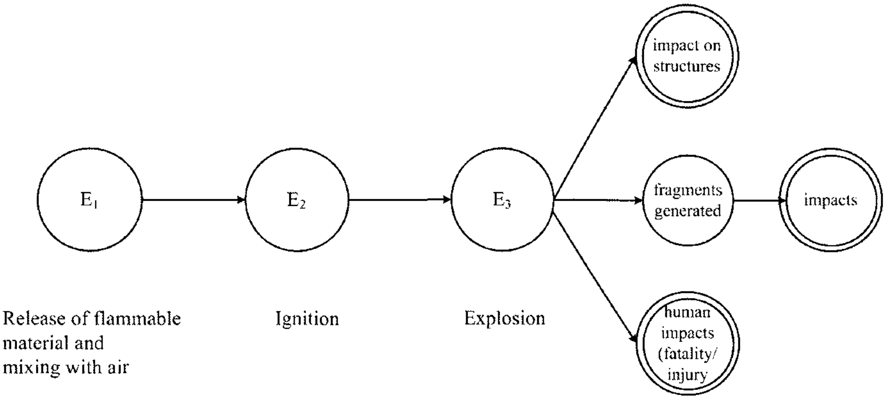

E1
E2
E3
Release of flammable material and mixing with air
Ignition
Explosion
impact on structures
fragments generated
impacts
human impacts (fatality/ injury

FIGURE 6-17 TYPICAL VAPOUR CLOUD EXPLOSION INCIDENT

## 6.7.2 Explosion Overpressure and Phase Duration

It was recognised since the time of the Flixborough incident that a facility design should include limiting explosion damage (Lawrence and Johnson 1974). It can be seen from Table 6-15 there are 4 key factors in an explosion. These are related to the overpressure which is the pressure rise above normal atmospheric pressure, the positive phase duration which is the time during which the pressure is above atmospheric pressure, the degree of confinement of the flammable mixture which causes acceleration of the flame front and influences the overpressure, and the impulse (area under the pressure-time profile).

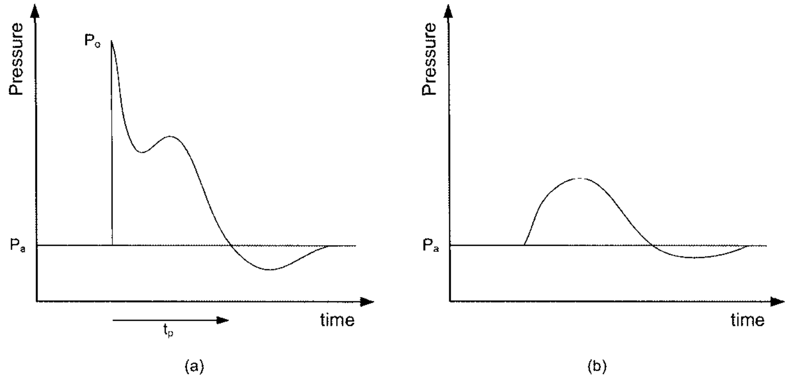


FIGURE 6-18 PRESSURE CHANGE PATTERNS FROM EXPLOSION EVENTS

Figure 6-18 shows two typical pressure change patterns which could be experienced from an explosion event. The first shows a step increase in pressure from atmospheric pressure $p_a$ to $(p_a + p_o)$, followed by a sharp drop in pressure over a period $t_p$, which is the positive phase duration (typically milliseconds). The pressure then reaches atmospheric pressure again and proceeds below atmospheric pressure during the negative phase duration, finally settling back to normal pressure as the shock wave passes by. This sharp rise in pressure in Figure 6-18(a) is typical of detonations where the propagation speed is anywhere between 2 and 10 km/s. Condensed explosives (e.g. TNT, PETN, RDX, C4) behave like this. For example, C4 plastic explosive has a detonation velocity of around 8.1 km/s. The maximum overpressures ($p_o$) can be as high as 15-18 bar (1500-1800 kPa). The second peak in Figure 6-18(a) is associated with the reflected pressure wave from the ground.

In the second case seen in Figure 6-18(b), the blast wave rises more gradually to the peak overpressure and then gradually subsides. The positive phase duration is longer than the shock wave but the overpressure is greatly reduced. Typically, these slower burning combustion processes have overpressures in the range 0.05 - 0.7 bar (5 - 70 kPa) and $t_p$ values around 0.3 - 1.5 seconds for process plant incidents. In offshore oil and gas facilities with plated decks, the flammable cloud is confined between the floor and roof of a deck. This confinement, together with the congestion of equipment on board can cause overpressures up to 2-3 bar or higher.

The last key factor is the degree of confinement. This is a very difficult factor to assess in practice as it has a significant and direct influence on the peak overpressure. The degree of confinement directly affects the combustion processes by improving mixing or turbulence of the burning flame front and thus helps accelerate the propagation of the pressure wave. This confinement and hence acceleration can help explain the dramatic change in patterns of blast damage seen in open areas versus confined areas. Here the explosion assumes the characteristics of a detonation with a significant increase in blast wave velocity. The degree of confinement directly affects the 'blast strength' often used in the TNO Multi-Energy model as discussed in Section 6.7.3.2. Any use of this factor needs to be accompanied by sensitivity analyses to assess its importance.

In the following sections we look at several approaches to predicting the physical effects resulting from explosions.

### 6.7.3 Methods of Estimating Explosion Impact

In the following three sections we discuss the principal models used for explosion predictions. These are the TNT equivalent model, the TNO multi-energy model (MEM) and use of computational fluid dynamics (CFD) models. Other models exist but in many cases have been superceded by the models discussed here.

#### *6.7.3.1 TNT equivalent models*

TNT equivalent models attempt to convert the amount of flammable material in the vapour cloud into an equivalent amount of TNT. Much is known about the blast effects of TNT through military and industrial use, hence the motivation to use well established data.

The procedure is relatively simple and the major steps in applying this method are:

- Estimate the size of the flammable fuel cloud
- Convert the fuel mass to a TNT equivalent
- Convert the target distance to a "scaled" distance
- Determine the overpressure from TNT correlations.

However, it must be borne in mind that there are some limitations to the method. These include:

- Under-predicts overpressure for partial confinement
- TNT-blast decays faster than VCE blast
- Gas explosions are variable in strength
- Efficiency of explosion is highly empirical
- Assumes detonation explosion
- TNT explosion is mechanistically different to VCE.

In particular the efficiency of the explosion, which is the fraction of total energy converted to blast energy, is highly variable.

**TABLE 6-16 THE TNT EQUIVALENT MODEL**

The TNT equivalent (kg) is given by:

$$W_{TNT} = \alpha.\frac{W.H_c}{H_{TNT}} \tag{6.32}$$

where:

| | |
|---|---|
| $W$ | = weight of fuel in the cloud (kg) |
| $H_c$ | = heat of combustion of the fuel (kJ/kg) |
| $H_{TNT}$ | = TNT blast energy (5420 kJ/kg) |
| $\alpha$ | = explosion efficiency. |

The explosion efficiency ($\alpha$) has considerable variability. Typically $\alpha = 0.04$ for hydrocarbons; $\alpha = 0.10$ for highly reactive substances. Some practitioners suggest that three classes can be used, based on reactivity:

| | |
|---|---|
| Class I: | $\alpha = 0.05$ (propane, butane, flammable liquids) |
| Class II: | $\alpha = 0.10$ (ethylene, ethers) |
| Class III: | $\alpha = 0.15$ (acetylene) |

Once the TNT equivalent is known the overpressure values are predicted using a "scaled" distance, based on the actual distance from the blast and the TNT equivalent. This scaled distance $z$ is given by:

$$z = \frac{R}{(W_{TNT})^{\frac{1}{3}}} \tag{6.33}$$

where: $R$ = distance from blast (m)
$W_{TNT}$ = kg equivalent of TNT (kg)

From extensive military testing of TNT in the USA and UK, field data has led to the representation of scaled parameter plots for overpressure, arrival and positive phase duration times as well as impulse. Figure 6-19 shows the scaled parameters against scaled distance as given in equation 6.30 (Lees 2001). These parameters are for a ground level blast where reflection is an additional contributor to the total overpressure.

The scaled parameters are defined as:

Scaled overpressure: $$P_s = P_o / P_a \tag{6.34}$$

Scaled positive phase duration: $$\tau_d = \frac{t_p}{W^{\frac{1}{3}}} \tag{6.35}$$

Scaled arrival time: $$\tau_a = \frac{t_a}{W^{\frac{1}{3}}} \tag{6.36}$$

Scaled impulse: $$i_s = \frac{i_p}{W^{\frac{1}{3}}} \tag{6.37}$$

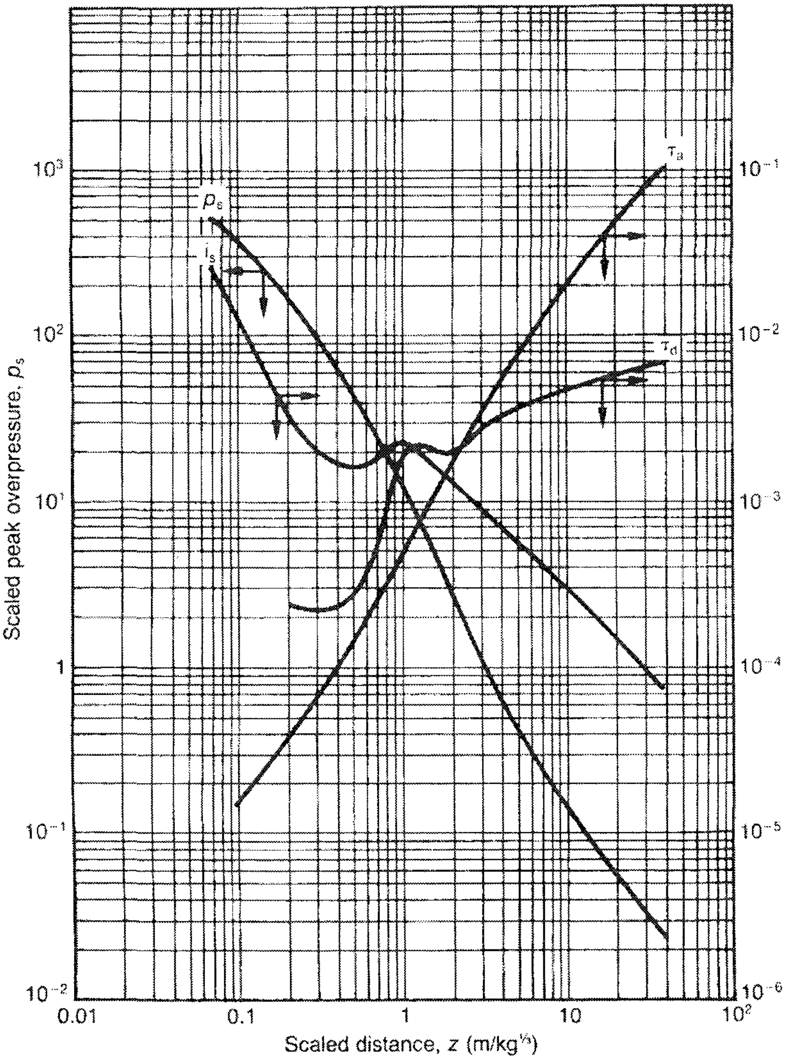


**FIGURE 6-19 SCALED PARAMETER PLOTS FOR TNT EXPLOSIONS (Lees 2001)**

For ease of computation, the scaled distance and peak overpressure are expressed in the following correlation, based on the curves developed by Brasie and Simpson (1968).

$$\log_{10}(10.\ z) = 0.082\ (\log_{10}p_o)^2 - 0.529\ \log_{10}p_o + 1.526 \qquad (6.38)$$

Where $p_o$ is the explosion peak overpressure in bars. Equation (6.38) is valid for $p_0$ falling in the range 0.01 to 1 bar.

**EXAMPLE 6-12 EXPLOSION OF PROPYLENE**

A propylene liquid storage tank of 25,000 kg capacity (at 20°C) suffers a major failure with the loss of propylene. Using the TNT equivalent method the overpressures can be estimated.

Relevant data includes:

| | |
|---|---|
| $\Delta H_v$ | = 438 kJ/kg |
| $C_p$ | = 2.6 kJ/kgK |
| $H_c$ | = 46,400 kJ/kg |
| Normal boiling point | = -47.8°C = 226 K |

The flash fraction from equation (6.7) gives

$$\phi = 1 - \exp\left[ - \frac{2.6}{438} (293 - 226) \right] = 0.33$$

The entrained fraction is $e = 0.33$, and cloud mass = $(e + ø)W_o = 16{,}500$ kg.

Equivalent weight of TNT is given by equation (6.32)

$$W_{TNT} = \alpha . \frac{W . H_C}{H_{TNT}} = \frac{0.1\ (16{,}500)\ 46{,}200}{5420} = \underline{14{,}000\,\mathrm{kg}}$$

The following table of distances, scaled values and overpressures can be then generated.

| Distance<br>R(m) | Scaled distance<br>Z | Overpressure<br>(kPa) |
|---|---|---|
| 50 | 2.1 | 160 |
| 100 | 4.2 | 39 |
| 200 | 8.3 | 13 |
| 500 | 20.1 | 4 |
| 1000 | 41.5 | 1.8 |
| 2000 | 83.0 | 8 |

It is estimated that severe structural damage will be experienced out to 100m and 90% window breakage to 500m.

### 6.7.3.2 Multi-Energy Model

The Netherlands Organization for Applied Scientific Research (TNO) has conducted extensive research into blast models (van den Berg 1985; van den Berg et al. 1991; Mercx et al. 1998, 2000). The TNO multi-energy model allows for blast strength to be incorporated. Using this technique it is possible to adjust predictions to account for partial confinement of the vapour cloud. The method considers the total cloud as a series of sub-explosions corresponding to the various confined or unconfined regions. The confined regions might be parts of the cloud located under tanks or vessels, hemmed in by buildings or other structures. Similar results are obtained from flame speed based models such as the Baker-Strehlow method (Baker et al. 1996; Tang and Baker 2000).

In comparison with TNT equivalent models of vapour cloud explosions where blast effects decay quicker than reality, the multi-energy model can help predict far field effects more accurately.

The key additional factor in this model is the 'blast strength' which ranges from 1 (insignificant) to 10 (detonative strength). Figures 6-20 and 6-21 show the overpressure and positive phase duration versus an energy scaled distance. Separate curves relate to the blast strength. The model is shown in Table 6-17.

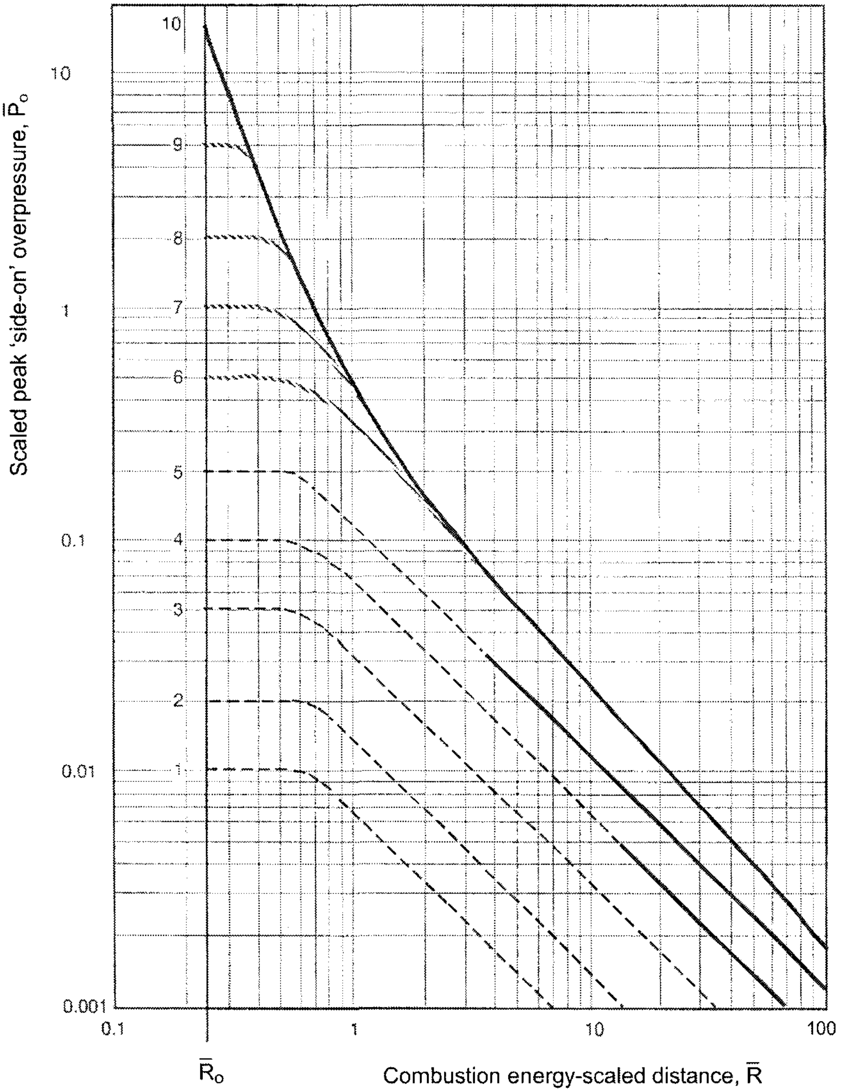


**FIGURE 6-20 SCALED PEAK SIDE OVERPRESSURE FOR MEM (BY PERMISSION OF ELSEVIER)**

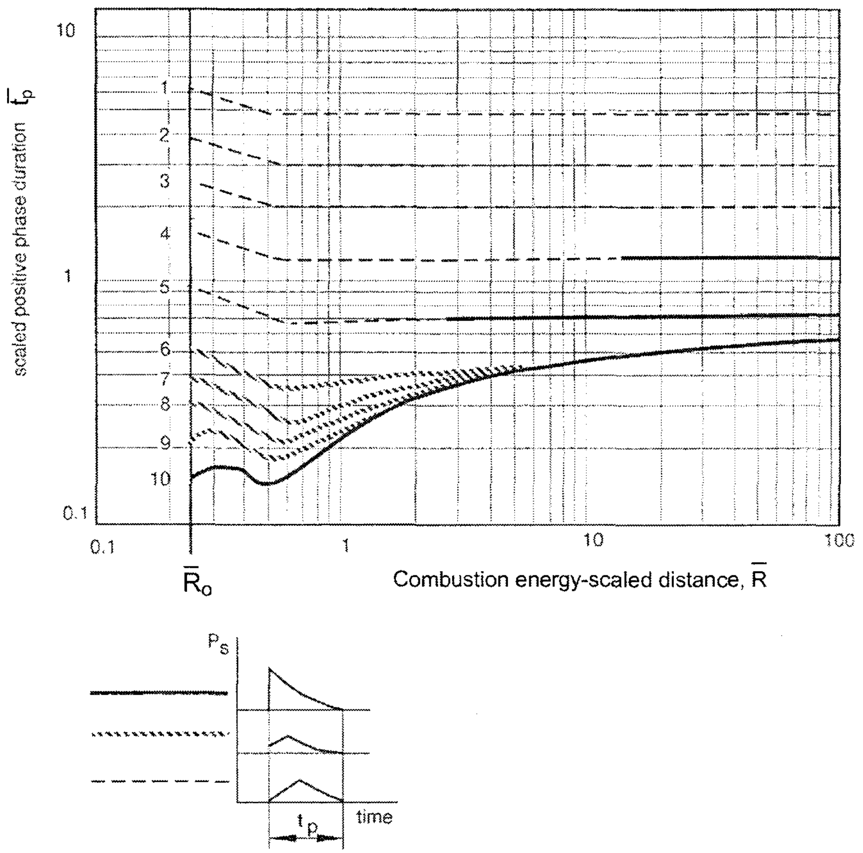


FIGURE 6-21 SCALED POSITIVE PHASE DURATION FOR MEM (BY PERMISSION OF ELSEVIER)

To apply this method the following steps need to be carried out.

a) Assign portions of the cloud to different areas (e.g. between buildings, under vessels, in open air)
b) Determine the fuel present in each zone (i.e. amount of gas-air mixture ($m^3$)) and total cloud energy, $E$ ($\equiv V_oE_c$), based on the heat of combustion of the fuel. A typical energy density $E$ is $3.5 \times 10^6$ J/$m^3$.
c) Assign initial strengths to these vapour cloud charges (e.g. 2 for open area, 5-6 confined, 7-10 highly confined).
d) Calculate scaled distances for each charge at nominated distances, $R$.
e) From figures for $\overline{P_o}$ and $\overline{t_p}$ versus $\overline{R}$, estimate overpressure and positive phase durations for each charge. If blast zones are located close to each other and the ignition is essentially simultaneous, then overpressures can be superimposed at target distances.

TABLE 6-17 THE MULTI-ENERGY MODEL (MEM)

The following parameters describe the multi-energy model (MEM):

Scaled overpressure: $$\overline{P}_o = \frac{P_o - P_a}{P_a} \quad (6.39)$$

Scaled positive phase duration: $$\overline{t}_p = t_p c_a \left(\frac{P_a}{E}\right)^{\frac{1}{3}} \quad (6.40)$$

Scaled distance: $$\overline{R} = R\left(\frac{P_a}{E}\right)^{\frac{1}{3}} \quad (6.41)$$

where:

| | | | | | |
|---|---|---|---|---|---|
| $P_o$ | = | side-on absolute blast overpressure (Pa) | $R$ | = | fuel-air charge radius (m) |
| $\overline{P}_o$ | = | scaled blast overpressure (-) | $\overline{R}$ | = | scaled distance (-) |
| $P_a$ | = | ambient pressure (Pa) | $\overline{t}_p$ | = | scaled positive phase duration (-) |
| $c_a$ | = | ambient velocity of sound (m/s) | $t_p$ | = | positive phase duration (s) |
| $E$ | = | combustion energy in fuel-air mixture (J) | | | |

The biggest challenge in the use of the multi energy method is the selection of the charge strength. This depends on a number of factors that include:

(i) the level of obstruction within the gas cloud.
(ii) the ignition strength, 'high' representing a vented explosion with 'low' being a spark or flame.
(iii) the level of confinement being either an unconfined volume or confined between surfaces.

A decision table can be constructed (TNO 1997) that considers all factors and relates these to the blast strength.

Mercx et al. (2000) attempted to provide a correlation for the charge strength $P_o$ based on 3 key factors:

(i) The volume blockage ratio (VBR) representing the proportion of the total volume occupied by obstacles,
(ii) The flame length, $L_f$ (m) representing the longest distance from the point of ignition to an outer edge of the obstacle configuration, and,
(iii) The average obstacle size $D$ (m).

The correlation also considered the scale of the situation and the fuel type by using the laminar burning velocity $S_L$ (m/s) and a scale factor $D$ (m). The correlation is

$$P_{CS} = a\left[\frac{(VBR)(L_f)}{D}\right]^b S_L^{2.7} D^{0.7} \qquad (6.42)$$

Two correlations were developed from equation (6.42). For 3D, open regions (no confinement):

$$P_{CS} = 0.84\left(\frac{VBR.L_f}{D}\right)^{2.75} .S_L^{2.7} D^{0.7} \qquad (6.43)$$

and for 2D, confined cases:

$$P_{CS} = 3.38\left(\frac{VBR.L_f}{D}\right)^{2.25} .S_L^{2.7} D^{0.7} \qquad (6.44)$$

Typically $S_L$ is 0.45 m/s (methane) and 3.5 m/s (hydrogen).

These were used to predict overpressures and were found to vary by a factor of 2 compared with CFD methods.

For offshore oil and gas facilities, Kinsella (1992) has suggested an approach for selecting the charge strength, accounting for three factors:

- Congestion: If congestion is more than the threshold of 30%, it is considered 'high'.
- Strength of ignition source: Low (spark, hot surfaces), high.(naked flames, welding)
- Parallel Confinement: Low for grated decks, high for plated decks.

**EXAMPLE 6-13 PROPYLENE EXPLOSION**

Consider the explosion incident in Example 6-12 but in this case 25% of the vapour cloud is highly confined whilst the rest is unconfined. The total amount was 14,000 kg or 190,820 m$^3$ of gas-air mixture. There are 2 zones to consider.

Zone 1 (confined):

$$V_o^1 = 0.25(190820) = 47705m^3$$

$$E^{(1)} = V_o^1.E_c = 47705(3.5\times10^6) = 1.67\times10^{11} J$$

Zone 2 (unconfined):

$$V_o^2 = 0.75(190820) = 143115m^3$$

$$E^{(2)} = V_o^2.E_c = 143115(3.5\times10^6) = 5.0\times10^{11} J$$

Consider the two distances of 200 and 1000 metres.

Zone 1 scaled distances are:

$$\bar{R}^{1}_{100} = 200\left(\frac{1\times10^{5}}{E^{(1)}}\right)^{\frac{1}{3}} = 1.68$$

$$\bar{R}^{1}_{1000} = 1000\left(\frac{1\times10^{5}}{E^{(1)}}\right)^{\frac{1}{3}} = 8.4$$

Zone 2 scaled distances are:

$$\bar{R}^{2}_{100} = 200\left(\frac{1\times10^{5}}{E^{(2)}}\right)^{\frac{1}{3}} = 1.17$$

$$\bar{R}^{2}_{1000} = 1000\left(\frac{1\times10^{5}}{E^{(2)}}\right)^{\frac{1}{3}} = 5.85$$

Using Figure 6-20, the scaled results for zone 1 (blast strength = 8) and zone 2 (blast strength = 2) can be estimated. Figure 6-21 gives the scaled positive phase duration.

At R = 200 metres

| Zone | $\bar{R}$ | Strength | $\bar{P}_o$ | $P_o$ (kPa) | $\bar{t}_p$ | $t_p(s)$ |
|---|---|---|---|---|---|---|
| 1 | 1.68 | 8 | 0.23 | 23.0 | 0.33 | 0.11 |
| 2 | 1.17 | 2 | 0.012 | 1.2 | 3.0 | 1.54 |

At R = 1000 metres

| Zone | $\bar{R}$ | Strength | $\bar{P}_o$ | $P_o$ (kPa) | $\bar{t}_p$ | $t_p(s)$ |
|---|---|---|---|---|---|---|
| 1 | 8.4 | 8 | 0.029 | 2.9 | 0.47 | 0.11 |
| 2 | 5.85 | 2 | 0.00232 | 0.23 | 3.0 | 1.54 |

This shows the contribution made at the respective distances by the zones of the vapour cloud using the different blast strengths and cloud quantities. The confined part of the cloud generates greater far field overpressures compared with the TNT equivalent model. ■ ■ ■

### 6.7.3.3 Models based on computational fluid dynamics

A number of gas explosion experiments with structures simulating modules of offshore oil and gas platforms were conducted by Christian Michelsen Research in Norway (Bjerketvedt et al. 1997). It was found that the measured overpressures were significantly higher than those predicted by available simple models. The need for a more fundamental approach was established.

The growing interest in the use of more fundamental approaches to explosions based on Computational Fluid Dynamics (CFD) has led to the development of a number of models, now routinely used for off-shore explosion assessments and situations with complex geometries. The MERGE project in Europe during the early 1990s sought to understand factors that would lead to improvements in CFD code predictions (Popat et al. 1996). Typical of the CFD codes are:

(i) AutoReaGas (TNO and Century Dynamics)
(ii) EXSIM (Exsim, Norway)
(iii) FLACS (GexCon, Christian Michelsen Research, Norway)
(iv) COBRA (Mantis Numerics, Advantica Technologies, UK)
(v) CFX-4 (AEA Technology, UK)

These models are modified CFD codes with particular submodels that deal with such issues as:

(i) Ignition and laminar flame propagation
(ii) Turbulent flame propagation
(iii) Combustion

The current status of CFD explosion modelling is given by Bull (2004) and Lea and Ledin (2002) who cover many issues related to the modelling, solution and validation of these codes. Of particular significance to CFD approaches are the following issues:

(i) Use of crude approximations to complex geometries
(ii) Considerable uncertainty in combustion sub-models
(iii) Importance of considering pre-existing turbulence, such as high pressure gas releases
(iv) Simple treatments of turbulence
(v) The need for more large-scale experimentation
(vi) The use of adaptive grid refinement and improved numerical solution schemes
(vii) Incorporation of flame distortion phenomena and flame interactions
(viii) Incorporating the interaction of blast-structure effects such that the movement of structures is considered on the propagation of the blast wave.

Despite the many challenges in developing and applying CFD explosion models, predictions from these codes in complex off-shore and on-shore process geometries appear to lie within a factor of 2 of the experimental data (Bull 2004). The use of such tools is a specialist area which is finding a growing acceptance and application base.

### 6.7.3.4 Assumptions and limitations

The TNT equivalent model can obviously be used in situations where dense phase explosions are relevant and geometries are simple. The use of TNT equivalent models for hydrocarbon-air mixtures is not recommended. However, for hydrogen-rich gases, Hawksley (1986) has recommended the use of TNT equivalent model with a 10% explosion efficiency, based on empirical data gathered from actual explosion events.

Where the TNT equivalent model is not applicable, the multi-energy model (MEM) or the use of CFD codes is preferred. Evenso, there are still significant uncertainties in these approaches.

In the case of the MEM there are two key characteristics to be estimated. These are:

(i) The size of the vapour cloud charge, $E$ and

(ii) $P_{CS}$, representing the maximum explosion overpressure for values of $\overline{R}$ less than $\overline{R}_o$. This allows selection of the appropriate charge strength (1 to 10).

The vapour cloud charge is easy to estimate, however, the continuing problem is the estimation of charge strength. The charge strength still remains an issue of major uncertainty despite attempts to correlate it with explosion tests.

In the case of CFD codes, there is still much to be done to improve the fidelity of the predictions in complex process situations (Bull 2004; Lea and Ledin 2002). There still exists significant issues to address in the CFD sub-models that deal with combustion processes, reaction kinetics, turbulence models and grid refinement to capture length scales of the problem at sensible computation times. For situations where there are complex geometries such as off-shore processing platforms, CFD tools provide more credible predictions than TNT and MEM methods. CFD codes require significant computation times for large-scale 3D applications and are not to be considered a tool for the amateur.

Another limitation in the application of CFD models for blast analysis in offshore oil and gas facilities is that the volume of module filled by flammable gas cloud is unknown, and hence a sensitivity analysis would be required, using various module fill fractions. Assumption of full module fill may give high blast overpressures and drag, introducing over-conservatism in structural design.

## 6.8 EFFECTS MODELLING OF DISPERSION

The release of a gas or vapour and its subsequent dispersion in the atmosphere is a significant event. Many instances occur of regulated releases such as those from power stations or boilers burning natural gas, oil or coal.

Other incidents involve accidental releases due to equipment or operational failures, e.g. the release of a toxic gas such as chlorine or ammonia from storage cylinders or vessels.

In these circumstances we are interested in the downwind concentration levels which might affect workers or local communities. It gives information on exposure levels and leads to data useful for emergency response procedures.

### 6.8.1 Types of Releases

Before dealing with predictive methods for downwind gas concentrations it is important to discuss the mode of release and the behaviour of the gas. The latter aspect is very dependent on the chemical nature of the substance (density relative to air, reactivity with atmospheric humidity) and the conditions (temperature and pressure) under which it is contained.

The first issue is the mode of release. This can be categorized as:

- Transient release
- continuous release

In the first case, there is a transient short duration release, or a momentary release of gas or "puff" which then subsequently disperses. This could occur when a safety device relieves the pressure in a system and then resets. In this case the puff of gas disperses influenced by the atmospheric conditions at the time (e.g. windspeed and stability of atmosphere).

In the second case, the release is continuous. This could be from a broken pipe, a split in a vessel or an emission from a stack. If the release varies slowly with time then we can consider it to be continuous. Where the release time is significantly shorter than the time to disperse to the distance of interest, then a transient model can be more appropriate.

The second major issue is to do with the density of the released gas in relation to that of the surrounding air. Anyone who has handled "dry ice" will know that the cold carbon dioxide ($CO_2$) spreads along the ground before it heats up and gradually disperses. This leads to three basic types of dispersion:

- positive buoyant dispersion
- neutrally buoyant dispersion
- dense gas dispersion

The first type occurs when the gas has a density lower than air. This can be due to the gas temperature of the molecular weight of the gas which is lower than air, e.g. hydrogen releases. The second type of dispersion occurs when the gas has a density similar to air. The third type behaves quite differently, with initial rolling along the ground until it gains heat by entraining air and disperses as a neutrally buoyant gas. This can be the case with gases like chlorine, ammonia or refrigerated hydrocarbons.

The result of these release types is that specific models are needed for each gas release. In some cases a number of models must be used in sequence (e.g. dense gas model to neutrally buoyant model) and assessment made as to when the transition occurs.

### 6.8.2 Characteristics and Key Factors in Gas Dispersion

The dispersion of gases in the atmosphere is a complex issue affected by many parameters. Table 6-18 sets out some of the principal parameters which ultimately affect the impact of these incidents.

TABLE 6-18 CHARACTERISTICS OF GAS DISPERSIONS

| TYPES OF RELEASES | ATMOSPHERIC and IMPACT |
|---|---|
| • transient or continuous release | • meteorological |
| • positively buoyant dispersions | - wind speed |
| • neutrally buoyant dispersions | - atmospheric stability |
| • dense gas dispersions | • topological stability |
| MODELS | - ground slope |
| • Sutton model | - roughness |
| • Pasquill-Gifford model | - obstructions |
| • Box, Top-hat and variant models for dense gases | • wind |
| | - direction |
| | - speed |
| | - turbulence |
| | - persistence |
| | • toxic load on receptors |
| | - breathing rate |
| | - exposure time |

Note that for the degree of dispersion, the geography of the area as well as the conditions in the atmosphere are important. In terms of final impact on people or animals the exposure time, breathing rate and gas concentration will determine the toxic load.

## 6.8.3 Dispersion Modelling

In attempting to predict downwind gas concentrations many models have been developed. These models essentially fall into two major groups:

- neutrally buoyant models based on the Pasquill-Gifford model
- dense gas models based on box or top-hat representations.

Within both groups there are two basic models which account for continuous releases and also transient releases.

### *6.8.3.1 Positively buoyant models*

Positive buoyancy occurs when either the released gas is above atmospheric temperatures or is of a formula weight below that of air. This is the case with such gases as hydrogen ($H_2$) and methane ($CH_4$). Hot stack gases and other process gases can act in a positively buoyant manner.

For stack gases, that are hot, plume rise models exist to predict the amount of rise above the discharge location based on both momentum and temperature. They are commonly used in predicting downwind concentrations of pollutants from stack emissions.

In the case of light hydrocarbon releases and gases such as hydrogen, computational fluid dynamics (CFD) is often the best predictive tool to employ. It is however an expensive option from both time and effort perspectives.

### 6.8.3.2 *Neutrally buoyant models*

**Continuous release**

In this case the predicted downwind concentration is given by a simple Gaussian model in Table 6-19.

**TABLE 6-19 GAUSSIAN MODEL FOR NEUTRALLY BUOYANT DISPERSION**

The Gaussian model for continuous dispersion is:

$$C(x,y,z;H)=\frac{Q}{2\pi u\sigma_y\sigma_z}\exp\left[\frac{-y^2}{2\sigma_y^2}\right]\left\{\exp\left[\frac{-(H-z)^2}{2\sigma_z^2}\right]+\exp\left[\frac{-(H+z)^2}{2\sigma_z^2}\right]\right\} \quad (6.45)$$

where

| | | | | | |
|---|---|---|---|---|---|
| $C$ | = | concentration downwind at location (x, y, z) (kg/m$^3$) | $u$ | = | windspeed (m/s) |
| $Q$ | = | release rate (kg/s) | $x$ | = | downwind distance (m) |
| $H$ | = | release height (m) | $y$ | = | crosswind distance (m) |
| $\sigma_y$ | = | horizontal dispersion coefficient (m) | $z$ | = | vertical distance (m) |
| $\sigma_z$ | = | vertical dispersion coefficient (m) | | | |

The co-ordinates ($x$, $y$, $z$) describe the distances downwind, crosswind and vertical from an origin at the start of the release point at ground level. This is shown in Figure 6-22 (Turner, 1994).

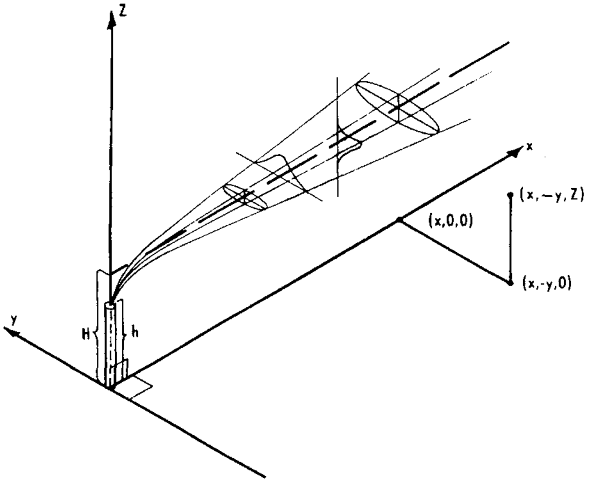


**FIGURE 6-22 CO-ORDINATE SYSTEM FOR GAS DISPERSION (Turner 1994, by permission)**

The dispersion coefficients are obtained graphically or numerically using the downwind distance and stability category of the atmosphere. This stability parameter (designated A to F) describes the degree of vertical mixing in the atmosphere. Category A describes an unstable atmosphere typical of a very sunny day. Category D is regarded as neutrally stable whilst Category F is very stable, typical of night-time conditions. The original stability categories are given in Table 6-22. It is necessary to make an assessment of the degree of insolation (solar radiation) present and note the windspeed range. It is clear that some incompatibilities exist, such that high windspeeds (> 6 m/s) with very unstable conditions like A do not normally co-exist. It is common to report stability-windspeed categories as A2 or D5 etc. Dispersion coefficients are then found from graphical presentations or from correlations such as those in Table 6-20 (CCPS 2000) for rural and urban conditions.

TABLE 6-20 PASQUILL'S STABILITY CATEGORIES

| Surface |  | Insolation |  | Night |  |
|---|---|---|---|---|---|
| wind speed at 10m height (m/s) | strong | moderate | slight | thinly overcast or $\geq$ 4/8 cloud | $\leq$ 3/8 cloud |
| $<2$ | A | A-B | B | - | - |
| 2 - 3 | A-B | B | C | E | F |
| 3 - 5 | B | B-C | C | D | E |
| 5 - 6 | C | C-D | D | D | D |
| $>6$ | C | D | D | D | D |

TABLE 6-21 DISPERSION PARAMETERS FOR CONTINUOUS PASQUILL-GIFFORD MODEL (CCPS, 2000)

| Pasquill-Gifford stability class | $\sigma_y$(m) | $\sigma_z$ (m) |
|---|---|---|
| Rural Conditions |  |  |
| A | $0.22x(1+0.0001x)^{-1/2}$ | $0.20x$ |
| B | $0.16x(1+0.0001x)^{-1/2}$ | $0.12x$ |
| C | $0.11x(1+0.0001x)^{-1/2}$ | $0.08x(1+0.0002x)^{-1/2}$ |
| D | $0.08x(1+0.0001x)^{-1/2}$ | $0.06x(1+0.0015x)^{-1/2}$ |
| E | $0.06x(1+0.0001x)^{-1/2}$ | $0.03x(1+0.0003x)^{-1}$ |
| F | $0.04x(1+0.0001x)^{-1/2}$ | $0.016x(1+0.0003x)^{-1}$ |
| Urban Conditions |  |  |
| A-B | $0.32x(1+0.0004x)^{-1/2}$ | $0.24x(1+0.001x)^{-1/2}$ |
| C | $0.22x(1+0.0004x)^{-1/2}$ | $0.20x$ |
| D | $0.16x(1+0.0004x)^{-1/2}$ | $0.14x(1+0.003x)^{-1/2}$ |
| E-F | $0.11x(1+0.0004x)^{-1/2}$ | $0.08x(1+0.0015x)^{-1/2}$ |

When the groundlevel concentration along the centreline of the plume is required, then Eq.(6.45) reduces to:

$$C(x,0,0;H)=\frac{Q}{\pi\, u\, \sigma_y \sigma_z}\exp\left[\frac{-H^2}{2\sigma_z^2}\right] \qquad (6.46)$$

since $y = z = 0$

The overall procedure is then to:

- select distance and release rate
- select stability category (A to F)
- determine dispersion coefficients
- obtain windspeed
- obtain release height
- calculate downwind concentration, C.

### EXAMPLE 6-14 NEUTRALLY BUOYANT DISPERSION

A rupture occurs in an overhead line 30 m above ground releasing 2.25 kg/s of vapour that can be considered as neutrally buoyant. Moderately stable conditions with a 4 m/s breeze exist. What is the ground level concentration at a distance of 500 m downwind?

For moderately stable conditions, stability category E is selected. Dispersion coefficients from Table 6-21 under rural conditions give:

$$\sigma_y = 29\text{m} \qquad \sigma_z = 13\text{m}$$

At the centreline using equation (6.46):

$$C = \frac{2.25}{\pi\ (29)(13)(4)} \exp\left[ -\frac{1}{2}\left(\frac{30}{13}\right)^2 \right] = 1.04 \times 10^{-4} kg = 33\,\text{mg/m}^3$$

### Instantaneous release

An instantaneous or transient release of gas can also be predicted. Using a Pasquill-Gifford approach the predicted downwind gas concentration is given by equation (6.47) in Table 6-24.

In this case the dispersion coefficients are somewhat different from those associated with the continuous release. It can be assumed that $\sigma_x = \sigma_y$. Lees (1980) quotes the dispersion coefficients as shown in Table 6-23. They are smaller than the equivalent continuous source coefficients.

### TABLE 6-22 INSTANTANEOUS GAS DISPERSION MODEL

The Pasquill-Gifford instantaneous release model is given by:

$$C(x, y, 0; H) = \frac{2Q^*}{(2\pi)^{1.5}\ \sigma_x\ \sigma_y\ \sigma_z} \exp\left[-\frac{1}{2}\left(\frac{x - ut}{\sigma_x}\right)^2\right] \exp\left[-\frac{1}{2}\left(\frac{H}{\sigma_z}\right)^2\right] \exp\left[-\frac{1}{2}\left(\frac{y}{\sigma_y}\right)^2\right] \tag{6.47}$$

at the point $(x, y, 0)$ i.e at ground level ($z = 0$) and with a release height of $H$

| | | | | | |
|---|---|---|---|---|---|
| $C$ | = | gas concentration (kg/m$^3$) | $u$ | = | windspeed (m/s) |
| $Q^*$ | = | gas release (kg) | $t$ | = | time (s) |
| $\sigma_x$ | = | downwind dispersion coefficient (m) | $H$ | = | release height (m) |
| $\sigma_y$ | = | crosswind dispersion coefficient (m) | | | |
| $\sigma_z$ | = | vertical dispersion coefficient (m) | | | |

### TABLE 6-23 DISPERSION PARAMETERS FOR INSTANTANEOUS PASQUILL-GIFFORD MODEL (Lees, 1980)

| Pasquill-Gifford stability class | $\sigma_y$(m) | $\sigma_z$ (m) |
|---|---|---|
| A | $0.18x^{0.92}$ | $0.60x^{0.75}$ |
| B | $0.14x^{0.92}$ | $0.53x^{0.73}$ |
| C | $0.10x^{0.92}$ | $0.34x^{0.71}$ |
| D | $0.06x^{0.92}$ | $0.15x^{0.70}$ |
| E | $0.04x^{0.92}$ | $0.10x^{0.65}$ |
| F | $0.02x^{0.89}$ | $0.05x^{0.61}$ |

### EXAMPLE 6-15 TANK RELEASE USING INSTANTANEOUS MODEL

The total mass of gas released from a tank is 30 kg. The wind velocity from the north is 4 m/s and there is a stable atmosphere of category D. The effective release height is estimated at 15m. Calculate the gas concentration at 500 metres south and 20 metres west of the release, 2 minutes after the release.

| | | |
|---|---|---|
| Here: | $x$ | = 500 m |
| | $y$ | = 20 m |
| | $u$ | = 4 m/s |
| | $Q^*$ | = 30 kg |

Using Table 6-23 the dispersion coefficients are:

$$\sigma_x = \sigma_y = 18\text{m};\ \sigma_z = 11.6\text{m}$$

Equation (6.47) gives:

$$C(500,100,0;15) = \frac{2(30)}{(2\pi)^{\frac{3}{2}}(18)(18)(11.6)} \exp\left[-\frac{1}{2}\left(\frac{500-(4)(120)}{18}\right)^2\right] *$$

$$\exp\left[-\frac{1}{2}\left(\frac{15}{11.6}\right)^2\right] \exp\left[-\frac{1}{2}\left(\frac{20}{18}\right)^2\right] = 1.278\times10^{-4}\ \text{kg/m}^3 = 128\ \text{mg/m}^3$$

■ ■ ■

### 6.8.3.3 Heavier than air gas dispersions

These are an important class of gas release events but their calculation requires much more sophisticated modelling procedures. A significant number of commercial packages such as DEGADIS (Dense GAs DISpersion (Spicer and Havens 1989)), HGSYSTEM (Shell 1994) or PHAST (DNV 2004) are available for these types of dispersion calculations. Some of these codes have been validated against field data in the USA and Europe.

In considering these events there are several categories of release which lead to dense gas behaviour. These include:

(i) gases with molecular weight greater than air (29 kg/kgmole) e.g. LPG and chlorine.
(ii) liquefied gases at cryogenic (below ambient) temperatures e.g. liquefied natural gas (LNG)
(iii) liquefied gases under pressure with boiling point below atmospheric temperature e.g. ammonia

The release of such gases leads to a series of complex phenomena where the gas passes through a number of flow regimes. These are:

(i) an initial buoyancy dominated flow that includes gravity spreading and air entrainment at the outer edges and the top surface.
(ii) a stably stratified flow where the cloud is progressing along the ground but has a change in density vertically through the cloud.
(iii) a regime of passive dispersion in the current air flow after the transition to neutrally buoyant conditions.

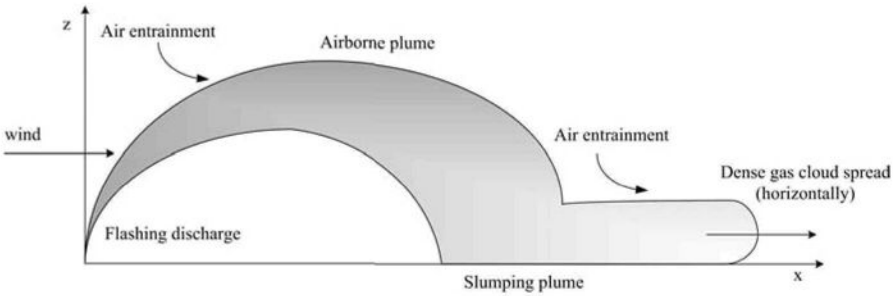


FIGURE 6-23 SCHEMATIC OF A TYPICAL HEAVY GAS RELEASE AND SPREAD

Most heavy gas dispersion models consist of a series of linked submodels. The HGSYSTEM is typical of this architecture, that addresses:

(i) Models for the source term
Here, submodels that predict the initial gas/liquid discharge in the form of flashing or non-flashing flows, multi-component vapour-liquid aerosols and some complex chemistry such as hydrogen fluoride releases. Pool evaporation models such as LPOOL (Cavanaugh et al. 1994) are often embedded.

(ii) Plume models
These track the release of materials through the stages of initial release and plume rise, the airborne trajectory followed by slumping, ground contact and subsequent gravity and wind driven cloud flow.

(iii) Heavy gas cloud models
These predict the gravity spreading of the cloud, the entrainment of air at the cloud surfaces, effects of heat fluxes from the ground and atmosphere. The thermodynamics of the time evolving cloud are tracked. At the point where the cloud spread leads to a passive dispersion situation, the standard Gaussian models are used to predict further dispersion.

Heavy gas models are complex tools that have their limitations. These include:

(i) The presence of obstacles within the initial plume and subsequent cloud path. These situations require other approaches such as CFD methods.

(ii) The presence of complex terrain, such as hills, valleys and sloping ground that cannot normally be handled by current heavy gas models.

(iii) Wind shifts often occur and these have effects such as "steering" the dispersion. Most models do not account for this.

When such limitations exist, then either customization of existing codes are required or CFD models can be used (Havens and Spicer 2002). Evenso, there are still significant issues to address and CFD is not a "silver bullet" for these situations. The experience with CFD heavy gas models and their validation is quite variable (McBride et al. 2001) and specialized ultra low speed (ULS) wind tunnels are providing reliable data for validation purposes (Havens and Spicer 2002).

The recent work on heavy gas CFD models suggest that flat terrain models can produce results that over-estimate hazard ranges by a factor of 5 and predicted directions can vary by up to 90°. Complex terrain, such as ditches can in fact provide areas of gas concentration increases above predictions of flat terrain models. Hence it is necessary to consider the use of appropriate, validated tools specific to the task.

Heavier than air gases that form acid mists by reacting with atmospheric humidity (e.g. sulphur trioxide, hydrogen chloride) pose interesting problems in gas dispersion. Unlike heavy gases that slump to ground, reactive gases form microscopic size aerosol mists, which tend to be suspended in air. Therefore, these water reactive gases are generally modelled as neutrally buoyant gases.

### 6.8.3.4 Free turbulent jets

Free turbulent jets of gas into still air are one of the most common source terms in incident modelling. They arise from gasket, flange or pipeline component failures as well as from vessels and their attachments. The turbulent jet can be characterized by a 3 stage development, as seen in Figure 6-24. This involves:

(i) Zone (1) near the gas orifice where a gas core exits into the ambient air, with some initial air entrainment at the orifice. If flashing liquids are released, then this is the zone where flashing occurs due to rapid pressure reduction. This is the depressurization zone which occurs within about 5 diameters of the discharge point.

(ii) Zone (2) where significant air entrainment occurs with gas being mixed with air so that the core disappears. The lateral gas concentration goes from a 'top hat' to a Gaussian profile.

(iii) Zone (3) represents the fully developed flow of the jet with typical Gaussian profile. This is a zone where eddy-dominated flow occurs. Both jet velocity and concentration profiles are Gaussian.

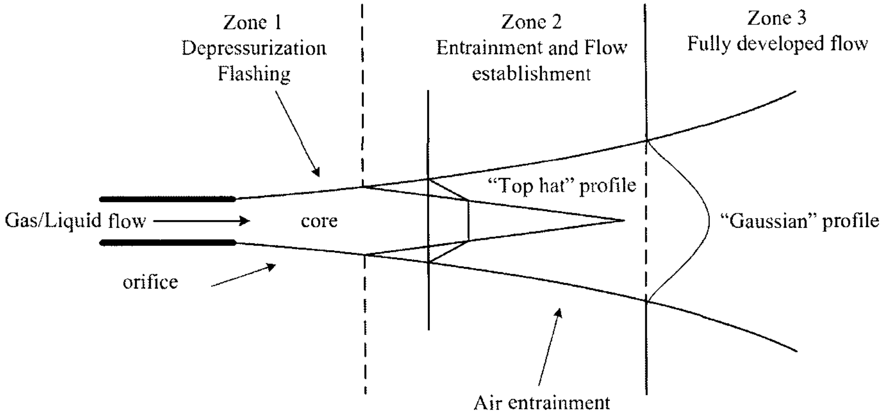


FIGURE 6-24 TURBULENT FREE JET DEVELOPMENT ZONES

A large amount of research has been done on many models. Various models are embedded within software systems such as FRED (Shell 2004), PHAST (DNV 2004) and EFFECTS (TNO 2004).

The shape of the jet is determined largely by the orifice shape and the presence of any obstacles. The jet density has an effect on the final behaviour of the flow field with light, neutral and heavy gases behaving quite differently. Wind effects are very important and greatly affect the interaction of the jet within the environment as the momentum effects dissipate.

Free jets of flammable or toxic materials are of interest because their interaction within the ambient conditions determines in the case of flammable materials the distance to the lower flammability limit (LFL). This is an indicator of hazard zones for fire events. In the case of toxics, the key factor is the concentration profile along the jet axis and then the subsequent dispersion of the gas into the environment.

The models used to estimate temperature and concentration profiles in the turbulent jet can be of two main types:

(i) Characteristics based on relatively simple correlations involving distribution constants that are specific to each gas. They depend on the gas to air relative density (Ricou and Spalding 1961). These distribution constants are then used to estimate the concentration and velocity distribution in any plane perpendicular to the jet axis at a distance from the orifice. They are useful, quick techniques to generate initial concentration profiles or isopleths.

(ii) Models based on solving the conservation balances for momentum, mass, species and energy for the system. These are fundamental, mechanistic methods that can also account for directional discharge aspects as well as wind effects. One such model is JINX (Cooper 2001) whilst others such as AEROPLUME (Shell 2004) and the Unified Dispersion Model (UDM) of DNV (Holt and Witlox 2000) are embedded into larger software systems.

In most cases, these fundamental free turbulent jet models are restricted to applications where there are no nearby obstacles or direct ground interaction in the case of downward facing releases. Some work by Cooper (2001) reports on model developments to handle jet grounding, interaction with obstacles such as pipes, storage vessels, steelwork and floors. Interactions effectively change entrainment rates and hence dilution as well as impose flow resistances. Further validation work to resolve the submodels is required.

In complex geometry situations such as off-shore installations and on-shore facilities, CFD codes can be used to improve flow-field predictions. The CFD dispersion model can be used to determine the volume of module filled by flammable gas cloud in offshore facilities, which can form an input to explosion CFD model. This approach has its own limitation in that the gas dispersion CFD models have not been fully validated for the congested environment. Research continues in this area.

### 6.8.3.5 Dispersion of fire plumes

It is not only the thermal radiation effects of fires that need to be considered in consequence analysis but in many cases the effects of fire plume dispersion, especially where toxic compounds exist in the fire plume. This is a very common occurrence in industrial and commercial fires, especially in the case of warehouse fires that contain flammable and combustible liquids and Class 6 substances such as pesticides, herbicides and poisons. The cocktail can be lethal and in the case of unrestricted fires a number of key factors come into play. These include:

(i) The substances in the fire
(ii) The degree of combustion of the major substances
(iii) The fire size (diameter) and energy release as convective heat

(iv) The atmospheric conditions such as windspeed, relative humidity, atmospheric stability and ambient temperature.
(v) The presence of nearby buildings
(vi) The release location (indoors, outdoors)

**EXAMPLE 6-16 PLANT AND WAREHOUSE FIRES**

- In October 1987, 25,000 people were evacuated from surrounding areas to a chemical storage warehouse in Nantes, France. This followed a warehouse fire in the building which contained large amounts of fertilizers. Combustion gases in the fire plume included chlorine, ammonia, nitric acid and nitrogen oxides. The subsequent contaminated fire water found its way into the river Loire.
- A fire and explosion at a pesticide packaging plant in Arkansas, USA in November 1998 caused the deaths of 3 firemen and injured a further 16. A large quantity of azinphos-methyl caught fire and exploded. The fire generated a large plume which spread over the plant and surrounding area.

One of the biggest challenges in determining impacts from fire plumes is the level of combustion products in the plume. A number of workers have sought to quantify combustion products under various conditions of oxygen availability. The product spectrum can change significantly if the fire is starved of oxygen. Two significant European studies have addressed aspects of this including:

- The Combustion of Chemical Substances and the Impact on the Environment of Fire Products (EU/STEP CT91-0109)
- Guidelines for Management of Fires in Chemical Warehouses (EU/EV5V-CT93-0275)

These projects obtained data for identification and quantification of fire products. Nelson (2000) provides a summary of the projects. Other workers such as Smith-Hansen and Jorgensen (1992, 1993) did microscale combustion experiments on a wide range of pesticides, fertilizers and polymers.

Christensen et al. (1993) and Christensen (1994) addressed ammonium nitrate combustion products and pesticides combustion. The most recent studies by Costa et al. (1999) described the combustion products from over 100 substances covering plastics, fabrics, chemicals and pesticides, whilst Vikelsoe and Johansen (2000) did small scale experiments on chlorinated pesticides, PVC and other chemicals.

All these studies provide important source data when considering the generation of fire products from a range of scenarios.

The mechanisms active in fire plume generation and subsequent dispersion are complex. The predominant mechanism is the buoyancy of the plume generated by convective heat from combustion. In most cases the convective to radiative contributions from the heat of combustion exceeds a 2 to 1 ratio. Hence there is a strong upward lift of smoke as well as unburnt substances and combustion products that subsequently interacts with the ambient conditions. On calm days fire plumes rise vertically with virtually no ground level concentration of combustion products near the fire. Strong winds deflect the buoyant plume and through convection and dispersion create, what could be, dangerous ground level concentrations of toxic substances. The strong buoyancy driven flow, entrains large amounts of ambient air that cools and slows the vertically rising plume.

Early work on plume rise by Morton et al. (1956) has been complemented by many other authors (Porch et al. 1986, 1988; Zonato et al. 1993). Plume rise concepts are well understood and convincing models are available.

Carter (1989) combined fire dynamics with a Gaussian plume model to estimate downwind concentrations of products for both open-air and warehouse situations. In this case the Gaussian dispersion coefficients were modified to account for building wake. Plume centreline estimates were based on the Moore model (1980) excluding the momentum effects of the plume discharge. This model provided a "first estimate" tool for assessing warehouse fire impacts. Plume height is known to vary as $x^{2/3}$ with $x$ being the downwind distance.

Along with modelling studies, Hall and co-workers (1995, 1998) carried out extensive wind tunnel testing of many scenarios related to fire plume dispersion from warehouses where there was partial roof opening to full roof openings or no roof. What is clear from these wind tunnel experiments is that:

(i) Ground level concentrations are a strong function of the buoyancy flux (related to convective heat release) which dominates fire events

(ii) Plume "lift-off" from the ground is strongly influenced by the ambient windspeed and occurs when the Briggs lift-off criterion of $L_p$ exceeds a value around 29. This corresponded to a buoyancy flux ($F/u^3L$) of 0.11 where $F$ is proportional to the fire heat output, $u$ is the reference windspeed and $L$ is the building height. Above 0.11 the plume lifts off into the air and ground level concentrations rapidly decrease.

(iii) Building shape plays an important role in determining downwind ground-level concentrations.

(iv) The number and type of openings in the roof affects downwind concentrations. More openings increase heat output through better fire ventilation and thus give higher buoyancy to plume.

(v) The wind angle to the building is an important factor.

(vi) Concentrations at ground level, downwind beyond the building wake, typically reduce as $x^{-0.8}$.

These complex factors make specific predictions of ground level concentrations extremely challenging. This is especially the case where nearby upstream and downstream buildings are present. In these cases, it is possible to use sophisticated CFD modelling (Ward 2004) or to use Gaussian models with modified dispersion coefficients that account for building geometry such as ADMS (Carruthers et al. 1999).

For situations where nearby building effects are important only CFD models provide any real chance of predicting the complex flow fields. What is clear is that one needs appropriate, validated models to carry out these predictions and that the source terms need to be carefully considered. Sensitivity studies are vital in checking output variations to source term changes and also the stage of the fire: whether initial, developing or fully developed due to the significant impact of buoyancy effects on ground level toxic concentrations.

## 6.9 REVIEW

Effects modelling is a vital part of risk management. It provides key information to a range of stakeholders that include designers, operators, emergency response personnel, town planners and government agencies. Effects modelling has reached a maturity over the last 20 years, with further validation from full-scale experiments providing valuable data for checking model predictions.

There is a growing trend in model development to address the non-standard situations through advanced computational methods such as CFD. This is particularly the case in congested situations such as off-shore platforms where complex geometries often defeat simplistic approaches to gas release, fire and explosion events.

Despite the significant advances which have reduced variability and uncertainty, sensitivity analyses are mandatory where effects can be significant on sensitive receptors (Quelch and Cameron 1994).

The fundamental chemistry of many events is still poorly understood, especially in reactive chemical events. Here, significant effort is evident in improving insights and understanding the phenomena. Software tools in the general area of effects prediction need to be used cautiously with underlying assumptions being fully appreciated.

## 6.10 REFERENCES

American Petroleum Institute (API) 1997, *Guide for Pressure Relieving and Depressurizing Systems*, 4th edn, API RP-521, American Petroleum Institute, USA.

Baker, Q.A., Tang, M.J., Scheier, E.A. and Silva, G.J. 1996, 'Vapour cloud explosion analysis', *Process Safety Progress*, vol. 15, no. 2, pp. 106-109.

Bjerketvedt, D., Bakke, J.R. and Van Wingerden, K. 1997, 'Gas explosion handbook', *Journal of Hazardous Materials*, vol. 52, no. 1, pp. 1-150.

Brasie, W.C. and Simpson, D.W. 1968, 'Guidelines for estimating damage from explosion', *Chemical Engineering Progress Loss Prevention*, vol. 2, pp. 91.

Bull, D.C. 2004, *A critical review of post Piper-Alpha developments in explosion science for the off-shore industry*, HSE Research Report #89, HMSO, Norwich, UK.

Carruthers, D.J., McKeown, A.M., Hall, D.J. and Porter, S. 1999, 'Validation of ADMS against wind tunnel data of dispersion from chemical warehouse fires', *Atmospheric Environment*, vol. 33A, pp. 1937-1953.

Carter, D.A. 1989, 'Methods for estimating the dispersion of toxic combustion products from large fires', *Chemical Engineering Research and Design*, vol. 67, pp. 348-352.

Cavanaugh, T.A., Siegell, J.H. and Steinberg, K.W. 1994, 'Simulation of vapour emissions from liquid spills', *Journal of Hazardous Materials*, vol. 38, pp. 41-63.

CCPS 2000, Center for Chemical Process Safety, *Guidelines for Chemical Process Quantitative Risk Analysis*, 2nd edn, AIChE, New York.

Chamberlain, G.A. 1987, 'Developments in design methods for predicting thermal radiation form flares', *Institution of Chemical Engineers Chemical Engineering Research Development*, vol. 65, pp. 299-309.

Christensen, V., Kakko, R. and Koivisto, R. 1993, 'Environmental impact of a warehouse fire containing ammonium nitrate', *Journal of Loss Prevention in the Process Industries*, vol. 6, pp. 233-239.

Christensen, V. 1994, 'Combustion of some pesticides and evaluation of the environmental impact', *Journal of Loss Prevention in the Process Industries*, vol. 7, pp. 39-48.

Cook, D.K., Fairweather, M., Hammonds, J. and Hughes, D.J. 1987, 'Size and Radiative Characteristics of Natural Gas Flares. Part 1 – Field Scale Experiments, and Part 2 – Empirical Model', *Chemical Engineering Research Development*, vol. 65, pp. 310-325.

Cooper, M.A. 2001, *A Model for jet dispersion in a congested environment*, HSE Contract Research Report 396/2001, HMSO, Norwich, UK.

Costa, C., Treand, G., Moineault, F. and Gustin, J.L. 1999, 'Assessment of the thermal and toxic effects of chemical and pesticide pool fires based on experimental data obtained using the Tewarson apparatus', *Process Safety and Environmental Protection*, vol. 77B, pp. 154-164.

Crowley, L.T. and Johnson, A.D. 1992, *Oil and Gas Fires: Characteristics and Impacts*, Research Report Offshore Technology Information, OTI92 596, HSE, UK.

Crowley, L.T. 1992a, *Behaviour of Oil and Gas fires in the presence of confinement and obstacles*, Research Report, OTI92 597, HSE, UK.

Crowley, L.T., 1992b, *Current fire research: experimental, theoretical and predictive modelling resources*, Res. Report OTI 92 598, HSE, UK, vol. 1.

Daesim 2004, *Daesim Studio: Risk Assessor*, Daesim Technologies Pty Ltd, Australia, Available at: http://www.daesim.com/ .

DNV 2004, *PHAST - Process Hazard Analysis Software Tool*, DNV Software, Available at: http://www.dnv.com/software/ .

Fire and Blast Information Group (FABIG) 1988, *Blast and Fire Engineering Projects for Topside Structures*, Steel Construction Institute, UK. Available at: http://www.fabig.com .

Fletcher, B. and Johnson, A.E. 1984, *The Discharge of Superheated Liquids from Pipes*, Institution of Chemical Engineers, Rugby, UK.

Guilbert, P.W. and Jones, I.P. 1996, *Modelling of Explosions and Deflagrations*, HSE Contract Research Report 93/1996, HMSO, UK.

Hall, D.J., Kukadia, V., Walker, S. and Marsland, G. 1995, *Plume dispersion from chemical warehouse fires*, Technical Report, Building Research Establishment, Garston, Watford WD2 7JR, United Kingdom.

Hall, D.J., Kukadia, V., Walker, S. and Marsland, G.W. 1998, 'Deposition of large particles from warehouse fire plumes–A small-scale wind tunnel model study', *Journal of Hazardous Materials*, vol. 59, pp. 13-29.

Hamins, A., Kashiwagi, T. and Buch, R. 1995, 'Characteristics of Pool Fire Burning', *Fire Resistance of Industrial Fluids,* ASTM STP 1284, American Society for Testing Materials, Philadelphia, USA.

Havens, J. and Spicer, T. 2002, 'New models predict consequences of LNG Releases', *GasTIPS*, Fall 2002, Gas Technology Institute, USA.

Hawksley, J.L. 1986, 'Unconfined vapour cloud explosions involving hydrogen rich gases - estimating the blast effects', *Loss Prevention Bulletin*, no. 68, The Institution of Chemical Engineers, Rugby, UK.

Holman, J.P. 1981, *Heat Transfer*, 5th edn, McGraw-Hill, USA.

Holt, A. and Witlox, H.W.M. 2000, *Validation of the Unified Dispersion Model*, DNV Software-Risk Management, Consequence Modelling Documentation, UDM6.0, London, UK.

Johnson, A.D., Shirvill, L.C. and Ungut, A. 1999, *CFD Calculation of Impinging Gas Jet Fires*, Offshore Technology Report OTO1999011, HSE, UK.

Johnson, A.D., Brightwell, H.M. and Carsley, A.J. 1994, 'A model for predicting the thermal radiation hazards from large-scale horizontally released natural gas jet fires', *Transactions of Institution of Chemical Engineers*, Process Safety and Environmental Protection, vol. 72 Part B, pp. 157-166.

Johnson, A.D. 1992, 'A model for predicting thermal radiation hazards from large-scale pool fires', *Institution of Chemical Engineers Symposium Series No. 130*, pp. 507-524.

Kawaramura, P.I. and Mackay, D. 1987, 'The evaporation of volatile liquids', *Journal of Hazardous Materials*, vol. 15, pp. 365-376.

Kinsella, K.G. 1992, 'A Rapid Assessment Methodology for the Prediction of Vapour Cloud Explosion Overpressure', *International Conference on Safety and Loss Prevention*, Singapore.

Lawrence, F.E. and Johnson, E.E. 1974, 'Design for limiting explosion damage', *Chemical Engineering*, vol. 7, January.

Lea, C.J. and Ledin, H.S. 2002, *A Review of the State-of-the-Art in Gas Explosion Modelling*, Health and Safety Laboratory Report HSL/2002/02, Fire and Explosion Group, Buxton, UK.

Lees, F.P. 1980, *Loss Prevention in the Process Industries*, 1st edn, Butterworths, UK.

Lees, F.P. 2001, *Loss Prevention in the Process Industries*, 2nd edn, Butterworths-Heinemann, Oxford, UK.

McBride, M.A., Reevs, A.B., Vanderheyden, M.D., Lea, C.J. and Zhou, X.X. 2001, 'Use of advanced techniques to model the dispersion of chlorine in complex terrain', *Transactions of Institution of Chemical Engineers*, vol. 79, Part B, pp. 89-102.

Mercx, W.P.M., van den Berg, A.C. and van Leeuwen, D. 1998, *Application of correlations to quantify the source strength of vapour cloud explosions in realistic situations: Final report for the project 'GAMES'*, TNO Report, PML1998-C53, Rijswijk, The Netherlands.

Mercx, W.P.M., van den Berg, A.C., Hayhurst, C.J., Robertson, N.J. and Moran, K.C. 2000, 'Developments in vapour cloud explosion blast modelling', *Journal of Hazardous Materials*, vol. 71, pp. 301-319.

Moore, D.J. 1980, 'Lectures on plume rise' in *Atmospheric Planetary Boundary Layer Physics, Developments in Atmospheric Science*, ed. A. Longhetto, Elsevier, Amsterdam, pp. 327-354.

Morton, B.R., Taylor, G. and Turner, J.S. 1956, 'Turbulent, gravitational convection from maintained and instantaneous sources', *Proceedings of the Royal Society*, vol. 234, pp. 1-23.

Nelson, G.L. 2000, 'Fire and pesticides: A review and analysis of recent work', *Fire Technology*, vol. 36, no. 3, pp. 163-183.

National Fire Protection Association. *Flammable and Combustible Liquid Codes*, National Fire Protection Association, Quincy, Massachusetts. NFPA 30:2000.

Peress, J. 2003, 'Estimate Evaporative Losses from Spills', *Chemical Engineering Progress*, April, pp. 32-34.

Popat, N.R., Catlin, C.A., Arntzen, B.J., Lindstedt, R.P., Hjertager, B.H., Solberg, T., Saeter, O. and van den Berg, A.C. 1996, 'Investigations to improve and assess the accuracy of computational fluid dynamic based explosion models', *Journal of Hazardous Materials*, vol 45, pp.1-25.

Porch, M., Stout, J.E., Cermak, J.E. and Peterka, J.A. 1986, *Physical Modeling of Large-area Fire Plumes*, Technical Report DNA-TR-85-364, Colorado State University, USA.

Porch, M. and Cermak, J.E. 1988, 'Scale-model simulations of large area fire plumes', *International Symposium on Scale Modeling*, July 18-22, Tokyo, Japan, Japan Soc. Mech. Engineers.

Pritchard, M.J. and Binding, T.M. 1992, 'FIRE2: a new approach for predicting thermal radiation levels from hydrocarbon pool fires', *Institution of Chemical Engineers Symposium Series No. 130*, pp. 491-505.

Quelch, J. and Cameron, I.T. 1994, Uncertainty representation and propagation in QRA using fuzzy sets, *Journal of Loss Prevention in the Process Industries*, vol. 7, no. 6, pp. 463-473.

Rew, P.J. and Hulbert, W.G. 1996, *Development of pool fire thermal radiation model*, HSE Contract Research Report 96/1996, HSE, London, HMSO, ISBN 07176 10845.

Ricou, F.P. and Spalding, B.D. 1961, 'Measurement of entrainment by axisymmetrical turbulent jets', *Journal of Fluid Dynamics*, vol. 11, pp. 21-32.

Shaw, P. and Briscoe, F. 1978, *Evaporation from Spills of Hazardous Liquids on Land and Water*, UK Atomic Energy Authority Safety and Reliability Directorate, Culcheth, Warrington.

Shell 2004, *FRED - Fire, Release, Explosion and Dispersion*, Shell Global Solutions, Available at: http://www.shellglobalsolutions.com/hse/software/fred.htm.

Shell 1994, *HGSYSTEM - Heavy Gas System V3.0*, Shell Internationale Research Maatschappij B.V., The Netherlands. Available at: http://www.hgsystem.com/ ,

Smith-Hansen, L. and Jorgensen, K.L. 1992, *Combustion of Chemical substances and the impact of the environment of the fire products: Microscale experiments*, Technical Report, Risø National Laboratory, Roskilde, Denmark.

Smith-Hansen, L. and Jorgensen, K.L. 1993, 'Characterization of fire products from organophosphorus pesticides using the DIN 53436 method', *Journal of Loss Prevention in the Process Industries*, vol. 6, pp. 227-232.

Spicer, T. and Havens, J. 1989, *User's Guide for the DEGADIS 2.01 Dense Gas Dispersion Model*, Report EPA-450/4-89-019, USEPA, USA.

Standards Australia. *The Storage and Handling of Flammable and Combustible Liquids*, Standards Australia, AS 1940:1993.

Tang, M.J. and Baker, Q.A. 2000, 'Comparison of blast curves from vapour cloud explosions', *Journal of Loss Prevention in the Process Industries*, vol. 13, pp. 433-438.

TNO 1992, *Methods for the Calculations of Physical Effects*, Yellow Book 2nd edn, CPR 14E, Director General of Labour, Voorburg, The Netherlands.

TNO 1997, *Methods for the Calculation of Physical Effects*, Yellow Book 3rd edn, CPR14E Part 1, Director-General for Social Affairs & Employment, The Netherlands.

TNO 2004, *EFFECTS - Calculating the physical effects due to hazardous material releases*, TNO Environment and Industrial Safety, Available at: http://www.mep.tno.nl/software/ .

Thomas, P.H. 1963, 'The size of flames from natural fires', *9th Int'l Combustion Symposium*, Combustion Institute, Pittsburgh, USA, pp. 844.

Turner, D.B. 1994, *Workbook of Atmospheric Dispersion Estimates - An Introduction to Dispersion Modeling*, 2nd edn, Lewis Publishers, ISBN1-56670-023-X.

van den Berg, A.C., 1985, 'The Multi-Energy Method - a framework for vapour cloud explosion blast prediction', *Journal of Hazardous Materials*, vol. 12, pp. 1-10.

van den Berg, A.C., van Wingerden, C.J.M. and The, H.G. 1991, 'Vapour Cloud Explosions: Experimental investigation of key parameters and blast modelling', *Transactions of IChemE.*, Part B, vol. 69, pp. 139-148.

Vikelsoe, J. and Johansen, E. 2000, 'Estimation of dioxin emission from fires in chemicals', *Chemosphere*, vol. 40, pp. 165-175.

Ward, A. 2004, *Application of Computational Fluid Dynamics to Modelling the near-field, atmospheric dispersion of combustion products in chemical warehouse fires,* PhD thesis, School of Engineering, The University of Queensland, Brisbane.

Wells, G.L. 1980, *Safety in Process Plant Design,* George Godwin Ltd, London, ISBN 0-7114-5506-6.

Zonato, C., Vidili, A., Pastorino, R and De Faveri, D.M. 1993, 'Plume rise of smoke coming from free burning fires', *Journal of Hazardous Materials*, vol. 34, pp. 69-79.

## 6.11 NOTATION

| | |
|---|---|
| AEROPLUME | Jet release model in HYSYSTEM |
| API | American Petroleum Institute |
| AS | Australian Standard |
| AutoReaGas | CFD explosion code by TNO/Century Dynamics |
| bar | Pressure unit (1 bar = 100 kPa) |
| BLEVE | Boiling liquid expanding vapour explosion |
| CCPS | Center for Chemical Process Safety |
| CFD | Computational fluid dynamics |
| CFX | General purpose CFD code, AEA Technology, UK |
| C:H | Carbon to hydrogen ratio |
| $CH_4$ | Methane |
| CO | Carbon monoxide |
| $CO_2$ | Carbon dioxide |
| COBRA | CFD explosion code, Mantis Numerics, UK |
| DEGADIS | Dense GAs DISpersion |
| EFFECTS | TNO effects software (The Netherlands) |
| EXSIM | CFD explosion code by Tel-tek and Shell Global Solutions |
| FABIG | Fire and Blast Information Group |
| FLACS | Flame acceleration simulator, CMRI Norway |
| FRED | Fire, release, explosion, dispersion software (Shell) |
| $H_2$ | Hydrogen |

| | |
|---|---|
| HF | Hydrogen fluoride |
| HGSYSTEM | Heavy gas system (Shell) |
| HSE | Health & Safety Executive, UK |
| JINX | Jet dispersion model (Advantica Ltd, UK) |
| K | Kelvin |
| kg | kilograms |
| kJ | kilo-Joules |
| kPa | kilo-Pascals |
| kW | kilo-Watts |
| LFL | Lower flammability limit |
| LNG | Liquefied natural gas |
| LPG | Liquefied petroleum gas |
| LPOOL | Liquid pool model (Exxon Research and Engineering) |
| m | metres |
| $m^2$ | square metres |
| $m^3$ | cubic metres |
| MEM | Multi-energy model |
| MERGE | EU project on |
| mg | milligrams |
| mm | millimetres |
| MPa | Mega Pascal |
| $N_2$ | Nitrogen |
| NFPA | National Fire Protection Association |
| $O_2$ | Oxygen |
| Pa | Pascals |
| PEMEX | Petróleos Mexicanos, Mexico |
| PETN | Pentaerythritoltetranitrate |
| PHAST | Process hazard analysis software tool (Det Norske Veritas) |
| RDX | Cyclo-trimethylene-trinitramine explosive |
| RH | Relative humidity |
| s | seconds |
| SIS | Safety instrumented systems |
| TNO | The Netherlands Organization for Applied Scientific Research |
| TNT | Trinitro-toluene |
| UDM | Unified dispersion model |
| ULS | Ultra low speed |
| VBR | Volume blockage ratio |
| VCE | Vapour cloud explosion |

This page is intentionally left blank

# 7
# VULNERABILITY MODELS

*"The moving finger writes; and, having writ, moves on: not all your piety nor wit shall lure it back to cancel half a line, nor all your tears wash out a word of it."*

*Omar Khayyam*

There is a sense of irreversibility in the impact of release of hazardous materials on vulnerable receptors. This has also influenced the risk perception among members of the public.

Having determined the physical effects from release events, it is important to relate the effects to final impacts on vulnerable receptors. This is the area of vulnerability analysis in hazard assessment. Although a well accepted analysis tool, the predictions can be accompanied by significant uncertainty that needs to be taken into the decision-making process. It is vital that the estimates are done with substantial knowledge of the source and circumstances under which vulnerability-models have been developed.

## 7.1 THE ROLE OF VULNERABILITY MODELS

In Section 5.2, we have said that there are two steps in determining consequences from hazardous incidents. These are:

- the physical effects of the event
  (gas concentrations, thermal radiation levels, explosion overpressures)
- the damage caused to the vulnerable receptor

(injury, death, level of burns, structural damage, environmental impairment)

The damage aspects are addressed by vulnerability models, using 'dose-response' relations. Dose-response data and the equivalent graphical representations show the outcomes or response of a dose on people, animals, structures or any nominated receptor. The dose can represent a quantity of a chemical exposure, an impulse from an explosion or a thermal dose. The response represents the level of injury sustained, deaths, physical damage to equipment or level of impairment. Hence the dose-response relation is a generic and common means of representing this relationship. A typical dose-response curve was seen in Chapter 5, Figure 5-2.

More generally we can use probit (probability unit) functions which represent intensity-damage relationships in an algebraic form amenable to computer implementation.

Probit functions have been developed for a wide range of vulnerability model situations. The probit variable $Y$ is generally given as:

$$Y = k_1 + k_2 \ln(V) \tag{7.1}$$

where:

Y = probit variable having mean of 5.0 and variance 1.0

V = a measure of intensity of the causal factor (e.g. thermal or toxic dose)

$k_1, k_2$ = equation constants related to the specific event

The form of the probability $P$ is given as:

$$P = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{Y-5} \exp\left(-\frac{1}{2}w^2\right) dw \tag{7.2}$$

Once the probit value has been calculated it is then possible to relate this to a fraction or percentage via tables, or a graph like the one shown in Figure 7-1 or a calculation such that

$$P = 0.5\left[1 + \frac{Y-5}{|Y-5|} erf\left(\frac{|Y-5|}{\sqrt{2}}\right)\right] \tag{7.3}$$

where *erf*(.) is the error function.

From this it can be seen that a probit value of 5 translates into a fraction of 0.5. This means that 50% of the receptors will suffer the specified level of damage.

As can be seen from the probit-fraction plot, the impact from a “dose” is highly nonlinear. A simple example is the exposure of people to solar radiation where some of the population are very sensitive to low doses whilst others are very tolerant to even high doses. Hence for a given dose the use of the probit function provides an estimate of the fraction of the exposed population affected for a specified level of intensity or dose.

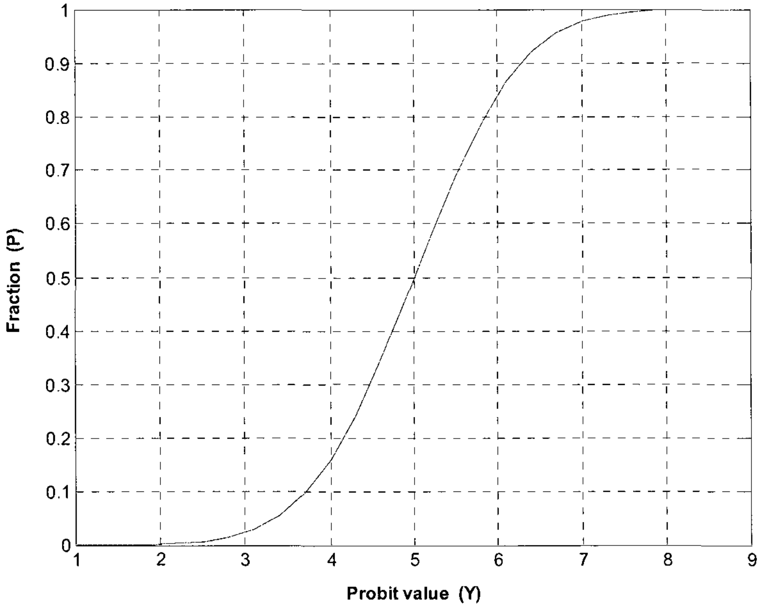


FIGURE 7-1 PROBIT VALUE VERSUS FRACTIONS

## 7.2 DOSE-RESPONSE MODELS FOR FIRES

Thermal radiation from fires and explosions causes a wide range of damage on people and structures. In this section impact on people is discussed whilst section 7.5 deals with structural impacts.

Table 7-1 gives an overview of general heat radiation impacts (Warren Centre 1986, Hymes et al. 1996).

TABLE 7-1 GENERAL EFFECTS OF THERMAL RADIATION

| Radiation Intensity (kW/m$^2$) | Impact |
|---|---|
| 1.2 | Received from sun in summer at noon |
| 1.6 | Minimum necessary to be felt as pain |
| 4.7 | Pain in 15-20 seconds, 2$^{nd}$ degree burns after 30 s. |
| 12.6 | 30% chance of fatality for continuous exposure<br>Minimum level to melt plastic tubing |
| 23.0 | 100% chance of fatality for continuous exposure<br>10% chance for instantaneous exposure |
| 35.0 | 25% chance of fatality for instantaneous exposure<br>Damage to process equipment |
| 60.0 | ~100% chance of fatality for instantaneous exposure |

Impacts rapidly worsen as both radiation intensity and exposure duration increase. This affects injury levels and probability of fatality. In terms of thermal radiation on people, the following impact levels are recognized (TNO 1992a, Hymes et al. 1996):

(i) First degree burns (limited to the epidermis or top layer of skin: ~0.12mm deep)
(ii) Second degree burns (penetration to the dermis or < 2mm deep)
(iii) Third degree burns (penetration into the subcutis, fat tissue)
(iv) Fatal burns

Of importance in assessing impact of thermal radiation is the wavelength. Impacts from nuclear explosions where wavelengths are in the UV-visible region (<400 nm) can be quite different from hydrocarbon fires where wavelengths are in the infra-red region (> 700 nm). This is because the higher wavelengths cause deeper skin penetration than the shorter wavelengths. Hence, the use of probit functions needs to be done carefully, recognizing the underlying assumptions and data.

Table 7-2 gives the probit equations developed by TNO in The Netherlands for impacts from hydrocarbon based fires.

**TABLE 7-2 PROBIT EQUATIONS – THERMAL RADIATION IMPACTS (TNO 1992)**

| Radiation ($t = s$, $q = W/m^2$) | | | |
|---|---|---|---|
| Fatality | $Y$ | $= -36.38 + 2.56 \ln (tq^{4/3})$ | (7.4) |
| 1st degree burns | $Y$ | $= -39.83 + 3.0186 \ln (tq^{4/3})$ | (7.5) |
| 2nd degree burns | $Y$ | $= -43.14 + 3.0186 \ln (tq^{4/3})$ | (7.6) |

Note that the intensity measure $V$ in equation (7.1) is given by $tq^{\frac{4}{3}}$. This represents a "dose" value.

Table 7-3 gives the commonly quoted fatality probit developed by Eisenberg (CCPS 2000). The data covered exposure times between 1.43 and 45.2 seconds, and incident heat fluxes between 10 and 586 kW/m$^2$.

**TABLE 7-3 PROBIT EQUATION - FATALITY IMPACT FROM RADIATION (CCPS 2000)**

| | | |
|---|---|---|
| Radiation | $t = s,\ q = \dfrac{W}{m^2}$ | |
| Fatality | $Y = -14.9 + 2.56 \ln \left( \dfrac{t.q^{\frac{4}{3}}}{10^4} \right)$ | (7.7) |

In both Table 7-2 and 7-3, the impacts do not normally consider the protective effects of clothing and hence they overpredict impacts where people are clothed. In the case where clothing ignites, it is often the case that 100% fatality is assumed.

Where the mitigating effect of clothing is considered, the percentage of exposed skin becomes important. This varies for the age group considered. For infants the exposed area is around 32% whilst for an adult it is around 20% (neck, head, arms and hands). Combined with the population distribution these assumptions reduce the impact to around 15% of the unprotected impact (TNO 1992a). The type of clothing and the attenuation of thermal radiation have not been discussed, and therefore, this level of reduction cannot be applied in all situations.

**EXAMPLE 7-1 FIRE RADIATION, LETHAL BURN**

Fire with 10 seconds exposure and heat flux of 45 kW/m$^2$.
Using probit equation (7.4) for fatality:

$$\begin{aligned} Y &= -36.38 + 2.56 \ln (\mathrm{t.q}^{4/3}) \\ &= -36.38 + 2.56 \ln(10 \times 45000^{4/3}) \\ Y &= 6.09 \end{aligned} \tag{7.8}$$

The probit-fraction relation gives an impact of 86% fatalities. If the effect of clothing is considered (impact reduced by a factor of 0.15) then fatalities drop to 13%. The Eisenberg probit, equation (7.7) gives a probit value of 4 and thus 16% fatalities compared with 86% from the TNO probit.

### 7.2.1 Variability in Probit Estimates

It is useful to compare the general predictions from various probit models for thermal impact on people. Figure 7-2 shows the probit value ($Y$) for a range of thermal loads and the subsequent predictions for the TNO and Eisenberg models. A significant difference exists and this is more clearly seen in Figure 7-3 which shows the fractional impact values ($P$) as a function of thermal load and probit model.

For a thermal dose value of $10^7$s (W/m$^2$)$^{4/3}$, the Eisenberg model predicts around 1% fatalities, whereas the TNO model gives around 45% fatalities. Clearly a significant difference to be considered, showing the difference in the underlying assumptions of the models.

Schubach (1995) gives a useful analysis of probit functions and shows that for long duration events, the Eisenberg probit produces extended effect distances and an overestimation of risk. He suggests that the exposure duration should be limited in applying these models.

The reduction of 85% in the fraction of fatality for the clothed skin compared to unprotected skin is considered optimistic. In risk analysis, when considering impact on vulnerable members of the population, it is better to make a conservative estimate by ignoring the protection offered by clothing.

### 7.2.2 Impact of Flash Fires on People

Flash fires due to combustion of a vapour cloud that has formed through dispersion of hydrocarbon vapour is a rapid event.

General consensus is that anyone within the cloud volume when ignition and fire occurs will be a fatality. This is a conservative assumption. Direct flame contact in these cases plus the ignition of clothing are key factors in determining the impact.

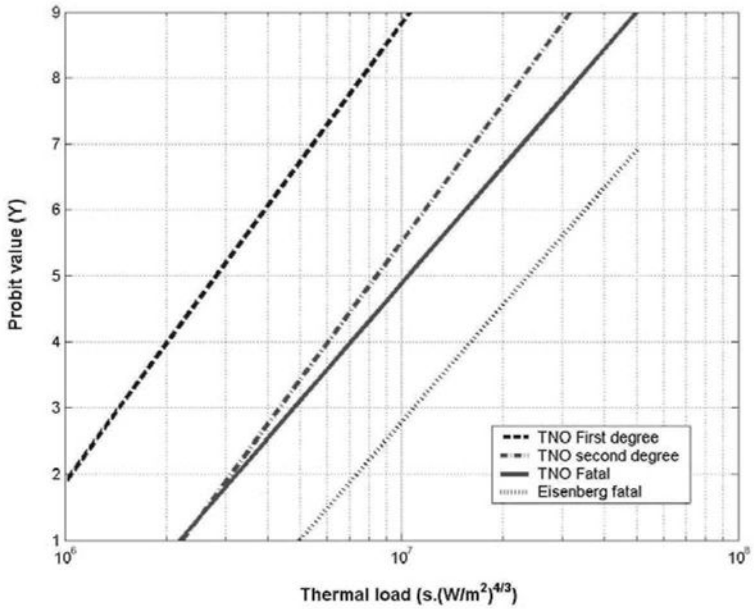


FIGURE 7-2 PROBIT VALUE VS. THERMAL LOAD FOR BURNS PROBITS

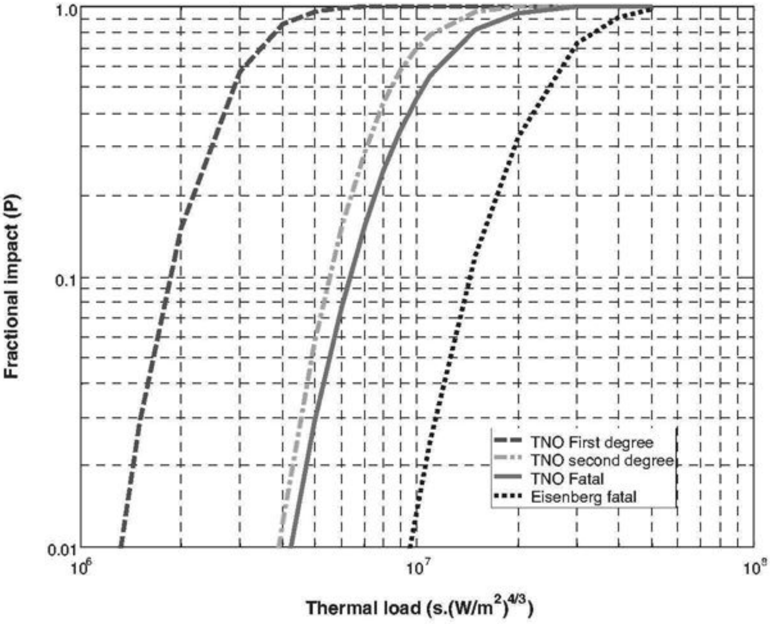


FIGURE 7-3 FRACTIONAL IMPACT VS. THERMAL LOAD FOR BURNS PROBITS

## 7.3 ESTIMATION OF EXPLOSION IMPACTS ON PEOPLE

In section 6.7.1 the characteristics of explosions and the effects from the blast wave were discussed. In particular, the peak overpressure and positive phase duration were key factors in the potential impact.

In considering the effects of blast on people there are many complexities that make predictions difficult. These include (HSE, 1998):

(i) Type of explosive and the quantity
(ii) Presence of reflecting surfaces that can magnify blast effects.
(iii) Location of explosion with respect to the targets of interest

and in certain cases,

(iv) The explosive device, its shape and primary fragments.

In terms of the potential impacts on people there are direct and indirect effects from the blast (TNO 1992a). These include:

(i) Direct effects: injury and death from pressure change that affects internal organs (lungs, gut etc.)
(ii) Indirect effects: include
  a) impact of fragments and debris generated by the blast
  b) bodily displacement causing impact of body parts (e.g. head) or whole body on nearby structures.
  c) building or structural collapse, in the case of people inside structures.

There are also the associated effects of heat radiation from the blast. The main direct and indirect impacts are:

(i) Rupture of eardrums
(ii) Lung damage (haemorrhage)
(iii) Head impact
(iv) Whole body displacement
(v) Impact from fragments and debris (non-cutting)
(vi) Glass fragments (cutting)

Table 7-4 gives typical blast effects related to a range of overpressures. Tables 7-5 and 7-6 give a range of probit functions that are applicable to these situations from several sources (TNO 1992a, Lees 2001). The references from Lees (2001) were originally developed by Eisenberg et al. (1975). Prugh (1999) gives a very useful coverage of blast effects on structures and personnel. However it must be stressed that many assumptions underlie these functions and data is often related to very specific circumstances. Hence, extreme caution is needed in applying them. As a first estimate of potential impact they can be useful. For further assessments it is advisable to refer to primary sources based on field data. Evenso, much of the literature is based on impacts from dense phase explosions, whereas most industrial accidents involve hydrocarbon based vapour cloud explosions (HSE, 1998) that have quite different pressure-time profiles and hence impact patterns.

TABLE 7-4 TYPICAL BLAST EFFECTS FROM EXPLOSION OVERPRESSURE

| Overpressure (kPa) | Effects |
|---|---|
| 0.3 | Loud noise |
| 1.0 | Threshold for breakage of glass |
| 4.0 | 90% window breakage. Damage to cladding. Minor structural damage. |
| 7.0 | Glass fragments fly with enough force to injure. Roof tiles removed. |
| 14.0 | Houses uninhabitable but not totally irreparable. Cement block buildings flattened. |
| 21.0 | Reinforced structures will distort. 20% chance of fatality inside a building |
| 35.0 | On-set of severe structural damage. House demolished. Large storage tanks could rupture. 15% chance of fatality outdoors, 50% chance indoors. |
| 70.0 | Almost complete demolition of all ordinary structures. Almost 100% chance of fatality indoors. |

In many cases an approximation of the pressure-time profile to a triangular shape is made, as seen in Figure 7-4. Here $P_o$ is atmospheric pressure; $P_s$ is the peak-overpressure and $t_p$ is the positive phase duration.

The pressure impulse $i$ is then approximated as:

$$i \cong \frac{P_s \cdot t_p}{2} \tag{7.9}$$

which represents the area under the pressure-time profile above atmospheric pressure $P_o$.

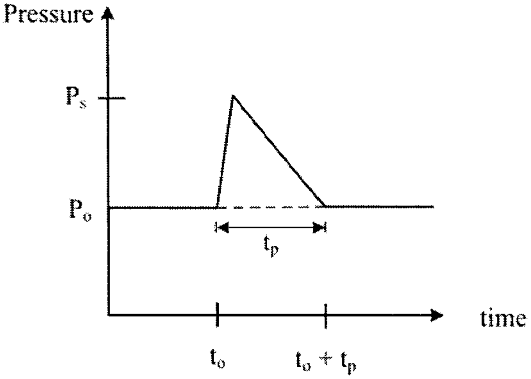


FIGURE 7-4 EXPLOSION PRESSURE-TIME PROFILE APPROXIMATION

TABLE 7-5 PROBIT EQUATIONS - BLAST IMPACTS (TNO 1992A, LEES 2001)

| | | | | |
|---|---|---|---|---|
| 1. | Eardrum damage: | $Y=-12.6+1.524\ln P_s$ | (TNO) | (7.10) |
| | | $Y=-15.6+1.93\ln P_s$ | (Lees) | (7.11) |
| | | where $P_s$ = peak overpressure (Pa) | | |
| 2. | Lung damage and death: | $Y=-77.1+6.91\ln P_s$ | (Lees) | (7.12) |
| | | $Y=5-5.74\ln S_1$ | (TNO) | (7.13) |
| | | where<br>$S_1=\frac{4.2}{\overline{P}}+\frac{1.3}{\overline{i}}$<br>$\overline{P}=\frac{P}{P_o}$ ; $\overline{i}=\frac{i}{P_o^{\frac{1}{2}}\cdot m^{\frac{1}{3}}}$<br>$P$ = actual overpressure on person depending on orientation<br>$P_o$ = atmospheric pressure $(Pa)$<br>$i$ = impulse $\left(\sim\frac{Pt_p}{2}\right)$<br>$t_p$ = positive phase duration (s)<br>$m$ = body mass (kg) | | |
| 3. | Head impact: | $Y=5-8.49\ln S_2$ | (TNO) | (7.14) |
| | | where<br>$S_2=\frac{2.43\times10^3}{P_s}+\frac{4\times10^8}{P_s\cdot i_s}$ | | |
| 4. | Whole body displacement: | $Y=5-2.44\ln S_3$ | (TNO) | (7.15) |
| | | where<br>$S_3=\frac{7.28\times10^3}{P_S}+\frac{1.3\times10^9}{P_S\cdot i_S}$<br>$P_s<9\times10^5 Pa$ | | |

TABLE 7-6 PROBIT EQUATIONS - BLAST FRAGMENTS/DEBRIS

| | | | | |
|---|---|---|---|---|
| 1. | Debris: | $Y=-13.19+10.54\ln V_o$ | (TNO) | (7.16) |
| | | where $V_o$ = velocity of fragment (m/s)<br>$m$ = mass of fragment (kg) > 4.5 kg | | |
| | | $0.1<\text{m}<4.5$ $Y=-17.56+5.30\ln S_4$ | (TNO) | (7.17) |
| | | where<br>$S_4=\frac{1}{2}mV_o^2$ | | |
| | | $0.001<\text{m}<0.1$ $Y=-29.15+2.10\ln S_5$ | (TNO) | (7.18) |
| | | where<br>$S_5=mV_o^{5.115}$ | | |

**EXAMPLE 7-2 EARDRUM RUPTURE FROM EXPLOSION**

Using the probit equation:

$$Y = -12.6 + 1.524\ln(P_s) \tag{7.19}$$

where $P_s$ is the peak overpressure (Pascals), the following fractional responses are seen from the variation in overpressure.

| Percentage Affected | Probit | Peak Overpressure (Pa) |
|---|---|---|
| 1 | 2.67 | 21500 |
| 10 | 3.72 | 42800 |
| 50 | 5.00 | 103800 |
| 90 | 6.28 | 240400 |

ref: TNO (1992a).

**EXAMPLE 7-3 BLAST FRAGMENT IMPACT**

A small fragment of 0.1 kg from the rupture of a pressure vessel impacts on a person some 60 metres from the event. The velocity of the fragment is estimated at 40 m/s.

Using equation (7.17) the value $S_4 = \frac{1}{2}(0.1)(40^2) = 80$

and the probit value
$$Y = -17.56 + 5.30\ln(80)$$
$$Y = 5.66$$

Hence the probability of fatality is approximately 70%.

## 7.4 DOSE-RESPONSE MODELS FOR TOXIC SUBSTANCES

### 7.4.1 Toxic Exposure Effects

The area of toxicology is complex and highly specialised. Most data on the toxic effects of substances are derived from animal experiments and then extrapolated or scaled to the human population. Some data exists for human exposure to certain substances such as chlorine and ammonia. These arise from actual incidents that were documented or from effects observed during times of war when certain agents were used as chemical weapons.

In general there are several observable effects and these depend on the chemical nature of the substance and its interaction with the body. Table 7-7 sets out the major exposure effects from irritation to asphyxiation and systemic damage.

**TABLE 7-7 TOXIC EXPOSURE EFFECTS**

IRRITATION

- respiration ($Cl_2$, $SO_2$, $NH_3$)
- skin
- eyes

NARCOSIS (hydrocarbons)

ASPHYXIATION

- simple ($N_2$, He)
- chemical (CO, HCN)

SYSTEMIC DAMAGE

Effects are often addressed through the use of limiting values of the substance's concentration for assumed exposure periods. In most cases these are applicable to occupational situations and not directly applicable to acute, accidental releases of materials. Such measures include:

a) Threshold limit values (TLV)
b) Short Term Exposure Limit (STEL)
c) Immediately dangerous to life or health (IDLH)
d) Permissible exposure limits (PEL): A maximum amount of concentration of a chemical that a worker can be exposed to under US-OSHA rules.

The above measures have limited application in most acute event situations. Definitions of the terms are given Section 5.2.2.3 in Chapter 5.

An approach originating in the USA that has been used for land-use planning issues relies on Emergency Response Planning Guidelines (ERPGs) that set three levels of possible exposure that relate to increasing effects on individuals in a community exposed to various substances. These include:

ERPG-1 level: maximum gas concentration for 1 hour exposure where only mild transient effects such as objectionable odour can be experience by most individuals.

ERPG-2 level: maximum gas concentration for 1 hour with no irreversible health effects or symptoms.

ERPG-3 level: maximum gas concentration for 1 hour not causing life threatening health impacts for nearly all individuals.

In some cases, the ERPG levels have been applied to risk based land-use planning guidelines to provide criteria for injury levels from toxic exposure from hazardous industry developments (DIPNR, 2003).

Some values of ERPG levels are given in Table 7-8 for selected substances. The complete listing is available from the American Industrial Hygiene Association (AIHA 2004). They are updated every 5 years and there are currently about 100 substances listed.

TABLE 7-8 ERPG LEVELS FOR SELECTED SUBSTANCES (PPM)

| Substance | ERPG-1 | ERPG-2 | ERPG-3 |
|---|---|---|---|
| ammonia | 25 | 150 | 750 |
| benzene | 50 | 150 | 1000 |
| chlorine | 1 | 3 | 20 |
| hydrogen sulphide | 0.1 | 30 | 100 |
| methyl isocyanate | 0.025 | 0.5 | 5 |
| nitrogen dioxide | 1 | 15 | 30 |
| sulphur dioxide | 0.3 | 3 | 15 |
| vinyl acetate | 5 | 75 | 500 |

Of primary use are probit relations that permit a wider range of acute impacts to be assessed. The following section deals with those dose-response representations.

In an important comparison of probit expressions for toxic exposure, Schubach (1995) points out the significant difference between the CCPS and TNO (1992) relations. He suggests that the TNO values are preferred because they recognize species differences in inhalation rates and sites of damage. Specific human data is always to be preferred over extrapolations and manipulations of animal toxicological data. However specific data only exists for certain substances such as chlorine and ammonia due to their past use in chemical warfare.

### 7.4.2 Vulnerability Models

Impact from exposure to toxic gases is commonly handled through the use of specific probit equations. Some are based on actual human exposure to the substance, many are extrapolated from animal testing. A number of sources quote specific probit relations including the US Coast Guard (1980), Director-General of Labour, The Netherlands (TNO 1992a) and the World Bank (1988). Other specific studies on chemicals such as chlorine and ammonia are available (Withers and Lees 1985a, 1985b, MHAP, 1987, 1988).

The key factors in assessing impact include:

(i) Exposed concentration and time of exposure
(ii) Whether the exposure is transient or sustained
(iii) The breathing rate of the individual
(iv) Opportunities of shelter indoors or escape from the toxic cloud

Table 7-9 gives a selected summary of currently available probit equations for a number of important substances indicating some alternatives. These are drawn from US Coast Guard data and from the Director-General of Labour, The Netherlands. In the case of The Netherlands, alternate probits based on extrapolation of $LC_{50}$ values were used (TNO 1992a).

### TABLE 7-9 PROBIT EQUATIONS - TOXIC EXPOSURE

The general form is: $Y = k_1 + k_2 \cdot \ln(tC^n)^*$

| Chemical | $k_1$ | $k_2$ | n |
|---|---|---|---|
| acrolein | -9.931 | 2.049 | 1 |
| ammonia | -35.9 | 1.85 | 2 |
| | -15.8 | 1.00 | 2 (TNO) |
| bromine | -9.04 | 0.92 | 2 |
| | -12.4 | 1.00 | 2 (TNO) |
| carbon monoxide | -37.98 | 3.7 | 1 |
| | -7.4 | 1.00 | 1 (TNO) |
| chlorine | -8.29 | 0.92 | 2 |
| | -14.3 | 1.00 | 2.3 (TNO) |
| hydrogen cyanide | -29.42 | 3.008 | 1.43 |
| | -9.8 | 1.00 | 2.4 (TNO) |
| hydrogen sulphide | -31.42 | 3.008 | 1.43 |
| | -11.5 | 1.00 | 1.9 (TNO) |
| nitrogen dioxide | -13.79 | 1.4 | 2 |
| | -18.6 | 1.00 | 3.7 (TNO) |
| phosgene | -19.27 | 3.686 | 1 |
| | -0.8 | 1.00 | 0.9 (TNO) |
| sulphur dioxide | -15.67 | 2.10 | 1 |
| | -19.2 | 1.00 | 2.4 (TNO) |

* In the case of TNO relations C = mg/m$^3$ otherwise C = ppm and t = minutes.

### EXAMPLE 7-4 PREDICTED IMPACTS FROM HF RELEASES

Hydrogen fluoride (HF) is commonly used in petroleum refinery alkylation units. Escape of HF and its subsequent dispersion is an important risk issue for nearby communities.

There exist several probit relations for HF impacts (HSE 1995). These include:

ten Berge (1986) $$Y_{tb} = -7.35 + 0.71\ln(C^2 t) \tag{7.20}$$

Rausch (1977) $$Y_r = -25.8689 + 3.3545\ln(\hat{C}t) \tag{7.21}$$

de Weger (1991) $$Y_{dw} = -8.4 + \ln(C^{1.5}t) \tag{7.22}$$

Mudan (1989) $$Y_m = -48.33 + 4.853\ln(\hat{C}t) \tag{7.23}$$

where $t$ = minutes exposure
$C$ = mg/m$^3$
$\hat{C}$ = ppm

Figure 7-5 shows the comparative predictions of the probit relations for 15 minutes exposure to HF gas. It is clear that there is a significant spread in predictions of fatality. At a gas concentration of 1000 ppm the fatality predictions range from 90% (Rausch) to 0% (Mudan) with the other probits in the 20 to 30%

fatality range. This variance reflects the differences in some of the underlying data, mainly animal experiments, and the subsequent scaling treatment of that data for use in human dose-response predictions.

The probit relationship developed by Mudan (1989) is widely used for longer duration exposures (30 to 60 minutes often quoted), where the c-t relationship is linear (HSE 1995, Lees 2001). This linear relationship has been used by the HSE (1993) to derive a Dangerous Toxic Load (DTL). A value of 2400 ppm is listed for a 5 minute exposure. DTL does not represent a lethal concentration, but could reflect serious injury requiring prolonged medical treatment.

What is clear is that significant variations can occur in vulnerability analyses and these variations must be addressed in the decision making process. It also emphasizes that the underlying assumptions of the probit functions should be clearly understood and the expressions not used blindly.

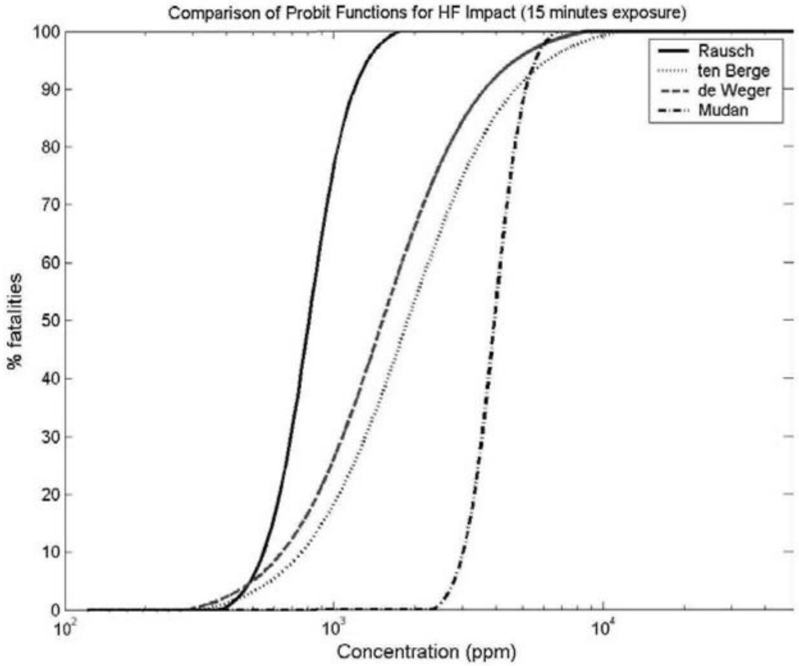


FIGURE 7-5 PROBIT COMPARISONS FOR HF EXPOSURE

### 7.4.3 Eco-system Impacts

Eco-system impacts require knowledge of:

(i) The receptor type (fish species, bird, animal, ...)
(ii) The uptake rate to determine the dose
(iii) The chemical of concern (COC)
(iv) The ecological endpoint being considered, such as mortality.

As shown in Figure 5-7, the environmental risk assessment framework can be extremely complex with many pathways for the COC to impact the ecological receptor.

In assessing impact on the receptor it is typical to use toxicity data such as that found in the ECOTOX database (USEPA, //www.epa.gov/ecotox/) or from the Registry of Toxic Effects of Chemical Substances (RTECS). Data from these sources are presented using various measures including:

Acute toxicity measures:

$LD_{LO}$, $LD_{min}$ : the lowest dose of a substance that may cause death under defined conditions. Typically in mg/kg of body weight.

$LD_{50}$ : lethal dose to 50 percent of a population

$LC_{50}$ : lethal concentration in an environmental medium to 50 percent of a population following a certain period of exposure. Typically expressed as mg/L for aquatic toxicity and $mg/m^3$ for inhalation toxicity.

In the case of lethal dose, it is important to recognize the routes of exposure. These can be via dermal (skin) or oral routes. In the case of lethal concentrations the exposure time needs to be considered as well as the uptake rate into the species.

Other important measures include:

NOEC : No observed effect concentration, which is the concentration that causes no observable effects on the organism, or

NOAEL/NOEL : No observed (adverse) effect level.

Chronic toxicity measures:

In these cases, where exposure occurs over long time scales there are no simple LC or LD measures available. Specialised studies, data and models are necessary to assess chronic impacts. Short-term testing protocols can provide some estimates of chronic toxicity (USEPA 2002).

Other important sources of toxicological information are to be found in:

TOXNET (//toxnet.nlm.nih.gov/ ) which includes

- IRIS: Integrated Risk Information System
- HSDB: Hazardous Substances Database
- GENE-TOX: Genetic Toxicology (Mutagenicity)
- ITER: International Toxicity Estimates for Risk

European Chemicals Bureau (//ecb.jrc.it/ )

Ecological impacts can be complex to assess and especially to quantify. The use of predictive models and toxicity data must be used carefully and cautiously. Expert assistance is normally required to provide credible analyses.

## 7.5 STRUCTURAL RESPONSE TO FIRES

Section 7.2 discussed the response of humans to heat radiation. This section considers the effects of heat radiation on structures. This is often an important aspect in domino effects where thermal impacts from an event lead to further system failures and propagation. This was the case in Mexico City in 1984 when the Pemex LPG facility was completely destroyed.

There are several important aspects that need to be considered, including:

(i) Direct flame impingement on vessels and structures and its impact.
(ii) Radiant impact on vessels and structures from nearby flames.

### 7.5.1 Direct Flame Impingement or Engulfment

In the case where a jet fire directly impinges on a structure or vessel, localised heating will take place and if no action is taken then structural failure will eventually occur. This will be determined by the state of the vessel contents, the location of the impingement (vapour or liquid space), the structural design as well as the emergency response taking place, e.g. water sprays or deluge systems.

Jet flame temperatures are typically in the range of 1300°C to over 1500°C depending on the degree of turbulent mixing. Failure of steel is dependent on the load or stress it carries but temperatures in the vicinity of 400°C to 600°C can precipitate structural failure. On unprotected structural steel or a pressure vessel shell, the time to the failure temperature can be less than a few minutes. Complex heat transfer calculations are required in order to assess the specific situation. Field studies of LPG vessels subject to propane and butane jet fires show that hot spots of over 500°C can occur on vessels even with conventional deluge systems (HSE 2000). These temperatures take in the order of 10 minutes to achieve.

Engulfment of vessels or tanks by pool fires is covered in many codes of practice that deal with vessel pressure relief or venting (AS1940 1993; AS1210 1997). Heat absorption is expressed in terms of a "wetted" area of flame and a correlation constant, typically as:

$$Q = cA^n \tag{7.24}$$

where Q = heat absorbed (kW)
A = area ($m^2$)
n = index
c = constant

Various standards such as API RP520, API Std 2000 for storage tanks recommend the use of estimates similar to equation (7.24). Engulfing fire heat fluxes of 150kW/$m^2$ are typical of these situations (Lees 2001). What is of importance here is the use of dynamic models that capture the heat transfer mechanisms in order to predict time-varying temperatures and pressures in the system.

### 7.5.2 Structural Response by Heatup Modelling

Heatup modelling is a useful tool for predicting the temperature-time history of structures subject to pool fire engulfment and jet fire impingement. The main uses are:

- Determination of the extent of passive fire protection (PFP) requirements for steel columns supporting pipe bridges in process plants, if there is a potential for pool fire engulfment.
- Determination of PFP requirements for primary steel supporting the equipment and modules in offshore structures.
- Estimation of time to failure of vessels containing volatile hydrocarbon inventory (time to BLEVE), with and without depressuring, and with and without deluge protection. The results provide optimum depressuring rates to prevent BLEVE, estimate PFP requirements, and emergency response planning to protect emergency crew.

Exposure of a vessel to external fire engulfment or impingement involves interaction between the physical components of the system (Hunt and Ramskill 1985, Davenport et al 1992). Specific parameters are:

- Fire characteristics (flame size, surface emissive power, area of engulfment, flame temperature)
- Vessel structure (dimensions, wall thickness)
- Vessel contents (physical and thermodynamic properties of the liquid and vapour, and the vessel fill level)
- Vessel vents (pressure safety valve (PSV) and capacity)
- Process flows in and out of the vessel
- The surroundings (ambient conditions, attenuation of thermal radiation by fixed water sprays).

A set of heat and mass balance equations need to be setup involving the following:

- Heat input to vessel by radiation and convection (liquid and vapour parts have to be separately modelled)
- Heat conduction from heated side of vessel wall to unheated side
- Heat absorbed by vapour and liquid in the vessel (in many instances, boiling heat transfer in the case of liquid)
- Heat losses from reflected radiation and convection to ambient air
- Thermodynamic equilibrium between the vapour and liquid phases within the vessel (complicated for mixtures)
- Heat and mass loss through PSV discharge as pressure rises from heatup (generally this is modelled as a intermittent discharge with reseating of the PSV, referred to as "chattering")

A number of temperature nodes may be selected, and constitutive equations developed. These have to be numerically integrated for each time step, with physical and thermodynamic properties calculated at the vapour and liquid temperature corresponding to temperatures at that time step. The longitudinal and hoop stresses are calculated, along with the reduction in the ultimate tensile strength with rising temperature. The computations are quite complex, especially maintaining the mathematical constraint of thermodynamic equilibrium within the vessel. Obviously, for load bearing structures, the heatup calculations are simpler.

In order to obtain more accurate estimates, it is necessary to interface the heatup calculations with a dynamic finite element model, where the stress distribution is calculated at each time step, using the existing temperature at that time. No commercial software is currently available.

A number of heatup modelling studies and experiments have been carried out on fire engulfment of vessels storing flammable inventory. Many of these studies have originated from offshore oil and gas industry, where there is no luxury of separation distance and the level of congestion, and hence fire engulfment potential, is high (Davenport et al 1992; Steel Construction Institute, 1992a; Roberts et al. 2000). Other studies focus on vessels containing liquefied flammable gas (LPG) subject to external flames (Moodie 1985; Moodie et al. 1985, 1988; Benyon, 1988; Birk 1988; Dancer and Sallett 1990; Venart 2000). None of the existing models for predicting the response of LPG vessels exposed to fire are ideal, but have been validated against experiments with small vessels.

There have also been experiments on the effectiveness of fixed water spray in attenuating fire impact and prevention of escalation (Schoen and Droste 1988; Gosse and Alderman 2001; Roberts et al. 2001).

The findings from various studies are summarised below:

1. The convective heat transfer coefficient from tank wall to liquid is greater than the corresponding value for vapour in the nucleate boiling regime, causing the vapour side wall temperature to rise faster than the temperature of a surface in contact with liquid.
2. For a vessel subjected to external flame impingement, the time taken for the initial discharge through the PSV is a function of the vessel inventory. The higher the level, the sooner the discharge occurs, as the vapour space available is smaller and therefore the pressure rise from thermal expansion is faster.
3. A two-step failure mechanism for vessel failure has been postulated – plastic deformation leading to an initial crack, following by a shear fracture. Time of failure is difficult to predict, but wall temperatures of 500–550°C have been suggested.
4. For process vessels containing LPG, which generally tend to contain less than 10 tonnes in inventory, the failure time is between 3 and 10 minutes, depending on the size of vessel.
5. Water spray cooling is effective against pool fires, as the radiative heat flux can be reduced by 55% for design water spray density of 10 L/min/m$^2$.
6. Conventional water spray of 10 L/min/m$^2$ applied from the top of the vessel, using standards such as NFPA 15 (1996), is ineffective against a jet fire attack, where most of the heat transfer is through convection

rather than radiation. Further, the water film breaks down in the region of blocked nozzles.

7. Higher water deluge density (2 to 3 times conventional value), directed specifically at the fire impingement area, would protect the vessel. However, the water spray quantity must be assessed as quantity actually applied to the surface rather than nozzle discharge rate, as the application is not uniform.
8. Passive fire protection (PFP) for jet fire attacks has been developed (Steel Construction Institute 1992a,b). The data suggest that an adequate PFP system can reduce the heat transfer to the vessel by a factor of 10 (HSE 1998).
9. Emergency depressuring of the target inventory to flare extends failure time, and may prevent failure in some instances. In general, a depressuring system designed to API 521 (1997) has been shown to be inadequate to prevent a BLEVE, even with fixed water sprays designed to NFPA 15 (1996). Larger depressuring rates would be required to protect against vessel failures (Institute of Petroleum 2003).
10. For atmospheric storage tanks designed with separation distances specified by NFPA 30 (2000), in the case of tank surface fires and bund fires, the flame drag and flame tilt may result in event escalation even at moderate wind speeds.
11. For an atmospheric storage tank designed to API 650 (1998) and engulfed by a bund fire, the time for vapour generated to exceed the vent capacity varies from 15 to 30 minutes. External cooling increases the failure time by 10 minutes. This means that the external fire from a leak could escalate to a tank surface fire unless a foam blanket system is used within that time.

The above summary indicates that, unless emergency action is effective within the first 5 minutes for a small pressure vessel containing LPG, or within 15 minutes for an atmospheric storage tank, the potential for escalation is high.

### 7.5.3 Radiant Heat Impact

In the case of nearby, non-engulfing fires, radiant heat is the mechanism of concern. These situations can be treated using view-factor methods as outlined in section 6.1.4.3. Care needs to be taken to obtain good estimates of flame shape and surface emissivity. View factor estimates need to be accurate.

In the case of steel 'I' beams, note that for a critical temperature of 500°C and an incident heat flux of 100 kW/m$^2$, the 90% failure limit is reached after 20 minutes for beams where the heat discharge area of the beam is 4 times the heat incident area. Where this ratio decreases, times to failure 'rapidly decrease TNO (1992a).

## 7.6 STRUCTURAL RESPONSE TO EXPLOSIONS

Buildings, tanks, vessels and other structures can sustain significant damage due to explosion overpressures and impulses. In turn, this can also lead to human injury and fatality. This area of vulnerability analysis is well studied and is complex by virtue of the blast wave interactions with other nearby structures as well as the many variations in the shockwave or pressure wave profiles.

The key concepts are given in Table 7-10 which outlines issues for consideration in analysing explosion responses.

### TABLE 7-10 PRINCIPAL FACTORS IN STRUCTURAL RESPONSE TO EXPLOSIONS

- Blast wave time characteristics: shock and pressure waves
- Blast interaction with structure: diffraction and reflection
- Air displacement: explosion wind and dynamic pressure
- Natural frequency of vibration for structure
- Pressure-impulse characteristics
- Structural materials: brick, steel, wood, concrete structures

Excellent discussions on structural responses to explosions are available from many sources. Useful summary references are given by TNO (1992a), Lees (2001) and CCPS (2001).

A number of useful probit functions have been developed to predict a range of structural responses to explosions. These are given in Table 7-11. These are sometimes based on scarce data and are often related to specific building types. So, again care needs to be exercised in their application. This is the key message of recent explosion and vulnerability reviews (HSE 2000).

### TABLE 7-11 PROBIT EQUATIONS - EXPLOSION (TNO, 1992A)

| Explosion | Buildings up to 4 storeys | |
|---|---|---|
| Minor damage: | $Y = 5 - 0.26 \ln V$ | (7.25) |
| | $V = \left(\dfrac{4600}{P_s}\right)^{3.9} + \left(\dfrac{110}{i_s}\right)^{5.0}$ | (7.26) |
| where: | | |
| $P_s$ | = overpressure (Pa) | |
| $i_s$ | = impulse (½ $P_s t_p$) | |
| $t_p$ | = positive phase duration (s) | |
| Major structural damage: | | |
| | $Y = 5 - 0.26 \ln V$ | (7.27) |
| | $V = \left(\dfrac{17500}{P_s}\right)^{8.4} + \left(\dfrac{290}{i_s}\right)^{9.3}$ | (7.28) |
| Collapse: | $Y = 5 - 0.22 \ln V$ | (7.29) |
| | $V = \left(\dfrac{40000}{P_s}\right)^{7.4} + \left(\dfrac{460}{i_s}\right)^{11.3}$ | (7.30) |
| Glass breakage: | $Y = -11.97 + 2.12 \ln P_s$ (single pane, older buildings) | (7.31) |
| | $Y = -16.58 + 2.53 \ln P_s$ (double glazed, newer buildings) | (7.32) |

It should be noted that the damage levels refer to work by Jarrett (1968) in the UK and are for brick constructions where:

a) minor damage: refers to window breakage, door displacement and roof damage.
b) major damage: refers to wall cracks, and collapse of some walls
c) collapse: refers to a total collapse of the building.

Prugh (1999) provides a summary of blast impacts through useful charts for a range of damage to industrial structures such as tall columns, reinforced masonry and concrete structures.

## 7.7 REVIEW

This chapter has presented the basic links between the predictions from effect models and estimation of impact impacts on vulnerable receptors. The chapter has focused on safety related vulnerabilities. There is a significant body of literature dealing with environmental impacts that requires specialized toxicological knowledge.

The techniques for vulnerability analysis rely heavily on field data. In some cases the field data is specific to certain building types or in the case of toxic effects relies on extrapolated or scaled data from animal experiments to predict human impacts. The chapter makes clear that the analyst needs to be aware of the underlying assumptions in the predictive models, and the breadth of data used in their development. Where possible reliable field data is always to be preferred over extrapolated data. The message is: "User beware"!

## 7.8 REFERENCES

American Industrial Hygiene Association (AIHA) 2004, Available at: http://www.aiha.org/.

American Petroleum Institute. *Guide for Pressure Relieving and Depressuring Systems*, 4th edn, American Petroleum Institute, Washington D.C. API 521: 1997.

American Petroleum Institute. *Welded Steel Tanks for Oil Storage*, 10th edn, American Petroleum Institute, Washington D.C. API 650:1998

Beynon, G.V., Cowley, L.T., Small, L.M. and Williams, I. 1998, 'Fire Engulfment of LPG Tanks: HEATUP, a Predictive Model', *Journal of Hazardous Materials*, vol. 20, pp.227-238.

Birk, A.M. 1988, 'Modelling the Response of Tankers Exposed to External Fire Impingement' *Journal of Hazardous Materials*, vol. 20, pp.197-225.

Dancer, D. and Sallet, D.W. 1990, 'Pressure and Temperature Response of Liquefied Gases in Containers and Pressure Vessels which are Subjected to Accidental Heat Input', *Journal of Hazardous Materials*, vol. 25, pp.3-18.

Davenport, J.N., Richardson, S.M. and Saville, G. 1992, *Thermal Response of Vessels and Pipework Exposed to Fire*, Prepared by Steel Construction Institute for Health & Safety Executive – Offshore Technology Information, OTI 92 610, HMSO, London.

CCPS 2000, *Guidelines for Chemical Process Quantitative Risk Analysis*, 2nd edn, Centre for Chemical Process Safety, AIChE, New York.

de Weger, D., Pietersen, C.M. and Reuzel, P.G. 1991, 'Consequences of exposure to toxic gases following industrial disasters', *Journal of Loss Prevention in the Process Industries*, vol. 4, pp. 272-276.

DIPNR 2003, *Hazardous Industry Planning Advisory Paper No 4: Risk Criteria for Land-use Safety Planning*, NSW Government Bookshop, Sydney, Australia.

Eisenberg, N.A., Lynch, C.J. and Breeding, R.J. 1975, *Vulnerability Model: A simulation system for Assessing Damage Resulting from Marine Spills*, Report CG-D-136-75, Enviro Control Inc., MD., USA.

Gosse, A.J. and Alderman, J. 2001, 'The Effectiveness of Water Deluge Systems in Mitigating Offshore Fires', *35th Loss Prevention Symposium*, American Institute of Chemical Engineers, Houston, Texas, Paper LPS-1a.

HSE 1993, *Toxicology of Substances in Relation to Major Hazards: Hydrogen Fluoride*, Health & Safety Executive, UK.

HSE 1995, *A Review of the Manufacture, Uses, Incidents and Hazard Models for Hydrogen Fluoride*, HSE Contract Research Report No. 79/1995 by WS Atkins Consultants Ltd, Health & Safety Executive, UK.

HSE 1998, *Review of Blast Injury Data and Models*, Research Report 192/1998, Health & Safety Executive, UK, ISBN 0717616177.

HSE 1998, *Review of Test data on the Performance of PFP Materials in Jet Fires*, Offshore Technology report – OTO 97 078, Health & Safety Executive, UK.

HSE 2000, *Efficacy of water spray protection against butane jet fires impinging on liquefied petroleum gas (LPG) storage tanks*, Res. Report 298/2000, HSE, HMSO, Norwich, UK.

Hunt, D.L.M. and Ramskill, P.K. 1985, 'The Behaviour of Tanks Engulfed in Fire - The Development of a Computer Program', *Institution of Chemical Engineers Symposium Series No. 93*, Assessment and control of major hazards, pp. 71-86.

Hymes, I, Boydell, W. and Prescott, B. 1996, *Major Hazards Monograph: Thermal Radiation: Physiological and Pathological Effects*, IChemE, Rugby, UK.

Institute of Petroleum UK 2003, *Guidelines for the Design and Protection of Pressure Systems to Withstand Severe Fires*, March.

Jarrett, D.E. 1968, 'Derivation of the British explosives safety distances', *Annals of the N.Y. Academy of Sciences*, vol. 152, pp. 18.

Lees, F.P. 2001, *Loss Prevention in the Process Industries*, Butterworths-Heinemann.

MHAP 1987, *Chlorine Toxicity Monograph*, Major Hazards Assessment Panel, IChemE., Rugby, UK.

MHAP 1988, *Ammonia Toxicity Monograph*, Major Hazards Assessment Panel, IChemE., Rugby, UK.

Moodie, K. 1988, 'Experiments and Modelling-An Overview with Particular Reference to Fire Engulfment', *Journal of Hazardous Materials*, vol. 20, pp.149-175.

Moodie, K., Billinge, K. and Cutler, D.P. 1985, 'The Fire Engulfment of LPG Storage Tanks', *Institution of Chemical Engineers Symposium Series No. 93*, Assessment and control of major hazards, UMIST, pp. 87-106.

Moodie, K., Cowley, L.T., Denny, R.B., Small, L.M. and Williams, I. 1988, 'Fire Engulfment Tests on a 5 Tonne LPG Tank', *Journal of Hazardous Materials*, vol. 20, pp. 55-71.

Mudan, K. 1989, 'Use of toxicity data in quantitative risk assessment of HF Alkylation Units', *American Institute of Chemical Engineers Summer National Meeting*, August.

National Fire Protection Association. *Standard for Water Spray Fixed Systems for Fire Protection*, National Fire Protection Association, Quincy, Massachusetts, USA. NFPA 15:2001.

National Fire Protection Association. *Flammable and Combustible Liquid Code*, National Fire Protection Association, Quincy, Massachusetts, USA. NFPA30:2000.

Prugh, R.W. 1999, 'The Effects of Explosive blast on Structures and Personnel', *Process Safety Progress*, vol. 18, no. 1, pp. 5-16.

Roberts, T., Buckland, I. and Beckett, H. 2001, 'Directed Water Deluge Protection of Liquefied Petroleum Gas Vessels', Hazards XVI, *Institution of Chemical Engineers Symposium Series No 148*, pp. 193-212.

Roberts, T.A., Medonos, S. and Shirvill, L.C. 2000, *Review of Response of Pressurised Process Vessels and equipment to Fire Attack*, Offshore Technology Report – OTO 2000 051, UK Health & Safety Executive, June.

Rausch, A.H., Tsao, C.K. and Rowley, R.M. 1977, *Third-stage development of the vulnerability model, A simulation system for assessing damage from marine spills*, US Coast Guard Report No. CG-D-5-78.

Schubach, S. 1995, 'Thermal Radiation Targets used in Risk Analysis', *Transactions of Institution of Chemical Engineers*, vol. 73, Part B, pp. 265-270.

Schubach, S. 1995, 'Comparison of probit expressions for the prediction of lethality due to toxic exposure', *Journal of Loss Prevention in the Process Industries*, vol. 8, no. 4, pp. 197-204.

Standards Australia. *The Storage and Handling of Flammable and Combustible Liquids*, Standards Australia. AS1940:1993.

Standards Australia. *Pressure vessels*, Standards Australia, ISBN 0733710123. AS1210: 1997.

Schoen, W. and Droste, B. 1988, 'Investigations of Water Spraying Systems for LPG Storage Tanks by Full Scale Fire Tests', *Journal of Hazardous Materials*, vol. 20, pp. 73-82.

Steel Construction Institute 1992a, *Experimental Data Relating to the Performance of Steel Components at Elevated Temperatures*, Prepared for the Health and Safety Executive – Offshore Technology Information, OTI 92 604, HMSO, London.

Steel Construction Institute 1992b, *Passive Fire Protection: Performance Requirements and Test Methods*, Prepared for the Health and Safety Executive – Offshore Technology Information, OTI 92 606, HMSO, London.

ten Berge, W.F. 1986, 'Concentration-time mortality response relationship of irritant and systemically acting vapours and gases', *Journal of Hazardous Materials*, vol. 13, pp. 301-309.

TNO 1992a, *Methods for the determination of possible damage*, CPR16E, Director General of Labour, The Netherlands, ISBN 90-5307-052-4.

TNO 1992b, *Methods for the Calculation of Physical Effect*, CPR 14E, Director-General of Labour, Voorburg, The Netherlands.

USEPA 2002, *Short-term methods for estimating the chronic toxicity of effluents and receiving waters to freshwater organisms*, US-Environmental Protection

Agency, Office of Water, 4th edition, EPA-821-R02-013, October, Washington DC.

USCG 1980, *Study to Modify the Vulnerability Model of the Risk Management System*, Report CG-D-22-80, Washington DC, US Department of Transportation.

Venart, J.E.S. 2000, 'Boiling Liquid Expanding Vapour Explosions (BLEVE) - Possible failure mechanisms and their consequences', Hazards XV, *Institution of Chemical Engineers Symposium. Series No.147*, pp. 121-137.

Warren Centre 1986, *Major Industrial Hazards: Technical Papers*, Sydney University, Australia, ISBN 09492629-37-9.

Withers, R.M.J. and Lees, F.P. 1985a, 'The assessment of major hazards: the lethal toxicity of chlorine, Pt 1: Review of information on toxicity', *Journal of Hazardous Materials*, vol. 12, no. 3, pp 231.

Withers, R.M.J. and Lees, F.P. 1985b, 'The assessment of major hazards: the lethal toxicity of chlorine, Pt 2: Model of toxicity to man', *Journal of Hazardous Materials*, vol 12, no. 3, pp 283.

World Bank 1988, *Techniques for assessing industrial hazards*, Technical Report 55, Washington DC.

## 7.9 NOTATION

| | |
|---|---|
| $\hat{C}$ | Concentration, ppm |
| AIChE | American Institute of Chemical Engineers |
| AIHA | American Industrial Hygiene Association |
| API | American Petroleum Institute, USA |
| BLEVE | Boiling Liquid Expanding Vapour Explosion |
| C | Concentration, mg/m$^3$ |
| CCPS | Centre for Chemical Process Safety, AIChE |
| $Cl_2$ | Chlorine |
| CO | Carbon monoxide |
| COC | Chemical of Concern |
| DIPNR | Department of Infrastructure, Planning and Natural Resources, NSW, Australia |
| DTL | Dangerous Toxic Load |
| ERPG | Emergency response planning guidelines |
| HCN | Hydrogen Cyanide |
| He | Helium |
| HF | Hydrogen Fluoride |
| HSE | Health and Safety Executive, UK |
| IChemE | Institution of Chemical Engineers, UK |
| IDLH | Immediately dangerous to life or health |
| kg | kilograms |
| kW | kilo-Watts |
| kW | kilo-Watts |
| kW/m$^2$ | kilo-Watts per square metre |
| $LC_{50}$ | Lethal concentration for 50% mortality to exposed species |
| $LD_{50}$ | Lethal dose for 50% mortality to exposed species |
| $LD_{min}$ | Minimum lethal dose |

| | |
|---|---|
| LPG | Liquefied Petroleum Gas |
| mg/L | milligrams per Litre |
| mg/m$^3$ | milligrams per cubic metre |
| MHAP | Major Hazards Assessment Panel, UK |
| $N_2$ | Nitrogen |
| NFPA | National Fire Protection Association, USA |
| $NH_3$ | Ammonia |
| nm | nano-metres |
| NOAEL | No Observed Adverse Effects Level |
| NOEL | No Observed Effects Level |
| OSHA | Occupational Safety and Health Administration, USA |
| $P_0$ | Atmospheric pressure, Pa |
| Pa | Pascals |
| PEL | Permissible exposure limits |
| PFP | Passive Fire Protection |
| ppm | parts per million |
| $P_S$ | Peak overpressure, Pa |
| PSV | Pressure Safety Valve |
| q | Heat flux (W/m$^2$ or kW/m$^2$) |
| RTECS | Registry of Toxic Effects of Chemical Substances |
| s | seconds |
| $SO_2$ | Sulphur dioxide |
| STEL | Short Term Exposure Limit |
| TLV | Threshold Limit Value |
| TNO | Netherlands Organization of Applied Scientific Research |
| $t_p$ | Positive phase duration, s |
| USCG | United States Coast Guard |
| USEPA | United States Environment Protection Agency |
| W/m$^2$ | Watts per square metre |

This page is intentionally left blank

# 8 ESTIMATING THE LIKELIHOOD OF INCIDENTS

*"Any theory based on experience is necessarily* statistical; *that is to say, it formulates an* ideal average *which abolishes all exceptions at either end of the scale and replaces them by an abstract mean. This mean is quite valid, though it need not necessarily occur in reality."*

*Dr Carl Gustav Jung*

In Chapter 3, the two-dimensional model discussed has two basic parameters; the severity of incident consequences and the likelihood of occurrence. In order to estimate the risk, we need both parameters. In Chapters 5 to 7, we covered the first of these parameters, namely consequence analysis. In this Chapter, we shall discuss the second parameter, namely estimation of likelihood.

The likelihood of an incident is a probability, and therefore is not deterministic. We cannot say when an incident may occur. We can only say what the probability of occurrence is. If this probability is high, it requires us to do something about it; if it is low, we may decide to live with it, taking every care that it remains low through a Safety Management System and administrative controls. Therefore, the likelihood estimate is one of the major sources of uncertainty in risk analysis. Consequently, it also poses significant challenges to the analyst.

In this chapter, the role of frequency analysis in hazard analysis is explored. Qualitative and quantitative evaluation methods are described. Failure rate data sources are listed. Uncertainty associated with the data is explained, along with precautions to be exercised in frequency estimation and its interpretation.

*The most important point to remember all the way through this chapter is that one should not become obsessive about obtaining a numerical value of likelihood, if it requires assumptions that cannot be reasonably justified, and would produce results whose uncertainty cannot be reasonably ascertained.*

## 8.1 THE ROLE OF FREQUENCY ANALYSIS

### 8.1.1 Need for Frequency Analysis

Frequency analysis involves the estimation of the likelihood of occurrence of accident events and the likelihood of various impacts following from these events. The term *frequency* is used when the estimation is quantitative. For qualitative estimates, the term *likelihood* is more appropriate.

Frequency analysis plays a major role in the management of risk in process systems. Some of these are highlighted:

- Without failure frequency estimation and incident propagation at subsystem levels, it is not possible to assess the risk. Analysis of industry accident frequency using statistical analysis techniques alone is insufficient to predict accident event frequencies without detailed analysis at decomposed levels of the system (Kirchsteiger 2001).
- Major capital cost decisions regarding the extent of safety systems requirements are made on the basis of risk assessment, and frequency assessment plays a key role in this decision.
- Since incident likelihood is essentially a probability, the assessment of frequency is an assessment of uncertainty.
- Not only the estimation of frequency, but associated minimisation of uncertainty is necessary for informed decision making.
- Because of the uncertainty band in a frequency assessment, careful interpretation of the results is required. This can be a considerable challenge both to the analyst, and to the decision makers.

### 8.1.2 Frequency and Probability

Two terms are often used in relation to likelihood estimation; frequency and probability. These two terms are sometimes loosely used interchangeably by the uninitiated. This practice is technically incorrect.

It is important to recognise the difference between frequency and probability.

*'Probability is the likelihood of a specific event or outcome, measured by the ratio of specific events or outcomes to the total number of possible events or outcomes. Probability is expressed as a number between 0 and 1, with 0 indicating an impossible outcome and 1 indicating an outcome is certain.' (AS/NZS 4360: 1999, p. 3)*

Probability is an abstract concept, and the philosophy of interpretation of the meaning of probability in the context of quantitative risk analysis (QRA) is discussed by Watson (1994) and Yellman and Murray (1995).

**EXAMPLE 8-1 MEANING OF PROBABILITY**

The probability of a fire water pump failing to start on demand is 0.005.

This means that if an experiment was conducted to give a demand signal for the fire pump to start 1000 times, the pump would fail to start on 5 occasions. Alternatively, the probability could be interpreted to mean that out of the number of times the system was required to operate, it has failed or it will fail 0.005 fraction of the time.

In process safety, probabilities are generally used as a measure of the reliability of protection systems, or the reliability of the barriers against realisation of a hazard.

*Frequency is a measure of the rate of occurrence of an event expressed as the number of occurrences of an event in a given time (AS/NZS 4360: 1999, p. 2).*

Frequency has a time element associated with it. The frequency of a major incident is often expressed on a 'per annum' basis. The frequency or failure rate of individual equipment or component may be expressed in terms of number of failures per million hours (calendar hours or operating hours, as specified).

**EXAMPLE 8-2 INCIDENT FREQUENCY**

The frequency of a minor fire in a process plant is 0.1 per year.

Several interpretations are possible, meaning the same thing:

- There is a 10% chance of a minor fire in a given year
- If 10 identical facilities operated under the same conditions, a minor fire could occur in one of them in a given year.

The relevant interpretation should be made depending on the context. In the estimation of likelihood, both the frequency and probability are important parameters, for assessing incident escalation. For instance:

$$\begin{aligned}\text{Frequency (major event)} &= \text{Frequency (initiating minor event)} \times \\ &\quad \text{Probability that the event is not controlled}\end{aligned}$$

**EXAMPLE 8-3 FREQUENCY OF ESCALATION**

Let us combine Examples 8-1 and 8-2 here.

The frequency of a minor fire is 0.1 per year (p.a.). Let us say that the plant equipment is fitted with an automatic deluge system, and a firewater pump is installed to supply deluge water. If the firewater pump fails to start on demand, there would be delay in mobilising alternative fire fighting measures, and hence the minor fire could escalate to a major fire.

Now the probability of the fire water pump failing to start on demand is 0.005. Therefore

$$\begin{aligned}\text{Frequency (major fire)} &= \text{Frequency (minor fire)} \times \\ &\quad \text{Probability (firewater pump failure to start on demand)} \\ &= 0.1 \text{ p.a.} \times 0.005 = 5 \times 10^{-4} \text{ p.a.}\end{aligned}$$

Note that we have included the units (p.a. = per annum) with the frequency value throughout. The probability value is dimensionless. It is good practice to tag the units of the frequency wherever it is used, so that the two parameters do not get confused in numerical manipulations.

In simple terms there are two areas of consideration in frequency assessment:

a) basic events - which could be the failure of a piece of equipment or the failure of someone to do something.
b) complex incidents - which are made up of a number of basic events that could be a combination of equipment and human failures.

## 8.2 QUALITATIVE AND QUANTITATIVE APPROACHES

### 8.2.1 Qualitative Estimates

When we talk of qualitative estimates of likelihood, we really mean it is an approximate semi-quantitative estimate related to a time frame.

In a qualitative estimate, the measure is descriptive, and uses the commonly understood shades of the language. The scale 'Almost Certain', 'Likely', 'Possible', 'Unlikely' and 'Rare' has been suggested in Chapter 3. But these words alone are insufficient to assess the likelihood of an incident, unless each term is associated with a measure. Table 8-1 below is a variation of Table 3-1.

TABLE 8-1 EXAMPLE OF QUALITATIVE ESTIMATE OF LIKELIHOOD

| Likelihood ↓ | Description |
|---|---|
| **Almost Certain** | Has occurred in the plant more than once |
| **Likely** | Near miss occurrences in the plant in question. Incident has occurred in similar plants several times. |
| **Possible** | Near miss has occurred at least once. Incident has occurred in industry. Event *may* occur once in plant lifetime |
| **Unlikely** | Event has not occurred in countries with a strong regulatory regime. Even *may not* occur during plant lifetime. |
| **Rare** | Event has not occurred in the industry. Event *may* occur, but only under exceptional circumstances. |

Table 8-1 is a convenient way of estimation as a first pass, but one cannot stop there. There are several limitations in stopping with the qualitative approach.

- Several process incidents in the high severity-low likelihood end of the incident spectrum can crowd into the 'Unlikely' or 'Rare' category, and without quantification, these incidents cannot be ranked.
- It is not possible to identify and rank the significant contributors to the likelihood of occurrence.
- Setting of risk reduction priorities is difficult and the 'risk dollar' can be misdirected.

It is useful to use the qualitative approach for initial screening, but even here, a conservative approach is required, and high severity incidents should not be screened out purely on the basis of a qualitatively ascribed ‘Rare’ likelihood.

- In order to understand the complex interactions of contributing factors that give rise to the incident, logic diagrams such as fault trees and event trees may be used, but not necessarily quantified at this stage.

### 8.2.2 Quantitative Approaches to Frequency Estimation

There are two basic approaches to the estimation of probabilities or frequencies for the accident events:

a) Direct use of statistical data on failure of plants or whole systems, or specific accident events (e.g. lost time injuries or near misses). This approach is often used in the insurance industry and may be termed an 'actuarial method', used for occupational health and safety (OH&S) type incidents. Historical injury data and trends may be used to estimate incident frequencies. Measures like Lost Time Injury Rate (LTIR) are often used.
The direct use of statistical data to predict the low frequency-high severity events is fraught with problems. For instance, an installation may have experienced an explosion after 10 years of operation. Assuming that the facility would be run for another 20 years, with continual enhancements in safety reliability, what is the likelihood of a similar event? We cannot say it is once in 10 years as the causes that led to the first event may have been eliminated, or additional process safety measures may have been introduced.

b) Breaking down the event into its contributing factors and causes, and variety of possible outcomes, using analytical techniques of reliability engineering. The analytical approach is more appropriate for the low frequency-high severity end of the incident spectrum. These aspects are illustrated in Figure 8-1.

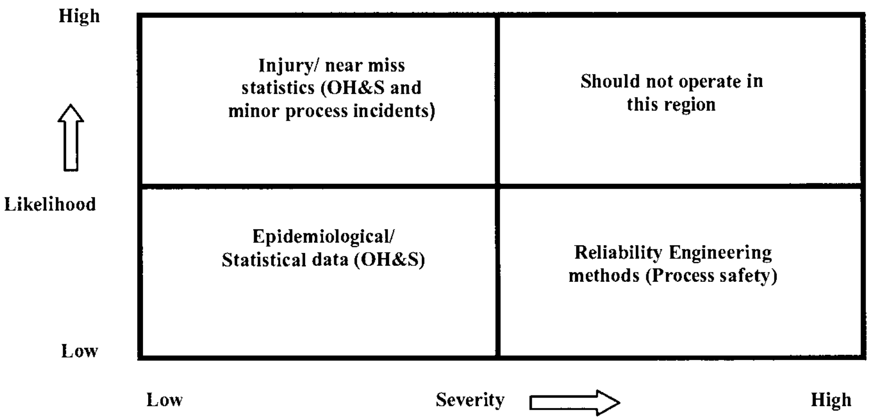

High
Likelihood
Low
Injury/ near miss statistics (OH&S and minor process incidents)
Should not operate in this region
Epidemiological/ Statistical data (OH&S)
Reliability Engineering methods (Process safety)
Low
Severity
High

FIGURE 8-1 FREQUENCY ESTIMATION ACROSS INCIDENT SPECTRUM

## 8.3 REPRESENTING COMPLEX FAILURE SYSTEMS

### 8.3.1 Factors Influencing Process System Failures

A major incident such as a fire or explosion does not occur without a number of contributing antecedent factors. The factors can be broadly divided into six categories:

1. Design
2. Fabrication and installation
3. Operating strategy
4. Environmental factors
5. Human factors
6. Safety management system (SMS)

Table 8-2 provides more details of these factors. Several of these factors could contribute to an event, either independently or in complex combinations (CCPS 2000). Human factors are discussed by Swain and Guttman (1983), Williams (1986), and HSC (1991).

### 8.3.2 Cause-Consequence Representation

The complex combinations of causes resulting in a process incident and the variety of consequences arising can be schematically represented by cause-consequence diagrams (CCPS 1992). The simplest form is the high level systems model, as shown in Figure 8-2.

TABLE 8-2 FACTORS INFLUENCING PROCESS SYSTEM FAILURES

| Category | Influencing factors |
|---|---|
| 1. Design | Incorrect standard<br>Inadequate definition of design basis<br>Failure of technical audit at design stage<br>Incorrect material selection<br>Inadequate safety margins<br>Inadequate design to cope with process deviations<br>Unbalanced forces<br>Absence or failure of change management in design changes<br>Systems interfaces (multiple parties designing different systems of the plant) |
| 2. Fabrication and installation | Quality system failure in fabrication and/or installation<br>Incorrect welding techniques/ welding specification<br>Inadequate non-destructive testing (radiography, magnetic particle test, hydrostatic tests)<br>Incorrect tolerances<br>High mechanical stress in rotating equipment<br>Incorrect alignment<br>Incorrect material of construction |
| 3. Operating strategy | Operating close to design limits of equipment and materials<br>Frequent stops and starts<br>Thermal cycling of high temperature equipment<br>Inadequate usage of standby equipment<br>Reactivity/ embrittlement<br>Incorrect start-up practices (accelerated load increase, failure to follow manufacturer recommended practice)<br>Process deviations and exceedence of safe operating envelope |
| 4. Environmental factors | Internal corrosion<br>External corrosion<br>Erosion<br>Vibration<br>Impact<br>Humidity<br>Ambient air quality (atmospheric salts, dust)<br>Ambient temperature extremes<br>Foundation settling<br>Subsidence/ seismic activity |
| 5. Human factors | Skill based errors<br>Rule based errors<br>Knowledge based errors<br>Competency training<br>Communications<br>Abnormal situation management |
| 6. Safety management system | Inadequate maintenance<br>Inadequate mechanical integrity inspections<br>Unauthorised modifications/ changes to procedures<br>Inadequate systems of work<br>Inadequate monitoring and feedback |

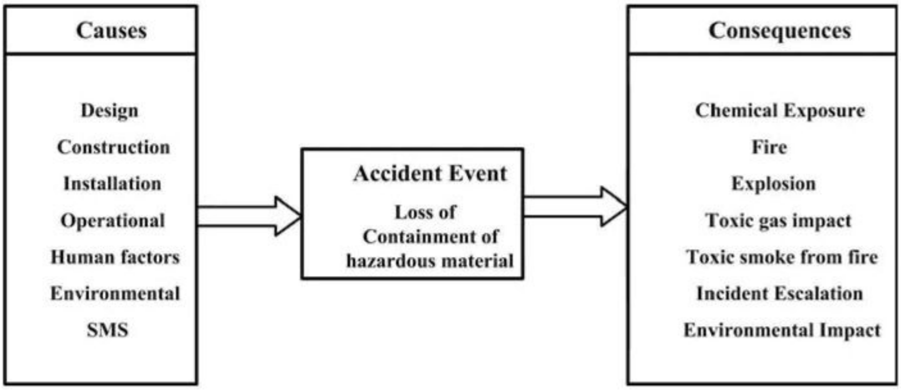


FIGURE 8-2 CAUSE-CONSEQUENCE REPRESENTATION

The advantage of the cause-consequence representation is that it gives a simple overview of the causes and the consequences of an event. However, this in itself is insufficient for frequency analysis as it does not show the following details:

- barriers in place to prevent the causes from occurring
- combinations of multiple causes that result in the accident event
- mitigation measures in place to prevent the consequences
- other recovery measures from the consequences

A more detailed representation is required to provide a full picture. This is described in the next section.

### 8.3.3 Cause-Consequence-Control Measures Representation

This model is similar to the cause-consequence model, but shows the barriers for prevention of the accident sequence on both the antecedent and consequence side of the accident event. Figure 8-3 illustrates the concept. The control measures are shown as prevention barriers that block the propagation of the cause to the accident event, and as mitigation barriers that block the consequences being realised.

Figure 8-3 is often referred to as the "Bow-Tie" diagram due to its shape, and was originally developed by the Shell Company.

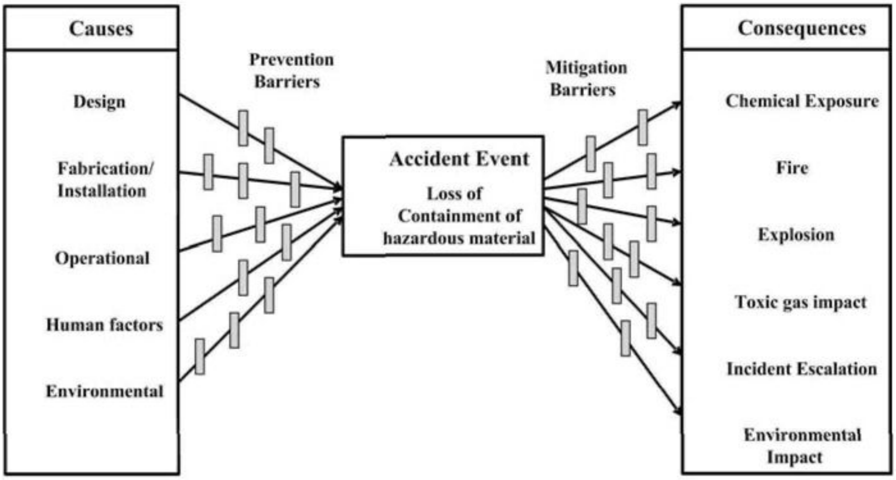


FIGURE 8-3 BOW-TIE REPRESENTATION OF CAUSE-CONSEQUENCE-CONTROL MEASURES

The following points are of interest:

- There is more than one barrier for each cause or each consequence. This is essential to ensure that a single point failure does not lead to the accident event or the consequence. There is some similarity to the layer of protection concept.
- The design basis should specify the number of *independent barriers* required, and their effectiveness, as a performance standard.
- The same barrier or control measure can appear in more than one branch. For instance, gas detection as a barrier can appear for both fire and explosion consequences. Emergency shutdown (ESD) as a control measure may appear in almost every branch on the right hand side of Figure 8-3.
- Not all the items listed in Table 8-2 need to appear as causes. Some of these can appear as barriers, failure of which, leads to the accident event. This is especially the case with most SMS items, which are essentially designed as barriers to prevent incident occurrence.
- It is hard to show all the barrier description in the bow-tie, without making it difficult to read. One way to overcome this is to tag the barriers, and have a tag legend attached to the diagram. Another alternative is that the diagram need not be shown as a bow-tie at all, except to illustrate the concept, but can be shown simply as a spreadsheet.

#### EXAMPLE 8-4 BOW-TIE MODEL FOR HYDROCARBON GAS RELEASE

The accident event is release of high pressure hydrocarbon gas, containing high concentration of hydrogen sulphide (sour gas). An early ignition would result in a jet fire, which, if it impinges on surrounding inventory, can cause incident escalation, resulting in a BLEVE. A delayed ignition could result in a vapour cloud explosion, with structural damage and secondary loss of containment. Delayed ignition or non-ignition can cause toxic impact from the $H_2S$ in the gas.

Figure 8-4 illustrates the bow-tie model. The list of causes is not exhaustive. The barrier legend is summarised in Table 8-3.

TABLE 8-3 BARRIERS AGAINST CAUSES AND CONSEQUENCES FOR HYDROCARBON GAS RELEASE INCIDENT

| Barrier No. | Description |
|---|---|
| $B_1$ | Material selection |
| $B_2$ | Corrosion allowance |
| $B_3$ | Corrosion monitoring |
| $B_4$ | Quality assurance |
| $B_5$ | Integrity inspection |
| $B_6$ | Higher wall thickness for small bore pipe |
| $B_7$ | Support/ minimise vibration for small bore pipe |
| $B_8$ | Gasket installation procedure |
| $B_9$ | Stores QA procedure for gasket issue |
| $B_{10}$ | High pressure alarm and operator intervention |
| $B_{11}$ | High pressure trip |
| $B_{12}$ | Pressure relief device (PSV) |
| $B_{13}$ | Gas detection and process isolation interlock |
| $B_{14}$ | Emergency response plan and preparedness |
| $B_{15}$ | Control of ignition sources (Permit to work, hazardous area classification) |
| $B_{16}$ | Firewater deluge |
| $B_{17}$ | Emergency depressuring to flare |
| $B_{18}$ | Personal protection equipment (PPE) |

The bow-tie representation may be used as a starting point for frequency estimation.

Since the causes on the left hand side of Figure 8-4 are independent, the frequency (failure rate) of each of the causes can be added to obtain the total failure frequency of gas release. In practice, however, this is difficult, as the failure frequencies of the individual failure modes may not always be available in the statistical databases. Therefore, the following approach is useful.

- where available, use individual failure mode frequencies
- where no individual failure mode frequencies are available, but only a total frequency for piping failure is available, there is no option except to use this as the gas release frequency.
- where failure frequencies are available for some of the individual failure modes, but not all, add the values for which data is available and subtract from the total failure rate. This residual value represents the combined failure rates of those failure modes for which no information is available.
- The frequency of vessel overpressuring is estimated by using the failure rates of process deviations that cause overpressurisation, and fault tree analysis (see Section 8.4)

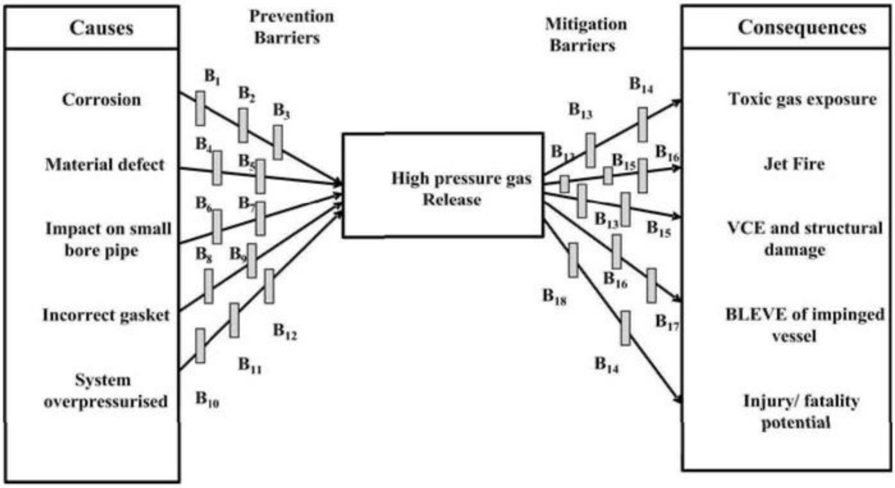


FIGURE 8-4 BOW-TIE MODEL FOR GAS RELEASE

While the causes are normally represented as frequencies, the consequences on the right hand side of Figure 8-4 are represented as probabilities. The reason for such representation is that it enables quantification of consequence frequency using the generic formula,

$$F_i = \sum_j f_j \cdot \prod_k p_k = \sum_j f_j (p_1 \cdot p_2 \cdots p_k) \tag{8.1}$$

where

$F_i$ = frequency of specified consequence $i$
$f_j$ = frequency of cause $j$ resulting in consequence $i$, and
$p_k$ = failure probability of independent protection layer $k$

### EXAMPLE 8-5 QUANTIFICATION OF GAS RELEASE AND BLEVE FREQUENCY

The information available on the frequency, relevant to the gas release scenario is given in Table 8-4. Frequency values are expressed in "per annum" units.

The sequence of events occurs as follows:

Release (demand on detection & isolation) → Detection/isolation failure → Ignition and flame impingement on inventory (demand on rapid action and depressuring) → Delayed action/depressuring system failure

The frequency calculations follow the same sequence:

Release frequency = Σ Frequency of component × number of components (Items 1 to 5 in Table 8-4)
= 1.27E-02 p.a.

Uncontrolled release = Initial release × detection isolation failure
= 1.27E-02 × 0.023 (Note 2 in Table 8.4)
= 2.92E-04 p.a.

Fire frequency = Uncontrolled release frequency × probability of ignition
= 2.92E-04 × 0.1
= 2.92E-05 p.a.

Frequency of flame impingement on inventory = 2.92E-05 p.a. × 0.5
= 1.46E-05 p.a.

BLEVE frequency = 1.46E-05 p.a. × 0.105 (Note 3 in Table 8.4)
= 1.53E-06 p.a.

■ ■ ■

Many process systems are more complex than the gas release event described in Example 8-5. Sections 8.4 and 8.5 describe estimation of frequency of a given consequence for complex systems using logic diagrams. Methods of sourcing and evaluating failure rate data for equipment and components are described in Section 8.7.

TABLE 8-4 FAILURE RATES OF EQUIPMENT AND COMPONENTS

| Item No. | Component | Failure frequency/ probability | Comments | Total frequency, p.a. |
|---|---|---|---|---|
| 1 | Pipe rupture | 3.0E-04 p.a. | Minor leak | 3.0E-04 |
| 2 | Pump seal | 4.0E-03 p.a./unit | Throttle bush failure. Single mechanical seal. Two pumps. | 8.0E-03 |
| 3 | Valve gland | 7.0E-04 p.a./unit | Significant leak. There are 5 valves | 3.5E-03 |
| 4 | Flange gasket | 3.0E-05 p.a./unit | There are 10 flanges (manual and actuated valve fittings) | 3.0E-04 |
| 5 | Small bore piping | 1.0E-04 p.a./unit | Full bore leak. There 6 instrument connection nozzles | 6.0E-04 |
| 6 | Gas detector | 1.8E-02 | Quarterly calibration and checks | |
| 7 | Shutdown valve | 5.0E-03 | Failure to operate on demand | |
| 8 | Ignition probability | 0.1 | Estimate based on flammable cloud area and review of ignition sources present | |
| 9 | Flame impingement on inventory | 0.5 | Based on review of installation and assessment of flame orientation | |
| 10 | Depressuring valve | 5.0E-03 | Failure to operate on demand | |
| 11 | Human error (delayed action, incorrect action) | 0.1 | Operator needs to initiate depressuring. Delay may result in escalation. | |

es:

1. Firewater deluge was not used in the escalation assessment due to jet flame impingement as it only delays escalation and does not prevent it.
2. Gas detector/ shutdown valve loop together constitutes one protection layer. Failure probability (1.8E-02+5.0E-03) = 0.023.
3. Human error and delayed depressuring /depressuring valve together constitute one protection layer. Failure probability (5.0E-03 + 0.1) = 0.105.

## 8.4 CAUSE-CONSEQUENCE MODELLING TOOLS

There are a number of tools or techniques which can help analyse complex failure situations where a particular final event like an explosion results from a logical combination of other more fundamental events such as initial release, cloud drift and ignition.

There are two main techniques we can use to represent complex failures and their subsequent effects. These are fault trees and event trees.

### 8.4.1 Fault Trees

A fault tree (and hence fault tree analysis or FTA) is a logical representation of a nominated event in terms of basic events or failures. We talk about the "top event" and the "basic events". Figure 8-5 shows the general picture of a fault tree, tracing the top event down the branches to the basic events.

Clearly, these basic events ($e_1$, $e_2$, ... $e_6$) are combined in some logical way to arrive at the top event (T). In the next section we will discuss those combinations.

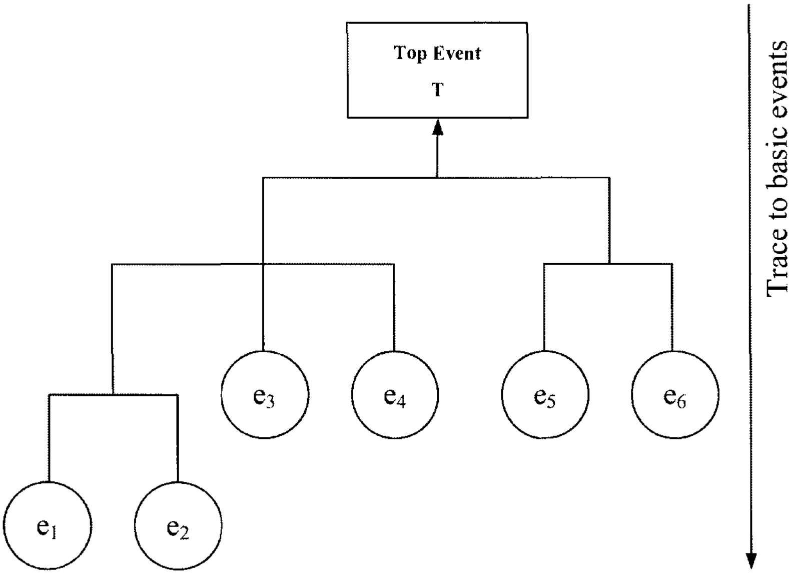


FIGURE 8-5 FAULT TREE STRUCTURE

### 8.4.2 Event Trees

Complementing the fault tree, an event tree (and hence event tree analysis or ETA) considers the possible outcomes from a particular nominated event by tracing the logical outcomes. Here the initiating event starts the tree and the final consequences are the outcomes. Figure 8-6 shows the general structure of such an event tree. They are often drawn horizontally because of the many branches that can exist.

The final outcomes ($c_1$, ... , $c_7$) are the result of logical operations at each branch as we proceed up the tree. Normally the branch divides into 2 at each point depending on whether a particular condition exists or not. Section 8.6 will deal with event trees in more detail.

A final representation is called the "cause-consequence diagram" which is essentially the two individual trees put together. One side of the tree goes back to the basic events (Fault Tree) whilst the other side traces the consequences (Event Tree) from the central incident (T).

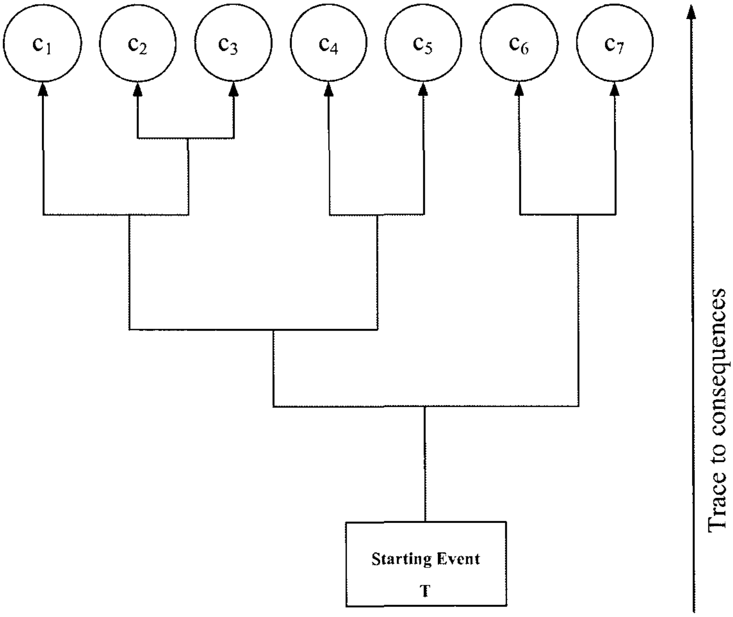


FIGURE 8-6 EVENT TREE STRUCTURE

## 8.5 FAULT TREE ANALYSIS

### 8.5.1 Basic Concepts

The fundamental concept in fault tree analysis is the translation of a physical system into a structured logic diagram (fault tree), in which certain specified causes lead to one specified TOP event of interest (Lee et al. 1985).

The tree depicts the causes of failure by working backwards from the 'top-event', identifying all contributors to the event. The tree structure is created by tracing back the top-event to possible causes (failure modes or base events), which may be component failures, human errors or any other events that can lead to the top event.

The concept of 'gates' forms the central focus of fault tree logic. A gate is a logic unit, in which branches of a section of the fault tree meet. Each branch is a component or sub-system failure or human error event. Two main types of gates are used in fault tree analysis, the 'OR' gate, and the 'AND' gate. The gates are explained in Example 8-6.

**EXAMPLE 8-6 GATES OF FAULT TREE**

Figure 8-7 illustrates the 'OR' gate using the ammonia tank filling Example 4.6 in Chapter 4. The TOP event for this gate is 'Overfilling of ammonia tank'. The branches leading to this gate are causes for overfilling.

1. Failure of local level gauge (LI)
2. LI indicates correctly, but local operator (Operator 1) fails to isolate when required level is reached.

It is clear that the occurrence of either 1 or 2 could result in the top event. The gate is therefore called the "OR' gate. The causes are sometimes referred to as 'demands' as these causes *demand* that a protection system operate to prevent the top event occurrence.

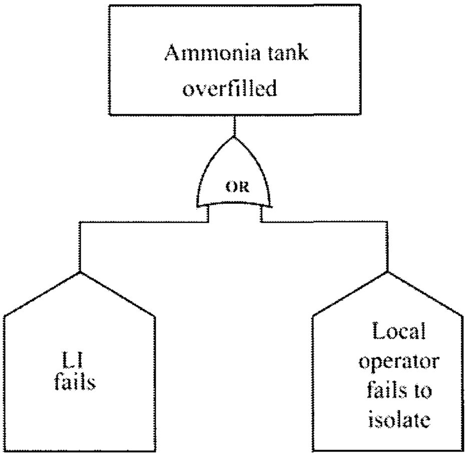


**FIGURE 8-7 EXAMPLE OF 'OR' GATE FOR DEMAND**

We know that protection against overfilling has been provided in terms of a high level switch to an alarm in the control room, and the procedure is for the control room operator to inform the local operator by radio to stop filling. The protection system failure can also be represented by a similar OR gate, as shown in Figure 8-8. The top event for this is 'Filling not stopped'.

1. Failure of level switch high (LSH)
2. Failure to alarm in control room (signal failure)
3. Control room operator (Operator 1) fails to inform local operator (Operator 2)
4. Local operator (Operator 2) fails to respond to control room operator instructions

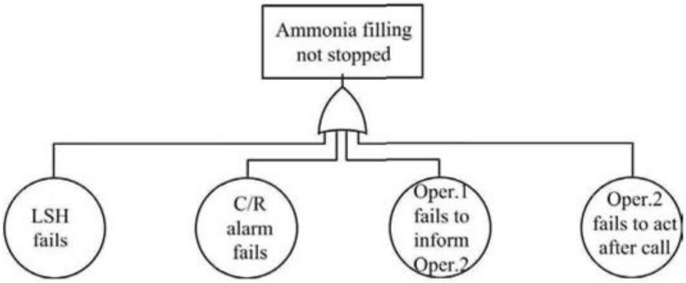

Ammonia filling not stopped
LSH fails
C/R alarm fails
Oper.1 fails to inform Oper.2
Oper.2 fails to act after call

FIGURE 8-8 EXAMPLE OF 'OR' GATE FOR PROTECTION FAILURE

When a *demand* occurs, *and* the *protection system fails to act* on demand, the process incident occurs - i.e. ammonia release to atmosphere. By making 'ammonia release to atmosphere' as the top event, we can now combine the two trees in Figures 8-7 and 8-8 into an AND gate, as shown in Figure 8-9.

The terms '*demand*' and '*protection system failure*' used in Example 8-6 are commonly used in FTA and need to be clearly understood.

**Demand**

The failure of an item of equipment or the development of an undesirable situation (e.g. high level in tank) that creates a 'demand' on the protection system to operate, e.g. level switch to alarm or close the inlet valve.

A 'demand' on the protection system to be brought into operation is generally expressed as a frequency (e.g. number of times/year).

**Protection system failure**

The protection system in response to a demand, fails to operate. The chance that the 'protection system would be in a failed state' when the demand occurs is expressed as a probability (dimensionless).

The undesirable top event occurs when there is a demand *and* the protection system fails. Therefore, the basic principles to note are that if the top event is a process incident. It is arrived at by joining a demand and a protection failure in an AND gate. Several useful examples are given by Tweeddale (2003).

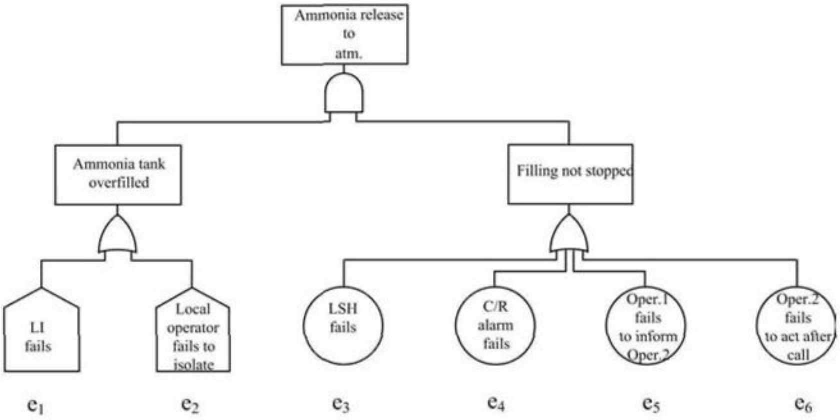


**FIGURE 8-9 EXAMPLE OF 'AND' GATE FOR PROCESS INCIDENT AS TOP EVENT**

When we use 'OR' gate structures, the output is formed by the sum of input frequencies or probabilities, as seen in Figure 8-9, provided the input events are independent. This is an approximation which is generally valid as it neglects the subtraction of the intersection of each event.

For the 'OR' gate and 2 basic events ($e_1$, $e_2$) we have for probabilities

$$P(T) = P(e_1) + P(e_2) - P(e_1).P(e_2) \quad \text{or} \qquad (8.2)$$
$$= 1-(1-P(e_1))(1-P(e_2)) \qquad (8.3)$$

For frequencies

$$F(T) = F(e_1) + F(e_2) \qquad (8.4)$$

When we use the 'AND' gate structures, the output is the product of the inputs. These can be probabilities, but there cannot be more than one frequency unit in an input to an 'AND' gate as the units of the gate output are infeasible.

For the 'AND' gate and 2 basic events ($e_1$, $e_2$) we have for probabilities

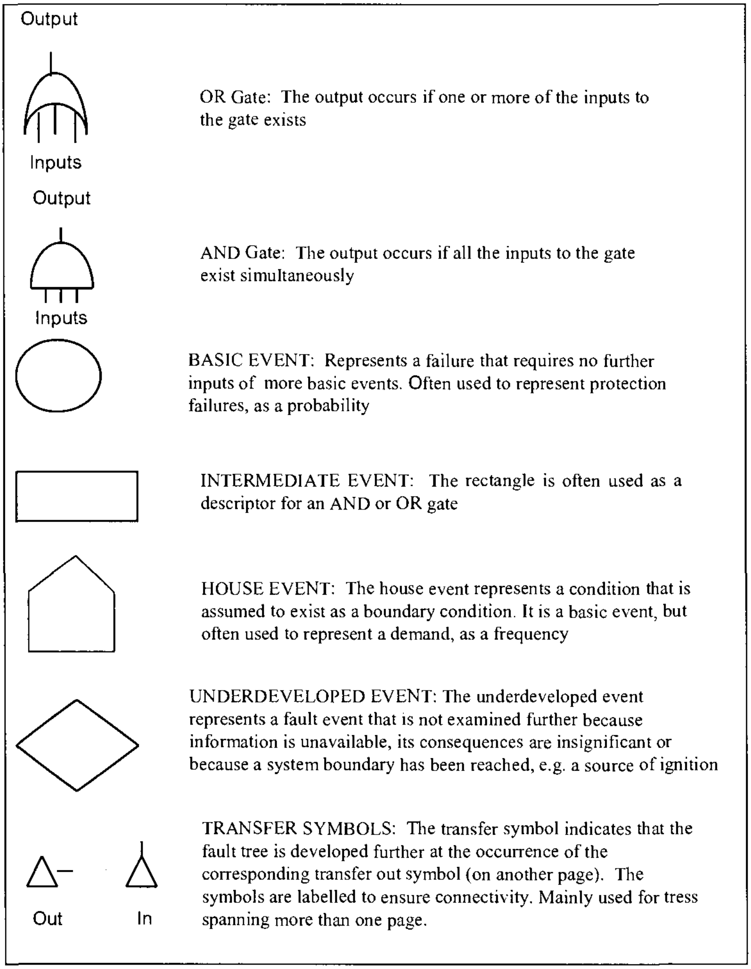
$$P(T) = P(e_1).P(e_2) \qquad (8.5)$$

For frequencies

$$F(T) = F(e_1).F(e_2) \text{ is not permissible but} \qquad (8.6)$$
$$F(T) = F(e_1).P(e_2) \qquad (8.7)$$
or
$$F(T) = P(e_1).F(e_2) \text{ are permissible} \qquad (8.8)$$

### 8.5.2 Symbols and Nomenclature for Fault Trees

Figure 8-10 shows the standard symbols and nomenclature adopted in fault tree analysis (Lees 2001).



OR Gate: The output occurs if one or more of the inputs to the gate exists

AND Gate: The output occurs if all the inputs to the gate exist simultaneously

BASIC EVENT: Represents a failure that requires no further inputs of more basic events. Often used to represent protection failures, as a probability

INTERMEDIATE EVENT: The rectangle is often used as a descriptor for an AND or OR gate

HOUSE EVENT: The house event represents a condition that is assumed to exist as a boundary condition. It is a basic event, but often used to represent a demand, as a frequency

UNDERDEVELOPED EVENT: The underdeveloped event represents a fault event that is not examined further because information is unavailable, its consequences are insignificant or because a system boundary has been reached, e.g. a source of ignition

TRANSFER SYMBOLS: The transfer symbol indicates that the fault tree is developed further at the occurrence of the corresponding transfer out symbol (on another page). The symbols are labelled to ensure connectivity. Mainly used for tress spanning more than one page.

FIGURE 8-10 FAULT TREE SYMBOLS (Lees, 2001)

### 8.5.3 Procedure for Fault Tree Construction

The construction of a fault tree appears a relatively simple exercise, but it is not always as straightforward as it seems and there are a number of pitfalls. Guidance on good practice in fault tree construction is given in Fusssell (1976), Fault Tree Handbook (Veseley et al., 1981), Lee et al. (1985), Doelp et al. (1984) and CCPS (2000).

Construction of a fault tree is a creative process. It involves identification of failure modes and effects. While fault tree analysis is regarded primarily as a tool to quantify the frequency hazardous events, the fault tree is of equal importance as a means of hazard identification, especially the logical combinations by which an accident event may propagate. Thus, fault trees created by different analysts may not be identical, due to style, judgement and/or omissions.

The principal elements in a fault tree are the top event, primary events, intermediate events, and the AND and OR gates.

There are four basic steps in fault tree construction and evaluation (Lee et al. 1985).

1. System definition
2. Fault tree construction (use failure modes and effects to develop relationships)
3. Qualitative evaluation (evaluation of independent combinations of events that result in the top event, known as minimum cutsets)
4. Quantitative evaluation (numerical evaluation of tree)

It is crucial to have a clear understanding of step 1 to ensure one is not lost in a maze of incorrect logic.

### 8.5.3.1 System definition

System definition consists of three stages:

1) Develop system chart
This is a description of how the system components are interconnected, and can be represented as a functional diagram. The piping and instrumentation diagrams (P&IDs), instrument loop diagrams and other signal line diagrams provide the necessary information for a functional diagram. Identify each component in the functional diagram, and its corresponding function.

2) Compile component failure modes and effects
It is essential to compile a list of failure modes and effects for the various components, prior to construction of the fault tree. Depending on the top event, not all failure modes of components would be necessary for the fault tree. For instance, an actuated valve may have several failure modes (failure to open, failure to close, internal leakage when closed, external leakage etc). If the fault tree is safety related, and the safety function is for the valve to close on demand, then the only relevant failure modes are failure to close on demand and internal leakage when closed. On the other hand, if the fault tree is related to production loss, then the failure mode of failure to open becomes important.

3) Define system boundary conditions
Fussell (1976) points out that the system boundary conditions should not be confused with the physical bounds of the system. The system

boundary conditions define the situation for which the fault tree is to be constructed. The boundary conditions are:

a) Top event. The top event in process safety analysis is often a hazardous event, resulting in a runaway reaction, loss of containment of hazardous materials, or major system failure resulting in production loss.
b) Other boundary conditions. The initial system configuration constitutes additional boundary conditions. This configuration should represent the system in the unfailed state. The configuration consists of two sets of elements:
   (i) Subsystems and components that prevent a deviation of a critical operating parameter such as pressure, temperature, composition etc. to outside safe operating envelope.
   (ii) Given that the deviation has occurred, subsystems and components that prevent the consequence of the deviation being realised. The layered protection model can be used identify the boundaries.

The events arising from these are intermediate events (demands and protection failures) in the fault tree.

Figure 8-4 is an example of system definition.

#### *8.5.3.2 Dependent failures*

A basic underlying assumption in fault tree analysis is that the events considered are independent, unless stated otherwise. In other words, the failure of one component or subsystem does not result in the consequential failure of another. In practice, there are many types of situations where events are not completely independent. In fault tree work this problem has been well known as 'common mode failure', 'common cause failure' (CCF), or 'dependent failure'. There are some subtle differences in these terms. It is generally acknowledged that common cause failures are a form of dependent failure where similar components fail at the same time due to the same cause. Edwards and Watson (1979) give a comprehensive coverage of common cause initiators (CCIs): relevant to fault tree analysis.

Some examples of dependency are:

- The same component sharing a control function and a trip function. This design is generally to be avoided, but some older installations do not separate these two. An example is a control valve being used as a shutdown valve as well.
- The failure of an equipment/component giving rise to more than one demand. An example is a runaway reaction in a reactor, causing both high pressure and high temperature conditions calling upon the protection systems to operate.
- Supply from a common utility such as electrical power or instrument air for pneumatically actuated instruments. If all the power is routed through a single switchboard, a failure of the switchboard will result in total loss of power, even if there is a standby power generator.

- Common degrading factors for several protection systems, such as vibration, corrosion, dust, humidity etc.
- A fire or explosion disabling a number of pieces of equipment simultaneously.

The dependency problem is particularly acute in systems where a very high degree of reliability is required, and where protective systems incorporating a high degree of redundancy are used. Dependent failure may take many and subtle forms, and are sometimes difficult to detect. There is a common susceptibility in the component concerned (Lees 2001).

Some situations which can cause dependent failure include:

- a common utility
- a common defect in manufacture or installation
- common exposure to a degrading factor (environmental conditions)
- an external influence
- a hazardous event and domino effects
- incorrect operation/maintenance
- operational overload on one equipment from failure of another

Not all dependent failures involve redundant equipment. Dependent failure is a crucial problem in high reliability systems.

**EXAMPLE 8-7 DEPENDENT FAILURES**

1. A cable tray carries a coaxial cable, carrying signals between field instruments and the control room. A single cable can carry several signals. Should the cable fail due to a fire, impact, electrical fault, or power failure, then all the protection systems to which the cable had carried signals could be disabled at the same time.
2. In an oxidation reactor, the safety system contains three independent oxygen analysers, high oxygen alarm/trip based on a two-out-of-three failure voting system. However, if all analysers draw the process gas sample from a single sampling point, a blockage of the sampling nozzle would disable all the analyser protection functions simultaneously.

According to Lees (2001), once the dependence potential has been identified, there are several ways of representing it in the tree:

- Continue to enter each fault separately as it occurs in the tree, but ensuring that each such entry is assigned the *same identifier*, so that the minimum cut sets are determined correctly.
- Enter the effect as a single fault under an AND gate higher up the tree.
- Common cause failure contributions are often embedded into the basic event failure values using a parameter such as the Beta factor method or multiple greek letter (MGL) method (CCPS 2000).

### 8.5.3.3 Qualitative evaluation of fault tree

An important aspect of fault tree analysis is that we should perform a qualitative analysis before doing any serious quantitative evaluation. In doing a qualitative analysis we can achieve the following outcomes:

- identify the key event combinations that lead to the top event (minimum cut sets)
- identify failures which are common to distinct parts of the tree - viz. common cause failures.
- gain an understanding of the key combination of events that dominate the occurrence of the top event and how the system could be changed.

**EXAMPLE 8-8 QUALITATIVE ANALYSIS OF FIGURE 8-9**

For ammonia overflow to occur, we must have an overfill situation, and the condition that the overfill is not stopped in time.

*Analysis*

The logic function which combines together the separate basic events to get the top event T can be written as:

$$T = (e_1+e_2).(e_3+e_4+e_5+e_6) \tag{8.9}$$

We can use frequencies for events 1 and 2 (demand) and probabilities of failures for all other events (parts of protection function) giving the frequency T as

$$f(T) = [f(e_1) + f(e_2)].\ [P(e_3)+P(e_4)+P(e_5)+(e_6)] \tag{8.10}$$

$$\begin{aligned} f(T) = {} & f(e_1).P(e_3) + f(e_1)P(e_4) + f(e_1)P(e_5) + f(e_1)P(e_6) + \\ & f(e_2).P(e_3) + f(e_2)P(e_4) + f(e_2)P(e_5) + f(e_2)P(e_6) \end{aligned} \tag{8.11}$$

The second and third order terms are neglected, as being small.

In this case we can see that the basic event combinations of $f(e_1)$ or $f(e_2)$ with any $P(e_i)$: $i = 3,4,5,6$ will lead to the top event. There are 8 second order cutsets in this tree and they are 'minimal' cutsets because neither is a subset of the others.

When a fault tree construction includes separate blocks for each demand/protection failure combination, the same block may appear in more than one branch. Alternatively, the same failure mode of a component may appear in more than one block. The initial fault tree then has to be 'reduced' to ensure that such duplications would not distort the top event frequency.

The qualitative evaluation consists of the generation of minimal cutsets. Since the top event can be reached through a number of possible paths, a cutset represents the collection of failure events in a given path.

For simple trees, the minimal cutsets can be obtained with the aid of Boolean algebra. Just as normal algebra adds or multiplies quantities which have a numerical value using normal rules of arithmetic, Boolean algebra operates on 'logical' quantities. Details can be found in a standard text on reliability engineering (Green and Bourne 1972, O'Connor 1991). For complex trees with a large number of inputs and gates, it is best to use fault tree synthesis software.

For Boolean operations, the reliability diagram is reduced to a logic diagram, as shown in Figure 8-11.

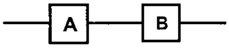
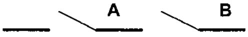
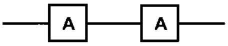
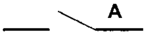
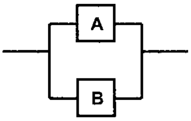
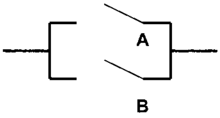
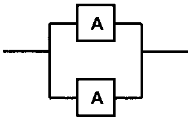
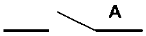
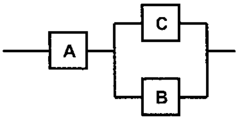
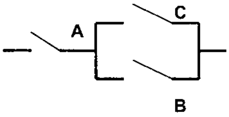
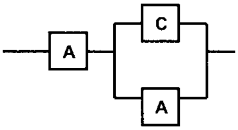
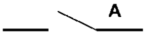
| No. | Reliability Diagram | Logic Diagram |
|---|---|---|
| 1. Series System |  |  |
| 2. Series System |  |  |
| 3. Parallel System |  |  |
| 4. Parallel System |  |  |
| 5. Series-Parallel System |  |  |
| 6. Series-Parallel System |  |  |

**FIGURE 8-11 LOGIC DIAGRAM EXAMPLES**

An "AND" gate may be represented by Row 1 in Figure 8-11. If A and B represent the same component, then one of them is redundant and therefore the system reduces to what is shown in Row 2. Thus

$A \cap A = A$ where $\cap$ is Boolean symbol representing an AND gate.

Similarly, an OR gate may be presented by Row 3 in Figure 8-11. If A and B represent the same component, then the reduced expression becomes (see Row 4):

$A \cup A = A$ where $\cup$ is Boolean symbol representing an OR gate.

In a series-parallel system (see Row 5), if A and B represent the same component, then the simplification as shown in Row 6 would result:

$A \cup (C \cap A) = A$

### EXAMPLE 8-9 REDUCTION OF FAULT TREE WITH DEPENDENT FAILURES

A liquid phase chlorination reactor is used to react chlorine gas and ethylene to produce 1-2 dichloroethane. A schematic of the feed system is shown in Figure 8-12.

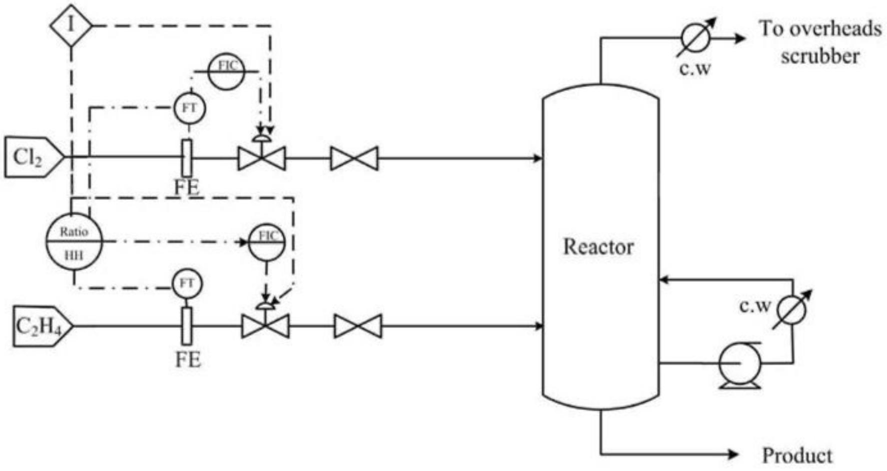


FIGURE 8-12 CHLORINATION REACTOR SCHEMATIC SIMPLIFIED

Chlorine ($Cl_2$) and ethylene ($C_2H_4$) at a set ratio are fed to a liquid phase reactor containing 1-2 dichloroethane. The chlorine feed flow controller set point is set by the operator. A programmable logic controller calculates the required ethylene flow based on a preset $Cl_2/C_2H_4$ ratio, and sends a set point signal to the ethylene flow controller. Each control loop consists of a flow sensor (FE), controller and feed control valve.

Should either control loop fail, the feed ratio between ethylene and chlorine would be upset. A high $Cl_2/C_2H_4$ ratio would result in the overheads scrubber capacity being exceeded, and excess chlorine released to atmosphere. This must be prevented. A $Cl_2/C_2H_4$ high high trip has been designed to initiate a reactor shutdown by closing both the feed flows. There is no independent shutdown valve on the feed lines, and the control valves are used as the shutdown valve. Such dependent arrangement was not uncommon in plants designed in the 1970's.

The top event (T) is the release of chlorine to atmosphere.

The demand events that can result in high $Cl_2/C_2H_4$ ratio are listed below. The list has been simplified by combining some individual components.

- Chlorine control valve sticks open (A)
- Chlorine control system (including sensor) malfunction (B)
- Ethylene control valve sticks closed (C)
- Ethylene control system (including sensor) malfunction (D)

The protection system failures that cause the top event are:

- $Cl_2/C_2H_4$ ratio high trip failure (E)
- Chlorine valve fails to close on demand (A)

The fault tree is shown in Figure 8-13. Note that the component A appears both in the demand branch and in the protection failure branch, indicating the dependence. This fault tree cannot be quantified as it is, and has to be reduced using Boolean logic. We have

$$T = (A+B+C+D).\ (E+A) \tag{8.12}$$

Applying the rules of Boolean reduction in Figure 8-13, this reduces to:

$$T = A + (B+C+D).E \tag{8.13}$$

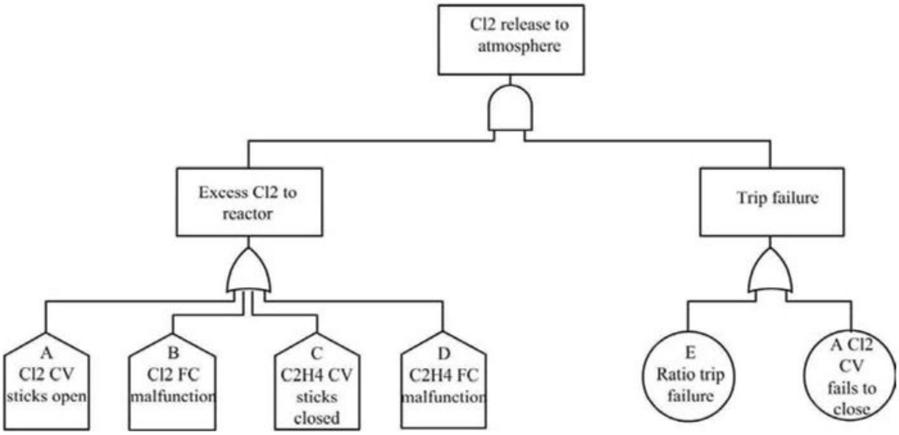


FIGURE 8-13 FAULT TREE SHOWING DEPENDENT FAILURE

The reduced fault tree is shown in Figure 8-14.

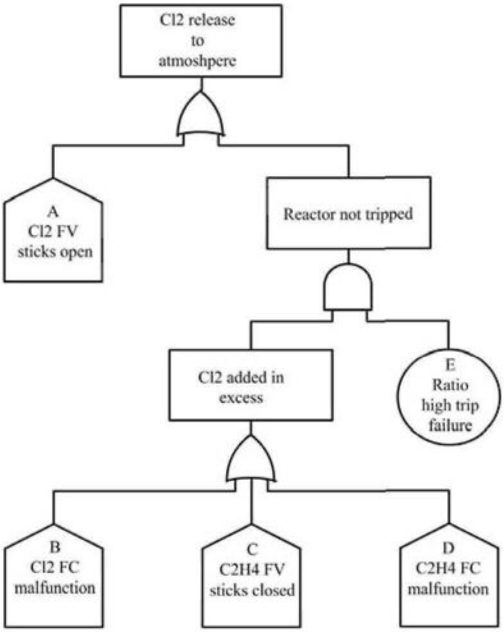


FIGURE 8-14 FAULT TREE AFTER BOOLEAN REDUCTION

## 8.5.4 Quantitative Evaluation of Fault Tree

Once the fault tree logic has been developed, the final step is quantification of the fault tree. For this assessment, failure rate data on the various base events are required. Data sources and availability are discussed in Section 8.7.

The following basic rules must be remembered in fault tree quantification, in order to maintain dimensional consistency:

- Frequencies of input components can be added in an 'OR' gate
- Probabilities of input components can be added in an 'OR' gate
- Addition of a frequency and a probability among the input components is forbidden in an 'OR' gate
- Probabilities of input components can be multiplied in an 'AND' gate
- A frequency and a probability of input components can be multiplied in an 'AND' gate
- Multiplication of two frequencies is forbidden in an 'AND' gate.

### *8.5.4.1 Reliability assessment of protective systems*

If there is a string of inputs into an 'AND' gate, arising from protection systems components, then the failure frequency data must be converted into a probability unit, by expressing the data as a 'probability of failure on demand'.

Many processes and equipment have specific protection systems. Every protection system failure can be placed in one of two categories:

1. The failure is revealed. In this case, a failure can be detected before an actual demand on the system occurs. One example is a protection system (say Emergency Shutdown or ESD) that is proof tested at regular intervals. Any failure that had occurred between two successive test intervals would be revealed.
2. The failure is unrevealed until the demand occurs. The protection system would not operate if it had failed, but there is no way of knowing this *a priori* if no proof testing is carried out.

A very useful parameter when considering failures in protective systems is the probability of unavailability or probability of failure on demand, known as Fractional Dead Time (FDT). This parameter is a probability and is the average fraction of time that the protective system is unavailable. If the frequency of a demand (demand rate D incidents per unit time) on a protective system is known, then a resulting 'hazard or incident rate' (HR/unit time) can be calculated. For low demand rates and small FDT's, the hazard or incident rate can be obtained by direct multiplication of the demand rate and FDT.

$$\mathrm{HR} = \mathrm{D} \,.\, \mathrm{FDT} \tag{8.14}$$

For revealed faults, a component can be in a failed or operational state when proof testing is carried out. Whether a protective system is working may be assessed from the following:

- If a demand occurs between proof test intervals and the protective system has to operate.
- At the next proof test done to check the system as part of a routine schedule.

The fractional dead time (FDT) of a single component protective system due to component failure is, therefore, a function of both the mean failure rate of the component ($\lambda$) and the proof test interval ($T_p$). The failure rate dictates on the average how often failures occur.

The fractional dead time is given by the expression:

$$FDT = 1 - \frac{1}{\lambda T_p}[1 - \exp(-\lambda T_p)] \tag{8.15}$$

If we expand the exponential series and truncate after the linear term, a simplified expression results as shown below:

$$FDT = 0.5\lambda T_p \quad \text{for} \quad \lambda << 1 \tag{8.16}$$

The above approximation may be interpreted as follows. If it is assumed that failures occur randomly at any time during a proof test interval, then, on average, over a large number of test intervals, a failure could occur halfway through the proof test interval. Within a proof test interval, the average time the system could be in a failed state would then be approximately ($T_p/2$).

In the event of an operator acting as the protection barrier (i.e. responding to an alarm and taking necessary action), the human error probability is directly used in the analysis.

The objective in safe design and operation is to reduce the FDT as much as possible. This can be achieved by either reducing the proof test interval ($T_p$), or by reducing the mean failure rate ($\lambda$) of the component, or both. However, indiscriminate increase in proof testing would not necessarily reduce FDT. Strictly speaking, FDT should take into account the following:

1. $\lambda T_p/2$ (as described above)
2. $\tau$ (duration of the test during which the protection system may have to be disarmed)
3. $\varepsilon$ (human error of leaving protection system disarmed after each test)

Therefore,

$$FDT = (1/2)\lambda T_p + \tau / T_p + \varepsilon \qquad (8.17)$$

If $\tau << T_p$, the term $\tau/T_p$ can be neglected, but $\varepsilon$ may not be negligible.

#### EXAMPLE 8-10 FRACTIONAL DEAD TIME

The failure rate of an emergency shutdown (ESD) valve is, say 0.05 p.a. The proof test interval is once in 6 months (2 tests/year). Each time the test is conducted, the ESD system is disarmed for approximately 1 hour. The general human error probability of omission to re-arm the trip is 0.003 per operation, for a simple but non-routine operation.

Thus, we have:

| | | | | | |
|---|---|---|---|---|---|
| $\lambda$ | = | 0.05 p.a. | $\varepsilon$ | = | 0.003 |
| $T_p$ | = | 0.5 year | FDT | = | 0.0125 + 0.000114 + 0.003 = 0.0156 |
| $\tau$ | = | 1/8760 (year) | | | |

The error in neglecting the last term is 19%.

It is commonly believed that if the system proof-tested more frequently, the reliability would improve. This is correct, but there is a limit to which this can be pushed. Let us assume monthly testing with $T_p = 1/12$ year.

Therefore,

$$\text{FDT} = 0.0021 + 1.14\text{E-}4 + 0.003 = 0.0052$$

In fact, the reliability from monthly testing turns out to be only three times better than half-yearly testing as human error begins to dominate.

If a protective system is never proof tested, the system will continue to degrade until it fails. The probability of failure on demand will increase as a function of time. An approximate formula for calculating the hazard frequency for a system comprising a component which can generate a demand for protection and an untested protection system is:

$$HR = D\lambda / (D+\lambda)$$

**EXAMPLE 8-11 HAZARD RATE FOR REVEALED AND UNREVEALED FAILURES**

Demand Event A (e.g. tank high level) has a frequency of occurrence of D = 0.1 p.a. based on experience.

Protection equipment Item B (high level trip) has a failure frequency of λ = 0.5 p.a.

Revealed Failure. Assume quarterly trip testing interval.

$$HR = D \,.\, FDT$$

$$FDT = 1 - \frac{1}{\lambda T_p}[1 - \exp(-\lambda T_p)] = 0.06$$

Therefore: $HR = 0.1 \times 0.06 = 0.006$ p.a.

Unrevealed failure:

$$HR = D\lambda / (D+\lambda) = 0.083 \text{ p.a.}$$

The quarterly testing reduces the hazard rate for the event by about 14 times compared to no testing. This clearly demonstrates the importance of regular function testing of protection systems, as part of the overall safety management system.

### *8.5.4.2 Analysis of systems with common cause failures*

An implicit assumption made by many analysts in fault tree analysis is to assume that the various inputs to the gates are independent. In practice, this is far from the truth. Therefore, it is essential to identify and treat the common cause issues in the analysis.

Two types of common cause failures are discussed here:

a) a situation where a component contributing to the demand is also used as a protection function (e.g. a control valve being used as a trip valve).
b) a situation where identical redundant components are used in a n-out-of-m voting system, where the components may all have a common failure mode from design or manufacturing defect, yet unknown.

The following example illustrates dependencies of type (a) above.

**EXAMPLE 8-12 QUANTIFICATION OF FAULT TREE IN FIGURE 8-14**

In this example, we have attempted to show how the reliability of a safety function is compromised by having a common system for both the control function and the protection function, as shown in Figure 8-14.

The failure rate data for the various components in Figure 8-14 are listed below:

| | |
|---|---|
| Chlorine control valve (A) | 0.2 p.a. |
| Chlorine flow control system (B) | 0.1 p.a. |
| Ethylene control valve (C) | 0.2 p.a. |
| Ethylene flow control system (D) | 0.1 p.a. |
| Ratio trip failure (E) | 0.005 (FDT) |

The quantified fault tree is shown in Figure 8-15.

The top event frequency is 0.202 p.a. (or once in 5 years). For chlorine release to atmosphere, with potential to cause serious injury and fatality to personnel in the plant, this value is high and unacceptable.

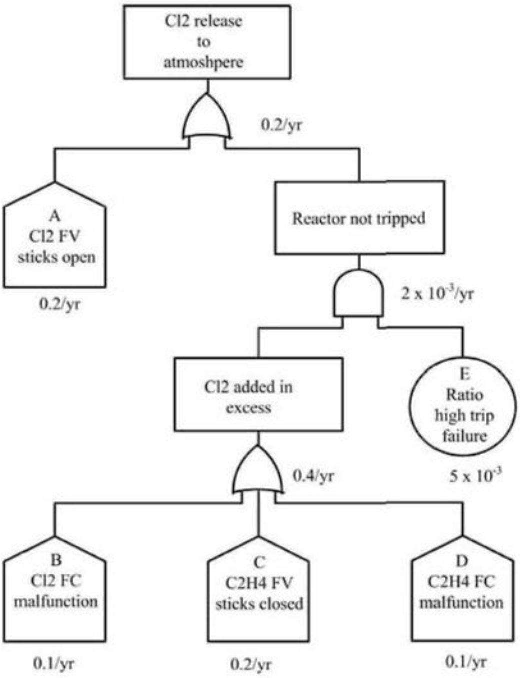


**FIGURE 8-15 QUANTIFICATION OF FAULT TREE IN FIGURE 8-14**

Let us include an independent shutdown valve (F) for chlorine feed, activated by the ratio trip. The FDT for the new shutdown valve is 0.01. The new fault tree is shown in Figure 8-16.

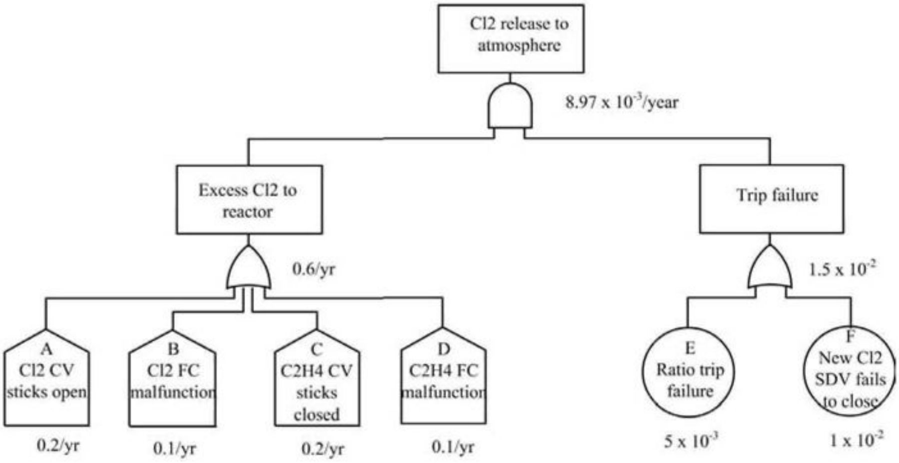


FIGURE 8-16 REACTOR EXCESS FEED PROTECTION REMOVING DEPENDENCE

The top event frequency becomes

$$T = (A+B+C+D). (E+F) = 0.00897 \text{ p.a. (once in 111 years)}$$

There is a 22-fold reduction in the frequency of the top event, by separating the control function and the shutdown function, using independent components. Even this frequency may be high, depending on the acceptance criteria.

One other point needs to be considered. The ratio trip has an implicit dependency as it depends on input from flow measuring elements in the flow control loops, and hence is not independent of the control function. Strictly speaking, independent flow elements need to be provided for each feed, and these should provide input to the logic solver for ratio trip.

Design enhancement to meet risk-based design standards are discussed in Chapter 9 and again in Chapter 13. The above example illustrates how progressive improvements in process safety can be demonstrated by fault tree analysis.

The contribution of dependent failure to overall failure rate is usually insignificant for two different and distinct components. However if diverse systems are not used, then the reliability of the system will be reduced due to the potential for dependent failures (Pan and Nonaka, 1996).

As mentioned in section 8.5.3.2, the Beta factor method can be used to express the degree of common failure modes between two or more components. When two identical pieces of equipment each with a failure rate of $\lambda$, are used for providing redundancy, the combined failure probability is given by:

$$\text{FDT (redundant system)} = (\text{FDT}_C)^2 + \beta. (\text{FDT}_C) \qquad (8.18)$$

where subscript 'c' denotes component. The second term above can sometimes dominate the overall failure probability. The value of $\beta$ is typically in the range (0.05, 0.30).

#### *8.5.4.3 Human error in fault tree analysis*

We have seen elsewhere in the layer of protection analysis that operator response to an abnormal situation is one of the protection barriers against an unwanted occurrence. Therefore, sometimes it becomes necessary to use operator error as one of the base events among the inputs to the protection failure gate. Human error also becomes an input to calculating the FDT, when it comes to failure to re-arm the protection function after proof testing.

One approach to this evaluation is to use task analysis to identify the range of activities involved in the protection function. Depending on the nature, frequency and complexity of the task, and the level of emergency of the abnormal situation, use a generic human error failure probability (see Section 8.7.5). This approach is preferred by the analysts as it enables quantification of the fault tree. However, a decision not to proceed to a higher layer of protection based on such analysis may lead one into a false sense of security, as there are too many variables related to human error and a point probability value oversimplifies the context.

Further discussion on the topic is given in Section 8.7.5.

### 8.5.5 Benefits and Limitations of Fault Tree Analysis

Fault tree analysis offers significant benefits in the area of hazard identification and assessment.

- Fault tree analysis can be used both as a hazard identification tool and as a hazard assessment tool. When used for hazard identification, the qualitative tree describes the logical combinations by which a top event could occur, so that barriers can be developed for the inputs to the various gates.
- The method helps to identify and rank significant contributors to the top event, and thus helps to focus on high profile contributors in developing risk reduction measures.
- By enabling quantification of the likelihood, various risk reduction options can be compared and ranked, and can be used in a benefit-cost analysis for decision making.
- Fault tree analysis can be used for verification of safety integrity level (SIL) of safety instrumented systems at the design stage, and to develop optimum function testing intervals for protection systems reliability maintenance regime.

With all its advantages, fault tree analysis is not without its limitations, arising mostly from the way it is used for quantification. Principal among these are:

- Consideration of dependence and common mode failures. Unless these are identified during the development of the tree, and treated appropriately by Boolean reduction and the use of β-factors for component redundancy, the top event frequency or probability would be erroneous.
- A good failure modes and effects analysis forms the basis for a good fault tree. Failure modes not identified are missing in the logic framework.

- Fault tree analysis can only make limited accommodation of human errors and human factors. Unless the process safety management system is of high quality, especially relating to human factors, a fault tree may yield results that are optimistic and lead to a false sense of security.
- While a fault tree can represent top events in all types of processes, quantification of a fault tree is not appropriate in processes where there are significant man-machine interactions, due to predominant influence of human factors.
- The generic failure rate data for component failures available in databases covers a wide uncertainty range. Therefore, a fault tree analysis using point values of failure probabilities should not be treated as absolute, but used for relative ranking only. A Monte Carlo method in conjunction with fault tree analysis would be required to estimate the degree of uncertainty in the top event frequency calculated.

## 8.6 EVENT TREE ANALYSIS

Event tree analysis is a complementary method to fault tree analysis. While fault tree analysis traces component failures and their logical combinations to the occurrence of a top event, event tree analysis starts with the top event, and follows through the sequence of possible outcomes that can result, depending on whether or not certain conditions along the sequence are fulfilled.

Event trees are primarily safety oriented in nature, being particularly suitable for the analysis of systems where time is a significant factor, for example, when manual intervention can avoid further development of an incident if applied within a specified time, such as opening a quench water valve to quench an exothermic reaction. Working forward in time from the top failure event, the successful operation or failure of each safety function is considered. The course of an initiating event would be decided, depending on the success or failure of each of the hazard control measures in the layers of protection provided.

### 8.6.1 Constructing Event Trees

Construction of an event tree consists of the following steps:

1. Define the initiating event. This can be the top event of a fault tree, or an event relating to loss of containment with or without ignition of hazardous material.
2. List the sequence of layers of protection provided in the facility (both hardware and administrative controls) to control the initiating event. These include detection, isolation, control of ignition, fire protection, explosion protection, pressure protection etc. These are the 'secondary' events of the tree.
3. Starting with the initiating event, develop two branches for the success/ failure of the first layer of protection. This protection forms a node of the event tree.
4. For each branch, apply the next layer of protection, and split each branch into two sub-branches (success/ failure of the 2nd layer of protection).

5. The process is carried on, with each branch doubling as the sequence progresses, until all the layers of protection are exhausted.
6. The final list of branches shows the final possible outcomes from the initiating event. It is possible that the same final outcome can occur in more than one branch. This only indicates the various pathways by which the final event is reached.

The tree is easy to construct, but in some cases, can become unwieldy as the number of nodes increases.

**EXAMPLE 8-13 EXAMPLE OF EVENT TREE FOR SOLVENT BATH**

An electrical equipment manufacturer uses trichloroethylene solvent for degreasing the equipment. The equipment is immersed in the solvent bath, whose temperature is controlled by a heater, equipped with an on/off temperature controller. Should the temperature controller fail, an independent temperature alarm high-high (TAHH) initiates a heater trip. If the trip fails, the bath would overheat and generate toxic vapours. If ignited, a toxic smoke cloud could disperse to populated areas in the neighbourhood.

The event tree is shown in Figure 8-17.

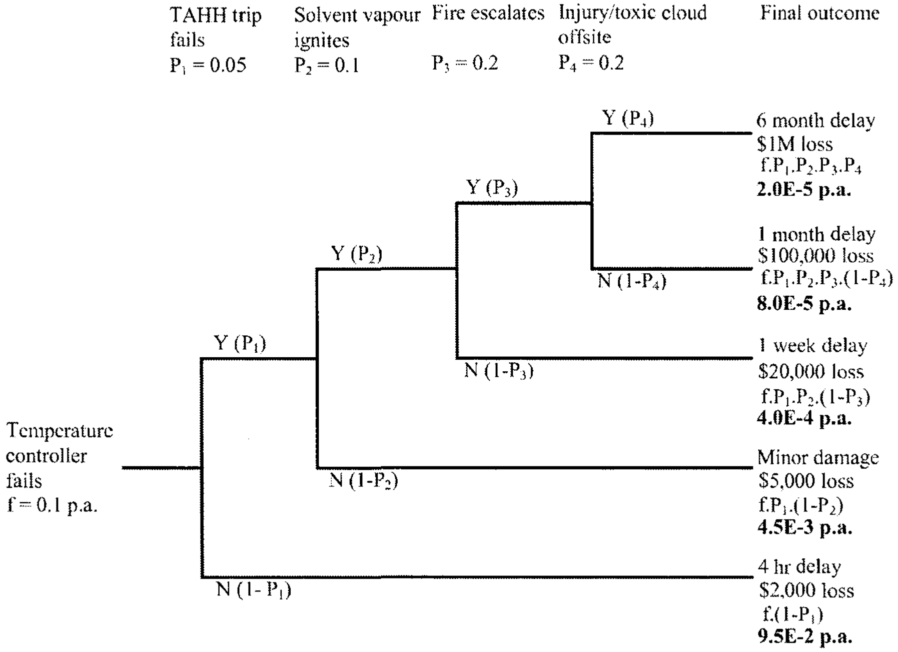

TAHH trip fails $P_1 = 0.05$
Solvent vapour ignites $P_2 = 0.1$
Fire escalates $P_3 = 0.2$
Injury/toxic cloud offsite $P_4 = 0.2$
Final outcome
Temperature controller fails f = 0.1 p.a.
Y ($P_1$)
N (1- $P_1$)
Y ($P_2$)
N (1-$P_2$)
Y ($P_3$)
N (1-$P_3$)
Y ($P_4$)
N (1-$P_4$)
6 month delay $1M loss f.$P_1$.$P_2$.$P_3$.$P_4$ 2.0E-5 p.a.
1 month delay $100,000 loss f.$P_1$.$P_2$.$P_3$.(1-$P_4$) 8.0E-5 p.a.
1 week delay $20,000 loss f.$P_1$.$P_2$.(1-$P_3$) 4.0E-4 p.a.
Minor damage $5,000 loss f.$P_1$.(1-$P_2$) 4.5E-3 p.a.
4 hr delay $2,000 loss f.(1-$P_1$) 9.5E-2 p.a.

FIGURE 8-17 EXAMPLE OF EVENT TREE FOR SOLVENT BATH

### 8.6.2 Quantitative Evaluation of Event Trees

Event tree quantification is much simpler than that for fault trees. The initiating event can be probability or a frequency, often the latter. The node values are success is (1-p). Thus a single node value helps to ascribe probabilities for both branches. FDT estimates as described above would be necessary for determining p, where appropriate.

The frequencies of the final outcomes are obtained by simply multiplying down the chain. Since the initiating event is a frequency and all other node values are probabilities, the final outcome would be expressed as a frequency. Figure 8-17 shows the quantified frequencies of the final outcomes.

A procedure for calculating explosion frequency in offshore oil and gas facilities using event tree analysis has been developed by Andrews et al. (1994). Event tree analysis as applied to dangerous goods transport in road tunnels is described by Saccomanno and Haastrup (2002).

### 8.6.3 Summary and Benefits of Event Tree Analysis

There are several benefits in the application of event trees in hazard assessment.

- Event trees are simple to construct and generally carry only two branches per node (yes/no).
- Event tree provides for one of the best tools for representing the variety of possible outcomes from a single initiating event, depending on the success or failure of the various layers of protection.
- Human interactions in terms of emergency response can be incorporated in the event trees.
- The dynamics of the incident progress (i.e. response time of each layer of protection, and hence cumulative time taken for the layer of protection to operate) can also be represented. This may be compared with time for escalation, so that effective emergency response strategy in terms of hardware and human response can be developed (Raman 2004).
- Quantification of the event tree readily reveals the significant contributor to the final outcome frequency, so that improvement measures can be developed and implemented.
- Event tree analysis is a precursor to quantitative risk analysis, by generating the final outcomes frequencies, which form the input to risk assessment.

## 8.7 FAILURE DATA

### 8.7.1 Data Availability

Failure data can be obtained from two principal sources:

- In-house records
- Generic databases

Data from an organisation's own operations records, when applied to that same process or facility is the most accurate data available. Data from other similar facilities within the same corporation or other industry sources is still better than generic data, as this reflects a wider database of similar corporate practices.

Unfortunately, in-house records of sufficient sample size to provide statistical significance are seldom available. The population size of equipment and components is small, and a long period of time is required to obtain statistically significant failure data for low frequency events.

Where in-house data is not available, or is not statistically valid, generic data from reliable databases have to be used.

## 8.7.2 Typical Data Sources

There are a number of databases in the literature for equipment failure rates. Some databases have been updated regularly such as the offshore reliability data, but others data back to the mid 1990's.

**Lees (2001)**

This source provides a selection of failure rate data published in the literature. It includes failure rate data used in the Rasmussen Report and data given by Smith in 'Reliability and Maintainability in Perspective'. In most cases however the data is not presented in sufficient detail to show failure modes, and equivalent hole sizes for leaks. Experienced judgement is required in the use of this data.

**Cox et al. (1991)**

This source reviewed leak frequency data for common equipment items in chemical process industries and obtained "best estimate" values. The authors used the "best estimate" values in a fire and explosion model and adjusted them until reasonable values were obtained for not only overall frequencies of fire and vapour cloud explosions, but also for the relative contribution of different fluid phases and individual leak sources. Hole size distributions are also given for the leak frequency data.

**IEEE Std 500 (1984)**

This database covers electrical, electronic, sensing component, and mechanical equipment reliability data for nuclear-power generation industry. The majority of failure rate data expresses equipment reliability, although some records include leak frequencies. The information is now dated, but is still a useful basis where more recent data is not available.

**CCPS (1989)**

This source provides generic reliability data for common process equipment. The database was compiled from a large number of data resources, principally from the nuclear industry but including the transport, natural gas, government and military, offshore oil and gas and chemical process industries. Leak frequency data is given for selected components in the database. However since the database is not independent but rather was constructed from other databases including OREDA and IEEE, it was not referenced for leak frequencies.

### OREDA 2002

The Offshore Reliability Data Handbook (OREDA) was prepared using maintenance records for offshore oil and gas installations in the Norwegian and UK sectors of the North Sea, and installations in the Adriatic Sea. The main emphasis is on reliability data, although some records do include loss of containment and leakage. Since environmental conditions play a significant role in the reliability of equipment, direct use of OREDA data for downstream process industry applications, especially in non-marine environments is not appropriate. Details are available at http://www.sintef.no/oreda/handbook.

### The Oil Industry E&P Forum (DNV Technica 1992, E&P Forum 1996)

This database is a compilation of failure rate data submitted by members of the Oil Industry International Exploration and Production Forum (E&P Forum). The database presents leak frequencies for common equipment items based on a review of data sources. The majority of data is based on records from the offshore oil and gas industry. As a companion, the quantitative risk analysis (QRA) datasheet directory was compiled by E&P Forum as a reference document for data and information used in risk assessments. In addition to summarizing the hydrocarbon leak and ignition database, the section on process leak and ignition includes a summary of leak frequency data.

### UK HSE Database

The Health & Safety Executive in the UK publishes offshore hydrocarbon release statistics (HSE 1997, 2000, 2001), mainly for use in the preparation of offshore safety cases and in quantitative risk analysis. The data is categorised into the type of hydrocarbon, severity of the release and type of installation.

### NPRD-95 (RAC 1995)

This database contains extensive reliability data on non-electronic components, along with failure modes, sample size and sample duration. Compiled mainly from military applications, its applicability to process industry must be limited to areas where no other process industry related data is available.

### British Telecom (1984)

British Telecom Handbook of reliability data for electronic components used in telecommunications systems. This reference contains electronic reliability failure rates (with grading of data sources) under the following headings: semiconductors, thick film circuits and hybrids; capacitors; fixed resistors; variable resistors; relays; wound components; attenuators; piezo electric devices; printed wiring boards; joints; connectors; display devices; keys; switches; surge protectors; optical fibre devices.

### MIL-HDBK-217F (1991)

This classic reference contains electronic component reliability failure rates. The data applies mainly for defence equipment which requires a much higher reliability for a one-off use, and may not be relevant for risk assessment of industrial installations. The handbook quotes base failure rate values for most electronic equipment together with scaling factors to take account of the most significant factors affecting these rates (operating temperature, etc).

### Other literature sources

There are a number of individual papers in the literature focusing on specific industry sectors. Useful references are:

- Blything and Reeves (1988) - Liquefied Petroleum Gas industry
- Smith and Warwick (1985) - Process pressure vessel failures
- Pape and Nussey (1985) - Failure frequencies of vessels, pipework and gaskets used in a risk assessment of a chlorine installation.
- Scarrone and Piccinini (1989) - This reference includes rates of regulator, pilot, slam shut valve, cut off valve, vent valve, filter; causes of failures include failure of diaphragms, seals (parts of the above).
- Dawson (1994) - European Gas Pipeline Incident Data Group (EGPIDG)
- Papadakis (1999) - References to onshore pipeline failure rate data
- Crawley et al. (2003) - References to onshore and offshore pipeline failure rate data
- World Offshore Accident Databank (WOAD) (DNV 1999)

One has to exercise extreme caution in quoting a number for failure rates from generic data in published literature, unless the original data source is verified and is valid. The following anecdote, narrated to one of us by the late Bert Lawley, the inventor of the HAZOP technique, illustrates the point. Lawley said:

> "I was writing a paper in which I had to emphasize the need to take the failure mode into account when using a generic failure rate. I wrote: 'Let us say that the failure rate of a valve failing open is 0.1 per year. Now this value may not apply to a valve failing fully open, as experience shows that most failures occur at the seat. Therefore, it may be more appropriate to split the failure rate and say that full bore failure could occur at 0.01 per year, and 10% of cross-sectional area open at 0.09 per year.'
>
> "Some years later, I needed specific data on this very subject, and asked my assistant to approach an organisation whether it could undertake a literature search for the specific data. A week later, the organisation responded, recommending the use of 0.1 per year for fail open case, with a 90/10 split for full bore and partial failures.
>
> When my assistant brought this result to me, I was intrigued as this is the very data I would have used based on experience, and asked my assistant to investigate the source of the data. To our amusement, the paper cited was that by one Lawley, the very paper I had published a few years before !"

### 8.7.3 Data Quality

When generic statistical data is used, it is essential to ensure that it is of adequate quality and of relevance to the application (Mancini 1978, CCPS 2000). The following points are of interest:

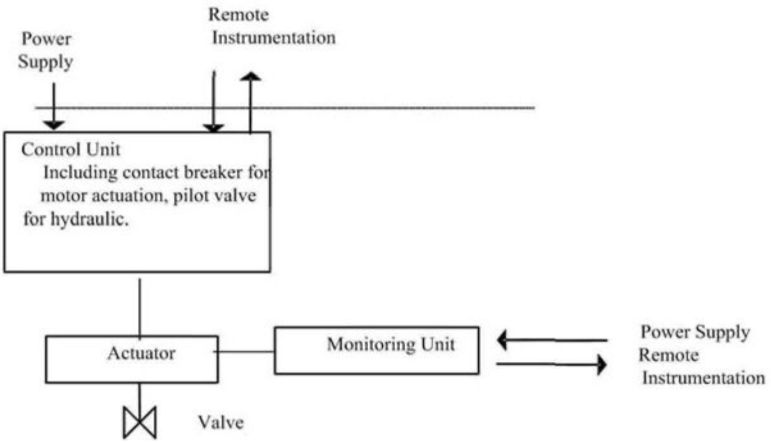
- Do not look for top event frequencies directly in the databases. The incidents are few and are normally the outcomes of various complex interactions, and may not apply to the analysis in question.
- Do not use component reliability data bases directly for major incident frequencies. These are to be used mainly as input to fault tree analysis.
- Review the source data for completeness and independence. The historical period must be of sufficient length to provide a statistically significant sample size.
- Different data sources may be compared to select the best estimate, but combining databases from different sources can lead to error as incidents could be duplicated.
- Check for data applicability. The historical record may include data over long periods of time (5 or more years). As the technology and scale of plant may have changed in the period, careful review of the source data to confirm applicability is important. This is particularly true of older databases such as IEEE Std 500.
- Be extremely careful if adjustments are made to historical data using an environmental factor, or based on management quality. It is easily possible to make over-confident assumptions.
- The underlying focus should always be 'industry best estimate', rather than optimistic or pessimistic estimates.
- Be aware of the range of uncertainty in the data. This may span two to three orders of magnitude.
- Be consistent in the application of the data, so that comparisons of results of analysis can be made on a common basis. When such comparisons are required, the relative values among the options become important rather than absolute numbers.

An example of how to select the data for specific failure modes is provided below.

**EXAMPLE 8-14 DATA SELECTION FOR FAILURE MODE**

The failure rate data for an emergency shutdown valve of an oil gas well on an off-shore production platform is given below (OREDA 2002). The operational mode is normally open and fail-safe-close. The internal operating environment is crude oil, gas or water. The external environment is marine, partially enclosed or in the open.

Item Boundary Specification: It is essential to note the boundary for the specification of failure rates. All items within the boundary (indicated by box) are included in the failure rate.



The failure rate data is shown in Table 8-5, selectively taken from an earlier edition of OREDA (1992), to illustrate the point.

TABLE 8-5 FAILURE RATE DATA FOR OFFSHORE ESD VALVE

| Taxonomy no. 1.2.1.3 | | Item: Process Systems/ Valves/ ESD | | | |
|---|---|---|---|---|---|
| Population | Installations | Aggregated time in service ($10^6$ hours) | | | |
| 322 | 12 | Calendar time *<br>6.4065 | | | |
| Failure mode | | No. of failures | Failure rate (per $10^6$ hours) | | |
| | | | Lower | Mean | Upper |
| Critical | | 64 | 6.46 | 9.17 | 12.29 |
| External leakage | | 2 | 0.09 | 0.28 | 0.85 |
| Faulty indication | | 4 | 0.25 | 0.56 | 1.26 |
| Fail to close | | 27 | 2.77 | 3.81 | 5.24 |
| Fail to open | | 15 | 1.36 | 2.12 | 3.25 |
| Internal leakage | | 1 | 0.03 | 0.14 | 0.63 |
| Overhaul | | 2 | 0.09 | 0.28 | 0.85 |
| Significant external leakage | | 1 | 0.03 | 0.14 | 0.65 |
| Seepage | | 1 | 0.03 | 0.14 | 0.63 |
| Significant internal leakage | | 7 | 0.00 | 1.12 | 2.64 |
| Spurious operation | | 3 | 0.17 | 0.43 | 1.06 |
| Unknown | | 1 | 0.02 | 0.14 | 0.65 |

The extracted data for various failure modes is shown in Table 8-6.

TABLE 8-6 EXTRACTED DATA FROM DATABASE

| Failure Mode | Reasons for Selection | Failure Rate x $10^6$ Hours (Mean) |
|---|---|---|
| External Leakage | Includes leakage and significant leakage. An ignition has serious downstream safety consequences | 0.56 |
| Fail to Close | Unable to isolate a downstream leak. Potentially serious. | 3.81 |
| Internal Leakage | Includes seepage, leakage and signification leakage. If a leak occurs downstream of valve, isolation may not be effective. | 1.26 |
| Unknown | Since it is listed as a critical failure and failure mode not known, better to include for conservative assessment. | 0.14 |
| Total | | 5.77 |

Spurious operation is listed as a failure mode. Since the valve is normally open, a spurious operation would refer to an unwanted closure. This would be a production interruption risk, but not a safety risk as being closed is the 'fail-safe' position for the valve.

Degraded failures include external leakage, but this would only be very small (otherwise it gets into the critical list), and can be handled safely by a planned shutdown for maintenance.

Out of the 9.17 failures per $10^6$ hours (critical failures, first line of Table 8-5), only 5.77 in $10^6$ hours (63%) contribute to a safety risk (failure to close on demand).

## 8.7.4 Estimating Failure Rates from Sample Population Data

Where in-house maintenance data is available for equipment and components, a statistical distribution may be fitted to the raw data. The processed data will provide the mean failure rate (for use in fault tree analysis), as well as the variance indicating the "spread" of the distribution and associated uncertainty.

### *8.7.4.1 Probability distributions*

The failures that occur during the useful life of an equipment are random failures. This means that a failure could occur at any time, and would not follow a set pattern. There are a number of probability distributions to represent failure rates and reliability data (O'Connor 1991, Lees 2001) of these, three distributions are used extensively in reliability analysis.

### *8.7.4.2 The reliability curve*

For many items, particularly electronic, the relationship of failure rate versus time can be modelled by the Weibull Distribution (commonly referred to as the "bathtub" curve as shown in Figure 8.18). The relationship conforms empirically to many processes. The bathtub curve is widely quoted in the reliability literature, but it should be emphasised that its applicability to all types of equipment, particularly mechanical equipment, is not established.

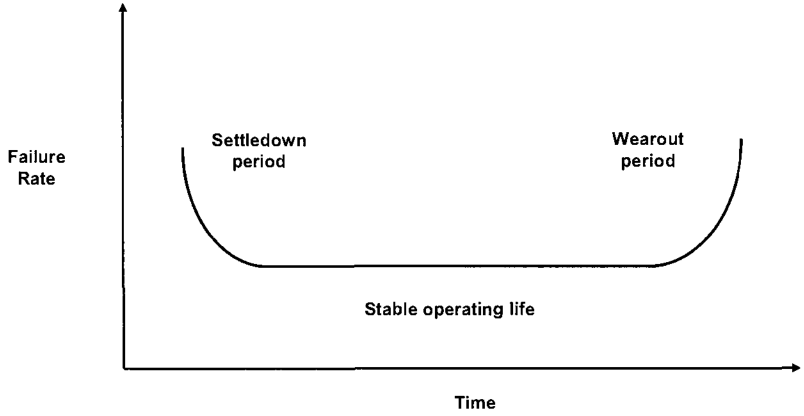


FIGURE 8-18 RELIABILITY BATH-TUB CURVE

In general, the failure behaviour of an equipment exhibits three stages:

Region 1: The equipment failure rate is relatively high. Such failure is usually due to factors such as defective manufacture, incorrect installation, learning curve of equipment user, etc. Most systems are designed to have a short or zero in service (by means of 'running-in' tests or commission, etc.) and a long useful life or Region 2 period.

Region 2: The equipment failure rate declines during normal operation until a constant rate is reached. Failures appear to occur purely by chance. Over this period the failure rate is essentially constant. This period is known as the "useful life" of the component. When reliability is of concern, arrangements are usually made to withdraw components from service before the wear-out phase begins.

Region 3: The equipment failure rate rises again as deterioration sets in, often described as wear-out failure.

### 8.7.4.3 Weibull distribution

The three regions represented by the reliability curve are together described by the 2-parameter Weibull distribution, with parameters $\eta$ and $\beta$.

Failure density function:

$$f(t) = \frac{\beta}{\eta}\left(\frac{t}{\eta}\right)^{\beta-1} \exp\left[-\left(\frac{t}{\eta}\right)^{\beta}\right] \tag{8.19}$$

Mean:

$$\mu = \eta\Gamma\left(1+\frac{1}{\beta}\right) \tag{8.20}$$

where Γ represents the Gamma function.

Variance:

$$\sigma^2 = \eta^2\left\{\Gamma\left(1+\frac{2}{\beta}\right) - \left[\Gamma\left(1+\frac{1}{\beta}\right)\right]^2\right\} \tag{8.21}$$

#### 8.7.4.4 Gamma distribution

The Gamma distribution is an alternative to the Weibull distribution. It also has 2-parameters (a and b), and simpler to use.

Failure density function:

$$f(t) = \frac{1}{b\Gamma(a)}\left(\frac{t}{b}\right)^{a-1} \exp\left(-\frac{t}{b}\right) \tag{8.22}$$

Mean

$$\mu = ba \tag{8.23}$$

Variance

$$\sigma^2 = b^2 a \tag{8.24}$$

#### 8.7.4.5 Negative exponential distribution

A reliability assessment often concentrates on Region 2 of the curve (useful life), since a piece of equipment is likely to be replaced by the time it reaches Region 3, based on a maintenance regime of monitoring and inspections. In Region 2, the failure rate is constant over the period of time. In other words, a failure could occur randomly regardless of when a previous failure occurred (i.e. no previous memory). This results in a negative exponential distribution for the failure frequency. Therefore, the failure rates used in fault tree analysis are the means of the negative exponential distributions. Obviously, this treatment is simplistic in the sense that the data sources for the failure rates may contain failures from Regions 1 and 3 as well.

Failure density function:

$$f(t) = \lambda \exp(-\lambda t) \tag{8.25}$$

Mean:

$$\mu = \frac{1}{\lambda} \tag{8.26}$$

Variance:

$$\sigma^2 = \frac{1}{\lambda^2} \tag{8.27}$$

A system comprised of components that are represented by the exponential distribution in series is also exponentially distributed. However, a system comprised of components exponentially distributed, but in any redundancy configuration is not exponentially distributed. The assumption of exponential distribution of a system in redundant configuration can lead to serious error (Murphy et al. 2002).

The use of negative exponential distribution has increasingly come into question as it is often not possible to establish when the useful life ends and the wear-out phase begins. Further, repair time distributions are definitely non-exponential. When fitting repair time distributions for maintenance data for system availability analysis (see Chapter 13), the log normal, Gamma or Weibull distributions are known to represent the data more accurately.

#### 8.7.4.6 $\chi^2$ test for goodness of fit

When a statistical distribution is fitted to a set of data, it is necessary to ensure that the distribution used is statistically valid. This is ascertained by the $\chi^2$ - test. In a sample population of $n$, for each observed value $x_i$, the corresponding expected value $E_i$ is calculated from the fitted distribution. The $\chi^2$ value is then calculated from

$$\chi^2 = \Sigma \ (x_i - E_i)^2/\mathrm{E_i} \qquad \text{(with n-1 degrees of freedom)} \tag{8.28}$$

If the $\chi^2$ value falls above the 90th percentile, then the distribution is considered valid for the set of data. Details are given in O'Connor (1991) and OREDA (2002).

### 8.7.5 Representation of Human Error in Fault Tree Analysis

A human error is an action that fails to meet some limits of acceptability as defined for a system. This may be a physical action (e.g. closing a valve) or a cognitive action (e.g. fault diagnosis or decision making). Human errors have been classified in the following categories (HSC, 1991).

a) Skill-based errors, are those arising during the execution of a well-learned, fairly routine task, such as calibration, testing, responding to process alarm etc.
b) Rule-based errors, are those that occur when a set of operating instructions or similar set of rules is used to guide the sequence of actions; either they are followed, or misunderstood, or a wrong sequence

is used such as not following the startup/shutdown procedures, preparation for maintenance, permit to work system, and the like

c) Knowledge-based errors which arise when a choice decision has to be made between alternative plans of action. Examples are decision making in an emergency - shutdown or continue to operate or fire fighting versus evacuation.

Human reliability analysis is concerned with the qualitative and quantitative analysis of human error and its subsequent reduction. However, predicting human error is a complex and difficult task and human reliability approaches have had great difficulties in demonstrating their accuracy and validity, often receiving criticism from various theoretical and practical viewpoints (Williams 1986, Dougherty and Fragola 1988, IAEA 1990, HSC 1991, Gertman et al. 1992).

There are various factors which affect human performance commonly referred to as Performance Shaping Factors (PSFs) (Swain and Guttman, 1983). Those considered to be of most importance are:

- Critical equipment control design;
- Training of operators;
- Communication and procedures;
- Instrumentation feedback and design;
- Preparedness (expected frequency of situation); and
- Stress.

When assessing the contribution of human error to a potential loss event, two distinct stages in the accident sequence should be considered: pre-accident and post-accident. The probability of human error which results in a hazardous situation which can lead to an accident is dependent on the status of the process safety factors in the operator's environment.

Two techniques are commonly used for human error rate predictions:

THERP:

1. Technique for Human Error Rate Prediction by Swain and Guttman (1983)

HEART :

2. Human Error Assessment and Reduction Technique (Williams 1986)

When estimating human error using the THERP handbook, the Performance Shaping Factors (PSFs) may be used to modify the value. A sample set of factors is provided in Table 8-7. The list is not exhaustive. A method of extracting PSFs from empirical data sources is described by Hallbert et al. (2004).

The HEART technique is similar to THERP. A HEART database is provided for nine generic task types. A basic error probability for each task type is assigned with upper and lower bounds. This value can be modified using a multiplier, from a selection of error producing conditions (similar to PSFs).

An abridged set of general guidelines for estimating the probability of operator error for various situations is listed in Table 8-8. More details are available in HSC (1991).

TABLE 8-7 SAMPLE PERFORMANCE SHAPING FACTORS

| **Human Error Factors:** | |
|---|---|
| 1 | Relatively frequent data logging |
| 2 | Single operator with no communication with others |
| 3 | High activity periods on plant |
| 4 | Unnecessary equipment cluttering control area |
| 5 | Radio communication effectiveness |
| 6 | Noisy environment |
| 7 | Personnel in noisy areas or wearing ear protection can hear alarms |
| 8 | Ergonomic hardware design in the control room |
| 9 | Satisfactory substitution of absentees (sickness, leave) |
| 10 | Frequency of absenteeism |
| 11 | Procedures for operator communication of options/accidents/near misses |
| 12 | Environment for personnel to communicate easily with superiors |
| 13 | Management well informed of actions and problems at operator level |
| 14 | Messages are unambiguous and unlikely to be misinterpreted |
| 15 | Team training in the transfer of information |
| 16 | Team training in Operations/emergency |
| 17 | Average number of yrs of experience of operations personnel |
| 18 | Degree of automation |
| 19 | Control system/operator interface design satisfactory |
| 20 | Alarms and trips data logged and sequenced |
| 21 | Remote isolation of critical valves |
| **Organisational Factors:** | |
| 22 | Can any process trips be bypassed by operator? |
| 23 | Use of temporary labels |
| 24 | Diagnosing alarms |
| 25 | Log books/plant records are up to date and readily available |
| 26 | Separation of regular and exceptional data |
| 27 | Formal communication procedures for all tasks |
| 28 | Clear procedures for handover between shift changes |
| 29 | System for instructions to be easily understood and followed |
| 30 | Operating instructions formally authorised |
| 31 | Use of occasional instructions |
| 32 | Emergency equipment in good order |
| 33 | Permit to work system and its effectiveness |
| 34 | Near-miss or incident reporting system |
| 35 | "Structured" approach to incident reviews |
| 36 | Incident information acted upon |
| 37 | Written safety policy |
| 38 | Degree of policy implementation |
| 39 | Formal change management system |
| 40 | Regular training of operators |
| 41 | Regular training in emergency procedures |
| 42 | Regular review of workforce performance |

The probability of human error in providing the correct response to an abnormal situation in the initial stages of high stress conditions is very high, and gradually reduces over time, as the person regains composure. This is shown in Figure 8-8.

While Table 8-8 and Figure 8-19 provide an apparently easy way out for the analyst intent on quantification, the human reliability data issue is not an easy one. The link between PSF and error probability is not clearly established. A good review of current research knowledge in human reliability quantification is provided by Sträter and Budd (1999) and Sträter (2004).

Once an accident sequence has started, the most important variable is the time the operators have to detect and correct errors. The chances of operators detecting and correcting a problem are better when they have 3 hours than if they have 3 minutes, before a serious condition results. Before a corrective action can be taken the operator must firstly, detect the problem; secondly, diagnose the problem and decide on a course of action, and; thirdly, implement the desired response.

**TABLE 8-8 GENERAL ESTIMATES OF PROBABILITY OF HUMAN ERROR (SOURCE: HSC 1991)**

| Estimated Error Probability | Activity |
|---|---|
| 0.001 | Pressing the wrong button. Error is not decision based, but one of loss of inattentiveness or loss of concentration. |
| 0.003 - 0.01 | General human error or commission, errors of omission, with no provision for reminder for error recovery. e.g. misreading label and therefore selecting wrong switch, forgetting to re-arm trip after function testing. |
| 1.0 | Conditional probability of error in a 2nd task, given an error in the 1st task, when two coupled tasks are carried out by the same person. |
| 0.1 | Failure to check plant condition after shift handover, in the absence of a written handover procedure or a checklist. |
| 0.5 | Failing to detect abnormal conditions during plant walk-through surveillance, in the absence of a specific checklist. |
| 0.2 - 0.3 | General error rate given very high stress levels where dangerous activities are occurring rapidly. |

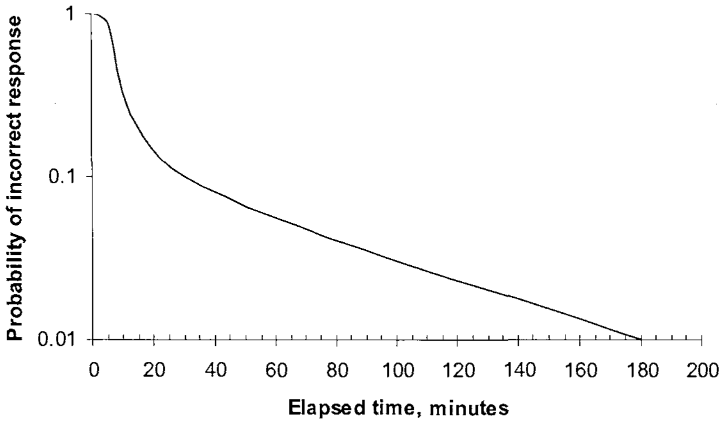


**FIGURE 8-19 PROBABILITY OF FAILURE BY CONTROL ROOM PERSONNEL TO CORRECTLY DIAGNOSE AN ABNORMAL EVENT**

## 8.8 UNCERTAINTY IN FREQUENCY ESTIMATION

### 8.8.1 Sources of Uncertainty

The main source of uncertainty lies in the failure rate data available. Some of these are listed blow.

- Most failure rates quoted are based on a negative exponential distribution, and may not be applicable for existing facilities with ageing equipment.
- The failure rates quoted in generic sources generally include an upper and lower bound on the failure rate, and the spread is rather large. Considerable judgement needs to be exercised in selecting a value within the given range.
- Many generic estimates are based on all failure modes reported in the maintenance history. However, in a particular application only one mode may be relevant. For instance, if isolation of inventory is the base event, then the failure mode is the shutdown valve failing to close. If the failure data includes the valve failing to open, then without splitting between failure modes, the likelihood estimate based on an all-mode value would tend to be pessimistic.
- Severity of the application and operating environment significantly influence the reliability. When selecting estimates to use, consideration should be given to the mode of operation, utilisation factor and design margins.
- The quality of maintenance practices on a site significantly affects the failure rate. The critical failure rate can be considerably reduced if incipient failure or degraded performance, which can be tolerated, is detected and the item repaired before complete loss of function occurs.
- One area of uncertainty is that the true extent of dependence in common cause failures is never known. This can, to some extent, be accommodated by the use of the β-factor, but the value of β used itself is subjective.
- The FDT calculation implicitly assumes that when a failure is detected during the function test, it is immediately rectified and the function restored. Experience has shown that in a number of accidents (Kletz 2001) a failed protective function had been left unrepaired for significant periods. Thus, an FDT based on immediate repair of a detected failure provides optimistic results, and a false sense of security. This also illustrates the point that without an effective SMS in place, a reliability analysis is meaningless.
- The inclusion of human error probability in numerical estimates has inherent uncertainties. While the THERP and HEART techniques have partial validation, the empirical modifications using PSFs or other multipliers is still based on judgement, and not fully proven.
- The use of quantification techniques for software reliability assessment is not appropriate. Extensive testing for software validation is still the accepted method in the industry, and by regulatory agencies. This particularly applies to programmable electronic systems used to carry out safety instrumented functions such as emergency shutdown. International

agencies such as TÜV undertake the testing and certification of such systems for various manufacturers.

## 8.8.2 Assessing Uncertainty

Two methods are often used for assessing the uncertainty in likelihood estimates. These are briefly described below. A more detailed discussion on decision making under uncertainty is provided in Chapter 11.

### *8.8.2.1 Sensitivity analysis*

The first method is to conduct a sensitivity analysis, using different failure rates within the range of data available, to determine which of the data has a significant impact on the final outcome. The data that have most influence on the top event frequency should be reviewed if the uncertainty band can be reduced.

Even if reduction in uncertainty is not possible, a sensitivity analysis provides the upper and lower bounds of the frequency within which the top event frequency may lie. This sensitivity analysis can be carried forward into the risk assessment.

### *8.8.2.2 Monte Carlo methods*

Another method of estimation of uncertainty is to use a Monte Carlo method as part of the fault tree or event tree analysis. Software packages are available that can carry out such simulations.

In this approach, instead of a point value for failure rate or probability, a probability distribution with its parameters is selected. The simulation generates random numbers using the specified probability distribution, evaluates the top event frequency for each random number used as input, analyses the output data and provides a mean value with values for specified confidence intervals.

Details are provided in Vose (2000), with recommended approach for stochastic analysis.

## 8.9 REVIEW

In this Chapter, we have presented the concepts of estimating the likelihood of occurrence of hazardous incidents. The distinction between probability and frequency has been highlighted. Techniques for both qualitative estimates and quantitative estimates have been presented. In both situations, adoption of a time frame is a pre-requisite for frequency estimation.

The cause consequence representation is an ideal tool for frequency estimation. This can be done either through the bow-tie diagrams, or a combination of a fault tree and an event tree, joined together by the top event. The fault tree is a top-down approach, starting from the top event and tracing the causes and combinations of causes that lead to the top event. The event tree is a bottom-up approach, starting from the top event, and tracking the various potential outcomes, depending on the success or failure of the various layers of protection against the realisation of the hazard impact.

A simplified approach to fault tree quantification using Boolean algebra was introduced. For complex fault trees, it is wise to use software that can generate the minimum cutsets.

Available data sources for generic failure rate data have been listed. One has to be aware of the uncertainty band associated with the generic data, while using point data for failure rates. Where a sample population of failures are available, some simple statistical distributions to fit the data have been introduced.

It has been emphasized that the uncertainty in risk estimation introduced by frequency analysis is significantly higher than that introduced by hazard effects and vulnerability analysis. Therefore, the estimated frequencies should not be treated as absolute, but best used for comparison of alternative options in managing risk.

Some methods of including human error contribution in incident likelihood estimation have been discussed. This provides a simple approach to quantification, but in reality, is more complex.

## 8.10 REFERENCES

Andrews, J., Smith, R. and Gregory, J. 1994, 'Procedure to calculate the explosion frequency for a module on an offshore platform', *Transactions of Institution of Chemical Engineers*, Part B, Process Safety and Environmental Protection, vol. 72, pp. 70-82.

British Telecom 1984, *Handbook of Reliability Data for Electronic Components used in Telecommunications Systems*, Issue 3.

Blything, K.W and Reeves, A.B. 1988, *An Initial Prediction of the BLEVE Frequency of a 100 Tonne Butane Storage Vessel*, Safety & Reliability Directorate, UKAEA.

Center for Chemical Process Safety (CCPS) 2000, *Guidelines for Chemical Process Quantitative Risk Analysis,* 2nd edn, American Institute of Chemical Engineers, New York.

Center for Chemical Process Safety (CCPS) 1989, *Guidelines for Process Equipment Reliability Data,* American Institute of Chemical Engineers, New York.

Center for Chemical Process Safety (CCPS) 1992, *Guidelines for Hazard Evaluation Procedures,* American Institute of Chemical Engineers, New York.

Cox, A.W., Ang, M.L., and Lees, F.P. 1990, *Classification of Hazardous Locations,* IChemE, Rugby, UK.

Crawley, F.K., Lines, L.G. and Mather, J. 2003, 'Oil and gas pipeline failure modelling', *Transactions of Institution of Chemical Engineers,* Part B, Process Safety and Environmental Protection, vol. 81, pp. 3-11.

Dawson, F.J. 1994, 'EGPIDG European Gas Pipeline Incident Data Group - Gas Pipeline Incidents', presented by F.J. Dawson - British Gas, at the *International Gas Union Conference*, Milan, Italy, June.

DNV Technica 1992, *Hydrocarbon Leak and Ignition Database*, E&P Forum Report No. 11.4/180, May.

DNV 1999, *WOAD - World Offshore Accident Databank*, Det Norske Veritas, PO Box 300, 1322, Hovik, Norway.

Doelp, L.C., Lee, G.K., Linney, R.E. and Ormsby, R.M. 1984, 'Quantitative fault tree analysis gate-by-gate metred', *Plant/Operations Progress*, vol. 3, pp. 227.

Dougherty, E.M. and Fragola, J.R. 1988, *Human Reliability Analysis: a Systems Engineering Approach with Nuclear Power Plant Applications*, John Wiley, New York.

Edwards, G.T. and Watson, I.A. 1979, *A Study of Common Mode Failure*, Safety & Reliability Directorate, Report R-146, UKAEA.

Fussell, J.B. 1976, 'Fault tree analysis: concepts and techniques' in *Generic Techniques in Systems Reliability Assessment,* eds. E.J. Henley and J.W. Lynn, Noordhoff, Leyden, The Netherlands, p.133.

Gertman, D.I., Blackman, H.S., Haney, L.N., Deidler, K.S. and Hahn, H.A. 1992, ' "INTENT"– A method for estimating human error probabilities for decision-based errors', *Reliability Engineering and System Safety*, vol. 35, pp. 127-136.

Green, A.E. and Bourne, A.J. 1972, *Reliability Technology*, John Wiley.

Hallbert, B., Gertman, D., Lois, E., Marble, J., Blackman, H. and Byers, J. 2004, 'The use of empirical data sources in HRA', *Reliability Engineering and System Safety*, vol. 83, pp. 139-143.

Health and Safety Executive, 1998, *Offshore Hydrocarbon Releases Statistics 1997*, Offshore Technology Report OTO 97 950.

Health and Safety Executive 2000, *Offshore Hydrocarbon Releases Statistics and Analysis 2000*, Offshore Technology Report OTO 2000 112, December.

Health and Safety Executive,2001, *Offshore Hydrocarbon Releases Statistics 2001 for the Period 1-10-92 to 31-3-01*, Hazardous Installations Directorate.

HSC 1991, *Study Group on Human Factors - Second Report: Human Reliability Assessment - A critical Overview,* Advisory Committee on Safety of Nuclear Installations, Health & Safety Commission, HMSO, London.

Institute of Electrical and Electronics Engineers. *Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power Generating Stations*, Institute of Electrical and Electronics Engineers, New York. IEEE:1984, IEEE Std-500.

International Atomic Energy Agency. *Human error classification and data collection*, IAEA, Vienna. TECDOC 5.38:1990.

Kirschsteiger, C. 2001, "How frequent are major industrial accidents in Europe?", *Transactions of Institution of Chemical Engineers*, Part B, Process Safety and Environmental Protection, vol. 79, pp. 206-210.

Kletz, T.A. 2001, *Learning from Accidents,* 3rd edn, Butterworth-Heinemann, Oxford.

Lee, W.S., Grosh, D.L., Tillman, F.A. and Lie, C.H. 1985, 'Fault tree analysis, methods, and applications - a review', *IEEE Transactions on Reliability*, vol. R-34, no. 3, pp. 194-203.

Lees, F.P. 2001, *Loss Prevention in the Process Industries*, Butterworths-Heinemann, Oxford.

Mancini, G. 1978, *Data and Validation*, C.E.C. Joint Research Centre, ISPRA, Italy, RSA 12/78, June.

Murphy, K.E., Carter, C.M. and Brown, S.O. 2002, 'The exponential distribution: the good, the bad and the ugly - A practical guide to its implementation', *IEEE 2002 RAMS Conference*.

O'Connor, P.D.T. 1991, *Practical Reliability Engineering*, 3rd edn, John Wiley.

OREDA 2002, *Offshore Reliability Data Handbook*, Prepared by SINTEF Industrial Management, Distributed by Det Norske Veritas, Hovik, Norway.

Pan, Z. and Nonaka, Y. 1996, 'Importance analysis for the systems with common cause failures', *Reliability Engineering and System Safety*, vol. 50, pp. 297-300.

Papadakis, G.A. 1999, 'Major hazard pipelines: a comparative study of onshore transmission accidents', *Journal of Loss Prevention in the Process Industries*, vol. 12, pp. 91-107.

Pape, R.P. and Nussey, C. 1985, 'A basic approach for the analysis of risks from major toxic hazards' in *The Assessment and Control of Major Hazards, Institution of Chemical Engineers Symposium Series No.93*, pp.367-387.

Raman, R. 2004, 'Accounting for dynamic processes in process emergency response using event tree modelling', *19th CCPS International Conference*, June 29-July 1, Orlando, Florida, pp. 197-213.

Reliability Analysis Centre 1995, *NPRD-95: Non-electronic Parts Reliability Data*, RAC, Rome, NY.

Saccomanno, F. and Haastrup, P. 2002, 'Influence of safety measures on the risks of transporting dangerous goods through road tunnels', *Risk Analysis*, vol. 22, no. 6, pp. 1059-1069.

Scarrone M and Piccinini, N. 1989, 'A reliability data bank for the natural gas distribution industry' in *Reliability data collection and use in risk and availability assessment*, ed. V. Colombari, *Proceedings of the 6th Euredata conference, Siena, Italy*, March 15-17, pp. 90-103.

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

Sträter, O. 2004, 'Considerations on the elements of quantifying human reliability', *Reliability Engineering and System Safety*, vol. 83, pp. 255-264.

Sträter, O. and Budd, H. 1999, 'Assessment of human reliability based on evaluation of plant experience: requirements and implementation', *Reliability Engineering and System Safety*, vol. 63, pp. 199-219.

Swain, A.D. and Guttman, H.E. 1983, *A handbook on Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications*, USNRC, Nurge/CR-1278, Washington, D.C., Sandia National Laboratories.

The Oil Industry International Exploration & Production Forum (E&P Forum) 1996, *Quantitative risk assessment datasheet directory*, E&P Forum Report No. 11.8/250, October.

Tweeddale, H.M. 2003, *Managing risk and reliability in process plants,* Gulf Professional Publishing.

US Department of Defense. *Military handbook - Reliability Prediction of Electronic Equipment*, US Department of Defense. MIL-HDBK-217F:1991.

Vesely, V.E., Goldberg, F.F., Roberts, N.H. and Haasl, D.L. 1981, *Fault Tree Handbook*, Nuclear Regulatory Commission Report, NUREG-0492, USA.

Vose, D. 2000, *Risk Analysis: A Quantitative Guide*, John Wiley.

Watson, S.R. 1994, 'The meaning of probability in probabilistic safety analysis', *Reliability Engineering and System Safety*, vol. 45, pp. 261-269.

Williams J.C. 1986, 'HEART – A Proposed Method for Assessing and Reducing Human Error' in *9th Advances in Reliability Technology Symposium*, University of Bradford, England.

Yellman, T.W. and Murray, T.M. 1995, 'Comment on 'The meaning of probability in probabilistic safety analysis' ', *Reliability Engineering and System Safety*, vol. 49, pp. 201-205.

## 8.11 NOTATION

| | |
|---|---|
| AS | Australian Standard |
| BLEVE | Boiling Liquid Expanding Vapour Explosion |
| $C_2H_4$ | Ethylene |
| CCPS | Center for Chemical Process Safety |
| $Cl_2$ | Chlorine |
| cw | cooling water |
| D | Demand Rate |
| E&P | Exploration and Production |
| EGPIDG | European Gas Pipeline Incident Data Group |
| ESD | Emergency Shutdown |
| ETA | Event Tree Analysis |
| FC | Flow Controller |
| FDT | Fractional Dead Time |
| FE | Flow Element |
| FT | Flow Transmitter |
| FTA | Fault Tree Analysis |
| FV | Flow Valve |
| HAZOP | Hazard and Operability Study |
| HEART | Human Error Assessment and Reduction Technique |
| HR | Hazard Rate |
| HSC | Health & Safety Commission (UK) |
| HSE | Health & Safety Executive (UK) |
| IAEA | International Atomic Energy Agency |
| IEEE | Institute of Electrical and Electronic Engineers |
| LI | Level Indicator |
| LSH | Level Switch High |
| LTIR | Lost Time Injury Rate |
| MIL-HDBK | Military Handbook |
| NPRD | Non-Electronic Parts Reliability Data |
| OH&S | Occupational Health & Safety |
| OREDA | Offshore Reliability Data |
| P&ID | Piping & Instrumentation Diagrams |
| pa | per annum |
| PPE | Personal Protection Equipment |
| PSF | Performance Shaping Factor |
| PSV | Pressure Safety Valve |
| QA | Quality Assurance |
| QRA | Quantitative Risk Analysis |
| SMS | Safety Management System |
| T | Function test interval, Top event |
| TAHH | Temperature Alarm High High |
| THERP | Technique for Human Error Rate Prediction |
| TÜV | Technischer Ueberwachungs Verein (Technical Supervision Society, Germany) |
| WOAD | World Offshore Accident Data |
| $\beta$ | $\beta$ - factor |
| $\varepsilon$ | Human error rate |

| | |
|---|---|
| $\lambda$ | Component failure rate |
| $\mu$ | Mean of statistical distribution |
| $\sigma^2$ | Variance of statistical distribution |
| $\tau$ | Duration of function test |

This page is intentionally left blank

# 9 RISK ESTIMATION

*The best-laid plans o' mice an' men*
*Gang aft a-gley,*
*An' lea'e us nought but grief an' pain,*
*For promised joy.*

*Robert Burns*

In this chapter, we shall discuss the estimation of risk. The concept of risk has been described in Chapter 1, and some ways of expressing risk outlined in Chapter 2. Generally, risk is a vague and ambiguous term and writings on risk tend to be correspondingly oracular in nature. We shall follow the definition in Chapter 1, relating to the process industries.

*Risk is the likelihood of a specified undesirable event occurring within a specified period or in specified circumstances* (Jones 1992*).*

Generally risk is expressed as a frequency, e.g. number of specified events per unit time. We find the following formula often quoted in the literature

Risk (Consequence/unit time) = (Consequence/event)×Frequency (event/unit time)

Sometimes risk is also expressed as a probability, e.g. probability of a specified event for a certain condition.

## 9.1 DEVELOPING RISK ESTIMATES

The results of the consequence and frequency analysis are combined for each outcome of each individual event, to obtain a measure of risk associated with each outcome. These risk contribution from each of the events may be summed to provide the total risk for the installation.

An estimate of risk can be qualitative or quantitative. Further, risk assessment component of overall process safety assessment takes its input from hazard identification (hazard register), consequence analysis results and frequency estimations, and provides a risk estimate as the output. Tixier et al. (2002) have reviewed 62 methods available, and have classified them into qualitative and quantitative, and deterministic and probabilistic. These have been referred to as risk analysis methodologies, but many cover all the precursor input to actual risk estimation, and can be more appropriately called process safety analysis tools.

In this chapter, the estimation of risk takes into account that the hazard register (from Chapter 4), consequence analysis results (Chapter 5 to 7) and frequency estimates (from Chapter 8) are already available.

### 9.1.1 Benefits of Risk Estimation

Measuring the risk either qualitatively or quantitatively serves the following purposes:

- For each category of risk, the risks of incidents can be ranked to identify the major risk contributors and provide a sound basis for risk management.
- The calculated risk levels can be compared with risk targets or criteria and/or the historical risk level of the industry, company or other installations.
- The significance of the calculated risk levels can be reconciled with risks from other activities.
- The risk levels of different design/operating options can be compared.
- Decisions can be made whether or not a certain level of risk is tolerable or whether or not to proceed with a project.

There is no single standard method of risk measurement and presentation. The most suitable method(s) depends on the information and resources available, the objectives of the risk assessment and the intended audience.

### 9.1.2 Basic Data Required for Risk Estimation

From the foregoing discussion, it is seen that there are two fundamental quantities required for risk estimation:

- magnitude of the event consequence
- likelihood of the event

The data may be qualitative or quantitative, depending on the measure required.

### 9.1.2.1 *Qualitative estimate*

For qualitative estimation of risk, the following information is required (see Section 3.4):

- Severity scale of the event
- Probability scale of the event

The risk matrix is often used to assign the risk level.

### 9.1.2.2 *Quantitative estimate*

For quantitative estimation of risk, the information requirement varies, depending on whether the effect of the event is omni-directional (i.e. independent of wind speed and direction and hence radially uniform) or multi-directional (i.e. dependent on meteorological conditions).

**Omni-directional incidents:**

These include pool fire, BLEVE, and vapour cloud explosion. Jet fires can also be omni-directional where release direction cannot be clearly ascertained.

- hazard radius, R (distance of impact to specified receptor, as discussed in Chapters 6 and 7).
- frequency of the event, f . For pool fires or jet fires, this would be release frequency times ignition probability.
- probability p of the specified impact on the vulnerable receptor from the event

For a given size of a flammable cloud, the vapour cloud explosion effect itself is omni-directional, but the cloud size and cloud drift depend on meteorological conditions.

**Uni-directional incidents:**

These include flash fire (dispersion of flammable vapour and ignition with no explosion effect), and toxic gas impact. Known direction jet fires can be regarded as uni-directional.

- probability of wind speed and associated Pasquill stability class for each wind direction. Generally the wind rose is divided into 8, 12 or 16 sectors), depending on the accuracy required.
- hazard zone dimensions for each category of wind speed/Pasquill stability class combination. The hazard zone is normally modelled as an ellipse, and

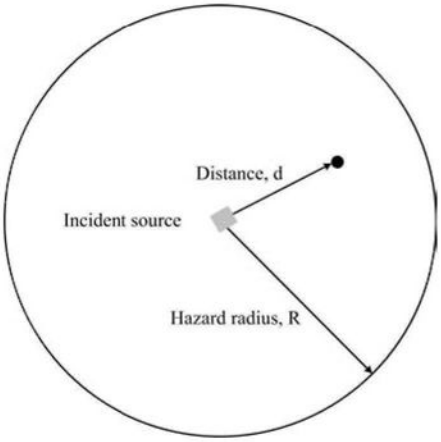
the data requires the major axis and semi-minor axis of the ellipse (isopleth length and maximum half-width from dispersion calculations)

- frequency of the event (e.g. for toxic release, this would be release frequency; for flash fire, this would be release frequency times ignition probability corresponding to the cloud size for the wind speed/weather stability class)

### 9.1.3 Procedures for Risk Estimation

#### *9.1.3.1 Omni-directional incidents*

The risk Ψ of a specified vulnerability at a given distance 'd' from the event source is calculated as follows (see Figure 9-1):



a) For $0 < d \leq R$ $\quad \psi = f.p$ (9.1)

b) For $d > R$ $\quad \psi = 0$ (9.2)

**FIGURE 9-1 RISK FOR AN OMNI-DIRECTIONAL INCIDENT**

#### *9.1.3.2 Uni-directional incidents*

In the case of uni-directional incidents, the downwind isopleth (contour of constant concentration) obtained from gas dispersion analysis looks like two differently shaped ellipses, sharing a common minor axis. However, it is represented for convenience as a single ellipse, with the isopleth length as the major axis and maximum half-width as the minor axis.

The hazard zone in this case is the area within the ellipse. Since the isopleths would be different for different wind speed/Pasquill stability classes, different hazard zones are created for each wind/weather category (see Figure 9-2).

Since the wind can be any one of the 12 or 16 directions chosen, the isopleth has to be evaluated downwind each time.

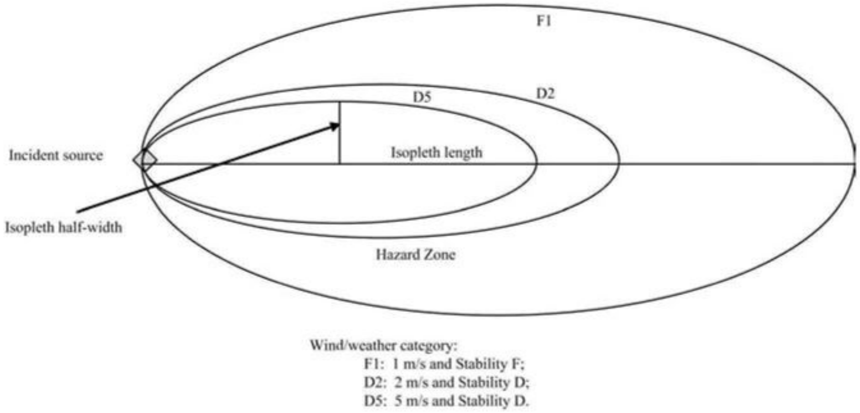


FIGURE 9-2 RISK FOR UNI-DIRECTIONAL INCIDENT

For a given wind speed/weather stability class, and wind direction, the risk is calculated in a manner similar to the omni-directional incident.

If the location of concern is within the hazard zone, then

$$\psi = f.p_{ws}.p_{wd} \tag{9.3}$$

where

$f$ = release frequency (p.a.)
$p_{ws}$ = probability of wind speed/stability class
$p_{wd}$ = probability of wind direction

If the location of concern is outside the hazard zone, then $\psi = 0$. More details on risk calculations are given in Section 9.4.

## 9.2 QUALITATIVE TECHNIQUES FOR RISK ESTIMATION

### 9.2.1 Risk Matrices and Variants

The characterisation of the risk associated with events developed in the hazard identification stage may be conducted using the *risk matrix* (see Section 3.4). The risk matrix is a graphical representation of the risk as a function of probability and consequence, and is very useful for a qualitative assessment and ranking of risks to enable priorities to be allocated.

A typical risk matrix has been presented in Figure 3-8 in Chapter 3. The matrix has five rows and five columns as shown. The rows show events of decreasing severity from top to bottom, and events of increasing probability from left to right. The matrix elements are grouped into four risk categories, Extreme (E), High (H), Moderate (M) and Low (L).

Risk ranking can be devoted to the following four areas:

- safety of personnel and public
- environmental impact
- financial impact (asset loss and loss of revenue)
- financial impact (down time and loss of revenue)

There are a number of variants to the risk matrix shown in Figure 3-8. These cover a 4x4 matrix and a 3x3 matrix, depending on the coarseness of the assessment.

Risk matrices can be used in two principal ways:

(i) The severity and frequency estimates can be performed for the situation where the effect of protective systems is not considered. This gives a "raw" risk score. Further semi-quantitative approaches such as layer of protection analysis (LOPA) can then be used to estimate final residual risk (see section 9.3.1)

(ii) The severity and frequency estimates incorporate all barriers of protection to produce a residual risk estimate directly on the matrix.

The particular approach needs to be clearly stated in the use of risk matrices.

### 9.2.2 Rule Sets for Severity and Likelihood Ranking

Rule sets should be developed for placing an unwanted outcome in a particular cell in the risk matrix. The rankings suggested for probability and consequence are shown in Tables 3-2 and 3-3 respectively in Chapter 3.

The rule sets can be modified to meet the corporate philosophy and risk criteria.

### 9.2.3 Risk Ranking and its Use

The advantage of the risk matrix is that events which require priority action from management to reduce it from an 'extreme or high risk' to 'moderate or low risk' can be easily seen using this graphical method.

The following general philosophy is suggested for managing risks:

- There should be no incidents in the matrix in the 'very high' risk category. In other words, all 'very high' risk incidents should be reduced to at least 'high' risk level.
- Every effort should be made to reduce 'high' risk incidents to 'medium' or lower. The ALARP principle (As Low As Reasonably Practicable) for risk reduction would apply in this instance.
- Effort should be made to reduce the 'medium' risk incidents to 'low'. Once again, the ALARP principle for risk reduction would apply.
- The residual risk should be maintained at that level and managed through the safety management system (SMS) and its effective implementation (see Chapters 11 and 14).

Sometimes the risk of an incident ranked as 'medium' in terms of safety impact on people can be 'high' in terms of loss of revenue from downtime. In such a case, additional expenditure to reduce the risk may be justified. The risk reduction in this case is a commercial decision, and if carried through, implicitly enhances safety as well. Hence the saying, "safety is good business".

The risk category is sometimes referred to as the "risk index".

### 9.2.4 Problems and Pitfalls in Using the Risk Matrix

The risk matrix is an elegant and easy-to-use tool, and does not require specialist training - that is how it appears on the surface. In fact, there are number of areas where the risk could be incorrectly addressed. If major decisions are made on the basis of the risk matrix and its findings alone, it is possible that either some high risks are not addressed at all due to incorrect screening, or incorrect allocation of priorities may occur.

This section highlights some of the dangers of incorrect use of the risk matrix.

1. Incorrect rule set for the range of safety consequences. If we use the matrix for OH&S alone, the range of consequence would vary from first-aid injury to disability and potentially a single fatality. Whereas, if the matrix is used for major hazards, the range would vary from lost time injury to multiple fatalities. It is difficult to cover the full range in a matrix of 5 or less cells for consequence category, without crowding the incidents in a few cells.
2. Incorrect rule set for range of financial loss. For a large transnational corporation, the loss of up to $1M may be in the 'moderate' category, but for a small to medium-size company, the same loss can be in the 'critical' category.
3. Incorrect rule set for likelihood range. For OH&S, the likelihood scale would cover a higher frequency (several times a year to one chance in 10 or 100 per year), whereas for major accident events, the scale could ranges from once a year to one chance in 10000 per year).
4. Incorrect specification of likelihood for a given consequence. For instance, the sequence of events resulting in an offsite fatality could be initial loss of containment of toxic material, failure to detect and isolate, and toxic impact offsite. The likelihood of the initiating event (release) could be rated as 'likely', but by time the chain of events is covered, the likelihood of the fatality could be rated 'rare'. The assessment is subjective, and therefore, the adequacy and effectiveness of the hazard control measures along the accident chain can be pre-judged without sufficient justification, giving a false sense of safety.
5. When there is doubt about the location of an event in a given matrix cell, it is always placed in a higher severity or higher likelihood cell, as the case may be, in order to be conservative.
6. Inadvertently screening out a potential higher risk incident. Incidents involving loss of containment of scheduled hazardous materials should always be treated as major accident events (at least 'high' risk initially),

as these have a potential to cause fatalities, and at the initial stage of assessment, the adequacy of the control measures and their effectiveness is unknown. Assumptions may have to be made, which must be subsequently verified and validated.

It should be remembered that the risk matrix approach is a screening tool. All 'high' and 'extreme' risk incidents identified in the risk matrix should be subjected to a next level rigorous analysis before decisions are made as to whether or not the risk is at ALARP level, and whether the hazard control measures provided are adequate. Layer of protection analysis (LOPA) in section 9.3.1 can be used to resolve some of the risks initially rated high or above by considering the available protection layers.

A qualitative ranking of incidents using a disaster value was suggested by Christen et al. (1994). This method, based on fuzzy set theory, can account for impact on people, ecosystems and property. The method does not address incident likelihood and hence is not suitable for risk ranking.

### 9.2.5 Risk Graphs and Calibration

A method for developing the requirements for functional safety of Safety Instrumented Systems (SIS) was developed by the Instrumentation, Systems and Automation Society (ISA) in the USA in 1996 (ANSI/ISA 1996). This was subsequently expanded into an international standard by the International Electrotechnical Commission (IEC 1998), and further extended to process industry sector (BS IEC 61511: 2003).

The functional safety requirement is specified in terms of a Safety Integrity Level (SIL). Safety integrity is defined as the probability of a Safety Instrumented System satisfactorily performing its function under all stated conditions within a stated period of time (ISA 2002).

The assessment of SIL comes under reliability estimation described in Chapter 8. However, the allocation of SIL to a safety function is essentially risk based. There is no single method for allocation of SIL and the following approach is based on IEC 61508 (IEC 1998). Different organisations have adapted this standard to suit their needs (EPSC 2000).

The risk graph method is based on a qualitative assessment of risk, using the standard equation

$$R = f.C \tag{9.4}$$

where

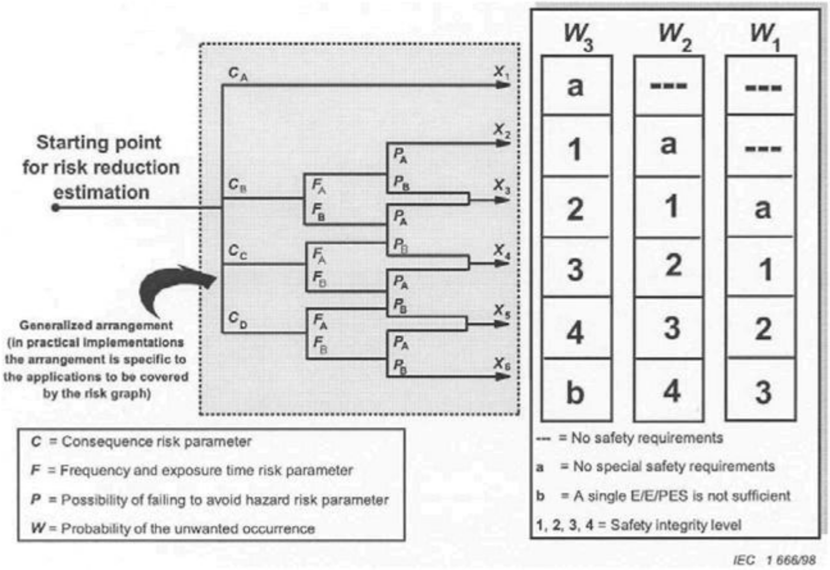
$R$ = risk with no safety-related system in place;
$f$ = frequency of the hazardous event with no safety-related system in place; and
$C$ = consequence of the hazardous event (the consequences could be related to harm associated with health and safety personnel, environmental damage, or asset damage and impact on operations)

The frequency of the hazardous event ($f$) is made up of three parameters:

1. Occupancy or fractional exposure time (F) in the hazardous zone (rare to more frequent or frequent to continuous). Generally, a fractional exposure time of < 10% is taken as rare to more frequent, and >10% is taken as frequent to continuous (UKOOA 1999, BS IEC 61511-2003).
2. Possibility of failing to avoid the hazardous event (P). The following requirements must be satisfied to select the probability of avoiding the consequence (BS IEC 61511.3-2003).
   - The operator will be alerted if the SIS has failed (i.e. fault alarm or revealed failure)
   - Facilities are provided for avoiding the hazard *that are separate to the SIS* and that enable escape from the hazardous area (safety category)
   - The time elapsed between the operator's alert to a hazardous condition and the occurrence of the event is longer than 1 hour or is definitely sufficient for the necessary actions.

   The above requirements are generally hard to meet, and therefore, in using the risk graph, the path for "No possibility to avoid the hazardous event" is chosen more often.
3. Frequency of unwanted occurrence (W). This is also the demand rate on the safety-related system to operate, and has to be assessed from information gathered in a HAZOP or FMEA study, and operational experience.

Based on the above parameters, the risk graph in Figure 9-3 may be used to allocate a SIL. In order to use Figure 9-3, we need to define a qualitative rule set for the risk parameters, as listed in Table 9-1.


Starting point for risk reduction estimation
$C_A$
$C_B$
$C_C$
$C_D$
$F_A$
$F_B$
$P_A$
$P_B$
$X_1$
$X_2$
$X_3$
$X_4$
$X_5$
$X_6$
Generalized arrangement (in practical implementations the arrangement is specific to the applications to be covered by the risk graph)
$W_3$
$W_2$
$W_1$
a
---
---
1
a
---
2
1
a
3
2
1
4
3
2
b
4
3
IEC 1 666/98

C = Consequence risk parameter

F = Frequency and exposure time risk parameter

P = Possibility of failing to avoid hazard risk parameter

W = Probability of the unwanted occurrence

--- = No safety requirements

a = No special safety requirements

b = A single E/E/PES is not sufficient

1, 2, 3, 4 = Safety integrity level

[redacted]

FIGURE 9-3 RISK GRAPH FOR SIL ALLOCATION (SOURCE: IEC 61508, REPRODUCED WITH PERMISSION)

[redacted]

TABLE 9-1 RULE SET FOR RISK PARAMETERS FOR SIL ALLOCATION

| Levels<br>Parameter | A | B | C | D |
|---|---|---|---|---|
| Consequence - Safety | $C_A$: Lost time injury | $C_B$: Disability injury/single fatality | $C_C$: Multiple fatalities | $C_D$: Catastrophic |
| Consequence - Environment | $C_A$: Local spill - contained | $C_B$: Onsite environmental impact - temporary impact | $C_C$: Major cleanup required - temporary impact | $C_D$: Catastrophic long term environmental damage |
| Consequence - Revenue loss/Asset damage | $C_A$: Short duration production loss/minor damage | $C_B$: Up to 1 week production loss/medium damage | $C_C$: Extended shutdown/major damage | $C_D$: Catastrophic, potential for loss of facility |
| Exposure | $F_A$: Rare to more frequent | $F_B$: Frequent to continuous | - | - |
| Probability of independent alternative to avoid danger | $P_A$: Independent alternative available | $P_B$: No independent alternative available | - | - |
| Demand Rate* | $W_1$: Low (< 1/30 p.a.) | $W_2$: Medium (1/30 to 1/3 p.a.) | $W_3$: High (> 1/3 p.a.) | - |

* Based on UKOOA (1999), BS IEC 61511.3 (2003)

| Levels<br>Parameter | A | B | C | D |
|---|---|---|---|---|
| Demand Rate* | $W_1$: Low (< 1/30 p.a.) | $W_2$: Medium (1/30 to 1/3 p.a.) | $W_3$: High (> 1/3 p.a.) | - |

* Based on UKOOA (1999), BS IEC 61511.3 (2003)

Because of choosing the $P_B$ route instead of the $P_A$ route for 'probability of independent alternative to avoid danger', the SIL determined is generally conservative. SIL values, which represent the probability of failure on demand for the SIS are given in Table 9-2.

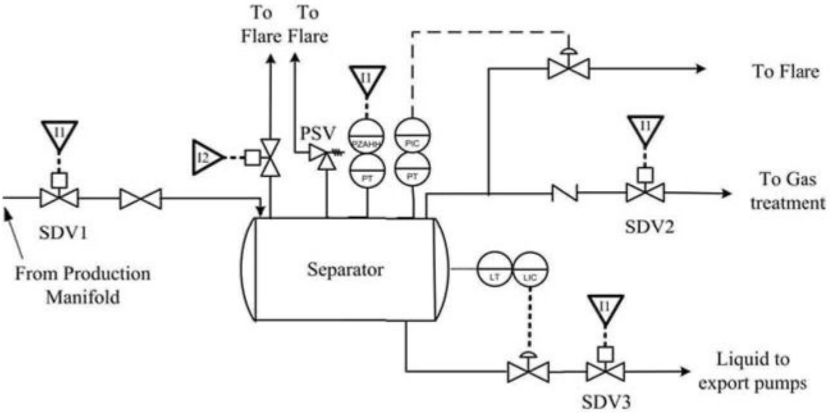
If a SIL 3 or SIL 4 is assessed using the risk graph, then the validity of this determination needs to be checked using the Layer of Protection Analysis (LOPA), as described in Section 9.3.2. SIL 4 determinations would not be implemented in process situations and other alternatives to reduce risk would be considered.

### EXAMPLE 9-1 SIL ALLOCATION FOR PRESSURE PROTECTION

A pressure vessel in an offshore oil and gas facility is equipped with a pressure safety valve (PSV) in accordance with the pressure vessel code requirements. Should the PSV discharge, it may not reseat properly and would create operability problems. Therefore, it is the requirement of API RP 14C (2001) that a safety instrumented system be installed as the first line of defence, with the PSV acting as the last line of defence. An operator or maintenance personnel could be present on deck for approximately 25% of the time during the shift.

The instrumented protection system is shown in Figure 9-4. It consists of a pressure sensor (1 out of 2 voting system), and a pressure high interlock to close the shutdown valve at the vessel inlet.

During normal operation, the vessel is controlled by both a pressure control loop and a level control loop, independent of the SIS, with high pressure and high level alarms.



Notes: 1. Pressure High interlock I1 shuts valves SDV 1, 2 and 3.
2. Interlock I2 for emergency depressuring through SDV4 to flare is manually initiated.

FIGURE 9-4 SIMPLIFIED P&ID OF SEPARATOR VESSEL

It is required to allocate a SIL value to the SIS.

- Consequence ranking: In the absence of a protection system, there is a potential for pressure vessel rupture, causing extended shutdown and major damage. Loss of containment of high pressure gas could result in an explosion with potential for multiple fatalities. There would also be environmental spill of oil to the sea surface (depending on the level of plating and drainage provided on the deck). Using Table 9-1, the following ranking may be allocated:
  Safety: $C_C$ (in the event of explosion); Environment: $C_B$; Asset damage/production loss: $C_C$. We choose $C_C$ as being the conservative estimate of all of the categories.
- Exposure: $F_B$ (frequent to continuous)
- Probability of alternative: $P_B$ (criteria in Section 3.2.5, Item 2 is not satisfied).
- Demand (how often will the SIS will be called upon to act): $W_3$

From the risk graph in Figure 9-3, we get SIL = 3.

We find that once overpressurisation has occurred, the PSV would discharge and provide pressure relief. The PSV is generally given an equivalent SIL of 2 (based on a regular preventive maintenance and testing regime), and hence the SIL required of the SIS would only be SIL 1.

As a sensitivity case, assume that the PSV is not sized to relieve the full inflow into the vessel, but only part of the flow (vapour). Therefore, the risk graph would require that the SIS be designed to SIL 3 requirement. This is a rigorous requirement, and would require significant redundancy.

One of the reliability estimation methods described in Chapter 8 may be used to calculate the probability of failure of SIS on demand, and verify that SIL 3 can be achieved by the SIS. ■ ■ ■

If we take a closer look at Figure 9-3, we can see that the risk graph allows for catastrophic events (Category D) to be protected by SIS, taking the SIL to a level of 4, if necessary. This is the frequency reduction approach for risk reduction, for fixed consequences. In contrast, UKOOA (1999) has taken the attitude that catastrophic events should be eliminated by inherently safer design (ISD), and therefore no SIL is applicable for Category D level. This is a prudent approach to adopt even for on-shore process plants. A brief discussion on inherent safety is provided in Chapter 12.

There are two major issues associated with the use of risk graphs:

a) Appropriate calibration of the risk graph
b) Justification as to why one should not go for a higher SIL value that that given by the risk graph.

### 9.2.6 Limitations of Qualitative Risk Estimates

In order to address the above issues, one needs to define a target risk, and work backwards to ensure that the SIS would achieve the target risk. Wass and Calder

(2004) provide some guidance on calibrating the risk graph based on risk targets. Target risk setting is described in Section 9.5.2. The risk graph is calibrated on the principle that a site's residual societal risk should lie in the middle of the tolerable region. Extrapolating the societal risk back to a single fatality, from amongst all the personnel at a plant, a single fatality every 100 years is taken as the single point of reference of acceptable residual risk for calibration of the risk graph. This residual risk must take account of all hazard scenarios on the plant, with potential to cause a single fatality. If the number of such hazardous scenarios is, say 10 per plant, then the acceptable residual risk from a single hazard scenario is once every 1,000 years. The necessary risk reduction for each box of the risk graph is established by dividing the target residual risk by the demand rate, probability of personnel being present (1.0 or 0.1) and probability of personnel avoiding harm (1.0 or 0.1). For example, if the demand rate is 0.1 per year, a person is likely to spend more than 10% of the time in the plant and there is no alternative to avoid the harm, then the SIL should be allocated to give a probability of failure on demand of 1 in a 100, or SIL 2. For events that can cause multiple fatalities (say 10), the SIL goes up by one level (i.e. the target risk comes down by one order of magnitude). The question of why do we stop with the allocated SIL level, and why not design for a higher level, is based on a cost-benefit analysis, and is described in Chapter 12.

Qualitative estimate of risk is useful for raking and setting priorities, but poses some limitations for effective decision making. Some of these are discussed below:

1. Calibration of risk matrix rule set. The allocation of risk ranking for an event is subjective in many instances, and may not be sufficient for decision making, especially if significant capital expenditure is involved, or major safety issues are involved.
2. Crowded cell. A number of events may receive 'high' ranking, and fall into the same cell in the risk matrix. Relative ranking between these events is not possible without some form of quantification. In attempting a refinement, we have seen some people naively trying to place events in different corners of the same cell! This practice is not recommended as it only adds more subjectivity to uncertainty.
3. Pitfalls in the qualitative assessment are already discussed in Section 9.2.4. Further, if a high SIL value (SIL 3 or 4) is obtained in the first pass, it does not automatically mean that a sophisticated SIS should be designed. The system can be subject to a Layer of Protection Analysis (LOPA) to determine whether or not such a high SIL is correct or justified (Marszal and Scharpf 2002). LOPA is discussed further in Section 9.3.
4. Events with high SIL values. Where the risk is judged to be high, requiring SIL 3 or above for an SIS, the assessment has to be reviewed rigorously for the assumptions involved. It was mentioned earlier that for catastrophic events (Consequence level $C_D$), UKOOA (1999) guidelines require inherently safer alternatives to be developed. A properly calibrated risk graph would produce reliable results (Timms 2003).

The main advantage of a qualitative approach is that it narrows down the field requiring quantification, thus reducing overall efforts required, as quantification is elaborate and time and resources consuming. In the case of SIL allocation, it can be verified by quantification, thus minimising uncertainty.

## 9.3 SEMI-QUANTITATIVE TECHNIQUES FOR RISK ESTIMATION

There are several techniques that sit between a qualitative and fully quantitative approach to risk estimation as seen in Figure 2-1. The most prominent of the semi-quantitative methods that has found significant use is the Layer of Protection Analysis (LOPA) method developed by the Dow Company (CCPS 2001). The next section describes the method and its application.

### 9.3.1 Layer of Protection Analysis (LOPA)

The Layer of Protection Analysis (LOPA) is based on the philosophy that for an initiating event, several independent protection layers (IPLs) can be developed and implemented, and that if a layer fails, there is another layer that would provide the protection function. This was seen in Chapter 3, Figure 3-7. The method provides a useful screening tool for more in-depth quantitative studies.

LOPA is similar to event tree analysis (see Chapter 8), with the difference that only the failure branches are traced at each layer (Marszal and Scharpf 2002). The risk quantification is similar to quantifying an event tree, by multiplying the probabilities along the chain. The primary initiating frequency can be arbitrarily set as 1, so that the final probability is the conditional probability of the specified outcome, given that the initiating event has occurred. If quantitative risk is required, then this conditional probability is multiplied by the primary initiating frequency.

LOPA focuses on a single event with a nominated consequence to assess the adequacy of the IPLs.

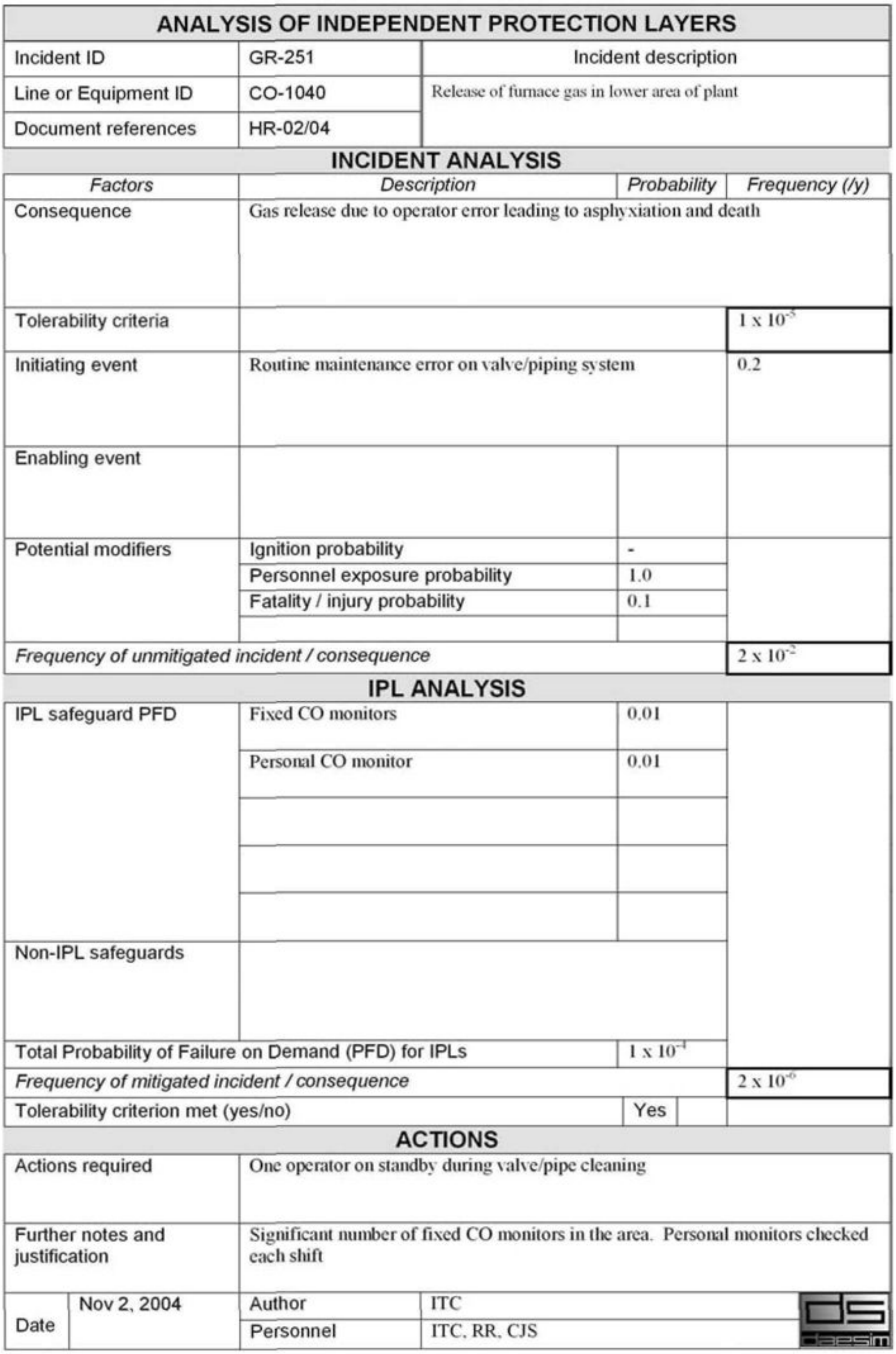
The consequence category must be clearly defined and can cover all those listed in Table 3-3 such as:

(i) Personnel or public injury or fatality
(ii) Environmental impairment
(iii) Social and heritage impacts
(iv) Plant and equipment damage
(v) Business and customer impacts
(vi) Legal impacts
(vii) Reputation and outrage impacts

To enable the LOPA method to be applied in a semi-quantitative risk estimation mode it is necessary to use existing risk tolerability targets for personnel and public fatality or injury or establish in-house targets for other risk categories.

Figure 9-5 shows a typical LOPA study sheet that can be used for documentation purposes.

The accident propagation sequence of Section 9.3.1 can be viewed as a form of LOPA, where Figure 9-5 can be represented in the form of an event tree of failure branches.



## ANALYSIS OF INDEPENDENT PROTECTION LAYERS

| | | |
|---|---|---|
| Incident ID | GR-251 | Incident description |
| Line or Equipment ID | CO-1040 | Release of furnace gas in lower area of plant |
| Document references | HR-02/04 | |

## INCIDENT ANALYSIS

| *Factors* | *Description* | *Probability* | *Frequency (/y)* |
|---|---|---|---|
| Consequence | Gas release due to operator error leading to asphyxiation and death | | |
| Tolerability criteria | | | $1 \times 10^{-5}$ |
| Initiating event | Routine maintenance error on valve/piping system | | 0.2 |
| Enabling event | | | |
| Potential modifiers | Ignition probability | - | |
| | Personnel exposure probability | 1.0 | |
| | Fatality / injury probability | 0.1 | |
| | | | |
| *Frequency of unmitigated incident / consequence* | | | $2 \times 10^{-2}$ |

## IPL ANALYSIS

| | | | |
|---|---|---|---|
| IPL safeguard PFD | Fixed CO monitors | 0.01 | |
| | Personal CO monitor | 0.01 | |
| | | | |
| | | | |
| | | | |
| Non-IPL safeguards | | | |
| Total Probability of Failure on Demand (PFD) for IPLs | | $1 \times 10^{-4}$ | |
| *Frequency of mitigated incident / consequence* | | | $2 \times 10^{-6}$ |
| Tolerability criterion met (yes/no) | | Yes | |

## ACTIONS

| | | | |
|---|---|---|---|
| Actions required | One operator on standby during valve/pipe cleaning | | |
| Further notes and justification | Significant number of fixed CO monitors in the area. Personal monitors checked each shift | | |
| Date Nov 2, 2004 | Author | ITC | |
| | Personnel | ITC, RR, CJS | |

**FIGURE 9-5 LOPA WORKSHEET**

An alternative method to event tree is to conduct a gap analysis. In this approach, a LOPA target is allocated, and credit factors for existing protection layer are subtracted from this target. The gap between the target and the sum of the credit factors indicates the SIL value yet to be achieved by an additional instrumented safety system, or suitable modification to existing protection layers such as redundancy. This approach is described by CCPS (2001) and Gowland (EPSC 2000).

The layers of protection for the event tree failure branch are:

- Basic process control, process alarms and operator monitoring
- Automatic action through safety instrumented system or emergency shutdown
- Relief devices
- External mitigation facilities (fire & gas, fire protection)

Occupancy can be handled as a modifier on the initial event frequency but this is useful only for safety of personnel and not for asset protection, where the exposure is 100% of the time when the plant is online.

The conditional probability of the outcome, given the initiating incident, can be taken as a measure of the overall safety integrity level.

The important characteristics of the IPLs are:

- Each safety layer must be independent of other protection layers
- Failure of one layer must not result in the failure of another layer
- Layers must have acceptable reliability
- If a layer is an administrative procedure, it must have written procedures, performance standard and auditability.

In performing the LOPA, frequency and probabilities are drawn from generic sources and team "best" estimates. The initiating event frequencies are order of magnitude estimates that can be based on risk matrix likelihood scales. Probabilities of failure on demand for the IPLs are typically generic values. For those events that are close to or over tolerability criteria, quantitative methods such as detailed fault and event trees plus effect and vulnerability models that constitute full QRA methods must be used as the next step in the risk assessment process.

The key limitations of LOPA include (Carter et al. 2003):

- inappropriate for complex event sequences
- does not easily deal with non IPL safety measures
- difficult to perform cost-benefit analysis
- human factors difficult to incorporate.

## 9.4 QUANTITATIVE TECHNIQUES FOR RISK ESTIMATION

Quantification of risk evolved as a natural progression from quantification of reliability, initially developed in the nuclear, electronic and aerospace industries.

Quantitative Risk Assessment (QRA) is a common usage in the process industry and other non-nuclear industries. In the nuclear industry QRA is synonymous with 'Probabilistic Risk Assessment' (PRA) or Probabilistic Safety Assessment (PSA) (Hayns 1999). Unlike reliability, QRA is still considered an evolving subject rather than a mature topic.

### 9.4.1 Quantitative Approach to Determination of SIL

An alternative to the risk graph for SIL determination is to use a quantitative method involving fault tree analysis. This approach also requires a target risk to be defined, and has the following steps (Macdonald 2004):

1. Define a target risk.
2. Evaluate the demand rate without safety instrumented protection. This step may involve a fault tree analysis, depending on the number of base events and their combinations, causing the demand.
3. Evaluate the hazard rate, allowing for all external and non-SIS protection. Hazard rate is the product of the demand rate and the probability of failure of protection on demand, as defined in Chapter 8. (For example, if the SIS is a pressure protection function, and a PSV is provided, allow for the probability of failure of PSV on demand in calculating the hazard rate). This step is an extension of the fault tree in step 2 above.
4. Calculate the probability of failure on demand required of an SIS protection, which is the ratio of the target risk and the hazard rate without SIS protection.
5. Using Table 9-2, allocate the SIL required for the SIS.

TABLE 9-2 TARGET FAILURE MEASURES FOR SIL ALLOCATION

| SIL | Probability of failure to perform design function on demand (continuous operation) |
|---|---|
| 4 | $\geq 10^{-5}$ to $< 10^{-4}$ |
| 3 | $\geq 10^{-4}$ to $< 10^{-3}$ |
| 2 | $\geq 10^{-3}$ to $< 10^{-2}$ |
| 1 | $\geq 10^{-2}$ to $< 10^{-1}$ |

EXAMPLE 9-2 PRESSURE PROTECTION

Let us repeat Example 9-1 using the quantitative approach. Since the event has the potential to cause multiple fatalities, select a target risk of $10^{-5}$ p.a.

It is known from experience that process deviations resulting in high pressure alarm occurs about once in 2 years, requiring operator intervention (demand rate).

The non-SIS protection are:

a) pressure high alarm and operator intervention
b) pressure safety valve, relieving to flare

Let us assume that for events that cause a pressure rise such as blocked outlet downstream, even if a high pressure alarm is raised, there is insufficient time for the operator to take effective steps.

The probability of failure of PSV on demand is taken as 0.005 (for a PSV that is maintained and tested at specified intervals).

An operator is likely to be present in the area for about 25% of the time.

Therefore, hazard rate without SIS function = 0.5 x 0.005x 0.25 = 6.25E-4 p.a.

Probability of failure on demand required of the SIS

= risk target/hazard rate

= $10^{-5}$ p.a./6.25E-4 p.a. = 0.016.

■ ■ ■ From Table 9-2, the SIS requires a SIL of 1 (closer to 2).

The SIL is highly sensitive to the demand rate, which needs to be estimated carefully. In a purely qualitative approach using the risk graph, the demand rate is arbitrary (based on experience), is one order of magnitude apart between levels, and hence may not give the right SIL under all conditions. Wherever possible, the quantitative approach is recommended.

A layer of protection analysis (LOPA) can be used to design the SIS to meet the required SIL.

### 9.4.2 Accident Sequence Development for Quantitative Estimation

The method of accident sequence development is similar to event tree analysis. The difference is that in an event tree construction, both success and failure paths are traced with their respective outcomes, in the accident sequence method, only the failure path is traced.

A generic model for event dependencies and accident propagation is shown in Figure 9-6, which is a simplified version of a model proposed by Paté-Cornell (1993), as applied to the Piper Alpha disaster in the North Sea in 1988.

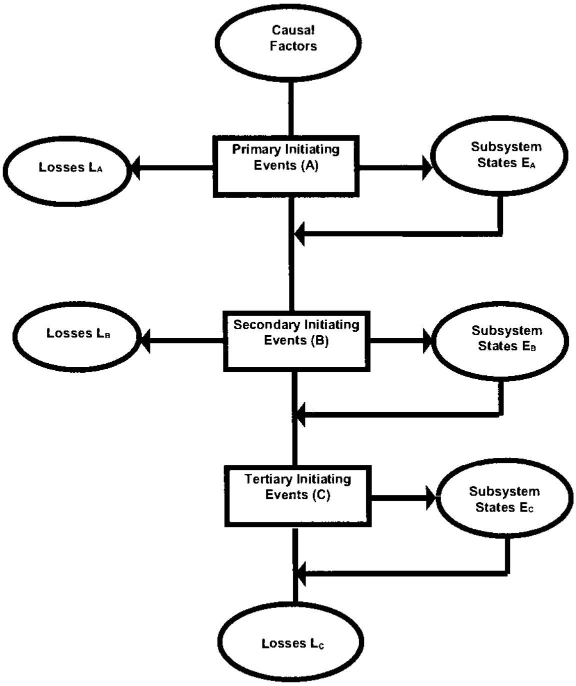


FIGURE 9-6 ACCIDENT PROPAGATION MODEL STRUCTURE

As the accident progresses, the subsystem states of a set of primary initiating events can become the secondary initiating events for the next escalation step. The subsystem state includes the condition that the protection layer at that stage had failed, thus unable to prevent the accident propagation. This is similar to the integrated model in Section 3.5.2 in Chapter 3.

### EXAMPLE 9-3 ACCIDENT SEQUENCE FOR BLEVE INCIDENT

The initiating event is a loss of containment from liquefied propane gas storage. The system boundary is defined as the propane vessel, fittings, pumps and associated pipework. A frequency of release can be calculated at the system boundary. Figure 9-6 is applied to the specific example to illustrate the accident propagation sequence in Figure 9-7.

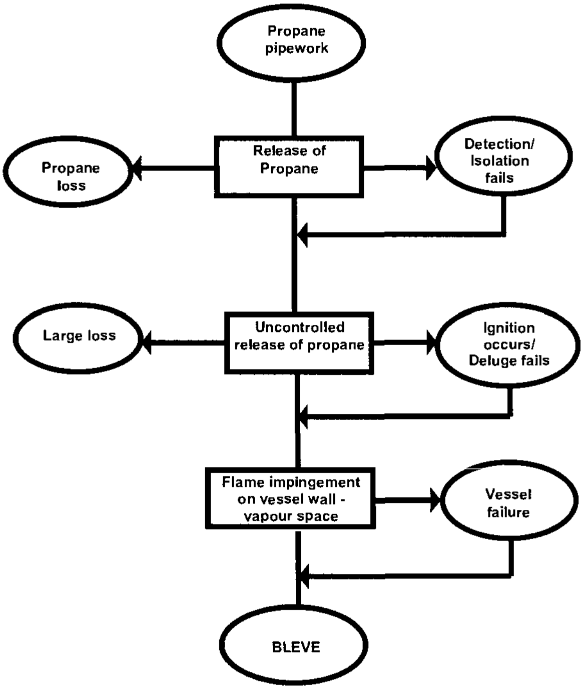

Propane pipework
Release of Propane
Propane loss
Detection/ Isolation fails
Uncontrolled release of propane
Large loss
Ignition occurs/ Deluge fails
Flame impingement on vessel wall - vapour space
Vessel failure
BLEVE

**FIGURE 9-7 EXAMPLE OF ACCIDENT SEQUENCE LEADING TO BLEVE**

Figure 9-7 is a simple example. In fact, there can be number of items in the subsystem state, and all of them should be listed in the accident sequence. These may in turn, give rise to a number of secondary and tertiary initiating events.

It is possible to ascribe a probability for each set of initiating events in the sequence and thus, a probability for each loss event. The product of these probabilities, together with the primary initiating frequency, gives a quantitative estimate of the risk of BLEVE. This risk can be compared against a performance target, and if considered high, additional barriers can be developed to stop the accident sequence. Conversely, if the risk is considered very low, no further action may be required, apart from maintaining the integrity of the barriers to accident propagation, through an effective safety management system.

The accident sequence diagram is a useful way of depicting the situation, especially the adequacy of barriers. The following precautions should be observed.

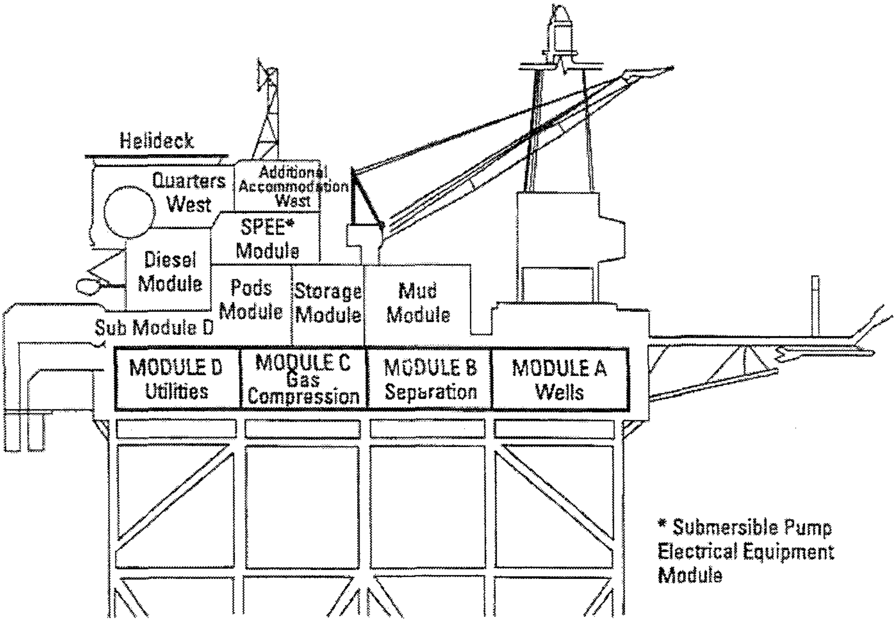
1. The intermediate events in the accident sequence should be properly quantified using the reliability estimation methods described in Chapter 8.
2. The accident sequence diagram can also be used qualitatively, but in such a case, the final event cannot be screened out as being of low risk, as the method is too subjective.
3. A first-cut assessment may be made by giving a probability estimate for the intermediate events. Some methods using a risk calculator advocate this approach. The weakness of this method is that some major accident events are liable to be screened out as being of low risk, as the assessment

of effectiveness and reliability of the hazard control measures could be optimistic.

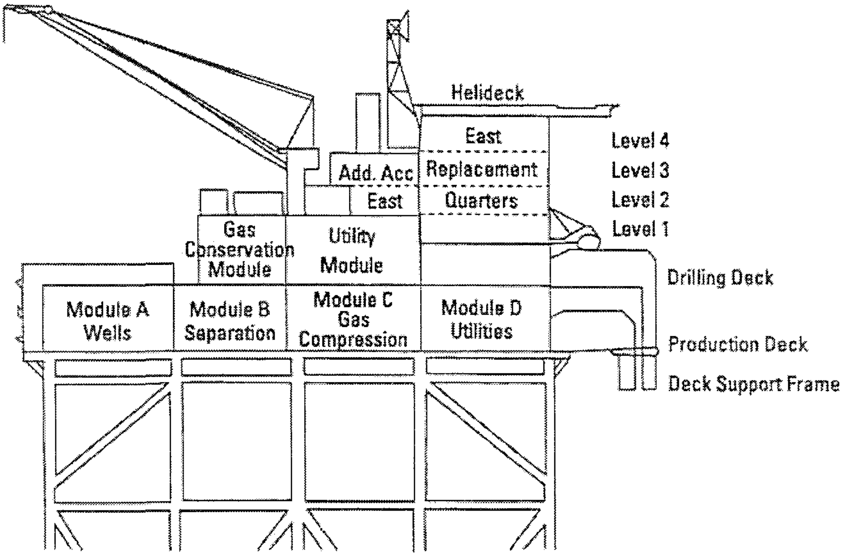
4. The accident sequence model is useful at the preliminary hazard analysis stage, to identify and rank the various incidents identified in the hazard identification stage, thus providing a direction and focus for a more detailed quantitative analysis.

It is essential that the entire accident propagation be modelled to provide a full picture of the risk. Generally, a small initiating event propagates and escalates into a major event through several stages, the intermediate propagation steps augmented by the inadequacy or failure of the installed hardware protection systems, and the absence or incompetence of the management system. This is illustrated by the Piper Alpha incident (Paté-Cornell 1993).

A schematic elevation diagram of the Piper Alpha topside modules is shown in Figure 9-8. If we apply the sequence in Figure 9-6 to Piper Alpha, it is clear that each step is quite complex, and consists of a number of interacting and sequential components.



The Piper Alpha platform: west elevation (simplified).



The Piper Alpha platform: east elevation (simplified).

**FIGURE 9-8 SIMPLIFIED ELEVATION OF PIPER ALPHA (Paté-Cornell 1993)**

A simplified presentation of the accident sequence is given below.

A: *Primary Initiating Event - First Explosion*

- Process Disturbance
- Two redundant pumps inoperative in module C; Hydrocarbon condensate pump "B" trips; the redundant pump "A" was shutdown for maintenance
- Failure of a flange assembly as the location of a pressure safety valve in module "C"
- Release of hydrocarbon condensate vapours in module "C" (approximately 45 kg which is 25% of module volume)
- First ignition and explosion
- Failure of firewall leading to damage of emergency systems in adjacent module

$E_A$: *Subsystem States after Primary Initiating Event*

- Immediate loss of electric power
- Failure of emergency lighting
- Control room failure
- Failure of public address/general alarm system
- Failure of radio telecommunication room
- Some people escape from 68' level to 20' level. Some jump into the sea.

$L_A$: *Losses after Primary Initiating Event*

- Loss of emergency systems (deluge, communication)

- Loss of helipad operation for rescue due to smoke
- Casualties in modules A, B and C.

B: *Secondary Initiating Event - Second Explosion*

- Rupture of firewall between modules B and C
- Rupture of a pipe in module B due to projectiles from B/C fire wall
- Large crude oil leak in module B
- Fireball and deflagration in module B
- Fire spreads to module C through failed B/C fire wall

$E_B$: *Subsystem States after Secondary Initiating Event*

- Fire in modules B and C spread to various containers (lube oil drums, industrial gas bottles)
- Pipes and tanks ruptured in modules B and C
- Smoke engulfing many parts of the platform preventing escape from deck to quarters
- Smoke ingress into living quarters
- Some survivors jump into sea from 68' and 20' levels
- Failure of firewater pumps. Automatic start had been turned off due to divers in water. Manual start pumps/damaged by C/D fire wall breach.

$L_B$: *Losses after Secondary Initiating Events*

- Some fatalities in quarters due to smoke ingress and asphyxiation
- Escalating damage to structures due to spread of fire
- Some people unable to be rescued from the sea.

C: *Tertiary Initiating Event - Jet fire from Process Riser*

- Rupture of riser (Tartan to Piper Alpha) caused by flame impingement from fires
- Third violent explosion and large fire and smoke engulf the platform
- Intense impingement of large jet fire on platform support structural members.

$E_C$: *Subsystem States after Tertiary Initiating Event*

- Most people trapped in living quarters
- Some survivors jump from the helideck into the sea (175' level)
- Collapse of platform at 68' level below module B
- Fourth violent explosion and rupture of Claymore gas riser
- Major structural collapse in various sections of platform
- Accommodation module overturned into the sea
- Rescue of survivors at sea (throughout the accident) by vessels on location.

$L_C$: *Losses after Tertiary Initiating Event*

- Human casualties: 167 (165 men onboard, and 2 rescue workers)
- Total loss of the platform
- Damage in excess of US$3 billion.

If the above events are depicted pictorially, Figure 9-6 will have interactions between $E_A$ and $L_A$, $E_A$ and $E_B$, $E_B$ and $L_B$, $E_B$ and $L_C$, and so on, making it extremely complex. Figure 9-6, however, does provide a simple framework for describing the initiation of an accident event and accident progression.

### 9.4.3 Estimation of Ignition Probability

One of the major areas of uncertainty in quantitative risk analysis is the probability of ignition. This probability directly affects the final risk value proportionately, and its reliable estimation is critical to risk quantification.

A simple empirical correlation models has been proposed by Cox et al. (1990), based on the release rate of flammable gas or liquid. The model does not account for the density of ignition sources in the vicinity of the release, and the effectiveness of control of ignition sources through the safety management system. Rew et al. (2004) have proposed a more sophisticated model based on ignition source density, and duration of presence of ignition source. Research in this area still continues.

### 9.4.4 Individual and Group Risks

Risk to people can be estimated in terms of injury or fatality. When risk is expressed in terms of injury, the type and extent of injury has to be defined clearly, e.g. first or second degree burns from fires, lung rupture from explosion overpressure, etc. In such a case, different injury risks are not directly comparable.

Historical fatality rate data are available for many industries and activities. When the risk is expressed in terms of fatality, a direct comparison of process industry performance with other industries is possible. Since a risk value by itself has no meaning except in relation to other risks, an estimate of fatality risk is useful, leaving aside the emotive aspects.

As described in Chapter 2, risk to people can be represented in two forms, individual risk and group risk. It is necessary to estimate the risk in both forms to obtain a full picture for decision making.

The following sections describe how the consequence assessment in Chapters 5 to 7 and the frequency assessment in Chapter 8 can be combined to calculate the risk. Only a basic outline of the technique is provided. More details can be found in CCPS (2000a; 2000b) and TNO (1999).

### 9.4.5 Estimation of Individual Risks

#### *9.4.5.1 Individual risk per annum for personnel risk*

Individual risk is defined as (Jones 1992):

> *The frequency at which an individual may be expected to sustain a given level of harm from the realisation of specified hazards.*

Individual risk (IR) is usually expressed as the probability that a person would be harmed in the course of a year, due to major accident events. For example, this may be expressed as a risk of chances in a million per year that a person may sustain a fatal injury due to an incident at a hazardous facility.

The calculation of individual risk at a geographical location within or near a plant assumes that the contributions of all incidents at the facility are additive. The total risk at each location is equal to the sum of the risks, at that location, of all possible incidents that could occur in a facility.

Individual risk is expressed in two forms:

a) Location Specific Individual Risk (LSIR). This parameter assumes that an individual is present at a given location, regardless of who it is. Typically, LSIR is applied in two instances:

   (i) Risk for any individual at a given plant location in the facility. The probability that someone could be present at that location is included in the risk estimation.
   (ii) Risk to a member of the public outside the site boundary. In this instance, a conservative assumption is made that a person is present continuously all the time (100% exposure time). It is also referred as 'peak individual risk'.

b) Individual Specific Individual Risk (ISIR). This parameter is applied to personnel on the site, and takes into account the fractional exposure of a specific person to the hazard. For an operator, this would be based typically on a 40-hour working week, and the fraction of the time spent in the plant.

### 9.4.5.2 Individual risk estimate

It should be noted that LSIR and ISIR are two distinct measures and are not comparable.

**Calculation of LSIR:**
The location specific risk at geographical location $(x, y)$ is given by:

$$\Psi(x, y) = \sum_i f_i \cdot p_{\text{impact}} \cdot p_{\text{exposure}} \qquad (9.5)$$

where $f_i$ = frequency of incident $i$ (p.a.)
$p_{\text{impact}}$ = probability of harm from individual incident (injury or fatality)
$p_{\text{exposure}}$ = probability that an individual may be present at $(x,y)$.

The summation is over all the incidents that have an impact on $(x,y)$. Therefore, the calculation of individual risk requires the evaluation of all the possible outcomes of each incident and their corresponding probabilities using fault tree/event tree analysis.

**Calculation of ISIR:**

ISIR is the most common form of risk measurement and presentation for risk to personnel in a hazardous facility. It is normally expressed as a risk of fatality, known as Individual Risk per annum (IRPA) and includes the exposure probability for the individual (< 100%).

### *9.4.5.3 Iso-risk contours for public risk*

Individual risk for offsite risk is normally presented in the form of risk contour plots. Risk contours show individual risk estimates at specific points on a map (see 2.5.1.1). It is used by government authorities in a number of countries to assess the risk levels from new and existing hazardous facilities as part of the decision-making process for land use safety planning (see Chapter 16).

Risk contours are calculated on the basis of peak individual risk, when applied to public offsite. For toxic release incidents, sometimes peak individual risk is assessed on the basis of time spent indoors and time spent in open air. In such a case, the rate of air changes in the building has also to be taken into account to estimate indoor concentrations, in the consequence analysis. While in theory this is a reasonable approach, in practice, air change rates would depend on the type of construction and occupancy, and assumptions have to be made, which may be difficult to substantiate. Therefore, risk at offsite residential areas is often estimated as peak individual risk to minimise uncertainty and maintain conservatism, and identified so in the study.

The calculation of risk for risk-contour plot is quite complex. For a given Cartesian grid, the risk for a uni-directional incident is calculated as follows:

1. Select a location in the Cartesian grid ($x_j$, $y_j$)
2. Initialise the risk at the Cartesian grid location to $\Psi=0$
3. Select a wind speed/weather stability class
4. Select a wind direction
5. Have available the hazard zone isopleth for the selected wind direction (from earlier consequence analysis)
6. If the Cartesian coordinate location is within the hazard zone, then the incremental risk contribution is given through equation (9.3), $\psi = f.p_{ws}.p_{wd}$, else $\psi = 0$.
7. Add the incremental contribution $\psi$ to the total contribution at that location, $\Psi$.
8. Repeat steps 4 to 7 for all wind directions.
9. Repeat steps 3 to 8 for all wind speed/stability class combinations.
10. Repeat steps 1 to 9 for all the grid locations.

The output is in the form a grid, with risk values at each grid location. By connecting all points of equal risk, an iso-risk contour is generated.

An example of a risk contour plot is shown in Figure 9-9.

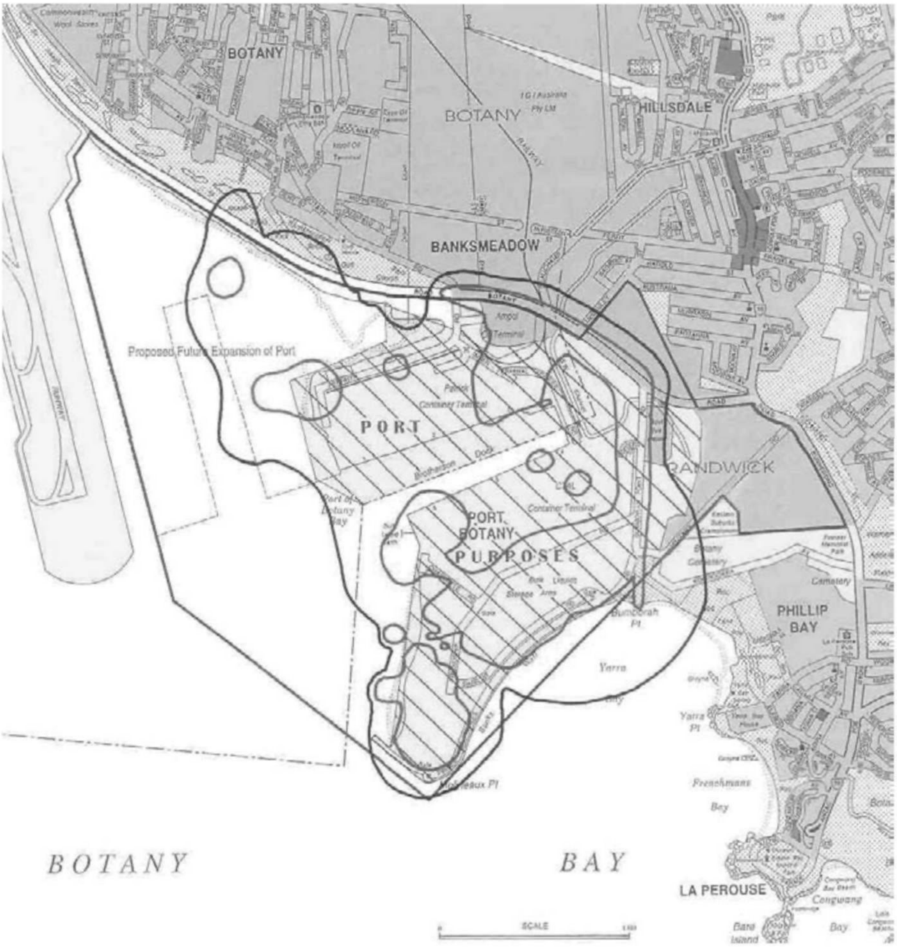


FIGURE 9-9 EXAMPLE OF RISK CONTOURS (SOURCE: DIPNR 2002, REPRODUCED WITH PERMISSION)

## 9.4.6 Estimation of Group Risk

Where incidents could cause multiple fatalities, individual risk estimation and risk contours are not sufficient to express the group risk (sometimes referred to as societal risk). While individual fatalities may be tolerated if infrequent, there is a high degree of societal aversion to incidents causing multiple fatalities, however infrequent.

### *9.4.6.1 Potential Loss of Life*

An average rate of fatality, referred to as the Potential Loss of Life (PLL) is often used for estimating risk to groups of plant personnel. PLL represents the expected average number of fatalities over the life of the facility, or over a given time period, such as one year.

The PLL is calculated for each incident, and summed over all the incidents, as shown below:

$$\text{PLL (p.a.)} = \sum_i f_i \cdot p_{f_i} \cdot n_i\theta_i \tag{9.6}$$

where

$f_i$ = frequency of incident $i$ (p.a.)

$p_f$ = probability of fatality from incident $i$

$n_i$ = number of people affected by incident $i$

$\theta_i$ = fractional exposure time of personnel in the plant area where incident $i$ could occur

PLL is expressed in fatalities per year. If the PLL per annum is multiplied by the lifetime of the facility, then we get the lifetime PLL. For a 30 year plant life, a PLL of 2 means that on average there are 2 fatalities during the life of the plant.

Detailed information on projected population distribution on a plant is required for this analysis. This includes the approximate fraction of the time spent in each plant section by all employees such as:

- plant operators
- maintenance personnel
- contractor personnel etc.

A risk integral (RI) has been suggested by Hirst and Carter (2002) as an alternative to the PLL. It is defined as:

$$RI = \sum_{N=1}^{N_{\max}} f(N) \cdot N^a$$

where $a > 1$. The RI is a disutility function, and averse to multiple fatalities. When $a$=1, we have the PLL.

### 9.4.6.2 Fatal Accident Rate

The fatal accident rate (FAR) is a measure of the average risk of fatality to personnel in a hazardous facility or industry. It is used extensively in industry as a measure of risk and was introduced in section 2.4.3.1.

Historical FAR is normally calculated using fatality statistics over a defined period and an estimate of the total number of hours worked by all employees over this period:

Care must be exercised in converting a PLL value into FAR for comparison with industry historical performance. The historical FAR represents the number of *actual fatalities* whereas the PLL represents an estimate of *potential fatalities*, none of which may occur. Do not expect these two figures to match. Therein lies the uncertainty in quantitative risk analysis.

### *9.4.6.3 F-N Curves*

F-N curves are also known as societal risk curves and have been extensively used in QRA for land-based industries. F-N curves are cumulative frequency-fatality plots, showing the cumulative frequencies (F) of events at which N or more fatalities could occur. They are derived by sorting the frequency-fatality (f-n) pairs from each outcome of each accidental event and summing them from the highest to lowest value of N to form cumulative frequency-fatality (F-N) coordinates on a log-log plot as seen in Figure 9-10.

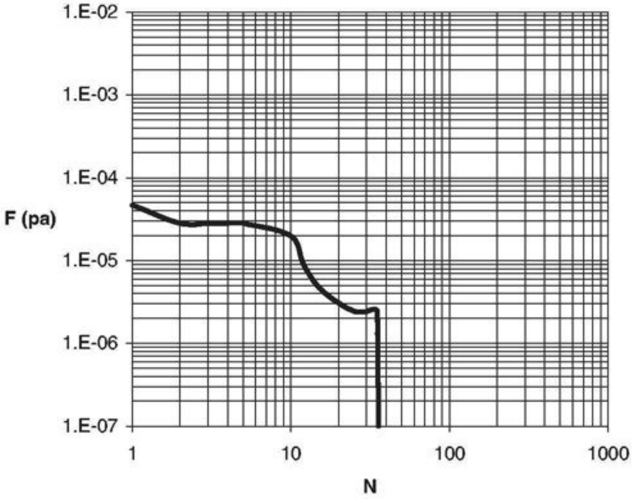


**FIGURE 9-10 EXAMPLE OF F-N CURVE**

F-N curves for land-based facilities include fatalities outside plant boundaries involving the public and employees in neighbouring industrial facilities. Therefore, the consequence analysis has to estimate the number of fatalities that can result outside plant boundaries for each incident outcome. This requires detailed information on population densities in the vicinity of the plant in question.

Unlike the aforementioned risk measures, F-N curves address two important issues. Firstly society believes that the assessment of number of people exposed to a particular risk is important. Secondly, society is more alarmed at single incidents involving multiple fatalities than a large number of smaller incidents causing the same number of fatalities over a long period of time. This aspect is discussed further in Chapter 15.

The use of F-N curves in decision making is discussed in Chapter 10.

An extensive study was carried out by Haastrup and Rasmussen (1994) in which F-N curves were constructed for 159 accidents, both from fixed facilities and transportation accidents. The study found the following:

- The F-N curves for both fixed installations and transport accidents were similar, indicating that once a loss of containment had occurred, the escalation path is similar in both cases.
- F-N curves for ammonia and chlorine incidents gave similar curves.
- F-N curve for incidents involving a BLEVE was above the curve for flammable gas release incidents without a BLEVE, indicating the higher severity of impact.

The study reinforced the applicability of the F-N curve representation of risk for a wide range of operations, involving both flammable and toxic materials.

### 9.4.6.4 *Rapid assessment of societal risk*

A rapid risk assessment method for estimating societal risk has been developed by Hirst and Carter of the HSE (2002), as a screening tool in assessing safety case submissions under the COMAH regulations. It is useful for a first pass risk evaluation to determine whether or not an in-depth risk assessment is necessary. It is based on a single "worst case" event that corresponds to the maximum consequences on the F-N curve.

This method consists of the following steps:

(i) Calculate the worst case accident footprint using the consequence models described in Chapters 6 and 7. This is the hazard radius for omni-directional incidents and the toxic isopleth for uni-directional incidents. A thermal dose, overpressure dose or toxic dose that can cause fatalities in 50% of the exposed population is suggested (i.e. probit value of 5).

(ii) Calculate the frequency of the worst case accident.

(iii) Estimate the total number of fatalities that could result from the population density within the hazard radius or hazard isopleth. We have a value of $N_{max}$, which is the right hand end of the F-N curve.

(iv) For omni-directional incidents, a slope of -1 is selected for the F-N curve. For uni-directional incidents, a slope of -2 is selected. This translates to the following Approximate Risk Indicator (ARI).

Omni-directional incidents:

$$ARI = f(N_{\max}) \cdot N_{\max} \left\{ \sum_{1} \left[ \frac{N^{a-1}}{N+1} \right] + N_{\max}^{a-1} \right\} \tag{9.8}$$

Uni-directional incidents:

$$ARI = f(N_{\max})N_{\max}^2 \sum_{1}^{N_{\max}} \left(N^{a-2}\right) \tag{9.9}$$

A value of 1.4 has been suggested for the exponent 'a' by Hirst and Carter (2002).

### 9.4.7 Linear Sources of Risk

For a fixed facility, the risk source is essentially a point source, or a number of point sources on a grid. The risk can therefore be represented as a risk contour, or as a risk grid. However, for transport of hazardous materials by road, rail, waterways or pipeline, the source of risk is linear. The linear source is static in the case of pipelines, but moving in the case of other modes of transport. The location of a release in such case is unknown, and can occur anywhere along the transport route. A slightly different approach is required for risk quantification of linear risks.

#### *9.4.7.1 Estimation of risk from linear sources*

The identification of hazards follows an approach similar to those described in Chapter 4. The external environment of the transport route plays a significant role in contribution to failure modes (e.g. road conditions, human error, driver fatigue etc for road transport; third party interference, soil erosion, subsidence etc for pipelines). Details of failure modes are provided in CCPS (1995). The risk calculation method is described in CCPS (1995) TNO (1999), and Bouissou et al. (2004).

The accident frequency is obtained from historical data as accidents per vehicle-kilometre for vehicular transport incidents. The release frequency for vehicle accidents is calculated as follows (Note: the term vehicle includes road trucks, rail cars and marine cargo carries).

Release/year = (Vehicle accident/km) x (vehicle movements/year) x
(km/vehicle movement) x (probability of release on accident)
(9.10)

For pipeline accidents, the following equation is used:

Release/year = (Pipeline failure/km-year) x (km/pipeline segment)
(9.11)

Pipeline release frequencies have been discussed extensively by EGPIDG (1994), and Fearnehough and Corder (1992).

For a given accident location and release scenario, the consequence analysis is made as if it were a point source, using local meteorological conditions if gas dispersion is required to be conducted. Event tree analysis is used to model the various outcomes, following a release, as described in Chapter 8. If an accident were to occur in a tunnel, then gas and smoke dispersion models using computational fluid dynamics (CFD) would be required to assess the consequences (Ciambelli et al. 1997).

When it comes to calculating risk, several point sources are postulated, at intervals approximately equal to the hazard consequence distance, and the risk grid generated for all the point sources simultaneously. The following points are of relevance:

- It is not necessary to cover the full length of the route, but only selected point sources, sufficient to cover the incidents hazard radii.
- The point source is located mid-way in a segment. For each point source, the frequency of the incident would implicitly include the segment of length, i.e. if the frequency is given as events/km-year, it is multiplied the segment length to express the frequency as events/year (see Figure 9-11).

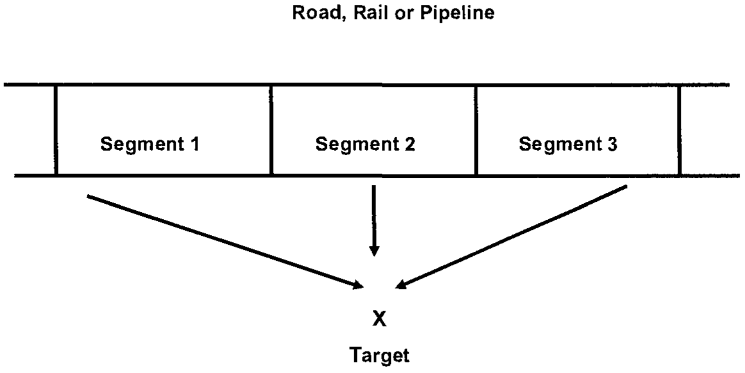


**FIGURE 9-11 CONTRIBUTIONS TO INDIVIDUAL RISK TO TARGET X**

- If there is a change in accident frequency, change in meteorological conditions, or change in direction of the route, then for each set of these conditions, a separate risk grid must be generated.

The risk grid represents peak individual risk. By incorporating the population density in the grid, an F-N curve for the linear source can be generated.

There are a number of ways the risk from a linear source can be represented (CCPS 1995).

1. Per year for pipeline risks, as pipeline is normally operational all the time
2. Per year, based on expected number of trips per year
3. Per trip
4. Per trip-km
5. Individual risk profiles or risk transects
6. F-N curves for community risk

The most common ways of risk representation are the risk transects and the F-N curves. These are described below.

### 9.4.7.2 Risk transects

Once the risk grid is calculated, the risk profile is generally generated not as a risk-contour, but as a graph showing the risk against transverse distance from the road/rail or pipeline. This profile is known as a *risk transect.*

The risk transect expresses peak individual risk along a line perpendicular to the linear source. An example is given in Figure 9-12 for high pressure natural gas transport by cross-country pipeline.

The risk transect would apply to a release from any location along the transport route.

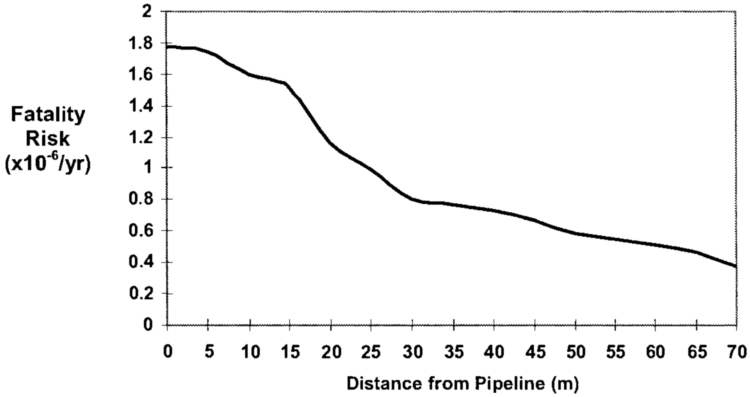


FIGURE 9-12 EXAMPLE OF RISK TRANSECT FOR NATURAL GAS PIPELINE

### 9.4.7.3 F-N Curves for Linear Sources of Risk

The main concern in linear sources is that the source poses a risk to people in populated areas, and to the biophysical environment. Therefore, it is essential that societal risk calculations are undertaken, and the risk is expressed as an F-N curve.

F-N curve calculation can be highly tedious for a long route, as the route has to be divided into hundreds of segments, and the population data obtained for each grid. In a long route, one would expect that much of the land surrounding the route would be rural, with fixed population centres along the route. In such a case, it may be necessary to generate F-N curves only for each population centre, thus optimising the efforts required. A route survey must be undertaken at the very beginning of the risk assessment exercise to determine the scope of work required.

The F-N curve is similar in shape to that shown in Figure 9-10.

### 9.4.8 Probable Loss Estimates

We have emphasized the fact that a risk measure is relative, and can only be interpreted in comparison to another familiar risk. The following questions arise:

- How can the risk measures be used in decision making?
- How do we know that we have reduced the risks to ALARP level?
- How low is low enough?

These questions are discussed at length in Chapter 10 under decision making under uncertainty. However, there is one additional risk measure that can be derived from the foregoing, which is a useful input to this decision making. This is referred to as the *probable loss*.

$$\text{Probable loss (\$/year)} = \text{Loss from an accident event (\$)} \times \text{Frequency of occurrence of specified loss event (p.a.)} \tag{9.12}$$

The loss from an accident event includes a number of costs. When added up, these costs are not trivial.

- asset damage and replacement costs
- loss of production during the period of investigation, repair and re-commissioning
- cost of investigation
- legal costs and compensation costs (if any)
- loss incurred from fall in stock price in the market, as a direct result of the incident
- cost of being unable to supply the market for a period, and loss of market share

If a major explosion in a process facility can result in a loss of approximately $1 million, and the estimated frequency of the incident is 0.1 per annum (once in 10 years), then

$$\text{Probable loss} = \$10\text{ M} \times 0.1 = \$100{,}000 \text{ p.a.}$$

It is the minimisation of probable loss that provides economic justification for expenditure on additional risk reduction measures. Further discussion on this is provided in Chapter 10.

Insurance companies generally use actuarial data from the industry to estimate maximum probable loss, as an indicator for setting insurance premiums.

### 9.4.9 Environmental Risk Estimation

Major environmental incidents such as the toxic fire and firewater runoff into the Rhine from the Sandoz facility in Switzerland, Exxon Valdez incident in Alaska, and cyanide release into the Danube from a gold processing facility in Romania have highlighted the risk of chemical and oil releases to the environment. Love Canal and establishment of a Superfund for cleanup are well documented.

In recent years, assessment and management of risk to environment from accidental release of chemicals has received significant regulatory attention. The Seveso Directive II by the Council of EU (1996) covers both safety of people and protection of the environment, among the member countries of the EU. The federal regulation by US EPA (1996) covers process safety management aspects related to prevention and management of accidental release of chemicals to the environment.

Since a loss of containment incident affects both safety and the environment, the process safety management principles are essentially the same for both. These are covered in Chapter 11.

Estimation of environmental risk is similar to the estimation of safety risk to people, but fraught with a few special difficulties. The estimation of frequency is identical, and event trees can be constructed for the pathways through which a loss of containment can reach the environment. The difficulty arises in estimating the environmental consequences, as vulnerability modelling and environmental fate modelling has a number of uncertainties. This is a rapidly developing area of research (Welsh 1992, Pritchard 2000).

One way of representing the risk of an environmental release is to use the F-M curve, where F is the cumulative frequency with which M or more tonnes of material can be released. The concept is identical to the F-N curve concept. Effectiveness of risk reduction measures can be shown as incremental changes in the F-M curves. We have found this concept particularly useful in the assessment of risk from oil spills in the handling of petroleum products in marine terminals, but the concept has a much wider application in environmental risk assessment.

### 9.4.10 Benefits of Quantitative Estimation

The most important benefit of a QRA is that it provides a basis for making management and engineering decisions which may not be possible without some form of quantification. The reason for this is that QRA combines the two major dimensions of risk, namely the consequences of identified incidents, and their corresponding frequency of occurrence. Other benefits are:

- Ability to rank risks for setting priorities for risk reduction
- Identification of significant risk contributors
- Estimation of probable loss for cost-benefit analysis
- Comparison of alternative options for risk reduction
- Comparison of alternative design options. This does not require a detailed assessment, but a concept risk analysis at a high level is sufficient, as ranking of options is the main objective (Crawley and Grant 1997).
- Comparison alternative transport routes for hazardous materials transport and route selection (Erkut and Verter 1995; Verter and Kara 2001).
- Verification of design to meet target performance standard for residual risk
- Identification risks to selected target groups onsite or offsite
- Useful tool for decision making in land use safety planning (HSE 1990)

- Ability to quantify business interruption risks and maximise online time
- Useful, but not the only input for demonstration of ALARP

For all of the above reasons, the QRA is a much preferred tool in process risk management.

### 9.4.11 Limitations of Quantitative Risk Estimation

There are a number of limitations to QRA which should be borne in mind in interpreting the results for decision making.

1. *Demand on resources*: A QRA requires a large amount of effort in terms of time, resources and data processing. One needs to be sure as to what the study results would be used for, before undertaking this venture.
2. *Spread of variance in failure rate data*: The failure rate data is generally obtained from generic data bases with possible adjustments to suit local conditions. This cannot provide a precise estimate of the frequency for the installation in question and hence there is a statistical error band in the data. This aspect has been highlighted in Chapter 8, and will be further explored in Chapter 10.
3. *Hypothetical incident scenarios*: The scenarios postulated for loss of containment are hypothetical, albeit based on historical data on industry accidents. A large number of scenarios need to be addressed, in order to provide a sufficient sample base to reduce the variance of probability estimates.
4. *Idealised models*: The mathematical models used for consequence analysis contain idealised approximations. This is a necessary part of modelling, but does introduce uncertainties in calculating hazard impact radii.
5. *Quality of assumptions*: A number of assumptions are required in postulating hypothetical failure scenarios, mathematical modelling of consequences, and effects of hazardous incidents. These are based on validated published data where available, and in many cases, judgement based on experience. The quality of assumptions spans a wide spectrum. It is necessary to list all the assumptions, and provide justification for each of the assumptions for an audit trail.
6. *Problems in quantification of human factors:* A risk analysis study only partially includes incidents caused by human error and management system failures and hence the risk estimated can be optimistic.
7. *Illusion of accuracy*: The sophistication of QRA software and the extent of computational efforts required create an illusion of accuracy in the mind of the reader. People tend to believe a number that is presented to them, as if it is deterministic. A sensitivity analysis is often required to test the assumptions and the data used (Nussey et al. 1993).
8. *Assumption of good industry standard*: It is often assumed that the facility operates to good industry standards, in applying generic failure rate data in QRA. Often, an investigation after an accident has shown that this assumption is not always true.

9. *Abnormal situation management*: Many incidents occur because of failure to diagnose and correctly respond to abnormal situations caused by process deviations. The QRA does not deal with this aspect effectively as abnormal situation management has to be managed through an effective process safety management system.

Brown (2001) sums up the issues related to setting numerical risk targets as a measure of achieving safe operation, that it is more important "*to think best practice, don't think numbers*", when it comes to measuring safety achievement.

> "*... a safe plant is achieved through a cocktail of inherently safe design, robust safety systems, appropriate mitigation and emergency measures, carefully crafted operating envelopes and instructions, suitably skilled staff, and possibly, above all, a 'safety culture'..*" (Brown 2001).

On balance, in spite of the limitations, QRA is still one of the best tools available for risk assessment, as long as the safety performance measurement is not 'number driven'. When a young analyst was frustrated during the course of the QRA on the uncertainty in failure rate data, a wise senior colleague said "It is not so much the accuracy of results that matters, but the holistic nature of the QRA *process*, which provides so much insight into the facility design and operation, as never before."

## 9.5 HUMAN FACTORS IN RISK ANALYSIS

One of the assumptions in risk analysis is that a facility is managed to at least average standards, with monitoring of performance by the corporation by a regulatory agency and corrective actions are implemented. This 'implicit' assumption underlies the use of generic failure rate databases for frequency analysis.

For a plant where high standards are expected to prevail, such an assumption may produce a pessimistic estimate of risk (erring on the side of caution). Where standards may slip over a period of time as the plant ages and management changes, the assumption of continued maintenance of average to good industry standards may not be valid. The HSE in the UK has recognised this, and has recommended the 'cautious best estimate' approach (Nussey et al. 1993).

### 9.5.1 Modification of Generic Failure Rate

Hurst et al. (1991) describe a method for modifying the generic frequency of pipework failures by a factor that takes into account human factors. They found that the total human contribution to immediate cause of failure was 41%.

Modification of the frequency of release by an audit of the safety management system has been suggested by Pitblado et al. (1990) and Hurst et al. (1996). This approach has not found universal acceptance.

For a plant in poor state of repair, a QRA is both irrelevant and misleading. For instance, multiplying the generic failure frequency by a factor >1 to reflect poor management standards may still produce a low risk, in which case, there would be no incentive to better the standards. As Tweeddale (1992) observes:

> *"It may be less important to assess risks on the assumption of good industry standards of management and operational standards, than to assess the probability of failure of that assumption."*

The main factors which contribute to (or influence) the variation in the base failure rates are:

- the quality and effectiveness of implementation of a company's Safety Management System (SMS)
- human factors and organisational climate/culture; and
- design standards used for the plant.

There has been much discussion among regulatory authorities on whether or not it is possible to apply some numerical factor to the "average" data to allow for non-average (good or poor) quality of safety management and human factors. The HSE in the UK is of the opinion that such allowances should be applied only within narrow limits (HSE 1989). An allowance to reduce the generic accident rate because of good quality of management in a specific situation could well be optimistic, given the possibility of changes over the years. Conversely, a large adjustment to increase the accident (failure) rates for poor quality would seem to imply that a level of safety below the average is tolerable, which is not the case.

What is required is a "cautious best estimate". Every attempt should be made to use realistic, best-estimate assumptions (whilst clearly defining the basis of the assumptions), but where there is difficulty in justifying an assumption, some conservatism in the estimate is preferred.

As a general guide, the generic failure rate (average) could be reduced by a factor of 2-3 for best practice management, and for unfavourable conditions, the average frequency could be increased by up to one-order of magnitude (HSE 1989). The numerical factors applicable to an installation can be arrived at after an audit of the facility and its operations. Obviously, there is an element of judgement in this semi-quantitative approach.

### 9.5.2 Integrated Model for Technical and Management Factors

The concept of modifying the failure frequency has been extended into an integrated model by Papazoglou et al. (2003). It is postulated that the overall influence of the SMS on a technical parameter is a function of the quality of delivery system ($y_i$) and the weighting factor ($w_{ij}$) assessing the relative importance of the i$^{th}$ management delivery system on the influence of the j$^{th}$ technical parameter, j being an index running over the basic events of an organisation category.

$$m_j = \sum_{i=1}^{n} y_i \cdot w_{ij} \tag{9.13}$$

where $m_j$ is the modification factor for the $j^{th}$ technical parameter.

The delivery systems and technical parameters are listed in Tables 9-3 and 9-4 respectively.

TABLE 9-3 **Delivery systems for affecting management systems**

| No. | Delivery system |
|---|---|
| 1 | Availability of personnel |
| 2 | Commitment, attitudes and aptitudes |
| 3 | Internal communication and coordination |
| 4 | Competence of personnel |
| 5 | Resolution of pressures and demands conflicting with safety |
| 6 | Plant/personnel interface |
| 7 | SMS elements and procedures |
| 8 | Delivery of correct spares/tools for repair/replacement |

TABLE 9-4 TECHNICAL PARAMETERS

| No. | Technical parameter |
|---|---|
| 1 | Static equipment |
| 2 | Rotating equipment |
| 3 | Pipework |
| 4 | Valves |
| 5 | Sensing instruments (flow, pressure, level, temperature, composition) |
| 6 | Protection systems (fire & gas system, shutdown valves, firewater) |
| 7 | Pressure relief devices |
| 8 | Human error in abnormal situation management (detection, response, recovery) |
| 9 | Human error in maintenance |
| 10 | Alarms and interlocks management |

Within each delivery system, and each technical parameter, a number of items arise, which are compiled into a checklist.

Weighting factors allocated for influence of delivery system on technical parameters are to be thoroughly reviewed, discussed with operations, and must have a consensus. The influence factor $y_i$ is assessed through a management system audit. A checklist for influence factors can be compiled from the information from the RASE project (Rogers 2000).

Papazoglou et al. (2003) found that when this integrated model was applied to an ammonia cryogenic storage facility, the frequency of tank overpressure varied by 4 orders of magnitude on either side of average (best case and worst case). This has raised awareness of the importance of management factors, at the same time adding more uncertainty to QRA results.

In our current understanding of human factors influencing failures, it is difficult to minimise uncertainty in a QRA by the modifier multiplier model. One way to approach this is as follows:

1. Undertake the influence factor assessment, not so much for obtaining a multiplier, but to identify areas where the SMS performance needs to be improved.

2. Ensure that the SMS performance is at least to average industry standard or better, in parallel with the conduct of a QRA.
3. Use the generic failure rates for QRA, so long as it is so stated, and so long as the results are not used in an absolute sense, but for relative risk ranking.
4. Ensure through a monitoring, auditing and feedback system, that the SMS effectiveness is maintained, in order to retain the validity of the QRA.

The development and implementation on effective process safety management system is described in Chapter 12.

## 9.6 RISK ASESSMENT

### 9.6.1 Tolerability of Risk

In assessing risk, the questions that often arise are:

- How safe is safe enough?
- What is an acceptable risk?
- How to strike an optimum balance between risk reduction and cost?

While there are no ready answers to the above, for process industries, the issues have been addressed in considerable depth during the last 20 years, particularly because of risk to the public in residential areas surrounding installations. Community risk perception has emerged as an important consideration in decision making by planning authorities. Therefore, the socio-political dimension has assumed as much importance as the technical dimension of risk.

Since the public do not have direct control over risks posed by industry, it behoves the regulatory agencies to set guidelines and targets for risk, to which the facility should be designed and operated. This enables the government to balance the need for economic development with land use safety.

Therefore, instead of asking the question, 'Is the industry completely safe?', the question should be rephrased as 'Is the residual risk after applying all the necessary safety controls low enough for the public to tolerate?' Thus, risk criteria setting, attempts to establish 'tolerable' residual risk rather than 'acceptable' risk (HSE 1988).

The concept of risk targets and some targets used in practice are discussed below. More information may be found in Chapter 10.

### 9.6.2 The Use of Risk Criteria

When we quantify a risk, there should be a standard to compare it against in order to arrive at an informed judgment as to whether or not the risk is low in relation to tolerability. Further, a single point target would not make sense, given the uncertainty band associated with risk estimation.

Another reason for establishing risk criteria is that design engineers in the industry will be encouraged to look for alternative, low cost means of risk reduction as part of inherently safer design, rather than arguing that the cost of risk reduction is prohibitive (Kletz 1982).

There has been general agreement among the regulators, industry and parts of the public that target risk criteria are necessary for decision making. Much effort has been devoted in the 1980s to selecting the numerical criteria. There are three main parameters in the selection of risk criteria (Holden 1984):

- how the risk is to be described quantitatively
- specification of a sound conceptual framework for decision making
- adoption of a numerical value as a target criterion.

After considerable public discussion, risk measures and targets have been well established for public risk from major hazard facilities.

### *9.6.2.1 Regulatory risk criteria*

**Peak Individual Risk**

Numerical risk targets in terms of frequency of occurrence of accident events resulting in injury or fatality to public from major hazard installations have been set by regulatory authorities in several countries around the world. No numerical targets or criteria have been set for employee risk, and it is left to the specific facility operator to demonstrate that the risks to employees have been reduced to ALARP levels.

Risk criteria have been established by a number of countries, for public risk from hazardous industries, from a land use safety planning perspective. A summary is given in Table 9-5.

**TABLE 9-5 SUMMARY OF RISK CRITERIA FOR INDIVIDUAL FATALITY RISK**

| Country | Risk intolerable above this level | Risk negligible below this level | Comments |
|---|---|---|---|
| Australia - NSW | Not used | 1 x $10^{-6}$ p.a. | For new plants near residential areas. |
| | Not used | 5 x $10^{-5}$ p.a. | Risk to be contained within site boundary. |
| Australia - Victoria | Not specified | 1 x $10^{-7}$ p.a. | For residential areas |
| | 1 x $10^{-5}$ p.a. | Not specified | Risk to be contained within site. |
| Australia - Western Australia | 1 x $10^{-5}$ p.a. | 1 x $10^{-6}$ p.a. | For residential areas |
| Denmark | 1 x $10^{-6}$ p.a. | Not used | Also to show that environmental contamination not above threshold values |
| France | 1 x $10^{-6}$ p.a. | Not used | Guideline only. Not mandatory |
| Germany | No numerical target | No numerical target | Safety analysis required. |
| Hong Kong | 1 x $10^{-5}$ p.a. | Not used | For new plants |

| | | | |
|---|---|---|---|
| The Netherlands | 1 x $10^{-6}$ p.a. | 1 x $10^{-8}$ p.a. | Suitability of operating staff should also be addressed |
| United Kingdom | 1 x $10^{-5}$ p.a. | 1 x $10^{-6}$ p.a. | For new housing near existing plants |

As mentioned earlier, compliance with the criteria may receive a planning permit to construct, but will not receive a licence to operate without demonstration of ALARP (see Chapter 10).

As well as fatality risk some jurisdictions also set out injury risk levels. In the case of the Department of Planning, Infrastructure and Natural Resources (NSW, Australia) injury risks cover thermal radiation, explosion overpressure and toxic exposure risks. Table 9-6 gives a summary (DIPNR 1990).

TABLE 9-6 SUMMARY OF RISK CRITERIA FOR INDIVIDUAL INJURY RISK

| Category | Criterion |
|---|---|
| Thermal radiation | < $50\times10^{-6}$ p.a. for heat flux of 4.7 kW/m$^2$ at residential areas<br>< $50\times10^{-6}$ p.a. for heat flux of 23 kW/m$^2$ at neighbouring hazardous installations |
| Overpressure | < $50\times10^{-6}$ p.a. for > 7 kPa overpressure at residential areas<br>< $50\times10^{-6}$ p.a. for > 14kPa at neighbouring hazardous installations or public buildings |
| Toxic exposure | < $10\times10^{-6}$ p.a. of exposure in residential areas not to exceed level of serious injury to most sensitive<br>< $50\times10^{-6}$ p.a. of exposure not to exceed acute responses (coughing, irritation) to most sensitive |

## Societal Risk

Because of the uncertainties associated with it, and several factors other than a numerical value of risk influencing decision making, no numerical criteria has been set for societal risk from industrial activities by the HSE in the UK. This has been followed by a similar decision by the state governments in Australia.

Even in the absence of formal criteria, it is useful to assess societal risk where is it is possible, and where relevant data is available with minimal uncertainty. A relative evaluation of risk reduction measures can be made by observing the movement of the F-N curve.

Hong Kong and the Netherlands have formally adopted a societal risk criteria for hazardous plants. In the U.K., societal risk criteria have been suggested for ports, but not for hazardous plants. A summary of the societal risk criteria is shown in Table 9-7.

TABLE 9-7 SUMMARY OF SOCIETAL RISK CRITERIA

| Country | F-N Curve slope | Maximum tolerable risk intercept with N=1 | Negligible risk intercept with N=1 | Limit on N |
|---|---|---|---|---|
| Hong Kong | -2 | $10^{-3}$ p.a. | $10^{-5}$ p.a. | 1000 |
| The Netherlands | -1 | $10^{-3}$ p.a. | - | 1000 |
| United Kingdom (for ports only) | -1 | $10^{-1}$ p.a. | $10^{-4}$ p.a. | - |

For land use planning decision making on the basis of societal risk, the HSE has developed approximate methods to calculate risk in the form of risk indicators (Carter et al. 2003). For land use planning purposes, the following limits have been suggested.

Approximate Risk Indicator (ARI):

| | |
|---|---|
| Broadly acceptable: | < 2000 (qualitative assessment sufficient) |
| Intolerable: | ≥ 500,000 (full quantitative risk analysis required) |
| Tolerable if ALARP: | 2000 ≤ ARI < 500,000 (semi-quantitative risk assessment to full quantitative risk assessment) |

These ARI values do not form part of the regulatory criteria, but provide a rapid assessment indication of where the risk lies, and whether or not further investigation is necessary.

#### 9.6.2.2 *Corporate risk criteria*

No legislative target has been set for risks to employees at the workplace. Many large companies have adopted internal standards below current industry average FAR values. The approach is performance-based, rather than prescriptive.

Many organisations have set numerical targets for lost time injury rates (LTIRs), based on historical figures. No target exists for FARs. The following LTIR targets may be suitable, but all these targets have some problems in their application.

1. LTIR target set to industry average, with the objective of not exceeding it. This approach would, however, implicitly concede that further reduction in LTIR is not achievable, which is clearly wrong.

2. LTIR target set to industry average in the short term, if actual LTIR is currently higher than industry average. There would be a tendency to stop there, once it is achieved.

3. A pragmatic approach is to set a target for each individual facility to better its historical performance progressively over a given time frame, with a view to achieving better than industry average performance.

For non-safety areas such as business interruption risk, an organisation would set its goals based on financial considerations.

## 9.7 REVIEW

In Chapter 9, we have described how the two arms of risk, namely incident consequence (Chapters 5 to 7) and incident frequency (Chapter 8), are combined to obtain an estimate of risk. The data requirements for risk assessment have been reviewed.

Qualitative risk assessment technique using risk matrices have been discussed, with references to the risk matrix and the rule sets provided in Chapter 3. Some of the limitations of qualitative measures, especially for decision making, have been highlighted.

The qualitative estimate also covered the determination of Safety Integrity Level (SIL) required for safety instrumented functions. The risk graph technique of IEC 61508 (1998) have been described in detail, with cautions on calibration of the risk graph using an appropriate rule set.

For semi-quantitative methods the LOPA technique was discussed together with its shortcomings.

Methods of quantitative risk analysis have been described briefly, with various risk measures. Individual risk (person specific and location specific individual risk), group risks (potential loss of life and F-N curves), and risks from linear sources (transportation risks) have been addressed. The estimation of probable loss from the QRA is outlined, as an input to decision making, described in Chapter 11.

Finally, the advantages and limitations of QRA have been discussed, in order to provide a balanced view to the reader. The role of human factors in QRA has been addressed, along with methods available for modification of failure rates to account for management systems and human factors. Such an approach appears to add more uncertainty to the QRA result. Use of generic failure rate database, together with a robust system of monitoring and auditing to maintain the SMS effectiveness provides a simpler alternative.

Available risk criteria for location specific individual risk and for societal risk have been summarised. The criteria vary in their application, but most of them fall in the risk band of $10^{-6}$ to $10^{-5}$ p.a.

## 9.8 REFERENCES

American National Standard Institute. *Application of Safety Instrumented Systems for the Process Industries*, American National Standard Institute, Washington, D.C. ANSI/ISA 84.01:1996.

American Petroleum Institute. *Recommended practice for analysis, design, installation and testing of basic surface systems for offshore production platform*, American Petroleum Institute, Washington D.C. API RP 14C:2001.

Bouissou, Ch., Ruffin, E., Defert, R., Pratts, F. and Dannin, E. 2004, 'A new QRA Model for rail transportation of hazardous goods', *11th International Symposium on Loss prevention*, Prague, 31 May-3 June, pp. 4283-4289.

Brown, M. 2001, 'Never ever? What is the measure? '(Editorial), *Transactions of Institution of Chemical Engineers*, Part B, Process safety and Environmental Protection, vol. 79, July, pp.195.

British Standard/IEC. *Functional Safety - Safety instrumented systems for the process industry sector - Parts 1 to 3*. BS IEC 61511:2003.

Carter, D.A. Hirst, I.L., Maddison, T.E. and Porter, S.R. 2003, 'Appropriate risk assessment methods for major accident establishments', *Transactions of Institution of Chemical Engineers*, Part B, Process safety and Environmental Protection, vol. 81, pp. 12-18.

CCPS 1995, *Center for Chemical Process Safety - Guidelines for Chemical Transport Analysis*, American Institute of Chemical Engineers, New York.

CCPS 2000a, *Center for Chemical Process Safety - Guidelines for Chemical Process Quantitative Risk Analysis*, $2^{nd}$ edition, American Institute of Chemical Engineers, New York.

CCPS 2000b, *Center for Chemical Process Safety - Evaluating Process Safety in the Chemical Industry: A user's Guide to Quantitative Risk Analysis,* American Institute of Chemical Engineers, New York.

CCPS 2001, *Center for Chemical Process Safety - Layer of Protection Analysis: Simplified Process Risk Assessment,* American Institute of Chemical Engineers, New York.

Christen, P., Bohnenblust, H. and Seitz, S. 1994, 'A methodology for assessing catastrophic damage to population and environment', *Process Safety Progress*, vol. 13, no. 4, pp. 234-238.

Ciambelli, P., Bucciero, A., Maremonti, M., Salzano, E. and Masellis, M. 1997, 'The risk of transportation of dangerous goods BLEVE in a tunnel', *Annals of Burns and Fire Disaster*, X(4), December.

Council of the European Union, 1996, Common Position (EC) No. 16/96 on Council Directive 96/82/EC on the control of major accident hazards involving dangerous substances, 19 March, Brussels, Belgium.

Crawley, F.K. and Grant, M.M. 1997, 'Concept risk assessment of offshore hydrocarbon production installations', *Transactions of Institution of Chemical Engineers*, Part B, Process safety and Environmental Protection, vol. 75, pp.157-163.

DIPNR 2002, Department of Planning Infrastructure and Natural Resources of New South Wales, *Port Botany Regional Risk Assessment Study*, Sydney, Australia.

DIPNR 1990, Department of Planning Infrastructure and Natural Resources of New South Wales, *Risk Criteria for Land use Safety planning, Hazardous Industry Planning Advisory Paper No. 4,* Sydney, Australia.

EGPIDG 1994, European Gas Pipeline Incident Data Group - Gas Pipeline Incidents, presented by F.J. Dawson - British Gas, at the *International Gas Union Conference*, Milan, Italy, June.

Erkut, E. and Verter, V. 1995, 'A framework for hazardous materials transport risk assessment', *Risk Analysis*, vol. 15, pp. 589-601.

EPSC 2000, *European Process Safety Centre - Safety Integrity: The Implications of IEC 61508 and other standards for the process industries*, The Institution of Chemical Engineers, Rugby, England.

Fearnehough, G.D. and Corder, I. 1992, 'Application of Risk Analysis Techniques to the Assessment of Pipeline Routeing & Design Criteria', *International Conference on Pipeline Reliability*, Calgary, Canada.

Goyal, R.K. 1993, 'Practical examples of CPQRA from the petrochemical industries', *Transactions of Institution of Chemical Engineers*, Part B, Process Safety and Environmental Protection, vol. 71, pp. 117-123.

Haastrup, P. and Rasmussen, K. 1994, 'A study of f-N curves for accidents involving highly flammable gases and some toxic gases', *Transactions of IChemE*, Part B, Process safety and Environmental Protection, vol. 72, pp. 205-210.

Hirst, I.L. and Carter, D.A. 2002, 'A 'worst' case methodology for obtaining a rough but rapid indication of the societal risk from a major accident hazard installation', *Journal of Hazardous Materials*, vol. A92, pp. 223-237.

Holden, P.J. 1984, 'Difficulties in Formulating Risk Criteria', *Journal of Occupational Accidents*, vol. 6, pp. 241-251.

HSE 1989, Health and Safety Executive, UK, *Quantitative Risk Assessment: Its Input to Decision Making*, HMSO, London.

HSE 1990, Health and Safety Executive, UK, *Risk Criteria for Land-Use Planning in the vicinity of Major Industrial Hazards*, HMSO, London.

Hurst, N.W., Bellamy, L.J., Geyer, T.A.W. and Astley, J.A. 1991, 'A classification scheme for pipeline failures to include human and sociotechnical errors and their contribution to pipework failure frequencies', *Journal of Hazardous Materials*, vol. 26, pp. 159-186.

Hurst, N.W., Young, S., Donald, I. and Muyselaar, A. 1996, 'Measures of safety management performance and attitudes to safety at major hazard sites', *Journal of Loss Prevention in the Process Industries*, vol. 9, no. 2, pp. 161-172.

International Electrotechnical Commission. *I International Electrotechnical Commission - Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, Parts 1 to 7*, International Electrotechnical Commission. IEC 61508:1998.

Instrumentation, Systems and Automation Society. *Safety Instrumented Functions - Safety Integrity Level Evaluation Techniques*, *Parts 2 to 4*, Instrumentation, Systems and Automation Society, North Carolina, USA. SA-TR84.00.022002:2002.

Jones, D.A. 1992, *Nomenclature for Hazard and Risk Assessment in the Process Industries*, 2nd edn, Institution of Chemical Engineers, Rugby, England.

Kletz, T.A. 1982, 'Hazard Analysis-A Review of Criteria', *Reliability Engineering*, vol. 3, pp. 325-338.

Macdonald, D. 2004, *Practical Industrial Safety, Risk Assessment and Shutdown Systems for Industry*, Elsevier Newnes Press.

Marszal, E.M. and Scharpf, E.W. 2002, *Safety Integrity Level Selection: Systematic Methods Including Layer of protection Analysis,* ISA - The Instrumentation, Systems and Automation Society, NC, USA.

Nussey, C., Pantony, M.F. and Smallwood, R.J. 1993, 'Health and Safety Executive's risk assessment tool RISKAT', *Transactions of Institution of Chemical Engineers*, Part B, Process Safety and Environmental Protection, vol. 71, pp. 29-40.

Papazoglou, I.A., Bellamy, L.J., Hale, A.R., Anezeris, O.N., Ale, B.J.M., Post, J.G. and Oh, J.I.H. 2003, 'I-Risk: development of an integrated technical and management risk methodology for chemical installations', *Journal of Loss Prevention in the Process Industries*, vol. 16, pp. 575-591.

Paté-Cornell, M.E. 1993, 'Learning from the Piper Alpha accident: A post-mortem analysis of technical and organization factors', *Risk Analysis*, vol. 13, no. 2, pp. 215-231.

Pitblado, R., Williams, J.C. and Slater, D.H. 1990, 'Quantitative assessment of process safety programs', *Plant Operations Progress*, vol. 9, no. 3, pp. 169-175.

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

Rew, P., Daycock, J. and Rushton, A. 2004, 'Ignition Probability of Flammable Gas Releases', *11th International Symposium on Loss Prevention*, Prague, 31 May, pp. 3359-3366.

Rogers, R.L. 2000, 'The RASE project risk assessment of unit operations and equipment', Available at: http://www.safetynet.de/EC-Projects/. (Can be downloaded).

Timms, C.R. 2003, 'IEC 61508/61511 - pain or gain?', *Process Safety Progress*, vol. 22, no. 2, pp. 105-108.

Tixier, J., Dusserre, G., Salvi, O. and Gaston, D. 2002, 'Review of 62 risk analysis methodologies of industrial plants', *Journal of Loss Prevention in the Process Industries*, vol. 15, pp. 291-303.

TNO - Committee for the Prevention of Disasters 1999, *Guidelines for quantitative risk assessment - 'Purple Book CPR 18E'*, The Director-General for Social Affairs and Employment, The Hague, The Netherlands.

Tweeddale, H.M. 1992, 'Balancing Quantitative and non-quantitative risk assessment', *Transactions of Institution of Chemical Engineers*, Part B, Process Safety and Environmental Protection, vol. 70, pp. 70-74, 1992.

UKOOA, 1999, UK Offshore Operators Association - Guidelines for instrument-based protective systems, Issue No.2, August.

US EPA, 1996, Environmental Protection Agency - Risk management programs for chemical accidental release prevention. Final Rule, 40 CFR Part 68, Federal register, Washington D.C., June.

Verter, V. and Kara, B.Y. 2001, 'A GIS-Based framework for hazardous materials transport risk assessment', *Risk Analysis*, vol. 21, no. 6, pp. 1109-1120.

Wass, M.A. and Calder, J. 2004, 'Practical Guidelines and Procedure for SIL Ranking under IEC 61508/61511', *11th International Symposium on Loss Prevention*, Prague, 31 May- 3 June, Paper AP192.

Welsh, S. 1992, 'Assessment and Management of Risks to the Environment' in *Major hazards onshore and offshore, Institution of Chemical Engineers Symposium Series No.130*, pp. 85-110.

## 9.9 NOTATION

| | |
|---|---|
| ALARP | As Low As Reasonably Practicable |
| ANSI | American National Standards Institute |
| API | American Petroleum Institute |
| ARI | Approximate Risk Indicator |
| BLEVE | Boiling Liquid Expanding Vapour Explosion |
| BS | British Standard |
| CCPS | Center for Chemical Process Safety |
| CFD | Computational Fluid Dynamics |
| CPR | Committee for the Prevention of Disasters (the Netherlands) |
| COMAH | Control of Major Accident Hazards (Regulation) |
| EGPIDC | European Gas Pipeline Incident Data Group |
| EPSC | European Process Safety Centre |
| EU | European Union |
| f | Frequency, p.a. |
| F | Cumulative frequency, p.a., as in F-N curve |
| FAR | Fatal Accident Rate |
| F-M curve | Log-log plot of cumulative Frequency- Tonnes of spill |
| FMEA | Failure Mode and Effects Analysis |

| | |
|---|---|
| F-N curve | Log-log plot of cumulative Frequency- Fatality |
| HAZOP | Hazard and Operability Study |
| HSE | Health and Safety Executive (UK) |
| IEC | International Electrotechnical Commission |
| IRPA | Individual Risk Per Annum |
| ISA | Instrumentation, Systems and Automation Society, USA |
| ISD | Inherently Safer Design |
| ISIR | Individual Specific Individual Risk |
| km | Kilometre |
| LIC | Level Indicator Controller |
| LOPA | Layer of Protection Analysis |
| LSIR | Location Specific Individual Risk |
| LT | Level Transmitter |
| LTIR | Lost Time Injury Rate |
| OH&S | Occupational Health & Safety |
| p.a. | per annum |
| PIC | Pressure Indicator Controller |
| PLL | Potential Loss of Life |
| PRA | Probabilistic Risk Analysis |
| PSA | Probabilistic Safety Analysis |
| PSV | Pressure safety Valve |
| PT | Pressure Transmitter |
| PZAHH | Pressure Trip and Alarm High High |
| QRA | Quantitative Risk Analysis |
| RI | Risk Integral |
| RP | Recommended Practice |
| SDV | Shutdown Valve |
| SIL | Safety Integrity Level |
| SIS | Safety Instrumented System |
| SMS | Safety Management System |
| UKOOA | United Kingdom Offshore Operators Association |
| US EPA | US Environmental Protection Agency |

# 10 DECISION MAKING UNDER UNCERTAINTY

*"One factor that makes risk probabilities potentially complicated is that experts often cannot provide absolute probabilities of risk factors. Instead, they commonly offer only relative risk levels. In other words, while experts can often offer insights into how to reduce certain risks, it is seldom that they can tell anyone what a given risk really is."*

*Norman Schulz*
*Intractable conflict knowledge base project University of Colorado, 2003*

In engineering design we are used to applying standard formulae, codes and standards, and arrive at an engineering solution, e.g. sizing of equipment. The information on which decisions are made is essentially deterministic, the uncertainty being confined to the range of accuracy of the design formulae used. The decision to construct is then straightforward, with some safety factor added to the design to cover uncertainty, e.g. an increase of 10-15% of the area of a heat exchanger.

When the consequence of a hazardous event is known, but the likelihood is known only as a probability, decision making has to be done under a cloud of uncertainty. The number of variables involved is large, and there are complex interactions. Therefore the decision makers need to be aware of a number of issues and seek additional information in order to make a balanced decision.

The decision making is not always on the part of a corporation only, which is mainly a commercial decision. There are also issues related to decision making in the public sector. This often involves approvals for commercial projects, build operate transfer (BOT) projects of public utilities and infrastructure, and decision to introduce new regulations that would affect the public and corporate life.

In the preceding chapters, we have described how to identify hazards and assess the risk both in terms of consequences of the loss event and the likelihood of occurrence. In this chapter, we shall take this concept one step further as to how decision making takes place when there is uncertainty on the information available. Here risk management is not viewed as a purely engineering process, but as a socio-technical process.

## 10.1 NATURE OF UNCERTAINTY

The main objective of performing a risk analysis is to support the decision making process. Often, risk analysis has to be conducted with a combination of insufficient data and engineering judgement, and the risk analyst is sometimes cynically referred to as the "shaman of the industry".

The uncertainty in risk assessment can be broadly divided into the following categories (Quelch and Cameron 1994, Apeland et al. 2002, Nilsen and Aven 2003):

1. Epistemic uncertainty
   This uncertainty is inherent to the deviations between the real world and its simplified representation in models. The deviations may be due to limitations in the analyst's knowledge of the phenomena, or lack of adequate data on the phenomena. This uncertainty is termed *epistemic*, i.e. arising from lack of knowledge only.
2. Quantified uncertainty
   The randomness inherent in the system creates uncertainty. Examples are the random failure of specific equipment or components, or the variability of human responses to the same dose of toxic gas. This randomness implies that, even if it were possible to measure a model parameter precisely (e.g. wind speed), and if the same model were used in all the calculations, there would still be variations in the results of repeated calculations, as the measured variable does not have an exact value.

Stone and Blockley (1993) have defined four types of engineering problems based on system failures, and suggested methods of approach in their assessment (see Table 10-1).

TABLE 10-1 TYPES OF ENGINEERING PROBLEMS

| Type | Description | Decision making | Possible method |
|---|---|---|---|
| 1 | Consequences known for certain | Certainty | Deterministic |
| 2 | Consequences precisely identified, but only probabilities of occurrence known | Risk | Bayesian |
| 3 | Consequences approximately identified, possibilities of ill-defined fuzzy consequence known | Vagueness | Fuzzy sets |

| | | | |
|---|---|---|---|
| 4 | Only some of the consequences (precise or fuzzy) have been identified | Open world | Interval probability support logic |

In process risk management, we can often find ourselves in Type 2 or Type 3 problem situations. Recent advances in hazard consequence analysis has helped to identify and define the consequences of hazardous incidents with less uncertainty, and hence risk based decision making has been widely accepted.

When the risk level has been quantitatively assessed, it still leaves the question of how wide is the band of uncertainty in the risk level. To treat the risk as a point value to be compared with a numerical target, and say ‘yea’ or ‘nay’ to a decision is oversimplifying the problem. Such an approach can and has in the past led to more problems than what was being solved. Risk should strictly be treated as a probability distribution with confidence limits on the expected value of the distribution.

In a similar approach to Stone and Blockley (1993), Cho et al. (2002) summarise the approaches as follows:

1. When historical data is sufficient and available, the probability of each risk on potential failure paths can be evaluated by using a simple frequency analysis.
2. If data is insufficient, probability theories such as the Bayesian approach is used by complementing the inadequacy of data by simulation.
3. If the data is not available at all, the probability of occurrence of each path may have to be assessed by subjective judgements based on experts’ experience and knowledge.

In order to apply the above methods for decision making, the limitations of risk analysis should be clearly understood.

## 10.2 LIMITATIONS TO RISK ANALYSIS

The risk assessment techniques described in the previous topics can be classified into two major classes, or a combination of these (Covello and Merkhofer 1987):

1. Methods based on the classical perspective
2. Methods based on modelling, both in the representation of causal relationships and in the use of probabilistic estimates.

Engineering risk assessment uses a combination of both the above techniques, and carries with it the limitations of each of the above.

### 10.2.1 Methods Based on a Classical Perspective

The classical approach directly uses the statistical database on risk, and attempts to fit probability distributions to the data from which predictions can be made. The following examples illustrate the technique.

**EXAMPLE 10-1 PREDICTIONS BASED ON HISTORICAL DATA**

a) In the petrochemical industry manufacturing vinyl chloride monomer (a raw material for PVC plastic), over a long period of time in the 1950s and 1960s, an average of 0.05% of the worker population developed a certain form of cancer. If no changes are made to the working environment, then the estimate of the inferred risk is that 0.05% of workforce will continue to develop this cancer. Such estimates are not uncommon in epidemiological studies.

b) In a process facility, there has been an average of 14 days per year of lost production from equipment failures. This amounts to 4% unplanned downtime for the plant that operates 350 days in a year. The insurance company inferred that 4% of unplanned downtime would occur each year, and had even included this in the assessment of deductibles and the premiums.

There are a number of limitations to the above method:

- The statistical database is generally limited. For statistical methods to be valid, an adequate sample size is required in the database. This is often not the case.
- The database does not reflect the uncertainty over the possible changes that may have occurred since the data were collected and cannot readily be updated to reflect changing information.
- The distributions fitted to the data carry their own uncertainties. For instance, log-normal and Weibull distributions have large 'tails'. The 'tail' is a convenient mathematical representation, but can heavily influence the mean and variance of the distribution.
- The classical method does not characterise the risk sources, exposures and their consequences, but focuses purely on the statistical occurrence of events, based on past data.
- In the classical method, the contributors to risk are not identified in a structured fashion and therefore it is difficult to develop a targeted risk reduction and management strategy.

The historical statistics method is inadequate or not suitable for decision making on major loss events, particularly where data availability is poor.

### 10.2.2 Methods Based on Modelling

The methods based on modelling include characterisation of risk sources through systematic hazard identification techniques, evaluation of consequences from effects and vulnerability models, and estimation of event outcome as a combination of several contributing factors using fault tree and event tree analysis. In other words, the modelling methods are based on the information provided in Chapters 5 to 9.

The measures of uncertainty in the model parameters are propagated through the overall model to obtain quantitative measures of risk with stated confidence limits.

### EXAMPLE 10-2 PREDICTIONS BASED ON MODELLING

In Example 10-1(a) we saw how the future cancer risk is predicted purely from historical data. In the modelling technique, the following measures would be used:

- Identify all sources of exposure to the chemical. These would include both accidental emissions of larger quantities and fugitive emissions as part of normal operation.
- Establish atmospheric concentration levels from stationary monitoring equipment.
- Evaluate individual exposure to the chemical both from work practices and the time spent in the area by a person, as well as individual exposure monitors carried by the person for fixed periods of time.
- Using the dose-response information available from animal bioassays, estimate the incremental risk of cancer to the individual.

The above method uses a number of modelling techniques, in addition to statistical data on dose-response relationships, in arriving at the risk estimate.

In Example 10-1(b), instead of accepting a 4% unplanned downtime, if a systematic hazard identification technique is used, the causes of the failure could be better established. A typical modelling approach would be as follows:

- Identify failure causes by a structured identification technique (e.g. FMEA). Identify failures from both linear and complex interactions. This would show that a shutdown could occur by the failure of one or more components, or a combination of events.
- Construct a fault tree or event tree to develop the logical paths by which the failure event (plant shutdown) could occur.
- Use the statistical database of component failures to quantify the tree. This part is common to the classical approach, but the database on component failures generally has a larger sample population.
- Identify the significant contributors to the top event. The analysis would invariably show that not all the component failures would result in the same downtime, as some of these can be replaced quickly and the plant started up again.
- Identify the measures that could be taken to minimise critical failures, e.g. improvements to preventive maintenance strategy, reliability centred maintenance, spare parts management to minimise downtime caused by lead time in obtaining spare parts.
- Finally, conduct a sensitivity analysis to quantify the extent to which unplanned downtime can be reduced. This increased productivity is the benefit against which the additional cost of maintenance, spare part inventory, etc. can be measured in order to make a decision.

The modelling approach, on the face of it, appears to provide better information than the classical approach. This is true to a large extent. However, the question is, can the modelling approach provide a high enough confidence for decision-making purposes? In answer to this, the limitations of the modelling approach should be appreciated.

In many instances, it is difficult to prove the validity of the model employed. A model is a simplified mathematical version of the real world, and necessarily involves approximations for the sake of simplicity and computational ease. In some instances, local environmental conditions, which models cannot fully account for, influence the event consequences.

**EXAMPLE 10-3 MODEL INACCURACY**

During the first Gulf War of 1990, the occupying Iraqi forces in Kuwait had set fire to the oil wells. The sulphur in the sour crude oil generated sulphur dioxide in the combustion process, which dispersed with the smoke plume in the atmosphere.

An attempt was made by a team of international scientists to model the atmospheric dispersion process. Twelve well-known air dispersion models were used. None of the models could predict the measured ground level concentrations of sulphur dioxide even closely. The predictions of atmospheric concentrations were always higher than the actually measured levels.

Subsequent investigation showed that the soil in the area contained significant limestone deposits, which absorbed the sulphur dioxide from the air, consequently giving lower atmospheric concentrations downwind. None of the scientists had accounted for this environment in the modelling.

Other problems with the modelling approach are:

- Complexities of some techniques require specialist assistance (finite-element modelling for structural damage assessment, computational fluid dynamic (CFD) models for gas dispersion and fire/explosion in congested areas).
- When modelling is used in risk assessment of exposure to chemicals (such as in Example 10-1, the extrapolation of animal experimental data to humans is fraught with a high degree of uncertainty.
- Most models either do not take into account the contribution of human error or management system failures to the risk event, or at best this impact is modelled poorly in our current state of understanding of human error situations. Therefore the risk estimated by modelling could only provide a measure assuming 'good management and good training of operators', where human error potential is low. A risk assessment of a labour-intensive facility using event tree logic would involve a higher degree of uncertainty.
- The probability distributions used in the modelling are often subjective and depend on the skill and experience of the analyst. While this subjectivity is acceptable for decisions relating to individual risk, there is no firm theoretical foundation for subjective probability distributions in group or societal risk decisions (Bier, 1999), e.g. siting a major hazard facility near population centres.

- Management and organisational factors have an effect on assessed risk. The influence is not only through human error, but also due to the fact that there is no single "correct" management style, corporate culture or organisational structure. For example, the effect on equipment failure rates due to poor maintenance practices is difficult to account for accurately in the analysis.
- As observed by Bier (1999), "It is easy to get a feeling for corporate culture. The prevailing philosophy in a particular organisation is progressive or reactive; rigid or flexible; inquisitive or defensive ... What is much more difficult is to assess the quantitative impact of that culture ..."
- Any risk assessed by modelling is only valid if the management and organisational factors with regard to managing risks are at or above industry average for the specific installation. Otherwise the risk assessed is not meaningful.

Often in the wake of a major accident event, the subsequent inquiry asks 'Could this incident have been anticipated or identified, and prevented?' Some people may answer in the affirmative. However, the number of variables in some complex interactions could be so large that it is not possible to accommodate all of them in a manageable model that can be quantified. This aspect is still the single greatest limitation of the methods based on modelling.

In spite of its limitations, the modelling method is the best tool available to date for risk assessment and obtaining information for risk management and decision making.

## 10.3 UNCERTAINTIES IN RISK ESTIMATION

### 10.3.1 Quantitative Risk Assessment and Uncertainty

Quantitative Risk Assessment (QRA) is mainly used as a decision support tool to demonstrate that the risks to people and the environment from a hazardous activity have been reduced to a level considered acceptable or tolerable, subject to meeting a number of criteria (see Sections 10.4 and 10.5). QRA is also used to compare the safety performance of a number of alternative design configurations, on a consistent basis.

Because of the uncertainties associated with QRA, it is necessary to understand the nature of the uncertainties, and, if possible, obtain an estimation of the uncertainty, to improve the decision making process.

### 10.3.2 Sources of Uncertainty

We have seen in Chapters 8 and 9, by frequency analysis and risk estimation techniques, point values of risk can be generated. We often use the expression that the risk is assessed 'conservatively' or 'pessimistically'. This means that the point value calculated is likely to be higher than the expected value of risk. Strictly speaking, we have no basis for making this statement unless the expected value of risk is known.

From the definition of risk in Chapter 1, we know that risk is a probability. Therefore, the probability would follow a statistical distribution. Once the distribution is known, then its mean and variance can be calculated, the mean providing the expected value, and the variance providing information on the band of uncertainty around the expected value, for specified confidence intervals.

The major problem is: What is an appropriate probability distribution for risk, and how can it be assessed? For this, it is necessary to understand the sources of uncertainty. A partial list is provided in Table 10-2, adapted from UKOOA 1999.

TABLE 10-2 SOME SOURCES OF UNCERTAINTY IN QRA

| No. | Uncertainty factor | Uncertainty type |
|---|---|---|
| 1 | Generic failure rate data from databases for loss of containment | Input data |
| 2 | Hole size or release rate distribution and duration for loss of containment scenarios | Input data |
| 3 | Ignition probabilities for loss of containment of flammables | Input data or dispersion model and identification of ignition sources |
| 4 | Generic failure rate data from databases for protection system components for fault tree/event tree analysis | Input data |
| 5 | Consequences of fires, explosions, and toxic releases (effects models) | Model |
| 6 | Consequences of fires, explosions and toxic releases (vulnerability models) | Model |
| 7 | Escalation analysis from fires and explosions | Model |
| 8 | Assumptions made by the analyst for modelling or adoption of certain data in preference to others | Engineering judgement |
| 9 | Human error rates used for risk quantification | Input data |
| 10 | Inadequate knowledge of the impacts of releases or reactivity hazards | Knowledge uncertainty |
| 11 | Subjective decisions by analyst in modelling. This is based on the experience of the analyst apart from the assumptions made in Item 8 above. | Analyst's experience level |

### 10.3.3 Estimating Uncertainty

Estimating uncertainty is a difficult exercise and is resource intensive. Therefore, the need to estimate uncertainty should first be established. If the QRA is used strictly for comparison purposes for selecting between alternative design configurations, the risk results are generated from the *same* source of generic data and compared on the *same* basis. Therefore, an estimation of uncertainty may not be necessary. On the other hand, if the calculated risk is higher than a level considered tolerable, then significant efforts need to be made to estimate uncertainty and to minimise it, in order to obtain a better picture of risk for decision making.

One simple way to estimate uncertainty is to conduct a sensitivity analysis on the principle assumptions made in risk analysis. Some of the areas of sensitivity analysis are:

- Loss of containment scenarios postulated (hole size, release rates, duration)
- Failure rates of equipment and protection systems

- Human error rate used in analysis
- Allowances for management factors in failure rates

The risk values obtained for the various sensitivity cases would indicate which assumptions are critical in influencing the risk and which are not. Attention can then be focused on the critical assumptions, with the view to making them more robust.

### 10.3.4 Fuzzy Set Techniques in Estimating Uncertainty

Fuzzy sets allow vague concepts to be defined in a mathematical sense. In classical set theory, an object either belongs to a set or does not belong to a set, whereas fuzzy set theory allows an object to have partial membership of a set. Using fuzzy sets, it is possible to represent a set A by a membership function $\mu_A(x)$ that maps the members of the set into the entire unit interval [0,l]. The value of $\mu_A$ (x) is called the grade of membership of x in A. Compared to crisp sets, fuzzy sets correspond to continuous logic: all shades of grey between black and white and all values between 0 and 1 are possible.

The concept of a continuous grade of membership (rather than a binary one) allows us to describe vague concepts in a more complete manner. A fuzzy set can also be viewed as a possibility distribution, as opposed to a probability distribution.

While a probability distribution is subject to the laws of statistics, the shape or structure of a fuzzy set is subject to few mathematical constraints. For example, the laws of statistics require that the sum of the probabilities associated with a random variable must equal 1. However, the sum of the grades of membership of a fuzzy set is not required to equal 1 and it is therefore possible for more than one member to have a grade of membership equal to 1. It is this flexibility of fuzzy sets that makes them ideal for representing vague concepts in risk assessment where the information available is often insufficient for use of probability theory.

The application of fuzzy sets for uncertainty estimation in risk analysis is described by Quelch and Cameron (1994) and Cho et al. (2002).

### 10.3.5 Monte Carlo Method

The direct inputs to the likelihood estimates can be expressed as probability distributions drawn from source data or from a combination of data points and expert judgement, or simple triangular distributions drawn from a few points. There are several Monte Carlo simulation packages that generate the final outcome distribution, with a mean (expected value of risk) and standard deviation (uncertainty).

This approach is more sophisticated than the fuzzy set approach and requires significant effort to generate the outcome distributions for complex QRA studies.

## 10.4 THE *DE MINIMIS* CONCEPT

In the *de minimis* concept, if the assessed value of risk is at or below a minimum risk level set as a target, the risk is considered acceptable, and below regulatory concern. This concept has been applied in the past for decision making on planning approvals for hazardous facilities near populated areas and vice versa.

A distinction must be made when the *de minimis* concept is applied for planning decisions, and for decisions to grant an operating licence that is generally under the jurisdiction of different regulatory authorities. The former decision is based on potential for offsite impact from major accident events in a process facility, using conservative assumptions, and the risk assessed is generally seen as the lower bound of tolerability (HSE 1988, 1989, 1990).

On the other hand, a licence to operate includes risks to personnel on site, and these risk levels generally exceed the *de minimis* level used for planning decisions. Decision making in such situations is based on the demonstration of the ALARP (As Low As Reasonably Practicable) principle by the operator.

## 10.5 CONCEPT OF ALARP

### 10.5.1 The Risk Triangle

To allow for the uncertainty in risk estimation, the risk range is divided into 3 groups, as shown in Figure 10-1 (HSE 2001).

**Region 1: Risk unacceptable.**

Risk is so high that it is not acceptable unless extraordinary circumstances apply. Risk reduction must be undertaken.

**Region 2: Risk tolerable if ALARP.**

Risk reduction measures must be implemented where reasonably practicable. That is unless further risk reduction is clearly not possible or the cost is disproportionate to the improvement gained.

**Region 3: Risk broadly acceptable.**

Risks must be managed to ensure that they remain at this level and, if practicable, continually reduced. In principle, the ALARP concept extends to this region as well.

In Australian regulations or guidelines, the boundary between the "broadly acceptable region" and the "tolerable if ALARP" region have not been defined, thus extending the ALARP concept to include the broadly acceptable region. UK HSE (2001) suggests a fatality risk level of $1x10^{-6}$ per annum at this boundary.

### 10.5.2 ALARP Concept

When the assessed risk is above the broadly acceptable level, but below the unacceptable level, then risk reduction is expected to be carried out by a corporation to a level 'As Low As Reasonably Practicable' (or ALARP).

The issue of applying the ALARP principle should be carefully considered as it can be highly subjective, as the questions of what is 'Low' and what is 'Reasonable' remain rather vague.

A corporation may argue that spending any money at all is not reasonable and that after designing the facility to current codes and standards, the residual risk is below the intolerable level, and therefore no further action is required.

On the other hand, the regulator may argue that the compliance with codes and standards alone does not result in a risk level below *de minimis* levels and hence additional risk reduction measures beyond the codes and standards would be warranted.

The term *as low as reasonably practicable* was originally raised in the Health and Safety at Work Act of the UK, administered by the Health and Safety Executive (HSE). The interpretation of these words is also provided in the Act.

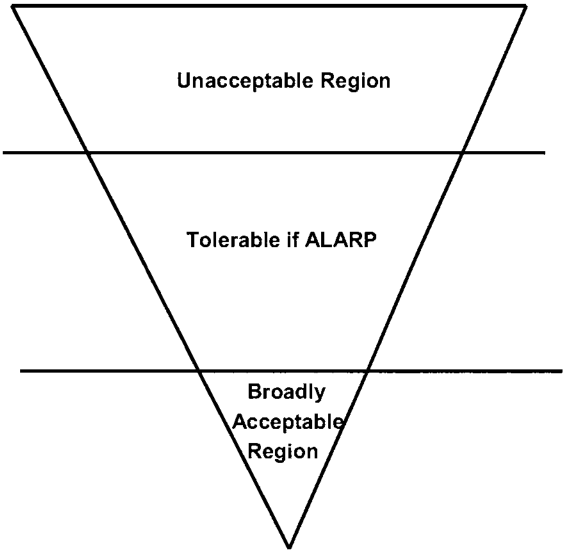


**FIGURE 10-1 THE UK HSE FRAMEWORK FOR RISK TOLERABILITY**

*'Reasonably Practicable' ... implies that computation must be made in which the quantum of risk is placed in one scale, and the sacrifice, whether in money, time or trouble, involved in the measures necessary to avert the risk is placed in the other; and that, if it be shown that there is a gross disproportion between them, the risk being insignificant in relation to the sacrifice, the person on whom the duty is laid discharges the burden of proving that compliance is not 'reasonably practicable'* (Kletz 1990).

In Australia, the UK HSE interpretation is generally adopted by regulators, even though the term 'reasonably practicable' in health and safety regulations is not explicitly defined. The Victorian Major Hazards Control Regulation (1999) uses the expression "so far as is practicable".

The guidance note on OHS (Major Hazards) Regulations in Victoria (2001) defines "practicable" as "having regard to":

- The severity of the hazard or risk in question
- The state of knowledge about the hazard or risk and means of removing or mitigating the hazard or risk
- The availability and suitability of ways to remove or mitigate that hazard or risk
- The cost of removing or mitigating that hazard or risk

Under this principle, an organisation needs to make a decision whether there are technically feasible and effective methods of reducing the risk and if so, whether or not the cost (including capital and ongoing maintenance or operating costs) required to obtain a reduction in risk is *grossly disproportionate* to the benefit gained.

The following factors come into consideration in assessing practicability under the ALARP principle:

1. Can the consequences be eliminated?
2. If elimination is not possible, can they be mitigated?
3. What are the possible mitigation measures?
4. Are the mitigation measures within engineering practicability?
5. If it is not practicable to design the mitigation measure due to engineering constraints, then can the likelihood of an occurrence resulting in the consequence be reduced?
6. What are the possible likelihood reduction measures?
7. Are the likelihood reduction measures within engineering practicability?
8. What are the benefits of the risk reduction measures? This may not be a reduction in public risk alone, but should also address risk to employees, benefits gained in minimising interruptions to operations etc.

Once a final set of practicable measures are compiled, the reasonableness criteria is applied. One of the tools used in quantitative risk analysis is the Cost of Preventing Fatality (CPF). It is also known as 'Implied Cost of Averting a Fatality' (ICAF). The HSE (2001) warns that the CPF should not be used as the sole criteria for determining if ALARP level is reached. It is necessary to demonstrate that the cost of additional risk reduction measures is grossly disproportionate to the benefits gained.

In contrast, the US Occupational Safety and Health Administration (OSHA) does not address the issue of how much its standards would cost the industry, but tends to be more prescriptive in its regulatory approach. It gives no formal indication of whether, in picking a suitable 'substitute' or a 'feasible' exposure level, any weight would be given to economic considerations as well as technological ones (Kletz 1990).

If the risk reduction options are compiled and costed, the selection of the relevant option can be justified in terms of costs and risks, to satisfy regulatory requirements and to meet corporate risk targets. A cost-benefit analysis becomes an essential tool in the implementation of the ALARP principle (HSE 2001).

Schofield (1998) has suggested that the alternative is to use the Bayesian approach, where a 'utility' value is allocated to each outcome. This may be termed 'disutility' for adverse outcomes, as we are discussing loss events. For each event, a set of utility expectation values is obtained. Maximum expected utility (or minimum expected disutility) is then used as the ALARP criterion for decision making. According to Schofield (1998), there is a fundamental difference between the terms 'practicable' and 'reasonably practicable'. The practicability of a risk reduction measure is concerned with technical feasibility without regard to cost of implementation, where reasonable practicability considers cost in relation to risk reduction (HSE 2004, Clause 6). Thus in the ALARP demonstration, the thrust is not in the direction of the regulator needing to show that the measure is *reasonably practicable*, but in the direction of implementation of the measure if the duty holder cannot show the measure to be *not reasonably practicable*. Schofield (1998) argues that in such cases the Bayesian approach of minimising disutility may be better than that of the classical probability interpretation. This is consistent with the arguments of Evans and Verlander (1997) for major transport accidents.

### 10.5.3 Societal Risk Considerations

The concept of F-N curves for risk representation of societal risk was described in Section 9.4.6.3.

Specifying the acceptability band on F-N curve requires two numerical decisions: its slope and its intercept on the vertical axis. The slope of the line is related to risk aversion of major accident events, relative to smaller accidents. In general, the steeper the slope, the greater is the aversion, and a slope of –1 may be taken to be accident size–neutral (Evans and Verlander, 1997). The intercept is typically determined with reference to standards set by similar decisions elsewhere (HSC, 1991).

An alternative to the F-N curve is based on the theory of decision making under uncertainty (Evans and Verlander, 1997). What is uncertain is the number of accidents of each size that will occur in any given period. Treating the occurrence of total accidents as a Poisson process with mean frequency f per unit time, and the probability that there are exactly n fatalities as *P(n)*, the frequency of accidents with n fatalities is *f.P(n)*. Decision making under uncertainty is done on the basis of expected utility, u. In this case, the expected value is related to fatality and hence the work 'utility' may not be the most appropriate. Evans and Verlander (1997) suggest the term 'disutility' if the measured quantity is an adverse outcome. They derive the formula

$$u = \sum_{n} n^{\beta} f(n) \tag{10.1}$$

where n is the number of fatalities and f(n) is the frequency with which the given number of fatalities may occur.

If we choose a value of β = 1, then u becomes the product of number of fatalities times the frequency with which the number of fatalities may occur, summed over all possible accident events. This is the same as Potential Loss of Life (PLL) and is a useful tool in making decisions. However, a threshold value must be chosen and PLL does not include consideration of aversion to multiple fatalities.

Evans and Verlander (1997) demonstrate that the criterion based on F-N curves does not come up with the same judgement for the same safety situation, and thus fails an essential logical test for a prescriptive criterion. On the other hand, minimising the expected disutility of incidents is preferable as a tool for decision making under uncertainty. For risk aversion to large scale accidents, $\beta$ is <1. Some authors have suggested a value for $\beta$ between 1.5 and 1.8 based on a judgemental value of human life. The petroleum industry tends to use $\beta = 1$, and minimising the PLL value is used as a tool in risk management. Hirst and Carter (2002) have used a value of 1.4 in the calculation of an approximate risk indicator (see Section 9.4.6.4).

For land use planning purposes, Section 9.6.2.1 gave limits for the ALARP triangle range in terms of approximate risk indicators (ARIs)(Carter et al. 2003).

The ARI values can be used in the boundary demarcation lines for the triangle in Figure 10-1, as a first pass assessment of societal risk to the public in the vicinity of major hazard installations.

### 10.5.4 Demonstration of ALARP

In general, decision making on the part of a regulatory authority to grant an operating licence is based on whether or not the corporation has adequately demonstrated that it has the capability to manage process safety to a risk level considered ALARP. Besides ALARP in a technical sense, the decision making process also integrates other relevant factors such as economic, social and political.

The following items provide guidance on ALARP demonstration.

1. Compliance with codes and standards.
   The first consideration is that the facility is designed to relevant codes and standards, consistent with current industry practice. Since codes and standards specify minimum requirements, such compliance, while necessary, is by no means sufficient for ALARP.
2. Meet regulatory and corporate criteria for risk levels
   The next step in the demonstration is a formally documented hazard identification and assessment process, including risk quantification, where there is numerical criteria available for comparison. However, meeting risk criteria alone is insufficient, as the risk assessment is associated with a number of uncertainties. Therefore, it is necessary to list the sources of uncertainties, and an attempt has been made to reduce uncertainty to the best effort possible. The objective is to demonstrate that the risk is within the acceptable range, and hence tolerable, subject to consideration of further risk reduction measures.
3. Verification scheme.
   This step involves peer reviews and third party reviews. Such verification is more common in the offshore oil and gas industry, as the installation needs to be certified by a marine classification society.
4. Critical evaluation of barriers to incident causes, and incident escalation.
   A bow-tie type analysis (see Section 8.3.3) or equivalent may be used. It is necessary to demonstrate that there are **independent and effective barriers** for each threat and for each consequence. The overall effectiveness of each control measure is assessed through the parameters

such as the effectiveness of the barrier in controlling the incident, its reliability, availability and survivability.

5. Identification of additional possible risk reduction measures. Three sources are used for identification of risk reduction measures:
   a) The significant contributors to risk are ranked in descending order, and risk reduction measures are identified for each contributor. Sensitivity analysis is carried out on the extent of risk reduction possible by the implementation of these measures.
   b) Additional barriers are identified where there are insufficient independent barriers in Step 4 above.
   c) Measures for improving the overall effectiveness of barriers identified in step 4 are identified.

   The risk reduction measures need not always be hardware measures. They can be procedural measures based on a Safety Management System (SMS). In fact, an effective strategy is to strive for a healthy balance between hardware and administrative controls (Tweeddale 2003).
6. Cost-benefit analysis of the risk reduction measures.

   The next step is to undertake a cost-benefit analysis of the risk reduction measures, to identify whether the expenditure on a control measure is justified. If not, this step needs to demonstrate that the costs of additional measures are grossly disproportionate to the benefits gained. For a discussion on cost-benefit analysis, see Section 10.6.2.
7. Robustness of the SMS

   It is not sufficient to demonstrate that there are hardware systems and procedures to prevent an accident or mitigate its effects. Since the SMS is the day-to-day driver for process safety management, it is also necessary to prove the robustness of the SMS. This includes the following:
   - a comprehensively designed SMS
   - a register of safety critical systems and activities
   - performance standards for safety critical systems and key performance indicators thereof
   - defined responsibilities and accountability
   - training and competency standards
   - auditing and feedback system for management information and control.
8. Stakeholder involvement

   There should be documented demonstration of stakeholder involvement. The stakeholder issues include:
   - Participation of workforce (employees and contractors) in the hazard identification and evaluation process
   - Communication of risk results and contributors, and the management of hazards to workforce
   - Communication of risk results to neighbourhood community (industrial and residential)
   - Emergency response plan for on-site emergencies
   - Emergency response/communication protocol for incidents that could have offsite impact on neighbouring industrial installations

- Emergency response for incidents that could have offsite public impact. The requirements vary. For instance, in the UK, this needs to be prepared by the local government authority (County level), with significant input from the facility management. In Australia, this emergency response procedure is prepared by the facility management, in consultation with local authorities (local government councils, fire authority and police where appropriate).
- Consultation with relevant regulatory authorities responsible for administering the major hazards regulations
- Communication of product safety information to users and customers through Material Safety Datasheets (MSDS)

9. Environmental considerations based on sustainability (Clift 1998) and the precautionary principle (Lofstedt 2003).

High among the priorities should be the incorporation of inherently safer design wherever possible to eliminate the hazard, so that corresponding mitigation measures may not be necessary. The challenges of inherently safer design are examined by Dalzell and Chesterman (1997), and further discussed in Chapter 12.

The demonstration of ALARP requires significant resources and effort and should not be treated lightly. To the question whether health and safety is a burden on business, Sir John Cullen, the former Chairman of the Health and Safety Commission in the UK said (Cullen 1994):

> *"There is a huge potential benefit, both economically and socially, which management has yet to realise. But when it does, I believe it will be by the end of the next decade, we shall have a socially acceptable industry capable of generating wealth."*

The major hazard control regulatory impact on the process industry in various industrialised nations in the last decade has succeeded to a large measure, in fulfilling this perception.

## 10.6 DEALING WITH UNCERTAINTY

The first step in dealing with uncertainty is to recognise uncertainty, its sources, perceptions influenced by lack of facts and precision in technical work, and its impact. Briggs (2004) provides a comprehensive guide in this area for the process industries.

## 10.6.1 Critique of Parameters Causing Uncertainty

In making capital investment decisions by a corporation, or decision to grant a planning approval or operating licence by the respective regulatory authority, the following parameters should be critically examined:

### *10.6.1.1 Assumptions made in process hazard analysis and risk assessment*

The analyst has to make a number of assumptions in conducting a hazard analysis and risk assessment. The necessity to make assumptions has been recognised as inevitable. The critique should cover the following:

- Have all the assumptions been fully listed?
- Are adequate justifications provided for the assumptions? These include:
  - research data
  - literature data
  - past incidents review
  - appropriateness of failure rate databases used
  - adjustments made to generic failure rate data based on environmental conditions or managerial influence factors
  - release modelling assumptions
  - consequence modelling methods
  - validation of software
  - engineering judgements made by the analyst
  - human error and performance
  - statistical validation if failure data is fitted to a distribution
- Justification for screening out an identified hazardous event from detailed analysis. This is sometimes done on the basis of perceived low frequency, but unfortunately has resulted in major incidents .

### *10.6.1.2 Confidence in the completeness of hazard identification*

It is necessary to develop confidence in the hazard identification method and the completeness of hazard identification. The issues are:

- The hazard identification techniques used and their appropriateness for the facility under consideration
- Evidence of reference to historical incidents in similar facilities and their relevance to the facility considered
- The composition of the hazard identification team and the experience of the facilitator
- Life cycle considerations in hazard identification.

### *10.6.1.3 Sensitivity analysis*

Estimation of uncertainty can be assessed by the extent of sensitivity analysis carried out. The issues are:

- What are the critical assumptions that influence the risk results?
- Has a sensitivity analysis been carried out on the assumptions?
- What is the dispersion of the data in the results and the standard deviation?
- Can the results be reasonably used to evaluate different plant configurations or risk reduction options, when compared on the same basis?

### 10.6.2 Cost-Benefit Analysis

Risk reduction measures can be hardware based, administrative controls based, or a combination of both. The general philosophy of risk management is that if a risk reduction, however small, can be achieved by administrative control (SMS procedures) using existing resources, then it should be implemented, and a cost-benefit analysis (CBA) may not be required.

When a hardware solution is identified, a CBA is generally conducted. It takes the following steps:

1. Calculate the monetary loss resulting from the accident event (asset loss, business interruption, consequential losses).
2. Multiply the frequency of the accident event by the loss estimate to obtain a probable loss per annum ($ pa).
3. Calculate the revised monetary loss as a result of the risk reduction measure. If the control measure is for mitigation of consequences, then the revised monetary loss would be lower. If the control measure is only a reduction in the frequency of the event without mitigating the consequences, then the loss value would remain unchanged.
4. Calculate the revised frequency of the accident, assuming the new control measure in place.
5. Calculate the revised probable loss (new frequency times new loss value in $)
6. The difference in the two probable loss values gives an indication of the reduction in loss by the implementation of the control measure. This can be treated as a *de facto* return on investment.
7. Evaluate the life cycle cost of the control measure. This includes both capital cost, design and installation cost, and on-going maintenance costs for the expected life of the component.

Using the reduction in probable loss and the cost of the control measure, the Net Present Value (NPV) can be calculated using a spreadsheet. The NPV is an indication of whether or not it is cost effective to implement the control measure. This exercise is repeated for all the additional control measures identified.

The CBA is simple to evaluate, but considerable information on the loss estimate would be required. This requires minimising uncertainty in the assessment of damage from accidents, replacement costs and downtime.

Some applications of risk based CBA, applied to process plants and pipelines are described by Goyal (1993), Noonan (1993), Woodward and Moosemiller (1996), and Mouney and Schmidt (1997).

The above concept can be applied plant wide, and the results can be expressed in the form of an F-$ curve, similar to the F-N curve, where F is the cumulative frequency with which a specified $ loss may occur. An example is given in Figure 10-2 (Chippindall and Butts 2004). A similar concept is discussed by Evans and Thakorlal (2004).

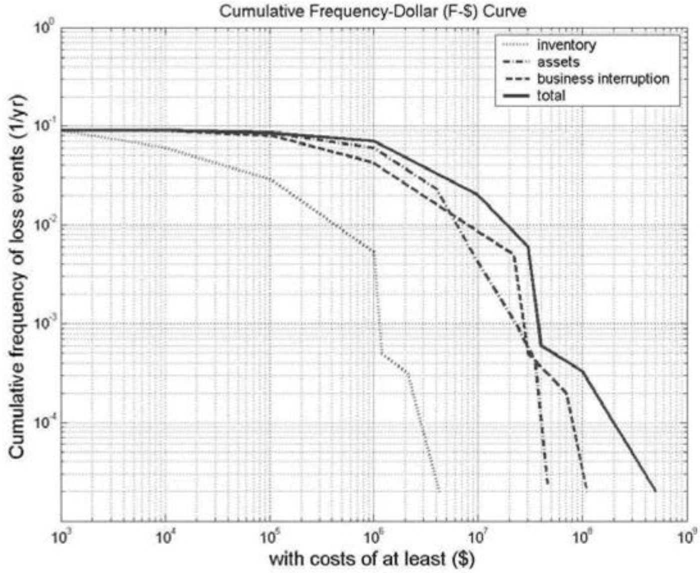


**FIGURE 10-2 F-$ CURVE FOR RISK OF ASSET LOSS**

The above approach for CBA is suitable for business decisions for business interruption risks and asset loss risks. However, the question of CBA for risk reduction measures that could reduce the risk of fatality needs to be addressed carefully. The CPF concept has been suggested in Section 10.5.2. However, this approach has received mixed response on philosophical grounds that it requires a monetary value to be placed on human lives.

The CPF is calculated as follows:

1. Calculate the PLL (p.a.) for the facility from risk assessment
2. Identify the risk reduction measures that could reduce this risk of fatality
3. Recalculate the PLL (p.a.) assuming the risk reduction measure is in place to get the incremental reduction, ΔPLL.

   CPF is calculated as:

$$\text{CPF} = \frac{\text{life cycle cost of the control measure}}{\Delta\text{PLL (p.a.)} \cdot (\text{Remaining life of the plant in years})} \qquad (10.2)$$

At what value of CPF one would make the investment decision is the point of debate. The HSE distinguishes between CPF and the Value of Preventing a Fatality (VPF), and cautions that VPF is not placing a value on life. It is another way of saying what people are prepared to pay to secure a certain averaged risk reduction.

The HSE has given guidelines on judging gross disproportion (HSE 2004b) in regard to fatality prevention. It uses a proportion factor (PF) defined as:

$$PF = \frac{CPF}{VPF} \tag{10.3}$$

and suggests that when PF is less than 1 the measure must be implemented. Moreover for exercising judgements on ALARP it also recommends:

(i) The proportion factor, PF is at least 10 for risks close to the tolerable/unacceptable boundary in Figure 10-1.

(ii) The proportion factor, PF is at least 1 and possibly at least 2 for risks close to the broadly acceptable boundary.

The VPF quantity has been the subject of much discussion and analysis. The HSE typically use a VPF of £1 million (at 2001) which is derived from road safety measures (HSE 2001). In the case of off-shore facilities, a CPF value of £6 million is regarded as a minimum (at 2003), equivalent to a PF of 6 (HSE 2003). Other values of ICAF (or CPF) can be extracted from data of countries belonging to the Organization of Economic Co-operation and Development (OECD). The values, between 1984 to 1994 suggest a range of between $US2 to 4 million (Skjong 2002).

### 10.6.3 Risk Based Decision Making

The philosophy of decision making supported by risk and decision analysis is discussed by HSE (2001) and Aven and Kørte (2003), who provide a model for decision making (see Figure 10-3).

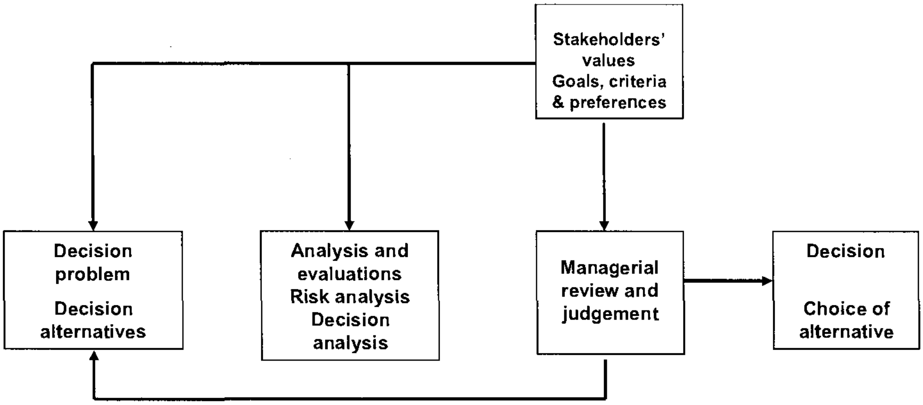


FIGURE 10-3 STRUCTURE OF DECISION-MAKING PROCESS

The main factors influencing the decision process are:

1. **Inherent safety**
   The first consideration is to review if every attempt has been made to incorporate inherently safer design principles into the project. These include elimination, substitution, minimising inventory, separation distances, choice of less severe operating conditions etc. They are described in Chapter 12.
2. **Cost-benefit analysis**
   The idea is to ascribe monetary values to the benefits, and rank the alternatives in terms of a Net Present Value (NPV) or a Return on Investment (ROI). This approach has been widely accepted for asset protection and minimising business interruption risks.
3. **Expected utility analysis**
   This analysis, applied in the reverse form of minimising disutility, requires assessment of choices among alternatives to define utility functions, and is difficult to carry out. The problems of applying this to F-N curves have been discussed earlier.
4. **Usefulness to decision makers and stakeholders**
   A decision that is seen as useful to all parties concerned (regulators, the corporation, public and other stakeholders) is ideal. This concept of 'all things to all' is not practicable, especially when siting a hazardous facility close to a population centre, where the society is said to benefit from the economic activity on the whole, whereas the local community perceives that it bears the brunt of the safety risk of accident events. Aven and Kørte (2003) suggest that it is more informative to focus attention on each consequence and associated uncertainty separately.
5. **Adequacy of ALARP demonstration**
   The adequacy of ALARP demonstration, using the various parameters listed in Section 10.5.4 becomes a critical input to decision making. The decision is based on risk analysis and decision analysis, managerial review and judgement, regulatory review and public participation, overall benefits to stakeholders, and the precautionary principle, where applicable (see Section 10.6.6).

It is recognised that it is not possible to satisfy every requirement of every stakeholder in the decision making process. The main considerations on the part of the regulator are protection of people (employees and public), protection of the biophysical environment (environmental impairment risk and sustainability issues), and protection of property, in that order.

### 10.6.4 Risk Transfer

A corporation generally transfers part of its risk to an insurance provider. These mainly cover asset loss and risk of injury of death to people from accidental events, business interruption risks, and environmental impairment liabilities.

It is hard to decide how much risk to insure and how much to retain. A risk based approach provides a useful tool for risks from major accident events (Chippindall and Butts 2004). In this approach, one should take care that the cost of losses includes not only the asset replacement cost and loss of production costs in the interim, but other consequential losses as well. Often the real costs tend to be much higher than those initially predicted.

### 10.6.5 Residual Risk

A facility management should never forget that the risk analysis and predicted low levels of risk represent the residual risk when the facility is managed well. Otherwise, the residual risk increases significantly and may exceed the ALARP tolerability zone.

The golden rule is:

*"the residual risk shall be kept at the estimated low levels by the effective administration of a robust SMS."*

The robustness of the SMS is reflected in the design of the SMS elements and the supporting procedures. The effectiveness is ensured by auditing and management feedback, followed by corrective actions. Chapters 11 and 14 cover these issues respectively.

### 10.6.6 Risk and the Precautionary Principle

The precautionary principle was part of the declaration at the 1992 Rio Conference on the Environment and Development (Principle 15). Other international conventions such as the UN Framework on Climate Change and the Convention of Biological Diversity refer to this principle.

The precautionary principle is a regulatory tool guiding the decision making process. There have been several interpretations of what the precautionary principle is over the last decade, and controversies still persist (Lofstedt 2003). There is, however, general consensus that when an activity raises threats to the human health or the environment, lack of full scientific certainty should not be used as reason for not undertaking cost-effective preventative or remedial measures.

Where any action is considered as necessary under the precautionary principle the Commission of European Communities (COEC 2000) recommends that the measures should be:

(i) proportional to the chosen level of protection:
   - measures proposed must not be disproportionate to the desired level of protection and should not aim at zero risk. Incomplete risk assessment may limit the options available to decision makers. A broad range of options should be investigated. In this sense the application of the precautionary principle shares much in common with ALARP.

(ii) non-discriminatory in application:
   - implying comparable situations should be treated in a similar manner.

(iii) consistent with similar measures already taken:
   - the means taken should be in-line with those already applied to similar situations

(iv) based on an examination of the potential benefits and costs of action or inaction:
- there is a need to evaluate and compare the likely positive or negative consequences for both short and long term.
- cost benefit analysis cannot be applied solely on economic grounds but must consider the broader socio-technical issues
- consideration must be given to the efficacy of measures and their public acceptability.

(v) subject to scientific review based on new knowledge and data:
- measures remain, subject to on-going inadequacy, imprecision or inconclusive nature of the scientific data. Measures can then be subject to change.

(vi) capable of assigning responsibility for producing the scientific evidence necessary for a more comprehensive risk assessment:
- this is an issue of "burden of proof" where prior approval processes would ensure that corporations provide the scientific evidence that reverses the position that it is "hazardous until proven otherwise". This clearly includes end-use chemical products used by the public.

The precautionary principle has been used by regulators as a means of satisfying a sceptical public with a distrust of both authorities and scientific testing results provided by corporations. The debate on genetically modified foods is a clear example.

In the case of process plant operations that can pose an acute risk to people and the environment from accidental events, in contrast to long-term health effects from low dose exposures, the risk based decision model in Figure 10-2, together with the comprehensive demonstration of ALARP principle, is the best tool currently available.

## 10.7 PITFALLS IN RISK BASED DECISION MAKING

The HSE in the UK has undertaken an evaluation program of risk assessment methodologies used in the industry, in order to identify common pitfalls in risk assessment (HSE 2003). The study covers a number of industries, not exclusively the process industry. A total of 26 case studies are listed in the study. The main pitfalls and lessons learnt for are equally applicable for the process industry, and are summarised below.

1. Risk assessment and cost-benefit analysis used to show that the cost of action required is disproportionate to the benefits, in order to justify an already made 'no action' decision. This use of ALARP in reverse. This also includes selecting the most expensive option to demonstrate that it is not reasonably practicable, rather than selecting and evaluating a range of risk reduction options.
2. Use of QRA carried out on one site applied to another similar site within the same corporation because of similarities in operation, but without regard to surrounding environment.
3. Not assessing societal risk in transportation accident hazards where a large number of people are likely to be affected.

4. Not considering the cumulative risks from all hazardous events on personnel, and applying a risk criteria for individual incidents only.
5. Using ISIR to show the risk is low, where LSIR should have been used as being more appropriate.
6. Consultant owns the study and not the Operator.
7. Risk analysis focused only on steady state operation of the plant and not start-up and shutdown hazards (not all operating modes addressed).
8. Failure to consider common cause failures in QRA
9. Incident escalation excluded in risk assessment by an incorrect assumption, where the time for effective activation of hazard control measures (hardware and procedural) is longer than time for incident escalation.
10. Optimistic assumptions rather than cautious best estimates in identifying possible outcomes, including use of accident statistics based on limited sample size.
11. Not establishing a clear link between the hazard and the control measures.
12. Risk assessment seen as a paper exercise to occupy shelves rather than a living document for use in hazard control.

## 10.8 REFERENCES

Apeland, S., Aven, T. and Nilsen, T. 2002, 'Quantifying uncertainty under a predictive, epistemic approach to risk analysis', *Reliability Engineering and System Safety*, vol. 75, pp. 93-102.

Aven, T. and Kørte, J. 2003, 'On the use of risk and decision analysis to support decision-making', *Reliability Engineering and System Safety*, vol. 79, pp. 289-299.

Aven, T. and Nilsen, T. 2003, 'Models and model uncertainty in the context of risk analysis', *Reliability Engineering and System Safety*, vol. 79, pp. 309-317.

Bier, V.M. 1999, 'Challenges to the Acceptance of Probabilistic Risk Analysis', *Risk Analysis*, vol. 19, no. 4, pp. 703-709.

Bier, V.M. 2001, 'On the state of the art: risk communication to decision-makers', *Reliability Engineering and System Safety*, vol. 71, pp. 151-157.

Briggs, M. 2004, *Handling Uncertainty: A Guide to Professionals in the Process Industries and related fields*, The Institution of Chemical Engineers, Rugby, England.

Carter, D.A., Hirst, I.L., Maddison, T.E. and Porter, S.R. 2003, 'Appropriate risk assessment methods for major accident establishments', *Transactions of IChemE*, Part B, Process Safety and Environmental Protection, vol. 81, pp. 12-18.

Chippindall, L. and Butts, D. 2004, 'Managing the financial risk of major accidents', Center for Chemical Process Safety *19th Annual International Conference*, Orlando, Florida, pp. 321-336.

Cho, H-N., Choi, H-H. and Kim, Y-B. 2002, 'A risk assessment methodology for incorporating uncertainties using fuzzy concepts', *Reliability Engineering and System Safety*, vol. 78, pp. 173-183.

Clift, R. 1998, 'Engineering for the environment: The new model engineer and her role', *Transactions of IChemE*, Part B, Process Safety and Environmental Protection, vol. 76, pp. 151-160.

Commission of the European Communities (COEC), 2000, *Communication from the Commission: on the precautionary principle*, COM(2000)1, Brussels, February 2.

Covello, V.T. and Merkhofer, M. 1987, 'The inexact science of chemical hazard risk assessment: a description and critical evaluation of available models' in *Insuring and Managing Hazardous Risks: From Seveso to Bhopal and Beyond*, eds. P.R. Kleindorfer and H.C. Kunreuther, Springer-Verlag, Berlin, pp. 229-76.

Cullen, J. 1994, 'Health and Safety: A burden on business?' *Transactions of IChemE*, Part B, Process Safety and Environmental Protection, vol. 72, pp. 3-14.

Dalzell, G. and Chesterman, A. 1997, 'Nothing, is safety critical', *Transactions of IChemE*, Part B, Process Safety and Environmental Protection, vol. 75, pp.152-156.

Evans, A.W. and Verlander, N.Q. 1997, 'Risk Analysis: What is Wrong with Criterion F-N Lines for Judging the Tolerability of Risk?', *Risk Analysis*, vol. 17, no. 2, pp. 157-186.

Evans, J. and Thakorlal, G. 2004, 'Total Loss prevention - Developing Identification and Assessment Methods for Business Risks', *Loss Prevention 2004*, 3 May-3 June, Prague, pp. 1207-1204.

Government of Victoria, 2000, *Occupational Health and Safety (Major Hazards) Regulations*, Melbourne, Australia.

Goyal, R.K.1993, 'Practical examples of CPQRA from petrochemical industries', *Transactions of IChemE*, Part B, Process Safety and Environmental Protection, vol. 71, pp. 117-123.

Health and Safety Commission (HSC) 1991, *Major Hazard Aspects of the Transportation of Dangerous Substances*, HMSO, London.

Health and Safety Executive (HSE) 1988, *The Tolerability of Risk from Nuclear Power Stations*, HMSO, London.

Health and Safety Executive (HSE) 1989, *Quantitative Risk Assessment: Its Input to Decision Making*, HMSO, London.

Health and Safety Executive (HSE) 1990, *Risk Criteria for Land-Use Planning in the Vicinity of Major Industrial Hazards*, HMSO, London.

Health and Safety Executive (HSE) 2001, *Reducing Risks, Protecting People - HSE's Decision Making Process*, HMSO, London.

Health and Safety Executive (HSE) 2003, *Good practice and pitfalls in risk assessment*, S. Gadd, D. Keeley and H. Balmforth, Research Report 151, HSE Books, Norwich, England.

Health and Safety Executive (HSE) 2003, *Guidance on ALARP for Offshore Division Inspectors Making an ALARP demonstration*, Available at: http://www.hse.gov.uk/offshore/circulars/enf38.htm .

Health and Safety Executive (HSE) 2002, 'HID's Approach to 'As Low As Reasonably Practicable' (ALARP) Decisions', Available at: http: http://www.hse.gov.uk/comah/circular/perm09.htm .

Health and Safety Executive (HSE) 2004, 'Principles and Guidelines to assist HSE in its judgements that duty holders have reduced risk as low as reasonably practicable', Available at: http://www.hse.gov.uk/ .

Hirst, I.L. and Caster, D.A. 2002, 'A 'worst case' methodology for obtaining a rough but rapid indication of the societal risk from a major accident hazard installation', *Journal of Hazardous Materials*, vol. A92, pp. 223-237.

Kletz, T.A. 1990, *Critical Aspects of Safety and Loss Prevention*, Butterworths.

Lofstedt, R.E. 2003, 'The precautionary principle - Risk, regulation and politics', *Transaction of IChemE*, Part B, Process Safety and Environmental Protection, vol. 81, pp.36-42.

Mouney, D.A. and Schmidt, M.E.G 1997, 'Fully quantitative predictive maintenance/inspection planning optimisation for chemical process plant components', *Process Safety Progress*, vol 16, no. 4, pp. ·262-268.

Noonan, F. 1993, 'On the use of acceptable risk constraints in resource allocation domains', *Transactions of IEEE*, pp. 186-190.

Quelch, J. and Cameron, I.T., 1994, 'Uncertainty representation and propagation in quantified *risk* assessment', *Journal of Loss Prevention in the Process Industries*, vol. 7, no. 6, pp. 463-473.

Schofield, S. 1998, 'Offshore QRA and the ALARP Principle', *Reliability Engineering and System Safety*, vol. 61, pp. 31-37.

Skjong, T. 2002, 'Setting Target Reliabilities by Marginal Safety Returns, *Joint Committee on Structural Safety (JCSS) Workshop on Reliability Based Code Calibration*, Zürich, March 21-22.

Stone, J.R. and Blockley, D.I. 1993, 'Hazard engineering and the management of risk', *Transactions of IEEE*, pp. 180-185.

Tweeddale, M 2003, *Managing risk and reliability in process plants*, Gulf Professional Publishing.

Woodward, J.L. and Moosemiller, M.D. 1996, 'Applying risk assessment principles to a batch distillation column', *Process Safety Progress*, vol. 15, no. 2, pp. 61-65.

WorkSafe Victoria Major Hazards Division 2001, *The Requirements for 'Demonstration' Under the OHS (MHF) Regulations*, Guidance Note 16, Revision I, 2 April.

## 10.9 NOTATION

| | |
|---|---|
| ALARP | As Low As Reasonably Practicable |
| ARI | Approximate Risk Indicator |
| BOT | Build Operate Transfer |
| CBA | Cost-Benefit Analysis |
| CCPS | Center for Chemical Process Safety |
| CFD | Computational Fluid Dynamics |
| CPF | Cost of Preventing a Fatality |
| FMEA | Failure Modes and Effects Analysis |
| F-N curve | Log-log plot of cumulative Frequency- Fatality |
| HSC | Health and Safety Commission (UK) |
| HSE | Health and Safety Executive (UK) |
| ISIR | Individual Specific Individual Risk |
| LSIR | Location Specific Individual Risk |
| MSDS | Material Safety data Sheets |
| NPV | Net Present Value |
| OHS | Occupational Health and Safety |

| | |
|---|---|
| OSHA | Occupational Health and Safety Administration |
| pa | per annum |
| PLL | Potential Loss of Life |
| PVC | Poly Vinyl Chloride |
| QRA | Quantitative Risk Analysis |
| ROI | Return on Investment |
| SMS | Safety Management System |
| UKOOA | United Kingdom Offshore Operators Association |
| VPF | Value of Preventing a Fatality |

This page is intentionally left blank

# 11 PROCESS SAFETY MANAGEMENT SYSTEMS

*"Out of this nettle, danger, we pluck this flower, safety".*

*William Shakespeare, Henry IV Part I, Act ii, Scene 3.*

In the preceding chapters, we have referred to the importance of a Safety Management System (SMS) to complement the process hazard analysis studies in order to maintain the integrity of safety critical equipment in a hazardous facility. This chapter is devoted to a detailed description of what constitutes the SMS, how it can be developed and implemented.

## 11.1 PLANNING FOR SAFE OPERATIONS

### 11.1.1 Introduction

We have seen how systematic hazard identification and risk assessment methods can be applied to new and existing process facilities. Much of the work is mainly carried out by a specialist multi-disciplinary team.

The following questions arise:

- How do we control the identified hazards in day to day operation and maintenance of the facility?
- How do we ensure the integrity of the hazard control measures that we have so carefully selected, designed and installed?

- What tools do we need for maintaining the risk at ALARP level, day after day?

The answer to all of the above is that we need a system consisting of policies, procedures and practices for managing process safety, in the same way we manage the business. The set of procedures and practices ensure that the barriers to prevent or mitigate the impact of major accidents are in place, and are effective.

The set of procedures and practices designed to prevent major accident events in a process facility, and manage incidents go by the name of the Safety Management System.

In the absence of an effective process safety management system, all the hazard evaluation and risk assessment become somewhat meaningless. Many investigations into major accidents in process plants have found that while there has been risk assessments carried out with volumes occupying the shelf, the process safety management system that was in operation had failed badly.

### 11.1.2 Principal Roles of the Safety Management System (SMS)

An integrated SMS has two principal roles, covering the full range of the incident spectrum:

a) Occupational health and safety (OH&S) management
b) Engineering and process safety management

#### *11.1.2.1 Occupational health and safety management*

Occupational health and safety (OH&S) management at the workplace addresses the low severity-high frequency end of the incident spectrum (see Section 1.3.1). These essentially cover work related injuries (e.g. slips, trips, falls, injury sustained during manual handling, man-machine interfaces, exposure to high noise levels etc.).

The main characteristics of the OH&S management system are injury prevention and rehabilitation. Training, education and managing human error plays a significant role in injury prevention.

Some organisations have managed this area so effectively that one to two million man-hours of no lost time injury is not uncommon. However, it is well established that these measurements are not sufficient to provide adequate feedback for managing process safety (EPSC 1996, Hopkins 2000, Columbia Accident Investigation Board 2004).

#### *11.1.2.2 Process safety management*

Process safety is directed towards the high severity-low frequency end of the spectrum, and requires safety management tools that are different to those required for personnel safety (e.g. slips, trips and falls, workplace health). Clearly there is some overlap between the two aspects of overall safety management.

In order to distinguish workplace injury related safety issues from process safety issues, the term Process Safety Management (PSM) is also used, more commonly in North America.

The likelihood of major accidents is generally very low. However, the absence of very unlikely events is not, in itself, a sufficient indication of good safety management (EPSC 1996). The space shuttle Columbia accident investigation board (2004) found that the ISO 9000 system tended to focus on process rather than outcome, and hence was not the appropriate tool for technical safety management.

We have taken an integrated view of Safety Management System (SMS) that includes both these roles. However, our attention to SMS in this chapter is confined essentially to process safety.

## 11.2 SAFETY MANAGEMENT SYSTEM – STRUCTURE AND COMPONENTS

### 11.2.1 System Requirements

The process of successfully managing safety consists of the following management functions (HSE 1991):

1. Safety Policy development and communication
2. Organisational development
   a) establishing and developing a safety culture within the organisation (leadership and commitment)
   b) defining inputs and outputs
   c) identification of resources required
   d) identification of training needs
   e) developing organisational structures for safety management
   f) allocation of responsibility and accountability
   g) a framework for converting policies into practices
   h) communication
3. Development and implementation of SMS
   a) specifically designed for the process facility in question
   b) development of criteria and guidelines such as setting performance standards
   c) development of formal systems and procedures such as how to carry out the tasks
   d) provision of adequate training in systems and procedures
   e) detailed work instructions including practices and behaviours
4. Development of a system to measure SMS performance through an auditing process.
   a) monitoring performance against standards
   b) reporting system for management feedback
   c) audit mechanisms
   d) mechanisms for corrective actions development and implementation
   e) periodic review of procedures and update

The above functions are illustrated in Figure 11-1.

Figure 11-1 is similar to the functions described by CCPS (1989) in terms of the classical management functions of planning, organising, implementing and controlling.

All the components of the SMS can be fitted into one or more of the above functions. An additional requirement of the SMS is that it should cover not only the operational stage, but also all the stages of the facility life cycle.

Dowell III (2002) points out that it is vital that there be performance standards first and these should form the basis for development of a standard or guideline. Skipping this step and delving into procedures from policy directly undermines the effectiveness of the SMS.

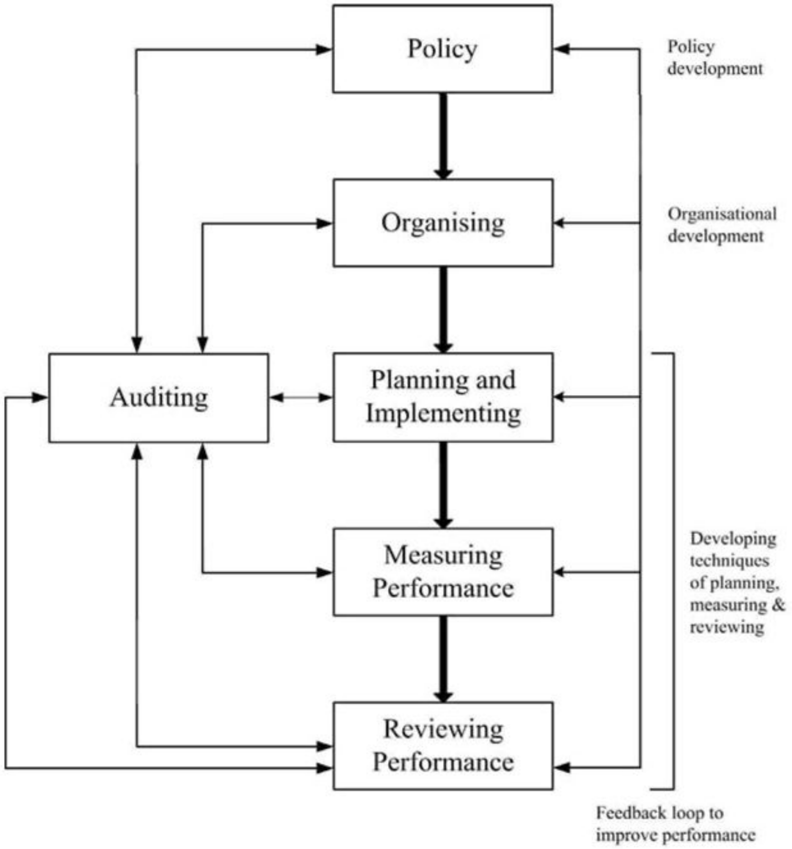

Policy
Policy development
Organising
Organisational development
Auditing
Planning and Implementing
Measuring Performance
Developing techniques of planning, measuring & reviewing
Reviewing Performance
Feedback loop to improve performance

FIGURE 11-1 SAFETY MANAGEMENT FUNCTIONS

### 11.2.2 Review of SMS Models

The SMS tends to integrate all aspects of safety into the ongoing activities of everyone involved in the operations - from the operator to the chief executive officer. The responsibility for safety is therefore both individual and collective.

This section summarises the various SMS models that have been developed. The differences between the models are minimal.

### 11.2.2.1 CCPS model

One of the earliest models for process safety management was developed by a team of industry experts and published by the Center for Chemical Process Safety of the American Institute of Chemical Engineers (CCPS 1989). The model is similar in structure to the quality model of ISO 9001 (2000) in that it has a number of core-elements and sub-elements under each core element.

The CCPS model has 12 core elements, and listed in Table 11-1.

### 11.2.2.2 OSHA PSM standard

The US Occupational Safety and Health Administration (OSHA) has in place a PSM standard covering a wide range of users of hazardous chemicals (OSHA 1992; Donnelly 1994).

The Final Rule of OSHA has 17 sections (or elements, to use a consistent terminology). The list of hazardous chemicals covered by the Rule was also published as an appendix. It is a flexible performance based approach to managing process safety.

The OSHA rules are compared with the CCPS model in Table 11-1.

The US EPA (1996) risk management program regulation has required the development and implementation of systems to prevent accidental release of chemicals. The requirements are consistent with those of the OSHA final rule (1992).

### 11.2.2.3 Seveso II Directive

The Seveso II Directive of the Council for European Union requires the implementation of a safety management system by member countries for the control of major accident hazards involving dangerous substances (Council of the EU, 1996). The directive itself defines two levels of requirements for SMS:

a) General requirement for all companies to produce a major accident prevention policy, designed to guarantee a high level of protection for human beings and the environment with appropriate means, including management systems.
b) Specific requirement by the operator of the site to demonstrate in a Safety Report, that both the major accident prevention policy and the SMS for implementing it have been put into effect.

The SMS elements of the Seveso II directive are not as structured as other SMS models. The elements compiled from the directive are listed in Table 11-1.

### 11.2.2.4 API Recommended Practice 750

An SMS model was developed by the American Petroleum Institute, directed to the oil and gas industry (API 750-1990).

The model has 11 elements (see Table 11-1). Management commitment, responsibility and accountability, and employee participation/communication have not been included as separate elements, but taken to be implicit in the other elements. The API model closely resembles the OSHA standards.

#### 11.2.2.5 COMAH requirements

The Control of Major Accident Hazards (COMAH) is the UK regulation (UK Government 1999) for the implementation of the Seveso II Directive. The SMS model elements are broader than the Seveso II Directive, but cover all the Seveso II elements given in Table 11-1. In addition, the audit element has been included.

#### 11.2.2.6 ISRS model

The International Safety Rating System (ISRS) of DNV (EPSC 1994; DNV 1994) is a safety auditing system and consists of 20 elements. It can be applied across a wide range of industries including the chemical process industry. Being very general, some specific needs of the chemical process industry need to be built into this system to make it effective.

Organisations in the process industry that have adopted the ISRS system, have expanded the scope of some elements such as chemical safety management, hazard analysis, process emergency planning and response and management of change, to reflect the specific needs of the process industries.

The system has been identified both as a management system and as an auditing tool, but in practice, many organisations have found that it serves better the auditing purpose.

#### 11.2.2.7 Other process industry models

An SMS framework has been developed by the Chemical Manufacturers Association (CMA 1990) in the USA, under the ‘Responsible Care’ program. The system elements are divided into four major categories:

- Management leadership in process safety
- Process safety management of technology
- Process safety management of facilities
- Managing personnel in process safety

In the offshore oil and gas production systems, there has been a significant change in the development and application of SMS since the Piper Alpha incident (Crawley 1999). The SMS adopted by the UK Offshore Operators Association (UKOOA) is essentially based on the HSE approach (HSE 1991).

TABLE 11-1 COMPARISON OF ELEMENTS OF SMS MODELS

| **anagement unction** | **CCPS** | **OSHA (USA) 29 CFR 1910.119** | **Seveso II Directive (96/82/EC)** | **API (RP 750)** |
|---|---|---|---|---|
| **olicy** | Policy<br>Safety culture promotion | a. Purpose<br>b. Application<br>Definitions | 1. Major accident prevention policy (MAPP) - Article 7 | |
| **rganising** | 1. Accountability: objectives and goals<br>10. Standards, codes and laws | c. Employee participation | 2. Organisation/Employee participation - Annex III c(i) | |
| **lanning and nplementing** | 2. Process knowledge and documentation<br>3. Capital project review and design procedures<br>4. Process risk management<br>5. Management of change<br>6. Process and equipment integrity<br>7. Incident investigation<br>8. Training and performance<br>9. Human factors<br>10. Standards, codes and laws | d. Process safety information<br>e. Process hazard analysis<br>f. Operating procedures<br>g. Training<br>h. Contractors<br>i. Pre-startup safety review<br>j. Mechanical integrity<br>k. Hot work permits<br>l. Management of change<br>m. Incident investigation<br>n. Emergency planning and response | 3. Staff selection and training including contractors - Annex III c(i)<br>4. Process safety information - Article 9.1(e), 13<br>5. Hazard identification and assessment of prevention and mitigation measures, including domino effects - Articles 8, 9.1(b) 9.1(c), Annex III c(ii).<br>6. Operating procedures - Annex III c (iii)<br>7. Maintenance procedures - Annex III c (iii) (covers systems of work)<br>8. Inspections (including mechanical integrity) - Article 18<br>9. Management of change - Article 10, Annex III c (iv) | 1. Process safety information<br>2. Process hazard analysis<br>3. Management of change<br>4. Operating procedures<br>5. Safe work practices<br>6. Training<br>7. Quality/integrity assurance of critical equipment<br>8. Pre-startup safety review<br>9. Emergency response and control<br>10. Investigation of process-related incidents |

| nagement<br>ction | CCPS | OSHA (USA) 29 CFR 1910.119 | Seveso II Directive (96/82/EC) | API (RP 750) |
|---|---|---|---|---|
| | | | 10. Incident reporting (including investigation) - Annex III c (vi)<br>11. Emergency plans - Article 9.1(d), 11 Annex III c (v) | |
| **suring and**<br>**iew** | 11.Audits and corrective actions<br>12.Enhancement of process safety knowledge | o. Compliance safety audit<br>p. Trade secrets | 12. Performance monitoring - Annex III c (vi)<br>13. Audit and review for improvement plans - Annex III c (vii)<br>14. Periodic Review of SMS and Safety Report - Article 9.5 | 11. Audit of process hazards management systems |
| **nments** | This is one of the earliest models. Later models have elaborated on this model. | Includes pre-startup review, but does not cover other aspects of life cycle. | The above elements are embedded in a Safety Report to be prepared by the facility management.<br>Covers facility life cycle. | RP 750 is almost identical to the OSHA PSM model. |

Jote 1: The term audit in COMAH refers to the effectiveness and suitability of the SMS itself in operation, and is different to routine monitoring of process afety performance, using key performance indicators. These are covered in elements 12 to 14 of Seveso II Directive.

Jote 2: The models are very much equivalent. Addressing the requirements of the model is more important than the actual format of the model. The lement of continual improvement needs to be present in any model selected.

Jote 3: There is no specific numbering order for the elements of the Seveso II Directive. Numbers selected here are based on similarity to the OSHA PSM nodel. Reference is made to the corresponding clause of the directive.

### *11.2.2.8 Individual corporation models*

In addition to the above models, individual chemical/oil and gas corporations have developed SMS standards internally, incorporating the same set of elements in different formats. Details can be found the references cited in Table 11-2.

TABLE 11-2 SMS MODELS OF INDIVIDUAL CORPORATIONS

| Corporation | Elements in SMS model | Reference |
|---|---|---|
| BP group | REALM1 (follows DNV's ISRS for management system components)<br>REALM 2 (covers health, safety, environment, product stewardship and security) | Read and Yeldham in EPSC (1996) |
| Dow | 13 | Gowland in EPSC (1996). Responsible Care program. |
| Du Pont | 14 (elements very similar to OSHA rule) | Kolk in EPSC (1996), grouped around technology, facilities and personnel. Auger (1995). |
| Hoechst Corporation | 18 | Niemitz et al. in EPSC (1996). Includes OH&S element, and environmental issues. |
| ICI | 19* | EPSC 1994. Includes OH&S element and product stewardship. Operational auditing and feedback. |
| Exxon Chemicals | 21 | Fröhlich in EPSC (1996). Elements form the Operational Integrity Management System (OIMS) framework. Integrates environmental, health and safety management. |
| Norsk Hydro | 12 | Bjerke in EPSC (1996). Includes OH&S, and uses a rating system for measurement. |
| BHP Billiton | 15* | Covers health, safety, environment and the community (BHP Billiton 2002) |
| Shell Chemicals | 106 procedures | "Responsible Care" program of the Chemical Industry (Shell Chemical Company, 2001) |

* Referred to as 'standards'

## 11.2.3 Relation to Environmental and Quality Management Systems

SMS shares a number of common concepts with the environmental management system as outlined in ISO 14001 (1996), and quality system of ISO 9001 (2000). The common elements are listed in Table 11-3.

TABLE 11-3 COMPARISON OF SMS, EMS AND QUALITY SYSTEMS

| nagement nction | SMS (based on Seveso II Directive) | EMS (ISO 14001) | Quality (ISO 9001) |
|---|---|---|---|
| licy | 1. Major accident prevention policy (MAPP) | 1. Top management commitment and leadership (Environmental policy ) | 1. Management responsibility (quality policy, organisation, management review) |
| ganising | 2. Organisation/Employee participation | Initial environmental review (optional)<br>6. Structure and responsibility<br>8. Communication | 2. Quality system |
| nning and plementing | 3. Staff selection and training including contractors<br>4. Process safety information (Safety Report)<br>5. Hazard identification and assessment of prevention and mitigation measures, including domino effects<br>6. Operating procedures<br>7. Maintenance procedures<br>8. Inspections (including g mechanical integrity)<br>9. Management of change<br>10. Incident reporting (including investigation)<br>11. Emergency plans | 2. Environmental aspects and impacts<br>3. Legal and other requirements<br>4. Objectives and targets<br>5. Environmental management programs<br>7. Training awareness and competence<br>8. EMS documentation<br>9. Document control<br>10. Operations control<br>11. Emergency response | 3. Contract review<br>4. Design control (design and development planning, design output verification, design changes)<br>5. Document control<br>6. Purchasing<br>7. Purchase supplied product<br>8. Product identification and traceability<br>9. Process control<br>10. Inspection and testing (receiving, in process, final)<br>11. Inspection, measuring and test equipment<br>15. Handling storage packaging and delivery<br>16. Quality records<br>18. Training<br>19. Servicing<br>20. Statistical techniques |
| asurement and nitoring | 12. Performance monitoring | 12. Monitoring and measurement<br>13. Non-conformance and corrective | 12. Inspection and test status<br>13. Control of non-conforming |

| nagement nction | SMS (based on Seveso II Directive) | EMS (ISO 14001) | Quality (ISO 9001) |
|---|---|---|---|
| | | and preventive action<br>14. Records | product (review and inspection)<br>14. Corrective action<br>17. Internal quality audits |
| ntinual provement | 13. Audit and review for improvement plans<br>14. Periodic Review of SMS and Safety Report | 15. EMS audit<br>16. Management review of EMS<br>17. Feedback to other elements for continual improvement | Continual improvement not specifically mentioned in Standard, audits are for non-conformances and not the quality system itself. |
| I&S issues | 15. Health<br>16. Personal protection<br>17. Injury prevention<br>18. Rehabilitation | | |
| mments | OH&S issues included in the list to provide an integrated SMS, but can be managed independent of process safety management. Document control not specifically stated. | Emphasis on document control and record keeping. EMS audit for continual improvement refers to the system and not audit of environmental performance, which is covered by elements 12 and 13. | Emphasis on document control and record keeping |

From Table 11-3, it is seen that there is similarity in the elements, but the scope and focus of these elements are quite different. There are interactions between elements of safety, environment and quality. For example:

- Emergency response for loss of containment incidents is essentially the same for safety and environment, and a single procedure would cover both.
- Purchasing, normally done under the quality system, has an impact on safety and the environment. An incorrect valve or gasket specification in purchasing can cause reaction hazards and possible loss of containment, when installed. Kletz (1994) describes a number of actual incidents.

Some organisations tend to manage safety through the quality systems, by adding additional elements to the quality systems.

There have been strong arguments for and against integrating safety, environmental and quality systems into a single management system (Shilitto 1995; CCPS 1997a). A detailed integration strategy is provided by Standards Australia (1999), but this deals with occupational health and safety and not process safety. Arguments in favour are:

- Economies of scale in not duplicating shared components
- The regulatory emphasis towards performance-based rather than prescriptive legislation
- Customer requirements in major contracts to provide health and safety environmental management, together with a quality system

While an integrated system appears attractive, in practice this has proved more difficult. The main problems are:

- The overlap between the three management system elements is not significant enough to effect a smooth integration.
- In many organisations, the systems have been operating for many years, and the need for integration is not seen, and the claimed economies of scale are not considered significant.
- The coordinating responsibilities of the systems tend to be with different departments within the organisation, presenting logistic difficulties in integration.
- While SMS and EMS emphasise continual improvements, quality systems do not have the same emphasis.
- The culture of quality tends to be different to the culture of safety and environment. The former is procedure-based and the latter, while having procedures for guidance, is predominantly behaviour-based, and measured by performance standards. The cultural integration becomes more difficult.
- There are special issues regarding regulatory constraints and criminal liabilities in safety and environmental management.

Since the SMS, EMS and quality systems are all under a single umbrella of organisational management, it is possible to achieve a good interface in information management of the three systems. A common database software may be used that incorporates the elements of the three systems in modular configuration, sharing common information.

The initial cost of setting up such an integrated information management system could be high, as existing information needs to be transferred, and significant data entry would be required. Once set up, the information system offers significant advantages.

- eliminates repeated data entry for stand-alone systems
- provides an integrated auditing regime
- captures compliance with regulations that overlap the three systems
- generates reports for management and for statutory reporting at specified intervals
- enables more effective performance monitoring, close out of corrective actions
- facilitates tracking of changes in regulatory requirements.

It is important to identify and cross-reference the relevant procedures in one management system (safety, environment or quality) that may have an impact on another system.

## 11.3 DEVELOPMENT OF SMS

Considerable planning and organising is necessary for the development of an SMS. Scattered stand-alone procedures that had been used in a haphazard fashion need to be integrated into a management structure. Failure to do so can cause major accidents. A process incident, which could have developed into a major explosion was attributed to the failure of a number of elements in the process safety management (Mannan, 1996).

### 11.3.1 SMS for Occupational Health and Safety

A recent development in OH&S management is the development of a Standard, similar to the ISO 9001 for Quality Management and ISO 14001 for Environmental Management. Its various versions are:

- AS 4801-2000 Occupational Health and Safety Management Systems – Specification with Guidance for use (Australia) and its companion AS/NZS 4804-2000 Occupational Health and Management Systems – General Guidelines on Principles, Systems and Supporting Techniques (Australia/New Zealand)
- OHSAS18001-1999 OHS Management Systems – Specification (UK) and its companion British Standard OHSAS/18002:2000 – Occupational Health and Safety Management Systems – Guidelines for the implementation of OHSAS 18001.

Equivalent Standards have been published in French and German.

The following sections describe the SMS elements in detail for process safety management. Since a structure is required for this description, the Seveso II model has been selected. The information given in this section, however, is equally applicable to the relevant OSHA PSM rules, and cross-referenced wherever applicable.

### 11.3.2 Accident Prevention Policy

Leadership is the most important element in an SMS. Without the commitment of the senior management, the development and implementation of a system is not only impossible, but will prove to be ineffective. One of the major roles of leadership is to foster a safety culture (Sorensen 2002).

The first step in the development of SMS is the major accident prevention policy (MAPP). Generally this is a corporate policy, and implemented across the organisation. Individual sites may have their own site safety policy, which is an amplification of the corporate policy.

Key features of the policy are:

- Signed by the CEO (corporate policy) and senior manager for the site (if local policy exists).
- Statement of commitment to protection of health and safety of employees, contractors, visitors and public.
- Generally includes a commitment to compliance with all regulatory requirements.

The presence of a written policy does not automatically ensure effectiveness of SMS in its application, but the absence of a policy is seen as a lack of commitment.

Sometimes the corporate safety policy is used to resolve potential conflicts between production goals and safety goals.

**EXAMPLE 11-1 SAFETY POLICY STATEMENTS**

In the 1980's, an organisation had a health and safety policy which contained a clause which was more specific than most policies, i.e.

- No activity takes precedence over safety.
- There shall be no recommendation that cannot be implemented (based on practicability).

At one time, an equipment item, unused for some time, required re-commissioning to meet production demands. The production manager gave orders for restart of the equipment. Since it had not been used for some time, the operators had concerns over the safety of the operation and wanted a thorough safety inspection prior to re-commissioning. This meant a few days delay in production and the manager was reluctant to do this, as he was reasonably sure that the equipment was safe. This could have resulted in an industrial dispute. Ultimately what resolved the issue was the clause in the policy 'No activity takes precedence over safety'.

Note: This issue should have been resolved by the Management of Change (MOC) procedure, which was only subsequently introduced.

The single most significant benefit of a formal safety policy is that, while demonstrating the corporation's commitment, it also assists in altering the mind set of the employees in adopting a safety culture within the organisation.

### 11.3.3 Organisation

This element refers to how safety management is organised in the corporation, and in each individual facility. The key items to cover are:

- An organisation chart showing position(s) with responsibility and accountability for process safety. This cannot be site safety manager or safety coordinator, whose task is to assist in coordination, communication and monitoring. Responsibility should belong to line management.
- A task matrix that outlines the elements of the SMS and person(s) responsible for implementation and monitoring. An example task matrix, shown in Table 11-4, is a useful format for representing the responsibility and accountability. Only the departments are shown in the task matrix example, but the positions/persons responsible within each department should be nominated on the matrix.

The task matrix readily demonstrates that process safety is not a single person's responsibility, but collectively borne by all persons in the organisation, from various departments.

TABLE 11-4 EXAMPLE OF PROCESS SAFETY ORGANISATION TASK MATRIX

| **SMS Element** | **Responsible Department** | | | | | |
|---|---|---|---|---|---|---|
| | **Site manager** | **Safety** | **Production** | **Engineering** | **Maintenance** | **Personnel** |
| Policy | | | | | | |
| Communications | | | | | | |

### 11.3.4 Communications

Communications cover a wide range of issues and at various levels. A full list of possible communications needs to be compiled, so that protocols and procedures can be developed. Typical examples are:

**Corporation level:**

- Safety policy (to be communicated to all employees)
- Safety alerts based on incidents and near misses (to all employees on the site, contractors, to managers of other sites in the organisation for information sharing)
- Incident investigation results (to site personnel, other parts of the organisation)

- Media relations
- Regulatory interfaces
- Special briefings

**Site level:**

- Site safety rules and practices (to all visitors, contractor personnel and new employees)
- Communication with regulatory authorities
- Communication with public/local resident groups
- Communications between departments (production, engineering, maintenance, contractors)
- Special briefings

**Intra-departmental level:**

- Shift change and handover (covers abnormal situations, process control problems, unfinished maintenance tasks)

There have been many reported cases of accidents caused by the lack of communication or miscommunication.

### 11.3.5 Staff Selection and Training

This is a critical area in managing risk. There have been a number of cases reported where inadequate training has resulted in incorrect diagnosis, incorrect response, failure to recognise and correct abnormal situations. These failures have resulted in a simple process deviation leading to major incidents (Kletz 1990, 1993, 1994, 2001).

Major issues to be addressed are:

1. Definition of skills and knowledge required, as part of job description.
   Job descriptions are normally written by the personnel department as part of the quality system, but operations has a significant input to this definition. The quality audit often has a checklist 'Do you have job descriptions for all positions?', and ticks off the list on sighting the document. The question to ask is - What are the skills and knowledge required for this position, and is it appropriately documented?
2. Assessment of qualifications
   This requires finding a fit between the person and job requirement. Technical skills, learning and communication abilities and other personality traits (attitude, aptitude) need to be considered.
3. Development of training program
   Training modules should be developed for both new employees and ongoing refresher training for existing employees, and contractor induction. They should include:
   (i) safety policy and how it is translated into practices
   (ii) process description
   (iii) process control
   (iv) hazards present and how they are managed

(v) hazardous properties of materials stored and handled, and material safety data sheets (MSDS)
(vi) the SMS framework and where the trainee fits in
(vii) operating/maintenance procedures
(viii) safe work procedures on site
(ix) detection of and response to abnormal situations (this is an ongoing learning curve for every individual)
(x) job task analysis technique
(xi) performance standards and measurement
(xii) communication protocol and requirements
(xiii) types of human error and how to minimise them
(xiv) training needs for ongoing refresher training
(xv) training in the use of special equipment (e.g. self-contained breathing apparatus)
(xvi) first attack firefighting (sometimes this training is provided to the industry by the fire brigade)

The management of human error is an important component in the training program. The adverse consequences of an incorrect action should be highlighted using industry case studies of accidents.

The training program development should also address the needs of the instructor, training documentation, visual aids, simulators, record keeping aids). The instructor may require formal external training on how to train others, such as a 'train the trainer' program.

There have been recent developments in dynamic operator training simulator for startup, shutdown and emergency operations procedures (Yang et al. 2001).

4. Measuring performance
   The key factors are:
   (i) Development of performance standards for competency
   (ii) Assessment of performance through written tests, observation at work, interviews, feedback from supervisors
   (iii) Continual improvement processes (retraining where required)
5. Records management
   Maintaining training records is essential. This is best done using a software database, accessible to the various department managers/supervisors. The database can also contain the frequency of training in each of the SMS elements for all staff, and produce planning reports for ongoing training.

### 11.3.6 Hazard Identification and Assessment

This element forms the equivalent of Process Hazard Analysis in the OSHA PSM rule. The hazard identification and assessment integrates all the earlier chapters in this book (Chapters 4 to 11). The main components are:

1. Identification of process hazards (from loss of containment, process deviations, reaction hazards etc.). The techniques described in Chapter 4 apply.

   Hazard identification is not an exercise that is undertaken by technical professionals alone with the assistance of a facilitator. Such an exercise defeats the intent of the SMS, which requires that there should be full knowledge of the process hazards among the workforce. Therefore, it is essential that there should be employee consultation and participation in this exercise. This is also required by the OSHA PSM rule, and all similar regulations such as Seveso II Directive as applied to member countries of the EC, and Australian major hazard facility regulations by governments of Victoria (2000) and Queensland (2001). For those employees who do not actually participate in the hazard identification workshop sessions, there must be a mechanism for communicating the information, and obtaining feedback to update the findings.

   The hazard register is the main output from this step.
2. Assessment of consequences of hazards

   The consequences of hazardous incidents such as fires, explosions and toxic releases are quantified for all the hazardous scenarios listed in the hazard register.

   The effects and vulnerability models in Chapters 5 to 7 are relevant to this analysis.
3. Estimation of likelihood

   The likelihood estimation can be qualitative or quantitative. The merits and limitations of both are discussed in Chapter 8. If a quantitative risk assessment is required, then the likelihood needs to be quantified.

   Regulations in many countries with respect to land use safety planning require a quantitative risk assessment expressed as risk contours, as an input to decision making. In such situations, a quantitative estimation of likelihood is imperative.

   Methodology of assessment is described in detail in Chapter 8.
4. Risk Assessment

   The consequence and likelihood are combined to obtain an estimate of the risk.

The risk estimate is undertaken iteratively with additional risk reduction measures where identified, for input to benefit-cost analysis, and for demonstrating that risks have been reduced to ALARP level.

Details of risk assessment and evaluation are provided in Chapter 9, and input to decision making in Chapter 10.

### 11.3.7 Documentation - Safety Report

This element covers Process Safety Information of OSHA PSM rule, and documentation of Process Hazard Analysis. CCPS (1995a) describes PSM documentation requirements, but this is mainly focused toward installations in the United States, for compliance with OSHA PSM rule.

The structure of the safety report and its components are described in Section 13.4.

### 11.3.8 Prevention, Mitigation Measures

This section covers the hardware measures in place for the prevention of major accident events, and the mitigation measures to control the incident and prevent escalation, should an event occur.

The corresponding procedural measures to ensure the integrity of these hardware measures are covered by the elements 'systems of work' and 'mechanical integrity'. These are described in detail in Chapter 12 on life cycle risk management. Only cross-references are made here. The main prevention and mitigation measures are:

1. Inherently safer design wherever possible (Section 13.3)
2. Equipment design features
3. Design to eliminate ignition sources as far as practicable
4. Design to control process deviations (safety instrumented systems)
5. Pressure protection (PSVs, rupture discs, depressuring systems)
6. Fire and gas detection systems
7. Active and passive fire protection
8. Explosion protection

All the above measures should also form part of the comprehensive documentation in the safety report mentioned in Section 11.3.7.

### 11.3.9 Management of Change

One of the core elements of the SMS is the Management of Change (MOC). It is necessary to explore this particular element in detail as many organisations have suffered significant losses in the past by not managing change effectively (Sanders 1993, 1996; Kletz 1995). The incidents at Flixborough (HMSO 1975) and Chernobyl resulted predominantly from the absence or failure of the change management process.

While MOC has been recognised as a vital component of SMS, independent SMS audits of many major hazard facilities still reveal many deficiencies in its implementation.

In order to implement a change management element in the SMS and to train personnel, the following are important (CCPS 1989):

- 'understanding' what is meant by change
- recognising and identifying such changes as they occur
- flagging such changes for appropriate review.

There is considerable diversity in the industry in the way the MOC process is implemented. Keren et al. (2002) provide an interesting summary from a benchmarking study. The main areas of differences are in the risk screening or ranking of MOC and on the process hazard analysis methodology used.

### *11.3.9.1 What is change?*

The definition of 'change' should be broad enough to include the following:

- changes to process technology
- changes of facility (modifications to equipment)
- permanent changes
- temporary changes
- variance procedures
- all modifications to procedures
- addition of new procedures
- deletion of procedures
- modifications to the organisation that could affect safety

Modifications to procedures and addition/deletion of procedures are common to both SMS and ISO 9001 document control element.

By using the word 'modification control' instead of 'management of change', we could be restricting the scope of what is meant by 'change'.

A change should exclude 'replacement of equipment in kind', as this is covered in maintenance procedures and would not change the operations. This is explicitly stated in the OSHA PSM rule.

Perron and Friedlander (1996) and Philley (2002) argue the case for including organisational changes such as downsizing in management of change for safety, and list a number of human factors contributing to accidents caused by organisational changes.

### *11.3.9.2 Components of change*

The components of change are listed in the previous section. A brief discussion on these is given below.

1. Change in process technology

The CCPS guideline (1989) lists six reasons for needing to change process technology:

- maintaining process continuity
- compensation for equipment unavailability
- startup or end-of-the-run shutdown
- experimentation (e.g. yield or quality improvement, new product)
- change in production rate
- new equipment.

In continuously operating plants, it may be necessary to make process changes to maintain smooth operating conditions, as a shutdown could be lengthy and the loss of production expensive. There must be safe limits to the changes that can be made, otherwise safety would be compromised.

A simple change to an interlock setting, if not subject to the MOC process, can create a hazardous situation.

**EXAMPLE 11-2 GAS ALARM LEVEL CHANGE**

Gas detectors were installed in the loading bays of a liquefied petroleum gas (LPG) bulk road tanker loading facility with a large quantity of gas storage. The alarms were set at two levels of the lower flammability limit (LFL): (i) low alarm at 20% LFL, alarm only and (ii) high alarm at 40% of LFL, initiating an automatic shutdown of the pumps and closure of the loading valves. The procedure specified that at alarm low, loading should be suspended and the leak investigated.

Due to fugitive emissions during coupling and decoupling operations, the low alarm occurred frequently, and considered a nuisance, causing frequent interruptions to the operations. The engineer in charge decided that the alarm level could be increased, and arbitrarily doubled the set levels, without an MOC review. This meant that a low alarm would now occur at 40% LFL and high alarm would occur at 80% LFL. This enabled smoother operation. The fact that peak to mean ratio of gas concentration can often be two to four times was ignored. In other words, when the average concentration was at 50% LFL, the peak concentration could reach LFL, but there would be no automatic shutdown.

By making an arbitrary change to the trip setting without MOC, the procedure had compromised the integrity of the shutdown interlock. The fact that there was no formal MOC procedure at that time, aggravated the situation.

This unauthorised change was identified in a formal SMS audit, and the situation was rectified. An MOC procedure was developed and implemented.

**EXAMPLE 11-3 CHANGE IN LUBRICANT**

Sometimes an 'innocent' change can result in a major hazard. In a wellhead platform offshore, the flowlines operate at pressure up to 150 bar, and hence the flange connections should have optimum torque and not overstressed. The conventional lubricant for the bolts was changed to a new anti-friction lubricant. This was not considered a 'change', and therefore was not subject to MOC. The flanges were connected after a shutdown, but were overstressed with the new lubricant.

No one was aware that the sulphur in the gas/condensate would react with a component in the new lubricant. Even if an MOC review was undertaken, it is doubtful whether this particular reaction hazard would have been identified, unless the review covered reaction hazards with the process gas with the lubricant.

Rapid corrosion of the bolts occurred due to the chemical reaction between sulphur in the gas and the anti-friction lubricant, and a full bore failure of the flow line occurred at the choke valve. By the time the subsurface valve shut the flow, up to 7 tonnes of gas had escaped. Fortunately the gas did not ignite. The platform shutdown button was pushed and the platform was evacuated via the free fall survival craft.

2. Change of facility

When an equipment change is planned, there should be careful consideration of the process safety implications. The organisational responsibility for approving such changes should be carefully defined, and approval should only be given after appropriate review has been completed.

Identification of all potential implications of the change is important. An example of a deficient hazard and operability (HAZOP) study is given below:

**EXAMPLE 11-4 REAGENT TANK RELOCATION**

A facility had a plant to produce demineralised water. The plant required sulphuric acid and caustic soda for regeneration of the ion exchange bed. There were two storage tanks to hold the two reagents, designed to the regulatory standards for spill containment, but located at some distance from the water treatment plant. The reagents were piped to the water treatment plant.

After some years of operation, it was decided to relocate the reagent tanks close to the water treatment area, as the existing storage area was required for other purposes. The MOC procedure was adopted, including a HAZOP study. However, the HAZOP never asked the question whether the relocated facility complied with relevant dangerous goods regulations since the HAZOP was missing the guideword from the list.

When the relocation was completed, an external audit found that the installation did not comply with the regulations for spill containment. The situation was rectified at additional cost, which could have been avoided if the HAZOP had been effective.

The above examples also illustrate the importance of external audits, which evaluate the effectiveness of the SMS.

3. Organisational change

One of the major problems faced by organisations is that movement of personnel is more frequent than changes to hardware. Change in people occurs both at the operational and at management levels. When experienced people leave or are transferred, the knowledge and history can disappear with them.

Before new personnel take their positions, it is necessary to have an MOC review in terms of the skill and training needs, and provide the necessary training, especially in identifying and managing abnormal situations.

The relocation of technical professionals away from the Esso Longford plant in Australia and their non-availability to provide advice to plant operations under abnormal situations was given as one of the contributors to the Esso Longford incident (Dawson and Brooks 1999). A similar situation with regard to increased dependence of NASA's technical professional on contractors was identified by the Columbia space shuttle accident investigation board.

The problems of downsizing have been described earlier (Perron and Friedlander 1996). The main problems are lack of staff, unqualified staff, changing employee attitudes, overburdened staff, and reduced operator interface with an increasingly automated process. Philley (2002) warns about a change of safety philosophy oriented towards minimum compliance rather than risk optimisation. This has been proved to be the case in a survey by Schweer et al. (2000).

## 4. Variance procedures

In any operation, situations arise which could not have been foreseen when the existing operating procedures were developed. Variations to the procedures may have to be quickly adopted. An ad hoc change by the operator may take the system beyond its design limits.

Therefore, the change management should incorporate a variance procedure. The procedure will require a review of the planned deviation, the reasons and justification for the deviation, safety, health and environmental considerations, control measures to be taken and the duration of the variance. The review should particularly identify if the variance would take the operation outside the safe design envelope (upper and lower bounds), which is not acceptable.

Variances should require approval by a suitable level of management, based on the process risks involved. Also they should be documented to ensure consistent understanding by all affected individuals and departments.

## 5. Permanent changes

The request for change should be made on an appropriately designed form, outlining the following:

- what change is proposed
- reasons for the change
- benefits gained by the change
- alternatives considered
- impact on process
- impact on regulatory requirements (i.e. requires new licence or licence amendment)
- health, safety and environmental considerations
- changes to hardware, procedures and drawings
- training needs for personnel to operate under changed conditions
- personnel who need to review the document and comment upon it
- whether the change requires a HAZOP or failure modes and effects analysis (FMEA) study
- if it is a hardware change, will it involve a corresponding change in operating or maintenance procedures?
- level of approval and authorisation.

Detailed documentation for the change should accompany the approval form. The documentation should be kept in the project files to ensure that proper documentation of design changes is maintained.

Implementation of procedural changes must include update of the relevant procedure through the document control system under the quality system procedures.

6. Temporary changes

In many incidents in the past, a post mortem review indicated that the incident occurred in a change intended to be temporary. The reactor modification at Flixborough was a temporary change for a short period until the reactor which suffered corrosion was repaired and ready to be reinstalled.

One of the major recommendations arising from the Flixborough incident Public Inquiry (HMSO 1975) was that any temporary changes to the hardware should be formally subject to a safety review, and the change implemented as it would be for new permanent installations.

The major considerations are:

- A time limit should be set for the temporary change, requiring re-approval if this limit were to be extended (i.e. a sunset clause)
- A temporary change should be viewed as if it were permanent and should be reviewed as such and adequately documented.
- All modified equipment and procedures should be returned to their normal mode at the end of the approved time for the change, unless the duration was extended subject to re-approval.

7. Level of scrutiny

There is considerable diversity in the industry on the level of safety scrutiny required for a given MOC. Keren et al. (2002) found the following:

- A detailed review using techniques such as HAZOP is conducted when:
  - All check points of change hazard review are not satisfied
  - Complexity of the change is significant
  - New materials are introduced
  - Changes occur in the process chemistry
  - A change exists with a major safety impact
- For simple cases, a "What-If" review was considered sufficient.

8. Abuse of the MOC Process

Every change incurs a cost. There must be some benefits arising from the change to justify the cost. This may not always be quantifiable, but the question of benefits must be raised and answered.

In some situations, plant personnel tend to use the MOC process to initiate changes that may not be justified. It is nice to have category or a hobby horse. In one organisation, the person responsible for processing the MOC requests was clearly overloaded with a significant backlog.

It is useful to introduce a screening process by which it can be decided *a priori* whether or not a change request goes through the MOC or not, and what priority should be allocated. One of questions to ask is - if the change is not carried out what are the negative impacts?

9. Electronic information management

Many organisations use paperwork to manage the change processes, but some organisations have moved to electronic information management. One immediate benefit is that unless the change is approved by all the nominated personnel, it does not proceed to the approval managers at the next levels. By nominating alternates to the signatories, the process is not held up.

The electronic approval system ensures that unauthorised hardware modifications cannot occur, as the budget for the expenditure has to be approved by an appropriate manager.

### 11.3.10 Systems of Work

The systems of work cover a number of procedures related to safe work practices in operation and maintenance. In the CCPS model (1989), the systems of work and mechanical integrity aspects (see Section 11.3.11) have been combined.

The main systems of work are:

1. Pre-startup safety reviews
2. Commissioning procedures
3. Operating procedures
4. Preparation for maintenance
5. Permit to work
6. Re-commissioning after shutdown
7. Decommissioning
8. Demolition procedures
9. Laboratory and other support services

Written procedures associated with the above must be clear and concise, and used for training. Guidelines have been developed (CCPS 1996, Walter and Mentzer 1996).

#### *11.3.10.1 Pre-startup safety reviews*

Many incidents occur during plant startup, and often attributed to unforeseen causes. This 'unforeseen causes' reason is no longer justified, both from a cost aspect such as project delays or equipment replacement and from a legal perspective. The pre-startup safety review has been specifically listed as a PSM element in the OSHA rule.

The review covers the following aspects:

- Check of installation against design specifications
- Check to ensure that safety, operating, maintenance and emergency procedures are in place and adequate
- Check that training has been completed on the procedures to employees and contractor personnel

- Verify in the field that actions from safety studies have been incorporated - e.g. HAZOP closeout actions, safety assessment study recommendations, last minute modifications are subject to MOC process.
- Verify that the safety instrumented systems are correctly wired to perform their functions.

There are many reported incidents from failure of pre-commissioning checks, or inadequate checks. A few examples below highlight the importance of this activity.

**EXAMPLE 11-5 PRE-COMMISSIONING CHECKS**

a) In a mineral processing installation, the HAZOP study action was to ensure that a feed solvent pump was tripped on high level on the downstream equipment. In fact there were at least six different interlocks tripping the same pump. Pre-startup check revealed that all the interlocks were wired to trip the wrong pump!

b) In a reformer plant for hydrogen production, the signal from the termination cabinet to the natural gas feed shutdown valve in the field had become disconnected in the termination cabinet. Someone had opened the cabinet after installation, and did not report it. This was discovered during pre-commissioning safety check, when the valve did not close when the shutdown signal was generated.

c) In multi-stream plants, it is not uncommon for one stream to be commissioned and operating, while the other parallel streams are isolated and installation is still being completed. The pre-commissioning check showed that the isolation spade was rated for 150 lb, whereas the piping system and flanges were rated for 300 lb! If this was not detected, there could be a major gas leak on startup.

d) A skid-mounted hydrogen compressor was subject to a HAZOP study prior to installation and commissioning. The HAZOP identified that during pre-commissioning, a check must be made to ensure that intrinsically safe barriers between field instruments and the DCS are installed in the termination cabinet. A pre-commissioning check had failed or was not carried out. A few days after the compressor was started and operating, a hydrogen leak occurred causing an explosion and the compressor ended up in several pieces.

■ ■ ■

### 11.3.10.2 Commissioning procedures

A commissioning safety study must be undertaken, as soon as a framework of commissioning procedures has been developed. The study mainly focuses on the adequacy and robustness of the procedures, with the view to improvements, before commissioning. The appropriate hazard identification techniques for this stage in the life cycle are described in Section 4.5.3.2. Main aspects are:

- Commissioning sequence
- Process isolations/de-isolations

- Pressure testing of equipment (test method - hydrostatic or pneumatic, test medium - water or other liquid, compressed air or nitrogen, source of supply, location of discharge, process isolations)
- Trips and alarms testing
- Communications
- Contingencies (e.g. if commissioning has to be abandoned halfway, and re-start has to be made)

### 11.3.10.3 Operating procedures

The purpose of a written operating procedure is to provide clear instructions for safely conducting the process activities associated with the procedure. The procedure must be communicated to all relevant employees, and be readily accessible for reference.

The procedures cover the following:

- Plant startup (cold startup after turnaround, and hot startup after a short duration planned or emergency shutdown)
- Shutdown (planned shutdown, emergency shutdown)
- Normal operation (responses to alarms)
- Operating limits for critical operating parameters (upper and lower bound operating limits, upper and lower bound safety limits)
- Hazardous properties of materials and MSDS
- Personal protection equipment requirements
- Special hazards (e.g. chemical reactivity)
- Safety systems and their functions
- Abnormal situation management (ASM)
- Provision for review and update

### 11.3.10.4 Abnormal situation management

Abnormal situations are defined as the development of non-optimal conditions that the automatic control equipment cannot cope with and thus requires human intervention (Nimmo 1995).

Particular attention should be paid to ASM, as incorrect management of the situation can result in the abnormal situation getting out of control, resulting in an accident.

Nimmo (1995) lists a number of causes for inadequate management of abnormal situations that have escalated into accidents:

- Absence of a clear understanding of what an abnormal situation is and its consequences in the event of an incorrect response
- Absence of clear procedures for dealing with abnormal situations (as opposed to emergencies)
- Inadequate time available for the operator to mount the correct response. This is a design deficiency, as this should have been identified at the hazard identification stage, and designed for using the layer of protection analysis.

- Significant role of human errors. One may recall that it is the incorrect diagnosis of the abnormal situation and response by one of the operators that triggered the Three Mile Island nuclear reactor incident.
- Control room ergonomics contributing to human error. This problem has been largely overcome in modern plants.
- Incorrect operating philosophy - the attitude that there should be no production interruption, whereas it may be safer to shut down, or let the installed safety instrumented system (SIS) initiate a shut down, as a response to an abnormal situation.
- Loss of organisational memory - information from earlier minor incidents is lost. How often we have seen the question asked - "what did we do when this alarm came up last time ...?"
- Absence of teamwork and effective communication.

### *11.3.10.5 Isolation procedures*

Process plant maintenance requires access to piping and equipment. In order to provide safe access for maintenance personnel, the first priority is to isolate the equipment or pipe section, and make it safe, before a Permit to Work (PTW) can be issued. Inadequate isolation has resulted in a number of accidents.

1. Process isolation

The main issues related to isolation as part of preparation for maintenance are (Townsend 1992):

- depressuring. If the system is under pressure, it must be depressurised first. Gas systems can be vented to a lower pressure system, flare or to a safe location to atmosphere, if permissible under environmental regulations. The classic accident of a person opening a 300mm (12") casing with a residual pressure of 35 kPag (5 psig), and struck by a load of over 250 kg is well known. He was told in the common jargon that the residual pressure was "5 pounds", and did not realise that it was 5 pounds per square inch.
- cooling down. Rapid cooling may cause vacuum buildup and the equipment may not have been designed for it.
- removal of hazardous liquids (draining to another vessel or a process drain)
- removal of hazardous vapour. Purging the equipment with air if it did not contain flammable vapour, or inert gas if purging flammable vapour.
- removal of solid residues. A clear procedure must be established in terms of cleaning medium, e.g. steam, access, presence of pyrophoric substances or toxicity of solids. Personal protection equipment (PPE) requirements must be established *a priori*, and provided.
- isolation from other plant or equipment. This may require insertion of a blind, or swinging of an installed spectacle blind. Make sure that the correct specification blind is inserted in the correct location. A master P&ID with locations of blinds, and a blinds list must be available. Some plants prepare this for each major shutdown, as part for shutdown planning.

- safe means of access and escape for maintenance personnel
- for work in sewers and drains, isolation may not be possible. During the work, there may be drains from other areas of the site. This is a particular hazard that must be planned against.

2. Electrical isolation

For any work carried out on equipment connected to electric drives including all rotating equipment, conveyors and overhead cranes, there must be electrical isolation of the drive carried out by an electrically competent person (lockout of isolator and/or physical removal of fuse).

High voltage isolation (above 1000V) can only be carried out by a person licensed to operate high voltage equipment.

Fixed gaseous fire extinguisher discharge in enclosures must be isolated before access for maintenance.

3. Lockout and tagout

Isolated equipment must be tagged out, and where relevant (specific valves, electrical equipment) should be locked out. The procedure should describe the various types of tags (personal danger tag, isolation tag, out of service tag etc), and requirements on when to use them who has the authority to remove the tags.

### *11.3.10.6 Permit to work*

The permit to work (PTW) procedure, along with the isolation procedures, forms the most important procedure for maintenance. A number of guidelines are available (HSE 1996; Australian Institute of Petroleum 1995).

The PTW covers:

- cold work
- hot work
- entry into confined spaces (atmosphere testing requirements)
- excavation (to prevent interference with buried utility pipes, cables)
- de-isolation (removal of spades, reconnect electrical equipment)
- re-commissioning after maintenance (leak testing)

The required isolation and completion of isolation is also entered in the PTW form. A format of a PTW form is provided by Townsend (1992).

One of the problems often encountered is that in a paper-based PTW system with multiple copies, there is a necessity to confine the form to a single page, at the expense of details.

Most organisations have moved to electronic generation of PTW, and therefore there is no restriction on number of pages. Additional fields can be added, and sufficient room can be provided to enter details. A recent software addition in this area is described by Ilife et al. (1999) and Naylor (2003).

Maintenance work may be carried out either by plant maintenance department and/or by contractors. For the latter, training in site safe work systems must be provided. More details are given the in Contractor management section (11.3.16).

### *11.3.10.7 Decommissioning and demolition procedures*

Decommissioning is carried out infrequently and therefore it is not possible to develop standard procedures. Important aspects to consider are:

- From the hazard identification of decommissioning (Section 4.5.3.3), specific procedures must be developed and implemented.
- Dismantling of decommissioned equipment will require a number of job safety analyses, each focused to the specific equipment.
- Activities associated with decommissioning can be covered by the isolation and PTW procedures.
- Site environmental survey must be undertaken to establish the levels of contamination, cleanup goals, and a remediation strategy. Liaison with environmental authorities would be required during this process.

Managing risks in decommissioning is discussed in more detail in Section 12.9.

### *11.3.10.8 Product sampling*

Plant operation requires process samples to be taken from the plant and analysed. Feedback is given to the operator on the quality of raw materials, intermediates and products, so that appropriate process adjustments can be made.

In some plants, operators collect the sample to hand over to the laboratory for analysis. In other plants, laboratory personnel collect the samples, analyse and provide the results to the operator/supervisor.

The laboratory procedures related to plant operation cover the following:

- List of process samples to be collected
- Frequency of sampling
- Sampling procedures
- Training in safe collection of samples

Routine sample collection may not be carried out under a PTW, but the plant operations approval must be obtained by laboratory personnel before sample collection.

Separate safety procedures are to be developed, governing laboratory safety (chemicals handling, fire safety, safe disposal of samples etc.)

## 11.3.11 Mechanical Integrity

One of the goals of safe operation is that the equipment used to store and handle hazardous materials are designed, installed, and maintained to prevent loss of containment and other accidents. Remson et al. (1995) identify some of the problems in developing and implementing a mechanical integrity program.

In this section, mechanical integrity covers three aspects:

1. Integrity of piping and equipment to prevent single-point failures that could result in loss of containment. These are sometimes referred to as 'fabric failures'.
2. Integrity of control system instruments to minimise potential for process deviations
3. Integrity of safety instrumented systems to provide the design reliability for controlling major hazards.

From the perspective of the OSHA PSM rule, maintenance procedures are covered in the systems of work in Section 11.3.10. Procedures for maintenance related training are covered in Section 11.3.5.

Inspection and testing, and equipment deficiencies/quality assurance are covered in this section.

The integrity aspects covered are:

1. Materials of construction
2. Fabrication and inspection procedures
3. Installation procedures
4. Equipment Register
5. Preventive maintenance
6. Integrity inspections and testing
7. Alarms and instruments reliability management
8. Spare parts suitability

### *11.3.11.1 Materials of construction*

The selection of correct materials of construction from design through to operation and maintenance is critical for maintaining mechanical integrity. Important considerations are:

- Specification of correct materials of construction for piping, valves, instruments, vessels, relief systems, tanks, pumps, compressors and other rotating equipment, and other equipment.
- Vessels and piping to industry standards (specify relevant design codes). Include corrosion allowances where necessary.
- Quality assurance in procurement of materials by fabricator
- Ensure no substitutes are accepted
- Material tracking system through a tagging procedure
- Instruments materials designed to chemical group and temperature class specification

### *11.3.11.2 Fabrication and inspection procedures*

There have been cases of pressure vessel failures due to incorrect fabrication. Procedures to assure quality of equipment during the fabrication phase need to be developed. These include:

- Specification of fabrication requirements in the mechanical design package
- Quality assurance in fabrication such as verification of welding procedures and welder qualifications, non-destructive testing (NDT) of welds, heat treatment, hydrostatic/pneumatic pressure testing, verification of dimensions and tolerances
- Factory acceptance tests for performance
- Independent inspection and certification where relevant

Project management controls may cover fabrication yard also.

### *11.3.11.3 Installation procedures*

In a greenfield site, installation is normally managed by the contractor, while the project manager maintains supervision. There should be a quality system to ensure that the equipment is installed according to design specifications and equipment supplier manuals. Incorrect installation of pipework (incorrect design, incorrect material, poor execution of work) has contributed to many pipework failures once the plant becomes operational (Kletz, 1999).

In a brownfield site, with a section of plant already operating, there are interactive hazards during installation, and this cannot be left to installation contractor alone.

The project management should ensure that the following procedures are in place. Some of these would be developed by the contractor for approval by the client, and some would be developed by client personnel. The list is not exhaustive, and brainstorming is required to construct a comprehensive checklist.

- Structural integrity of steel
- Installation plan, including the sequence
- Handling of heavy equipment by crane. Incorrect crane capacity or incorrect handling can bring a structure down (see Figure 11-1). Job safety analysis of each heavy lift above a specified capacity. Dropped object study forms a routine component in safety analysis of offshore oil and gas installations, but is not so common in onshore process plants, as crane operations are relatively infrequent, and generally carried out during a plant shutdown.
- Ensuring the integrity of cranes and hoists prior to lifts to prevent dropping of loads. There has been cases of equipment items weighing up to 7 tonnes that have been dropped from height, with fortunately no injuries, but significant project delays.
- Adequacy and integrity of scaffolding
- NDT of field welds
- Handling of sensitive equipment such as instruments and analytical equipment
- Working at heights
- Proper bolting techniques (material, torque setting)
- Access procedures for heavy vehicles and mobile cranes
- Effective communications

- Quality assurance of installation (clearances, tolerances, alignment)
- Field testing of earthing (grounding)

If installation were to take pace in one part of the plant area while an existing plant is already in operation (i.e. simultaneous operations), then significant additional planning is required. The main issues are:

- Potential for installation having an adverse impact on existing plant operations to be identified and prevented
- Potential for an emergency in operating plant to affect installation activities to be identified and emergency actions planned for
- Positive process isolation of operating plant from new installation
- Contractor training for coping with incidents during simultaneous operations
- Effective communications

Using a comprehensive checklist generated specifically for the targeted installation, relevant procedures or work instructions must be developed and relevant project/contractor personnel trained in the procedures.

### *11.3.11.4 Equipment register*

It is essential to compile an equipment register. This will contain all the equipment (vessels, tanks, valves, instruments, relief devices etc). The fields of this electronic database should contain, as a minimum, the following:

- tag number
- description and type of equipment (e.g. modulating valve, on/off actuated valve, pressure transmitter, centrifugal pump etc.). Need to provide relevant detail here.
- service
- frequency of inspection (external inspection of vessels, internal inspection, non-destructive testing, instrument calibration etc.)
- procedure reference (test procedure is cross-referenced)
- special characteristics (high or low corrosion rating, cryogenic duty, high temperature service, lined equipment etc.)

The equipment register forms the basis for mechanical integrity inspection planning and for preventive maintenance.

### *11.3.11.5 Preventive maintenance*

Preventive maintenance (PM) is the system by which inspections and tests are carried out on equipment at scheduled intervals to detect incipient failures or degradations, so that action can be taken to rectify the problem before it develops into a major failure.

PM is generally extended to equipment where failure to identify incipient failures could result in a major breakdown or major process deviation. Some examples are:

- equipment subject to wear and tear (rotating equipment such as pumps, compressors, centrifuges, conveyors etc.)
- sensing instruments that form part of the control loop (calibration of pressure, temperature, flow, and level sensors and analysers)
- modulating valves that are part of the control loop
- critical safety equipment such as fire protection system, fire and gas detection system
- equipment prone to fugitive emissions
- personal protection equipment (personal gas monitors, breathing apparatus etc.)
- process drains for blockage

Key components of PM are:

- List of equipment that need PM (can be taken from equipment register)
- Frequency of PM and actual activity involved (daily, weekly, monthly etc.)
- Procedures for conducting PM
- Training for maintenance personnel
- Feedback of equipment deficiency
- Action taken and closeout
- Record keeping

PM is best managed by using a software database that automatically generates the job request at scheduled intervals. The database can be made to generate inspection checklists as part of the job request to facilitate the work. The maintenance planner generally completes the database entry from feedback on the job request form.

### *11.3.11.6 Integrity inspections and testing*

Integrity inspections are carried out at less frequent intervals than PM, and generally during a plant turn around. Inspection is a statutory requirement for many items of equipment. Typical equipment include:

- pressure vessels (statutory)
- atmospheric storage tanks (external and internal, statutory)
- pressure safety valves (statutory)
- pressure/vacuum valves
- flame arresters
- critical process pipework (may need thickness testing or other NDT inspections)

- insulated equipment/pipework (inspection of corrosion underneath insulation)
- bunds/dikes
- equipment/pipework support structures
- cooling towers
- electrical continuity of earthing of equipment containing flammable materials (resistance measurement)
- inspection of electrical equipment in classified hazardous areas for integrity

Deficiencies are documented, corrective actions are devised and implemented. All action taken is also documented, with date of completion, in the database.

Predictive Trend Analysis can be used as a tool in system integrity management. Information gathered from monitoring of maintenance parameters are analysed using statistical distributions or time series analysis to predict future trends and time for failures. From the results, the preventative maintenance strategy is improved, and failures at their incipient stages are attended to before a catastrophic failure occurs.

### *11.3.11.7 Alarms and instruments management*

This section describes the need for function testing of alarms and interlocks, in accordance with the required schedule in order to maintain the Safety Integrity Level (SIL) allocated to the SIS.

Key issues are:

- Compilation of an alarms and interlocks register
- Description, tag number, function of interlock, test frequency
- Test procedure (including bypass procedures)
- Sign off after trip is re-armed
- Keeping of test records
- Fault reporting, corrective action and closeout

### *11.3.11.8 Spare parts suitability*

It is essential that critical spare parts are carried in the store, especially of safety systems, to minimise downtime of protection equipment. Further, equipment spares should conform to correct specifications. There is considerable potential for human error in this area.

Key issues are:

- Compilation of spare parts register
- Description, tag number and function
- Specification (cross-reference to equipment specification register)
- Parent equipment to which spare part belongs
- Reference to purchasing QA procedure
- Location in stores

### 11.3.12 Emergency Plans

Managing emergencies is a major subject in itself, and is discussed separately in Section 11.5.

### 11.3.13 Investigation and Reporting

In managing process safety, it is of utmost importance that all incidents and near misses are reported and investigated. The reporting of near misses in the SMS procedure is important as industry experience has shown that approximately one major injury occurs for 600 near misses (Jones et al. 1999).

Once an incident or near miss is reported, it needs to be investigated to determine the causes, so that actions may be developed to prevent a recurrence of the incident, and similar incidents in the future.

Important considerations in the investigation are (Kletz 2002):

- Identify root causes. The 'stop line' may be extended beyond a simple 'human error' to the effectiveness of the SMS in the way it is implemented and monitored. Tuli and Apostolakis (1996) emphasize the importance of including organisational issues into root-cause analysis.
- Constitute an expert investigation team. The composition of the team would depend on the potential severity and complexity of the incident. Sometimes, third party participation would be required. Depending on the nature of the incident, there may be investigation by safety regulatory authorities.
- The report should be clearly written, with causes identified, and recommendations for improving process safety. The actions may include changes to design, installation of additional safeguards, changes to procedures and training of personnel.
- The results of the investigation, especially root causes of the incident or near miss, and actions arising should be communicated to all employees and appropriate contractor personnel.
- There should be senior management commitment, including allocation of responsibility and resources (people and budget), to ensure that the recommendations are followed through, implemented and closed out within an agreed time period.
- Record keeping. The investigation report findings must be linked back to the hazard identification and analysis, and update of the hazard register, where appropriate.

### 11.3.14 Performance Measurement

No risk management system can be considered effective unless its performance is judged against measurable parameters. Therefore, the SMS must include, within itself, a provision for performance measurement and continual improvement.

The development of key performance indicators (KPIs) and comparison with actual performance would reveal non-conformances, and provide an indication of the effectiveness, from which corrective actions may be developed.

### 11.3.15 Periodic Review

The SMS should include a procedure for periodic review of the SMS document itself. Key features are:

- Is the SMS still applicable as it stands?
- What has changed in the plant that needs to be reflected in the SMS?
- How can the findings of audits and any incident/near miss investigations be incorporated into the SMS?
- Has there been a change in regulatory requirements?

A working party must be set up by senior management for this review. The output is an updated SMS and associated procedures.

Once the SMS is updated, it must be implemented through refresher training.

### 11.3.16 Contractors

The services of third parties are required throughout the facility life cycle, as shown in Figure 3-1, and therefore, play a key role in the management of process safety.

There are a number of aspects to management of contractors:

- Contractor selection based on contractor's safety performance and programs.
- Ensuring safety of contractor personnel while working on the site (installation, commissioning, maintenance during routine operation and turnarounds). This overlaps partly with OH&S management, and is the responsibility of the contractor.
- Information to contractor personnel of major hazards on the site (fire, explosion, toxic releases), and material safety information.
- Training for contractor personnel in the facility's systems of work (Section 11.3.10).
- Induction on emergency action plans.
- Emphasis on the importance of returning an equipment after maintenance to 'fit for purpose' status.
- Monitoring of contractor performance
- Interface document that describes the relationship between the Company SMS and the Contractor SMS.

### 11.3.17 Audit

A procedure should be developed for auditing the SMS and its effectiveness in achieving the objectives of the MAPP. Audits can be internal, external or both.

The findings of the audit are fed back to senior management, for updating the SMS where appropriate.

Auditing methods are described in Chapter 14.

## 11.4 IMPLEMENTATION OF SMS

### 11.4.1 Implementation Model

Once an SMS is developed, it must be implemented. There is no single 'right' way of implementing the system. Figure 11-2 depicts an adaptation of the pyramid model described by Dowell III (2002). It provides a useful framework for converting the procedures to practices.

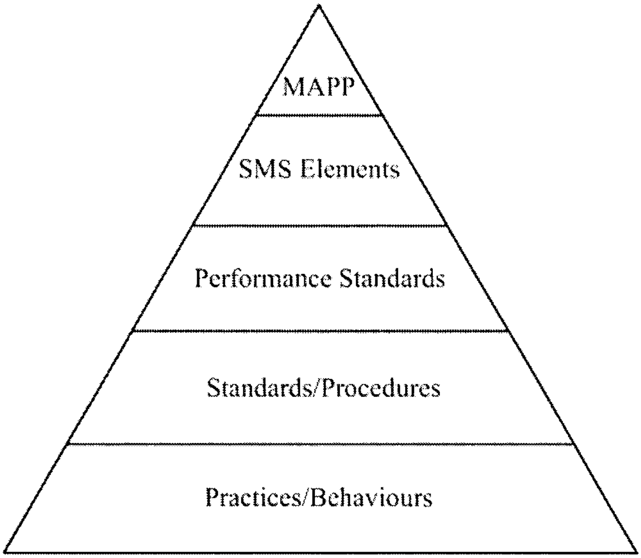


**FIGURE 11-2 PYRAMID MODEL FOR POLICY TO PRACTICES**

A most important level in the pyramid model is that between the statement of SMS elements and procedures, namely the performance standards (PS). The PS define what performance needs to be achieved, but not what or how it should be done. This is outlined in the procedures.

SMS implementation requires translating the Major Accident Prevention Policy (MAPP) into practices and behaviour. The sequence of layers in Figure 11-2 should be followed for effective implementation.

Implementation of SMS can be summarised in answering the following questions:

1. What are the safety critical systems (SCS) in controlling the hazards in the facility? These include hardware items to prevent loss of containment (i.e. vessels, tanks and pipework); managing control system deviations (e.g. alarms and interlocks), protection systems (e.g. pressure relief,

Safety Instrumented Systems, emergency depressuring), and mitigation measures (e.g. fire protection).
A register of SCS needs to be compiled, with all relevant specifications, design and operating limits.

2. What safety critical activities (SCA) are required to maintain the integrity of the safety critical systems? These include all the procedures covered in the preceding sections training, systems of work, mechanical integrity management, inventory management etc.
   A register of SCA is also required. The register outlines the organisation position responsible for implementation of these activities, the frequency, and cross references the relevant procedure by which the activity is carried out.
3. What are the performance standards of these safety critical systems and activities? In other words, what criteria must be met by the SCS/SCA in order to achieve safe operation?
4. How do we ensure that the PS are being met? PS monitoring and reporting, and auditing are the tools.

Details of the implementation in an organisation are described in detail by CCPS (1997b). Key points are:

- Pilot testing in one area or one facility of the organisation. After this test, the results should be assessed against the objectives of the plan and some areas of the plan may have to be revisited for fine tuning.
- Conduct information sessions across the organisation to all employees by outlining the regulatory requirement for SMS and the benefits it would bring. Obtain commitment of the employees for compliance with the system and procedures once in place. Often, formation of an implementation team within the facility, consisting of personnel from different levels of the facility and from different departments (production, maintenance, technical services, safety etc.) is more effective.
- Design and provide training at all levels, and to contractors. Training should include responsibility and accountability, the procedures themselves and the reason thereof, performance standards, performance monitoring and feedback.

### 11.4.2 Performance Standards

A performance standard can be numerical or non-numerical. Some examples of performance standards are given below:

1. *PSV xxx shall be available 100% of the time, when the plant is online.*
   The associated SCA will include maintenance interval, isolation of PSV for online maintenance, and ensuring that the standby PSV is lined up correctly.
2. *The high level protection interlock LAHH xxxx shall meet a Safety Integrity Level of 2 (i.e. it should be available on demand at least 99% of the time).*

The SCA describes the interlock function testing interval, person responsible, and function testing procedure, including bypass of interlock, and rearming after completion of test.

3. *Accidental polymerisation of monomer shall be prevented during transport.*
The SCA describes the addition of inhibitor, the name and quantity of inhibitor to be added, and testing of inhibitor concentration in the monomer.

The above examples clearly show that without performance standards, the procedures in themselves are difficult to implement effectively.

### 11.4.3 Monitoring and Evaluation

As mentioned earlier, performance monitoring of SCSs and SCAs is necessary to obtain a continual feedback on how well the SMS is being practised. This requires the following:

- Development of key performance indicators for the SCS and SCA.
- Comparison of actual performance with the KPI, and identification of non-conformances.
- Instigation of corrective action to maintain required performance.

The measuring of safety performance may be divided into three categories (EPSC 1996), for management convenience.

- Measuring plant and equipment
- Measuring systems and procedures
- Measuring people

Some performance measurement methods are described by Sweeney (1995). Fakhru'l-Razi et al. (2003) describe a statistical model for measuring effectiveness of training maintenance contractors for plant shutdown.

Samdal et al. (2004) have developed an integrated KPI for corporate monitoring purposes by Norsk Hydro. The KPI is an average availability based on the reliability and availability of instrumented protection systems, and mechanical integrity of vessels and piping. While the integrated KPI is suitable as a high level indicator, individual KPIs in each of the safety critical areas are necessary for day to day management of a process facility, a fact acknowledged by Samdal et al. (2004).

## 11.5 EMERGENCY PLANNING AND RESPONSE

### 11.5.1 Emergency, Crisis and Disaster

We need to make clear distinctions between three key concepts—'emergency', 'crisis' and 'disaster'. These terms are sometimes used interchangeably, but they have different consequence scales, warranting different action plans.

An '*emergency*' is a present or imminent event that requires prompt coordination of actions to protect the health, safety, or welfare of people, and to limit damage to property and the environment.

An example of emergency is loss of containment of a flammable or toxic material in a process facility. It cannot normally be managed alone by the person discovering the incident, and requires a team effort for control. If controlled quickly, significant harm to people, property or the environment may not eventuate.

A '*crisis*' is similar to an emergency, but may be regarded as the implications to the corporation in the aftermath of an emergency, in terms of threat to the corporation's image and profitability.

A crisis can also arise from non-process emergency causes. The responses to a crisis would be much more than that required for an emergency response.

A '*disaster*' is an event which afflicts a community, the consequences of which are beyond the immediate financial, material, or emotional resources of the community.

An uncontrolled emergency can turn into a disaster, e.g. the loss of Piper Alpha oil and gas platform in the North Sea, and the Bhopal toxic gas release incident in India.

### 11.5.2 Planning for Emergencies

It is imperative that an emergency is immediately detected and controlled, before the scale escalates. Emergency planning consists of the following components:

1. Identification of possible emergency scenarios. The Hazard Register (see Section 4.4.7) provides an input to this.
2. Decision on the scale of emergency to be planned for. This is quite critical. If the scale planned for is only a flange leak of a toxic gas, but there is a potential for line rupture and a larger release, then the impact may be felt offsite. There has been much debate since September 11, 2001, that the scale of emergency planned for, must be much larger, given terrorism as a new hazard.
3. Preparation of emergency response plan
4. Training in emergency preparedness (training of personnel, communication, testing of plan)
5. Administration of the plan (documentation, periodic review and update, approval and audit).

There have been a number of articles, guidelines and books written on the preparation of emergency response plans (Scott 1992; Lees 2001; CCPS 1995b). Canadian Standard CAN/CSA-Z731-95 (1995) and the guideline from the Queensland Department of Emergency Services in Australia (1998) provide comprehensive methodologies for emergency planning for both onsite and offsite. The Canadian Standard covers a wide range of industries and requires some tailoring for the process industry.

### 11.5.3 Pre-incident Plans for Specific Emergencies

An emergency plan is normally a broad scheme, aimed at controlling all possible emergencies on a site. Therefore it would lack detail when it comes to specific emergencies such as a fire, toxic gas leak, etc. Pre-incident plans are prepared to address such specific emergencies. In a pre-incident plan, a specific scenario is selected. The consequence of this scenario (e.g. fire) is modelled in detail to obtain impact distances and escalation potential. The measures to control the emergency are developed step-by-step, including the sequence of activities to be carried out, specifying the personnel involved. The sequence follows the dictate of the general Emergency Response Plan (ERP). Special requirements, if any, are identified in the sequence, including first attack, and actions to be taken to prevent escalation until the arrival of external emergency services.

Pre-incident plans are most useful in identifying any special requirements in combating an emergency, and in identifying the sequence of emergency control and manpower requirements. In addition, they provide a valuable training tool for the emergency crew.

Crew resource management for decision making under stress are highlighted by Fleming and Lardner (2000). Key items for evaluating emergency preparedness are listed by Swan (1999).

### 11.5.4 Dynamic Processes in Emergency Response

In a loss of containment emergency involving flammable materials, there occur competing dynamic processes. On the one hand the established emergency response comes into action, with a pre-planned action sequence. Simultaneously, the initial incident tends to grow in scale, depending on the level of process safeguarding provided, and their reliability.

A pre-incident plan should account for the dynamics of emergency control versus escalation, which can determine the ultimate course of the emergency. Should escalation occur before the incident is controlled, the safety of emergency response crew is endangered, besides asset damage on a larger scale.

The competing dynamic processes of incident escalation and incident control can be assessed using event tree analysis (Raman 2004). Escalation times for impinging fires, assessed from heatup analysis (see Chapter 7) are compared with required response times from the emergency crew. The method allows for design enhancements and makes the emergency response plan more robust.

## 11.6 ROLE OF SOFTWARE SYSTEMS IN RISK MANAGEMENT

The Canadian Standard for emergency planning for industry (1995) has been developed into a computer software package. This software is reported to take the user step-by-step through the process of creating an emergency plan as outlined in the Standard.

The software CAMEO focuses on hazardous industries with toxic gas release potential. This program has a toxic gas dispersion package integral to it, so that in the event of such emergencies, the downwind area affected can be modelled on-line, and action can be taken to evacuate sections of community outside the facility boundary. The package also has provisions for input of street names, names and addresses of individuals, and street directory information, to facilitate public emergency services for an organised and orderly evacuation of the area local to the emergency.

The Dutch Fire Inspectorate, with the assistance of TNO in the Netherlands, has developed a computerised decision support system for quick, real-time evaluation of the development of a toxic disaster. The system is called 'IRIS', which is the Dutch acronym for 'Information and Calculation System for Incidents involving Hazardous Substances'.

Computer software is useful for pre-incident planning. The Shell Shepherd suite of programs offers a useful tool for pre-incident planning (Shell Global Solutions, 2004).

## 11.7 SMS FOR SMALL FACILITIES

There are a number of small facilities operating with significantly lower inventories of hazardous materials, but still pose a risk to land uses immediately surrounding the facilities, should an emergency occur. These companies are resource limited, generally do not have a formal SMS, and essentially adopt a 'reactive' approach, with management implementing ad hoc procedures in response to safety incidents. This approach relies on the skills of individuals, rather than a system of procedures to guide them.

The Chemical Safety Board accident investigation database covers a number of small facilities (CSB 2003).

Since small companies do not have a large asset base, it is more imperative that they have some form of PSM in place, as an accident event may result in significant financial loss other liability exposures, threatening the viability of the operation. Unfortunately, if there is no legal requirement on their part by virtue of their size, a system may not be developed.

### 11.7.1 Problems in SMS Development for Small Facilities

A review of the SMS elements for major hazard facilities indicates that a number of elements are either not applicable, or, even if applicable, the small facility is unable to implement them. Some of the difficulties are (Chia et al. 2001):

- Lack of understanding of major hazards
- Lack of adequate resources
- Lack of adequate skills
- Poor perception of the importance of SMS, which is seen as burdensome
- Mistaking between OH&S management and PSM, the latter being viewed as duplication of efforts

### 11.7.2 Suggested Framework for Small Facilities

Since it is a regulatory requirement in many countries that the small facility should have an OH& S management system or OH&S management plan, it may be easier to expand the functions of the overlapping elements in the OH&S management plan to capture the essential requirements of the PSM. The OH&S management standards (AS 4801-2000; British Standard OHSAS 18001-1999) can be used as a basis for a small facility SMS.

By using this approach, the company management does not feel that an additional layer of procedures has been superimposed on it. Where there is no overlap, those SMS elements considered critical can be included, with corresponding additional procedures.

A framework is suggested by Chia et al. (1999). A set of model procedures for small to medium-sized facilities has been developed by EPSC (2000).

An integrated system that covers the full safety spectrum would benefit all facilities, large and small.

## 11.8 REVIEW

In Chapter 11, we have introduced the concepts related to management of process safety. Distinctions between process safety and occupational health and safety have been highlighted. The management model itself is based on the UK HSE model for successful safety management.

A number of SMS models have been introduced. The differences between the models are minimal, and they consist of essentially the same elements arranged in different formats. The SMS model described in the Seveso II Directive has been used for detailed discussion. The concepts are equally applicable to offshore oil and gas production operations.

Considerable discussion has been devoted to management of change, systems of work, mechanical integrity, and abnormal situation management. The need for root cause analysis in accident investigation, tracing back to SMS failures and organisational factors has been emphasized, by stretching the 'stop line' beyond simply human error.

The need for pre-incident planning in emergency preparedness has been highlighted, with particular emphasis on competing dynamic processes of incident control and incident escalation, in the wake of an emergency.

An SMS cannot be effectively implemented unless performance standards for the various elements are developed. The performance standard as an intermediate step between SMS elements and procedures is shown by a pyramid model.

The need for small to medium-sized facilities has been discussed. The OH&S management system can be extended to incorporate essential PSM elements for small facilities. A large number of recently published literature references are provided for the interested reader.

## 11.9 REFERENCES

American Petroleum Institute. *Recommended Practice RP 750 - Management of process hazards*, Washington D.C. API 750:1990.

Auger, J.E. 1995, 'Build a proper PSM program from the ground up', *Chemical Engineering Progress*, January, pp. 47-53.

Australian Institute of Petroleum, 1995, *Guidelines for the establishment and operation of a permit-to-work system*, Melbourne, Australia.

BHP Billiton, 2002, 'Health, Safety, Environment and Community Management Standards', Issue No.2, December. Available at: http://www.bhpbilliton.com.

British Standards. *OHS Management Systems – Specification*, British Standards, UK. OHSAS 18001:1999.

Canadian Standards Association. *Emergency planning for Industry: Major Industrial Emergencies. A National Standard for Canada.* Canadian Standards Association. CAN/CSA–Z731–95:1995.

CCPS 1989, *Center for Chemical Process Safety - Guidelines for technical management of chemical process safety*, American Institute of Chemical Engineers, New York.

CCPS 1995a, *Center for Chemical Process Safety - Guidelines for process safety management documentation,* American Institute of Chemical Engineers, New York.

CCPS 1995*b, Center for Chemical Process Safety - Guidelines for technical planning for on-site emergencies,* American Institute of Chemical Engineers, New York.

CCPS 1996, *Center for Chemical Process Safety - Guidelines for writing effective operating and maintenance procedures*, American Institute of Chemical Engineers, New York.

CCPS 1997a, *Center for Chemical Process Safety - Guidelines for integrating process safety management, environment, safety, health and quality,* American Institute of Chemical Engineers, New York.

CCPS 1997b, *Center for Chemical Process Safety - Guidelines for implementing process safety management systems*, American Institute of Chemical Engineers, New York.

Chemical Manufacturers Association (CMA) Inc. 1990, *Responsible Care: Process safety code of management practices*, Washington D.C. September.

Chia, S., Long, B. and Raman, R. 2001, 'Development and implementation of a safety management system for small facilities', Paper presented at the *2001 Spring National Meeting*, Houston, Texas, April 22-26.

Columbia Accident Investigation Board Report 2004, Vol.1, Available at: http://www.caib.us.

Council of the European Union, 1996, *Common Position (EC) No. 16/96 on Council Directive 96/82/EC on the control of major accident hazards involving dangerous substances,* 19 March, Brussels, Belgium.

Crawley, F.K. 1999, 'The change in safety management for offshore oil and gas production systems', *Transactions of Institution of Chemical Engineers*, Part B, Process Safety and Environmental Protection, 77, pp. 143-148.

CSB 2003, US Chemical Safety & Hazard Investigation Board, Available at: http://www.csb.gov

Dawson, D. and Brooks, B. 1999, *Report of the Longford Royal Commission: The Esso Longford gas plant accident,* Government Printer for the State of Victoria, Melbourne, Australia.

DNV 1994, *Det Norske Veritas - International Safety Rating System*, 6th edn, DNV Industry Ltd, London.

Donnelly, 1994, 'An overview of OSHA's process safety management standard (USA)', *Process Safety Progres*, April, pp. 53-58.

Dowell, A.M. (III) 2002, 'Getting from policy to practices: The pyramid model (or what is this standard really trying to do?)', *Process Safety Progress*, March, 13-18.

EPSC 1994, *Safety Management Systems: Sharing experiences in process safet,. European Process Safety Centre*, published by the Institution of Chemical Engineers, Rugby, England.

EPSC 1996, *European Process Safety Centre - Safety Performance Measurement*, (ed.) J. Van Steen, J., Published by the Institution of Chemical Engineers, Rugby, England.

EPSC 2000, *European Process Safety Centre - SHE Management System for Small to Medium-sized Enterprises*, Published by the Institution of Chemical Engineers, Rugby, England.

Fakhru'l-Razi, A., Iyuke, S.E., Hassan, M.B. and Aini, M.A. 2003, 'Who learns when workers are trained? A case of safety training of maintenance contractors' workers for a major petrochemical plant shutdown', *Transactions of Institution of Chemical Engineers*, Part B, Process Safety and Environmental Protection, vol. 81, pp. 44-5.

Fleming, M. and Lardner, R. 2000, 'It's all gone pear-shaped', *The Chemical Engineer*, 6 July, pp. 16-19.

Government of Queensland, 2001, *Dangerous Goods Safety Management (DGSM) Act and the DGSM Regulations*, Queensland Government Printer, Brisbane, Australia.

Government of Victoria 2000, *Occupational Health and Safety (Major Hazard Facilities) Regulation*, gazetted 1 July, Melbourne, Australia.

HMSO 1975, *The Flixborough disaster - Report of the court of inquiry*, Her Majesty's Stationary Office, London.

Hopkins, A. 2000, *Lessons from Longford - The Esso Gas Plant Explosion*, CCH Australia, ISBN 1-86468-422-4.

HSE, Health and Safety Executive UK. 1991, *Successful Health & Safety Management*, Health and Safety Series booklet HS(G) 65, HMSO, London.

HSE, Health and Safety Executive UK. 1996, *Setting up and Running a Successful Permit-to-work System: How to do it,* HMSO, London.

Ilife, R.E., Chung, P.W.H. and Kletz, T.A. 1999, 'More effective permit-to-work systems', *Transactions of Institution of Chemical Engineers*, Part B, Process Safety and Environmental Protection, vol. 77, pp. 69-76.

Jones, S., Kirchsteiger, C. and Bjerke, W. 1999, 'The importance of near miss reporting to further improve safety performance', *Journal of Loss Prevention in the Process Industries*, vol. 12, pp. 59-67.

International Organization for Standardization ISO, *Quality Management Systems - Requirements*, International Organization for Standardization, ISO 9001:2000.

International Organization for Standardization ISO, *Environmental Management Systems - Specification with guidance for use*, International Organization for Standardization, ISO 14001:1996.

Keren, N., West, H.H. and Mannan, S. 2002, 'Benchmarking MOC practices in the process industries', *Process Safety Progress*, vol. 21, no. 2, pp. 103-112.

Kletz, T.A. 1990, *Critical aspects of safety and loss prevention*, Butterworths.

Kletz, T.A. 1993, *Lessons from Disaster - How organisations have no memory and accidents recur,* Institution of Chemical Engineers, Rugby, England.

Kletz, T.A. 1994, *What went wrong? Case histories of process plant disasters,* 3rd edn, Gulf Publishing Company.

Kletz, T.A. 1995, 'Some loss prevention case histories', *Process Safety Progress*, vol. 14, no. 4, pp. 271-275.

Kletz, T.A. 1999, *Hazop and Hazan - Identifying and assessing process industry hazards,* 4th edn, The Institution of Chemical Engineers, Rugby, U.K.

Kletz, T.A. 2001, *Learning from Accidents,* 3rd edn, Butterworth-Heinemann, Oxford, UK.

Kletz, T.A. 2002, 'Accident investigation - missed opportunities', *Transactions of Institution of Chemical Engineers*, Part B, Process Safety and Environmental Protection, vol. 80, pp. 3-8.

Lees, F.P. (ed.) 2001, *Loss Prevention in the Process Industries*, vol. 2, Chapter 24, Butterworths-Heinemann, Oxford. (A number of additional references on emergency planning are listed here).

Mannan, S. 1996, 'Boiler incident directly attributable to PSM issues', *Process Safety Progress*, vol. 15, no. 4, pp. 258-261.

Naylor, J. 2003, 'Electronic permit-to-work', *The Chemical Engineer*, February, **32**.

Nimmo, I. 1995, 'Adequately address abnormal operations', *Chemical Engineering Progress*, September, pp. 36-45.

Occupational Health and Safety Administration. *Process safety management of highly hazardous chemicals*, Occupational Health and Safety Administration, USA., Federal Register, Washington DC. OSHA 29 CFR 1910.119:1992.

Perron, M.J. and Friedlander, R.H. 1996, 'The effect of downsizing on safety in the CPI/HPI', *Process Safety Progress*, vol 15, no. 1, pp.18-25.

Philley, J. 2002, 'Potential impacts to process safety management from mergers, acquisitions, downsizing, and re-engineering', *Process Safety Progress*, vol. 21, no. 2, pp. 151-160.

Queensland Department of Emergency Services 1998, 'Emergency Planning Guidelines for Industry', Australia New Zealand Hazardous Industry Planning Taskforce, Chemical Hazard and Emergency Management (CHEM) Unit.

Raman, R. 2004, 'Accounting for dynamic processes in process emergency response using event tree modelling', *19th CCPS International Conference*, June 29-July 1, Orlando, Florida, pp. 197-213.

Remson, A.C., Farmer, J.H. and King, C.S. 1995, 'PSM's most common struggle: Implementing mechanical integrity', *Process Safety Progress*, vol. 14, no. 4, pp. 232-237.

Rogers, R.L. and Hallam, S. 1991, 'A chemical approach to inherent safety', *Transactions of Institution of Chemical Engineers*, Part B, Process Safety and Environmental Protection, vol. 69, pp. 149-152.

Samdal, U.N., Flotaker, H.P. and Oien, K. 2004, 'Key performance Indicator for Technical Safety', *11th International Symposium Loss Prevention 2004*, Prague, pp. 1197-1206.

Sanders, R.E. 1993, *Management of change in chemical plants: Learning from case histories*, Butterwoths-Heinemann, Oxford, UK.

Sanders, R.E. 1996, 'Human factors: Case histories of improperly managed changes in chemical plants', *Process Safety Progress*, vol. 15, no. 3, pp. 150-153.

Scott, J.N. 1992, 'Succeeding at emergency response', *Chemical Engineering Progress*, December, pp. 62-65.

Schweer, D. Scholz, G. and Heisel, M. 2000, 'What are process safety management audits telling the operators?', *Hydrocarbon Processing*, October.

Shell Chemical Company 2001, 'Responsible Care, Management Systems Verification', Available at: http://www.shellchemicals.com .

Shell Global Solutions, 2004, Shell pre-incident planning software details, Available at: http://www.shelpipa.com.

Shilitto, D.E. 1995, ''Grand Unification theory' or Should safety, health, environment and quality be managed together or separately?', *Transactions of Institution of Chemical Engineers*, Part B, Process Safety and Environmental Protection, vol. 73, pp. 194-202.

Sorensen, J.N. 2002, 'Safety culture: a survey of the state-of-the-art', *Reliability Engineering and System Safety*, vol. 76, pp. 189-204.

Standards Australia., *Step by step guide on integrating management systems - health and safety, environment, quality.* Standards Australia, Sydney, Australia. Handbook HB 139 (Interim):1999.

Standards Australia. *Australian Standard for Occupational Health and Safety management Systems – Specification with guidance for use,* Standards Australia, Sydney. AS 4801:2000.

Swan, R. 1999, '... Accidents will happen ... ', *The Chemical Engineer*, 27 May, 17.

Sweeney, J.C. 1995, 'Measuring process safety management', *Plant Operations Progress*, vol. 11, no. 2, pp. 89-98.

Townsend, A. 1992, *Maintenance of process plant*, The Institution of Chemical Engineers, Rugby, England.

Tuli, R.W. and Apostolakis, G.E. 1996, 'Incorporating organizational issues into root-cause analysis', *Transactions of Institution of Chemical Engineers*, Part B, Process Safety and Environmental Protection, vol. 74, pp. 3-16.

UK Government 1999, *The Control of Major Accident Hazards Regulations 1999,* Statutory Instrument 1999 No.743, Her Majesty's Stationary Office, London.

US Environmental Protection Agency. *Environmental Protection Agency - Risk management programs for chemical accidental release prevention.* US Environmental Protection Agency, Federal register, Washington D.C. June, Final Rule, 40 CFR Part 68:1996.

Walter, R.J. and Mentzer, W.P. 1996, 'Write better procedures for process safety management', *Chemical Engineering Progress*, September, pp. 59-67.

Yang, S.H., Yang, L. and He, C.H. 2001, 'Improve safety of industrial processes using dynamic operator training simulators', *Transactions of Institution of Chemical Engineers*, Part B, Process Safety and Environmental Protection, vol. 79, pp. 329-338.

## 11.10 NOTATION

| | |
|---|---|
| AIChE | American Institute of Chemical Engineers |
| ALARP | As Low As Reasonably Practicable |
| API | American Petroleum Institute |
| AS | Australian Standard |
| ASM | Abnormal Situation Management |
| BS | British Standard |
| CCPS | Center for Chemical Process Safety (AIChE) |
| CEO | Chief Executive Officer |

| | |
|---|---|
| cm | centimetres |
| CMA | Chemical Manufacturers Association (USA) |
| COMAH | Control of Major Accident Hazards (UK) |
| CSB | Chemical Safety Board (USA) |
| EMS | Environmental Management System |
| EPSC | European Process Safety Centre |
| ERP | Emergency Response Plan |
| EU | European Union |
| FMEA | Failure Mode and Effects Analysis |
| HAZOP | Hazard and Operability Study |
| HMSO | Her Majesty's Stationary Office |
| HSE | Health & Safety Executive (UK) |
| IChemE | The Institution of Chemical Engineers, UK |
| ISO | International Organisation for Standardization |
| ISRS | International Safety Rating System |
| kPag | kilo-Pascals gauge |
| KPI | Key Performance Indicator |
| LAHH | Level Alarm High High |
| LFL | Lower Flammability Limit |
| LPG | Liquefied Petroleum Gas |
| MAPP | Major Accident Prevention Policy |
| MOC | Management of Change |
| MSDS | Material Safety Data Sheet |
| NASA | National Aeronautics and Space Administration |
| NDT | Non-Destructive Testing |
| OH&S | Occupational Health and Safety |
| OSHA | Occupational Safety and Health Administration (USA) |
| P&ID | Piping & Instrumentation Diagram |
| PM | Preventive Maintenance |
| PPE | Personal Protection Equipment |
| psig | pounds per square inch gauge |
| PSM | Process Safety Management |
| PSV | Pressure Safety Valve |
| PTW | Permit To Work |
| QA | Quality Assurance |
| RP | Recommended Practice |
| SCA | Safety Critical Activity |
| SCS | Safety Critical System |
| SIL | Safety Integrity Level |
| SIS | Safety Instrumented System |
| SMS | Safety Management System |
| UKOOA | UK Offshore Operators Association |
| US EPA | United States Environment Protection Agency |

This page is intentionally left blank

# 12 LIFE CYCLE RISK MANAGEMENT TOOLS

*"All our life is but a constant adjustment of our changed and unchanged attitudes to our changed and unchanged circumstances"*

*Samuel Butler*

Risk is present in every aspect of the life cycle of a facility. Therefore it requires us to identify the risks in every phase of the life cycle and develop methods to manage them. While life cycle risk management of sorts has been practised for many years, the adoption of the integrated approach to life cycle risk management is yet to become a standard practice in the industry.

The identification and active management of life cycle issues, is often undertaken too late in the project, when the final design has been approved for construction, or even later, when the facility is being built. This late assessment may find that risk from the operation of the facility falls in the "intolerable" range, when measured against corporate and regulatory requirements. This may necessitate a re-design, major modification and/or implementation of expensive hardware changes which ultimately leads to both schedule and capital expenditure blowouts. There may also be additional operating costs and production interruption costs.

Good risk management demands that potential problems are identified *a priori* in the project, starting right from the concept design/FEED stage.

Sometimes, risk management is seen in the context of an operating facility, with focus on operations and maintenance. While the operations phase is the longest in a facility life cycle, say 25 to 30 years compared to the 3-5 years for design and construction, it is essential that a corporation adopts an integrated risk management strategy over the facility life cycle.

In this chapter, we have provided an integrated model for life cycle risk management in terms of life cycle phase, tasks associated with each phase and the activities involved.

## 12.1 PROCESS SYSTEM LIFE CYCLE COMPONENTS

The standard ISO/IEC 15288: 2002 calls for a risk management process as part of system life cycle management, applied to each stage of the system 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 phases are shown in Figure 12-1.

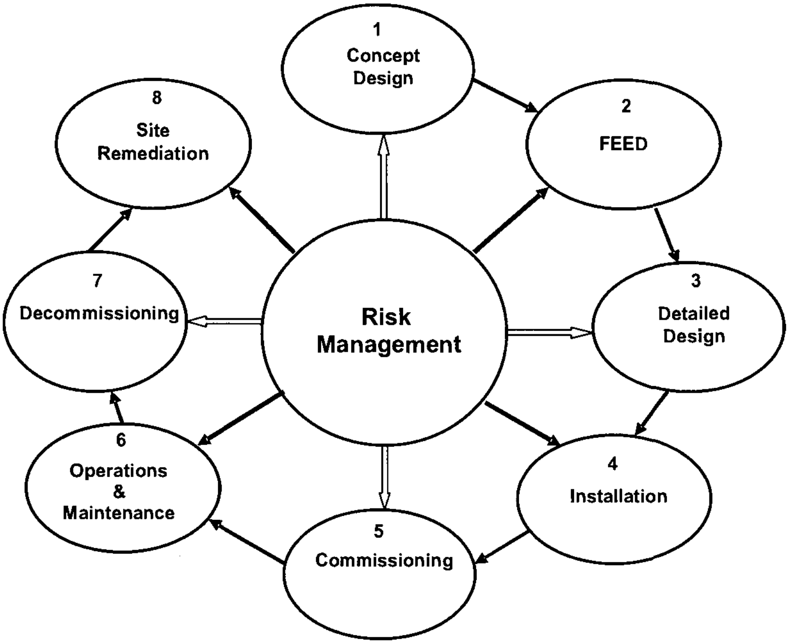


FIGURE 12-1 RISK MANAGEMENT AND FACILITY LIFE CYCLE

If we study the phases carefully, each phase may be executed by a different engineering contractor. Phases 4 and 5 (sometimes 3 to 5) generally go together, following a tendering process. The only phase which the organisation directly manages is Phase 6, and even here, outsourcing of maintenance is on the increase. As the saying goes, all these engineering houses "do the same thing, but do it quite differently". The common thread is the project management team from the client organisation. Even these project teams can be different between front end engineering design (FEED) and engineering, procurement and construction (EPC) phases. Achieving consistency and alignment to corporate practices during the different phases requires special skills and extensive planning.

The life cycle concepts have been extended to integrate three interactive life cycles (Howell et al. 2002):

- Process engineering life cycle covering steps 1 to 4
- Operations life cycle covering steps 5 and 6
- Business life cycle dealing with the corporations strategic and financial decisions

## 12.2 RISK MANAGEMENT STEPS IN THE LIFE CYCLE

### 12.2.1 Parameters Influencing Life Cycle

Once a process technology has been selected, the major parameters influencing the project life cycle are:

1. Inherently safer design (ISD), and other built-in safety and loss prevention features for operational integrity.
2. Life cycle cost. This is often not easy to calculate. It is important to ensure that a "cheap solution" to save some capital at the design stage does not add significant operating costs year after year. This is not uncommon as the objective of the Project Manager is to deliver the facility to operations on schedule and at or below budget, whereas the objective of the Operations Manager is to produce the budgeted end product at the lowest possible cost. Any misalignment in this area should be identified early in the project.
3. Process safety in detailed engineering design. This requires code based loss prevention measures, interfaced with safety analysis of identified hazards using process hazard analysis techniques.
4. Engineering safety in construction and installation phases. This aspect, complementing the occupational health and safety issues in construction, is critical to successful commissioning, without last minute panic-driven modifications. The issue of constructability looms large at this stage, the roots of the problem tracing back to the engineering design.
5. Commissioning. Effectively managing the interfaces between different vendor packages, as well as the interfaces between upstream and downstream plants and shared utilities is of critical importance.
6. Operability and maintainability. Ease of operation, process control, maximise on-line maintenance to reduce downtime, suitable redundancy to improve plant availability, striking a healthy balance between availability and capital/operating costs.
7. Issues relating to cleanup and remediation of site once operations cease. This can be a significant cost under environmental regulations, and prevention of site contamination at design stage needs foresight, as this cost is often seen to be a capital investment with no return, rather than managing the risk of potential future liability.

Each of the above parameters needs to be addressed using different risk management tasks and appropriate tools.

### 12.2.2 Risk Management Model

Each life cycle phase in Figure 12-1 is associated with a number of tasks, and each task, in turn, is associated with a number of activities.

Figure 12-2 shows the risk management model for life cycle risk management of the facility.

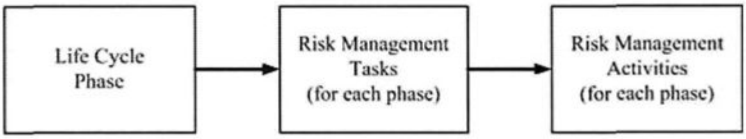

Life Cycle Phase
Risk Management Tasks (for each phase)
Risk Management Activities (for each phase)

FIGURE 12-2 INTEGRATED RISK MANAGEMENT MODEL FOR FACILITY LIFE CYCLE

The tasks associated with each life cycle phase are summarised in Table 12-1. Note that inherently safer design (ISD) is a task present in nearly every phase, and can be applied at any time during the life cycle, even though its influence is greatest at the design stage.

TABLE 12-1 LIFE CYCLE RISK MANAGEMENT TASKS

| Life cycle phase | Risk Management Tasks |
|---|---|
| Concept Design | • Apply inherently safer design (ISD) hierarchy during process synthesis<br>• Define process safety philosophy<br>• High level hazard identification<br>• Define high level performance standards (e.g. system availability, risk targets - corporate, regulatory)<br>• Identify and manage human error |
| Front End Engineering Design (FEED) | • Apply inherently safer design (ISD) hierarchy<br>• Project quality management plan<br>• Refine process safety philosophy where required<br>• Define safety critical systems<br>• Hazard identification<br>• High level process hazard analysis<br>• Integrate safety analysis and loss prevention<br>• Set process safety directions for detailed design<br>• Identify and manage human error |
| Detailed design | • Apply inherently safer design (ISD) hierarchy<br>• Project quality management plan<br>• Develop safety engineering design basis (address interfaces with other engineering disciplines - process, instruments, piping, structural, electrical, mechanical)<br>• Define safety critical systems performance standards |

| Life cycle phase | Risk Management Tasks |
|---|---|
| | • Hazard Identification<br>• Detailed Process Hazard Analysis<br>• Loss prevention design, integrating safety analysis<br>• Assess life cycle costs<br>• Design verification for integrity<br>• System availability analysis to confirm design availability<br>• Management of change procedure developed and implemented<br>• Identify and manage human error<br>• Address constructability issues and interfaces with design<br>• Incorporate de-commissioning issues in design |
| Construction and Installation | • Develop checklist based on construction hazard identification, including mechanical integrity issues<br>• Ensure equipment "fit for purpose" at fabrication stage<br>• Installation quality management<br>• Construction safety management plan and implementation<br>• Development and implementation of relevant SMS elements (e.g. permit to work)<br>• Management of simultaneous operations (existing plant operation/maintenance, drilling (oil and gas industry), construction of new plant/extensions)<br>• Management of interface safety issues<br>• Identify and manage human error |
| Commissioning | • Pre-commissioning safety review<br>• Integrity testing of mechanical equipment<br>• Loop testing of control and safety instrumented systems<br>• Identification of commissioning hazards<br>• Implement prevention/mitigation measures<br>• Identification and management of plant interfaces<br>• Development and implementation of all remaining elements of SMS<br>• Development and implementation of Environmental Management System (EMS)<br>• Identify and manage human error |
| Operations and Maintenance (O&M) | • Abnormal situation management<br>• SMS performance monitoring<br>• Process safety auditing and management feedback<br>• Corrective actions<br>• Mechanical integrity and condition monitoring<br>• Reliability Centred Maintenance (RCM)<br>• Continual improvement<br>• Inherent safety in perspective and identify opportunities throughout plant life<br>• Identify and manage human error |
| Decommissioning /demolition | • Decommissioning safety review<br>• Decontamination of out of service equipment<br>• Identify and manage human error |

| Life cycle phase | Risk Management Tasks |
|---|---|
| Cleanup/ remediation | • Site testing<br>• Environmental remediation plan<br>• Implementation of plan<br>• Identify and manage human error |

It can be noticed that the same tasks appear in a number of activities. The depth to which each task is assessed would vary in the life cycle phase. Identification, assessment and management of human error are common elements underlying all tasks and activities.

Details of the activities associated with the risk management tasks are provided in the following sections.

## 12.3 INHERENTLY SAFER DESIGN

### 12.3.1 Concepts of Inherent Safety

The concept of inherent safety was first raised by Trevor Kletz in 1976, following the Flixborough accident and subsequent commission of inquiry. The concept, like Occam's Razor, is simple and has become proverbial (Kletz 1978, 1996)-

*"What you don't have cannot leak, or burn".*

The concept has been crystallised into a hierarchical system by Kletz (1984, 1985, 1991, 1994, 1996, 1998), CCPS (1996), and described in Section 12.3.2.

The basic philosophy of inherent safety is "build safety into the design" rather than have "add-on" systems. Therefore, inherent safety reduces the severity of the hazard and the likelihood of a hazardous incident simultaneously.

There is a misconception that inherent safety is a discrete activity carried out by specialists or a series of stand-alone safety studies. In other words, the safety engineering discipline is perceived as a stand-alone discipline, independent of other engineering disciplines in a project (process design, instruments and electrical, piping and structural, mechanical). Nothing can be farther from truth. Dalzell and Chesterman (1997) note that inherent safety is a living process where all decisions on "safety in design" are documented and communicated to all other engineering design disciplines and operators. This is essential so that the reasons for each inherent safe decision that establishes the design limits and operating parameters are well understood and not subject to possible revision or impairment in subsequent design reviews. The difference between inherent safety and other aspects of engineering safety is explained by Hendershot (1995).

### 12.3.2 Inherently Safer Design Hierarchy

The hierarchy of ISD consists of a set of keywords as shown in Figure 12-3. In many ways, elimination is a subset of all other principles and therefore has not been discussed separately.

The demarcation between the principles in Figure 12-3 is schematic. In reality, there is a significant overlap. Some inherently safe measures may share more than one principle.

Lutz (1997) has extended the above principles to include the following:

- Avoid knock-on effects - layout spacing, fail safe shutdown, open construction
- Make incorrect assembly impossible - standardise and make unique valve and piping standards
- Making status clear - avoid information overload and complicated equipment
- Tolerance - make equipment robust, processes that go to bad quality rather than an uncontrolled reaction or condition
- Ease of control - less hands-on controls, more controls that take advantage of the phenomena inherent in the system
- Administrative controls/procedures - always plan for administrative controls to be minimised

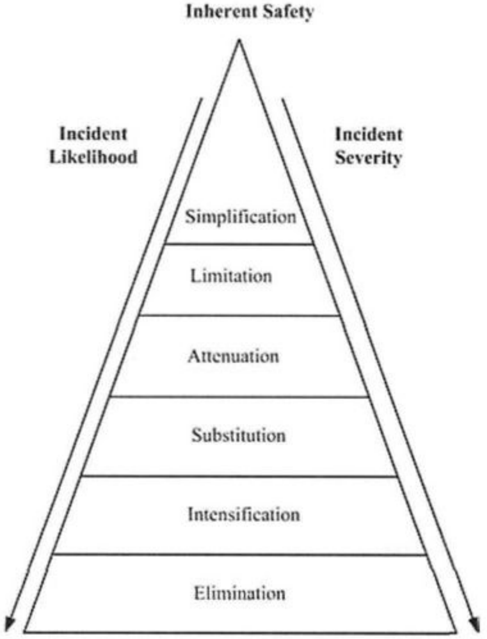


FIGURE 12-3 INHERENT SAFETY PRINCIPLES

Several of the inherent safety principles have found their way into design guidelines such as API RP 14C (2001) for offshore oil and gas facilities. A good checklist for process plants, arranged in terms of unit operations, is provided by Englund (1996). A similar checklist can be found for offshore oil and gas installations in API RP 14J (2001). An overview of the methods for hazard identification and assessment for offshore oil and gas installations is provided by

BS EN ISO 17776 (2002), but this reference is equally applicable to onshore process facilities.

### 12.3.2.1 Intensification

Intensification consists of two aspects:

- reducing the inventories of hazardous materials in process and storage
- reducing the size of the process equipment itself.

The latter has been referred to as process minimisation (Hendershot 2000).

In the past, raw material and intermediates were stored in large quantities to minimise plant downtime. This practice had also contributed to higher risk as well as increase in working capital. It is well established that the large quantity of methyl isocyanate, the intermediate for carbamate pesticides, stored at the plant in Bhopal was a major contributor to the disaster.

Improvements in integrity inspections, reliability centered maintenance practice, and 'just in time' inventory management practices have enabled the process industry to achieve significant reduction in the storage of hazardous materials without losing production. Similarly, changes in process technology have helped to design smaller equipment for the same process duty. Several examples are given by Englund (1990, 1991, 1996), Hendershot (2000). Some guidelines are listed below:

- Question the need for intermediate storage and/or the quantity required to store
- Optimisation of piping system design (Getz 1996), line sizing and piping runs to minimise hold up inventory
- Reduce dust explosion potential by increasing particle size where possible
- Design of bunds or dikes to prevent or minimise accumulation of flammable or toxic materials in a pool and evaporating
- Plate heat exchangers and printed circuit heat exchangers replacing the conventional shell and tube exchangers
- Vapour phase reactors replacing liquid phase reactors
- Higee distillation processes
- Mircro-reaction technology
- Chemical approach (process route)
- Materials selection
- Use of glandless (canned) pumps for toxic liquids

Process intensification should start at the concept design stage, as it may be too late to change inventories once detailed design is complete. The choice of the reaction route, at the concept design stage, is a key decision that influences the inherent safety of the process.

The Dow F&EI and CEI are useful tools for assessing alternative materials and inventories, as part of inherent safety considerations (Hendershot 2000, Khan et al. 2003).

**EXAMPLE 12-1 PROCESS INTENSIFICATION**

There have been several examples of process intensification in the literature.

a) For the case of a chlorine pipe rupture, a reduction in chlorine line size from 50mm to 25mm would reduce the dispersion distance to a concentration of 20 ppm from 5.4 km to 1.9 km (Hendershot 2000).
b) In the manufacture of substituted nitrocarbonamide, one route is to prepare nitrobenzoyl chloride intermediate. However, the latter is known to be unstable, and subject to violent thermal decomposition. An alternative safer route involved the nitration of aromatic acyl halides at a much later stage in the process, after the acid group had been reacted further (Rogers and Hallam 1991).
c) In process/process heat exchange containing reactive chemicals, avoid direct heat exchange between the materials, to prevent contact in the event of a heat exchanger leak, but use indirect cooling through an intermediate, non-hazardous liquid.
d) In blending processes involving combustible hydrocarbons, steam is used to heat the mixing vessel. The system is designed to ensure that the maximum possible steam pressure (and hence temperature) is less than the flash point of vessel contents.
e) In gas processing plants, it may be necessary to conduct emergency depressuring of high pressure gas inventory to the flare. This would result in low temperatures in process piping. In order to prevent to prevent cryogenic embrittlement, low temperature carbon steel is selected in the design.

### 12.3.2.2 Substitution

If intensification is not possible, an alternative is substitution. The principle behind substitution is: Can we use a safer material instead of the initially intended hazardous material and still achieve the process objective?

Some key elements in substitution are:

- The chemical approach (process route, intermediates produced, reagents used, material compatibility, catalysts used, solvents chosen)
- Use of higher flash point materials, compared to flammable materials
- Use of less reactive materials

**EXAMPLE 12-2 SUBSTITUTION**

a) There are two routes to manufacturing substituted acetophenone. One is by oxidation with hydrogen peroxide, with potential for a large exotherm on loss of agitation. The second is by air oxidation using catalyst, and provision to turn off the air which arrests the reaction immediately (Rogers and Hallam 1991).
b) It is common to use a carrier solvent with a higher flash point in the solvent extraction units of mineral processing plants, instead of a flammable solvent used in the past that had caused a number of fires.

c) The gradual phasing out of chlorofluorocarbons as a refrigerant substituted by hydrofluorocarbons over the last decade (still ongoing in many parts of the world) is a significant step in global environmental protection.

While process intensification may be difficult at later stages of a project and in operating plants, the substitution option is available without major changes to plant and equipment and less expensive than one would imagine.

### *12.3.2.3 Attenuation*

Should a hazardous material be used, how can it be used under less hazardous conditions, and how can a loss of containment be prevented?

Examples of attenuation are:

- Operating at lower pressures and temperatures such as storing liquefied gases such as propane or butane, and toxic gases such as chlorine or ammonia as refrigerated liquids at atmospheric pressures rather than at ambient temperatures.
- Storing materials under diluted conditions rather than in concentrated form, if it is the latter form that is used in the process (e.g. acids)
- minimise potential for loss of containment. These include:
  - reduction of leak paths (selection of materials, corrosion allowances, seal less pumps)
  - reduction of leak sources (minimise flanged connections, specify minimum requirements for small bore connections such as nozzle size and monoflanges for instrument connections)
  - reduction of failure from vibration and impact (impact protection, pipe support)
- maximise reliability of equipment (inspection, testing, radiography of welds, quality assurance in design, fabrication and installation)
- selection of process control and monitoring equipment, design to cope with process deviations
- subsea manifolding in the case of offshore oil and gas installations to minimise the number of risers

### *12.3.2.4 Limitation*

Limitation involves minimising the size of an incident. Limitation requires the comprehensive identification of hazards, the consequences of realisation of hazards, and contributors the hazard effects.

Four types of limitations can be designed:

1. Minimise the rate and quantity of hazardous material release
2. Reduce the impact radius of incident
3. Prevent escalation
4. Provide segregation/separation

Severity limitation measures include the following:

- minimise leak rate (spiral wound gaskets and ring joints (RTJ) for higher pressures)
- provide adequate remote process isolation to minimise the size of isolatable inventories
- Reduce evaporation area for spills
- provide adequate separation distances between process units, between plant and control room, and between facility and populated areas - facility layout
- Measures like passive fire protection and mounded storage of large liquefied gas storage vessels can reduce the potential for structural failures and BLEVE.
- Fire proofing of support structures (e.g. pipe bridge support, distillation column skirts)
- Use of fire and blast walls for offshore oil and gas facilities design
- Pressure relief and depressuring

Examples for process plants are provided by Edwards and Lawrence (1993), Englund (1995), Bollinger et al. (1996), and Kletz (1998). For offshore oil and gas facilities, the challenges and examples are provided by and Khan and Amyotte (2002), and Chia et al. (2003). Some examples are listed below.

### EXAMPLE 12-3 EFFECTS LIMITATION

a) In a toxic chemical storage, it was found that the dike size was large and a leak and evaporating pool resulted in large dispersion distances (large surface area). By progressive design, the evaporation area was minimised and a significant reduction in hazard distance was achieved (Ferguson 2004).

b) In offshore facilities design, a risk based approach for structural design against vapour cloud explosions has been routinely adopted in the last 10 years. Using CFD models and the layout geometry for gas explosion modelling, the blast overpressure at an exceedence frequency of $10^{-4}$ per annum is often used as design criteria for equipment support and primary structural steel.

c) The use of risk-based separation distances between hazardous facilities and population centres has been used by regulatory authorities routinely for planning development decision making (HSE 1989, 1990). More details on this subject are given in Chapter 15.

d) In offshore oil and gas platforms, segregation between hazardous inventories and accommodation facilities is achieved by locating the wellheads, process facilities and accommodation on three separate platforms, linked by bridges. Such developments have been popular in shallower waters.

e) In the 1980's and 1990's there was a significant expansion in the port facilities of Sydney harbour, in Port Botany. The developments included large LPG storage terminals and large bulk storage terminals for chemicals. Even during the development in the 1980's it was recognised by planning regulators that unless inherent safety principles were enforced, the facilities may affect the safety of future land development at the port. The result was a set of mounded storage tanks for LPG on two of the facilities (BLEVE protection), and a set of refrigerated LPG storage tanks on another.

f) Since the time of the Flixborough incident in 1974, there has been significant attention paid to the location and protection of controls rooms in process plants. Inherent safety principles include blast protection of control room building, separation distance between control room and plant (where possible), and location of control room upwind of prevailing wind direction.

### 12.3.2.5 Simplification

In the simplification step, we try to reduce the opportunity for error and malfunction. While abnormal situation management is useful, the question is, can we avoid abnormal situations or minimise them, so that there is less potential for operator error?

Some of the principles involved are the following:

- Challenge the need for an equipment or an instrument. If the process can safely operate without it, why do we need it? In this sense, the approach is similar to value engineering.
- Select component with inherently lower failure rates. For example, if a pressure switch has a higher failure rate than a pressure transmitter, as indicated by generic failure rate data, then why not have a transmitter instead of a switch?
- Avoid the tendency that every analogue input to the DCS should have a high and a low alarm. This became the practice in the late 1980's with increasing use of distributed control systems. The danger is that there can be too many alarms, many of them clearly unnecessary, can cause information overload and confuse the operator, and divert attention from the more critical ones.
- In critical process control areas, evaluate the option of redundancy as a failure may lead to an uncontrolled incident.
- A higher level HAZOP at the FEED stage may help in achieving design simplifications.

Remember Occam's Razor - the simplest solution has often been proved to be the best.

**EXAMPLE 12-4 SIMPLIFICATION**

An ammonia plant designed in the late 1970's was being upgraded. A level controller in a knock out pot in the reformer section of the plant maintained a level in the vessel and excess liquid was discharged to an atmospheric open pit on the plant. During the HAZOP study of the upgrades, it was found that if the knock out pot level controller failed and the pot emptied, hydrogen rich gas would be released at the atmospheric pit, where personnel could be working, with serious consequences.

There was some debate in the HAZOP session about providing redundant instrumentation to shut off the gas flow on loss of level, the safety integrity level required, etc. Given the severity of the incident, the approach of reducing the likelihood alone was not considered adequate. It was finally decided to direct the hydrogen to the flare system so that no atmospheric emission, especially at ground level, would occur. Changes to piping would be required, but the approach eliminated the problem by using inherent safety principles.

■ ■ ■

### 12.3.3 Challenges to Inherent Safety

Inherent safety is now widely practised in the process industry, in both design and operation, although many may not formally recognise this. In spite of these efforts, the adoption of inherent safety is not universal. There are several hurdles to overcome, as observed by Khan and Amyotte (2002, 2003), and Gupta and Edwards (2002).

- There is still a lack of awareness of the inherent safety concept among design contractors and corporations. There are exceptions, as observed by French et al. (1996), and Preston and Hawksley (1997).
- Among those who are aware of the concept, there is a lack of understanding of how to apply inherent safety principles in projects. Most designs are code-based, whereas inherent safety is largely innovative and needs lateral thinking.
- Often in the early stage of projects, sufficient time is not allocated to consider inherent safety aspects. This may be considered a corporate failure, as the driver for inherent safety at this stage should be the senior management. Once the FEED phase is completed, and the project proceeds to detailed design stage, there is a high degree of reluctance on the part of the project management to change anything in the design in favour of inherent safety.
- The computer aided process design tools do not effectively account for process safety, especially with respect to cost of inherently safer design, as the quantification of process economics in this area is yet to be well developed (Rushton et al. 1994).
- Development of processes based on alternate process routes for inherent safety requires significant investment on the part of development organisations, which may not see any return for that investment when there is no guarantee of the process being adopted in the market.
- There is a mindset in most people in the industry that traditional systems of control and mitigation are needed, which blocks the switch to inherently safer design. This mindset, as contrasted to inherent safety, is challenged by Dalzell and Chesterman (1997).

The challenge faced by the industry and regulators is how to make inherent safety a part of the routine thinking process - a cultural shift. The drivers are expected to emerge from four sources:

1. Regulatory requirements for approvals requiring a demonstration of how inherent safety has been incorporated into the design as far as has been practicable.
2. Incorporation of inherent safety principles more and more into standards and codes of practice, and providing a common basis for both designers and operators.
3. Increasing demand from developing countries where the process industry is growing rapidly, and whose needs are greater due to high population densities in the vicinity of hazardous facilities.
4. Contributions from research in developing simpler methods for measuring inherent safety through some form of index, thus making it easier to use (Edwards and Lawrence 1993).

The ignorance impediment is now largely dispelled. There has been a significant amount of discussion in the engineering profession on this matter. However conservatism and inability to address ISD issues in the design and management process is still a significant factor. The issue of time pressures on design is always a convenient and comfortable position to adopt but is largely discredited by the significant life cycle benefits that can be gained through upfront ISD applications. Certainly in some cases, prescriptive engineering standards can inhibit some ISD applications but these are quite rare and often regulatory authorities can be flexible in design standard application where the intent of the standard is met and exceeded.

Inherent safety is not limited to the early stages of the design. While intensification becomes more difficult as the design gets finalised, other principles of inherent safety can be applied at any time of the life cycle.

## 12.4 PROCESS SAFETY IMPLEMENTATION AT DESIGN STAGE

### 12.4.1 Defining Safety Philosophy

It is essential that the safety philosophy for a facility design be developed at the FEED stage, and carried through to the detailed design stage. The safety philosophy document is a high level document, which demonstrates how the corporate safety policy is translated into the project requirements. The main items to address include:

- Applicable regulations
- Applicable codes and standards
- Application of inherently safe design principles (all of the elements in the preceding sections)
- Safety goals (identify hazards, eliminate, prevent, mitigate, protect people, environment and property)
- Commitment to HAZOP studies at least at two levels (FEED and detailed design)
- Pressure relief
- Emergency shutdown
- Emergency depressurisation

- Fire and gas detection
- Fire protection
- Explosion protection
- Control and monitoring system
- SMS requirements
- Reliability requirements including redundancy
- High level performance standards for safety critical systems
- Level of operator intervention versus automation

One of the causes of failure in technical systems has been identified by Busby and Chung (2003) as the mismatch between the expectations of the corporation and those of the design contractor. The safety philosophy document must therefore be prepared by the corporation at the tender stage, so that the design contractors have a good understanding of the safety in design requirements.

### 12.4.2 Hazard Identification

A hazard identification (HAZID) must be carried out at all stages of design, the level of detail varying at the concept stage, FEED stage and detailed design stage. At the concept stage, a review of historical incidents in similar processes and similar plants would provide significant input in the following areas:

- process selection
- shaping the safety philosophy
- preliminary project costing

Table 4-12 in Chapter 4 suggests the various HAZID techniques that can be used at the design stage.

### 12.4.3 Safety Performance Standards at Concept Stage

At this stage, it is possible to define safety performance standards only at a high level, but these do influence process synthesis. Some performance standards are:

- Risk to personnel. This includes Individual Specific Individual Risk (ISIR) and Location Specific Individual Risk (LSIR).
- Risk to public outside plant boundary. This is often set by a regulatory authority for land use safety.
- Plant availability (e.g. 96% of the time)
- Environmental risk targets
- Qualitative standards such as prevention of escalation
- Product quality standards where applicable

### 12.4.4 Project Quality Plan

A project quality plan is prepared for the various stages in the project. This plan covers a wide range of activities, of which safety forms only a small part. The plan is normally based on ISO 9001 principles.

### 12.4.5 Process Safety Design Basis

One of the first requirements at the detailed design stage is development of the process safety design basis. The general approach is to identify and eliminate hazards as an integral part of the design process. Where hazards cannot be eliminated, their significance should be evaluated and mitigation measures are to be designed against those hazards considered significant (reducing the severity of the incident, or reducing the likelihood of the incident, or both).

The approach to secure these priorities is the implementation of the following design hierarchy:

a) Hazard identification
b) Hazard prevention
c) Hazard control
d) Incident mitigation
e) Management of controls

Item (e) is normally covered by the Safety Management System. While item (e) is not directly concerned with design, the design activity will generate a set of hazard control and mitigation measures which need to be fed back into the SMS.

The process safety design basis document interfaces with a number of design basis documents of the project such as process, piping, structural, mechanical and instruments. These need to be cross-referenced where appropriate, while ensuring that there is no conflict among these documents. In many instances, the process safety design basis document underlies the other documents, and feeds into them.

### 12.4.6 Inherent Safety Principles in Design

It is useful to prepare a checklist of ISD items that can be reviewed as part of the design. A partial list is given below to provide an understanding for the reader.

- Layout (separation distances, ventilation to aid dispersion, minimise congestion)
- Storage (inventory, venting, inerting, diking design, minimise evaporation from spills)
- Process equipment
- Process piping (minimum pipe size wherever possible, optimise pipe runs, thermal relief for trapped inventory in pipework)
- Rotating equipment (pumps, compressors, fans and blowers, steam and gas turbines, monitoring vibration, temperature, vendor requirements)
- Process materials and conditions (corrosion, hydrogen embrittlement, low temperature embrittlement, mercury embrittlement of aluminium etc.)
- Location of heating, ventilation and air-conditioning (HVAC) air intakes (prevent potential for gas ingress)
- Control room location and inherent safety requirements
- Process control (redundancy, backflow prevention, operability, reliability)
- Pressure relief (PSVs, rupture discs, discharge location)
- Emergency depressuring

- Isolatable inventories and their relative sizes
- Reactive chemicals and special precautions in storage and handling

## 12.4.7 Performance Standards

Performance standards need to be defined for safety critical systems. These can be qualitative or quantitative, and capable being verified for closeout during the design and construction phase. The main safety critical systems are:

### *12.4.7.1 Hazard prevention systems*

- Control systems to maintain critical process parameters to within specified operating limits
- Protection of pipework and vessels from overpressure, including pressure relief, safety instrumented system (SIS) such as High Integrity Pressure Protection System (HIPPS) (Summers 2000)
- Flammable and toxic gas detection
- Fire detection (Senecal et al. 1999)
- Emergency shutdown (ESD)
- Location of automatic isolation valves (inventory segregation)
- Depressuring and blowdown
- Drainage
- Safety Integrity Level (SIL) assessment to ensure adequacy of SIS design
- Monitoring system for rotating equipment
- Manual alarm call points
- Mechanical handling and impact protection
- Integrity of small bore piping (minimum size for nozzles, abrasion, vibration and impact protection)
- Design of isolation of pressure relief devices for testing (Edwards and DeMichael 1999)

For offshore installations, dropped objects protection and structural reserve strength ratios for environmental loads (high wave, tide, wind loads) are important safety critical items.

The performance standards should cover the following parameters:

- Functionality
- Reliability
- Availability
- Survivability

**EXAMPLE 12-5 PERFORMANCE STANDARDS**

Some examples of performance standards are given below to illustrate the concept.

a) *The control and protection system(s) of process facilities shall be designed such that no single failure during operations can lead to unacceptable hazardous conditions* (this requires the DCS and the SIS logic solver to be separate entities).

b) *Two independent instrument systems shall control abnormal operating conditions outside of the design envelope of critical process variables* (e.g. alarm at one level with operator intervention, and possibly an interlock at the next level initiating a process trip, both independent)

c) *The detection of potentially hazardous process conditions and the logic solving to pre-defined levels of process shut-down shall cope with documented criteria of reliability* (this can be either specified or determined in a SIL study)

d) *The SIS shall remain operational during the worst likely hazardous conditions* (i.e. the hardware deployed operates in fail-safe mode, all the logic control panels are located in safe areas and the field equipment is designed to withstand the design accidental loads)

e) *During normal maximum flaring conditions (other than emergency flaring), the maximum thermal radiation levels on open areas where personnel may be present and on locations where structures and equipment are exposed shall be within the limits recommended by API RP 521*

f) *The design of ventilation system for enclosures shall prevent ingress of flammable or toxic gas into the enclosures* (this can be translated into gas detection in ventilation air intake and automatic shutdown of HVAC)

■ ■ ■

### 12.4.7.2 Hazard mitigation systems

The mitigation systems are designed to prevent escalation of an incident until it the emergency event can be brought under control. The design features include:

- Development of fire zones in the facility
- Active fire protection (firewater pumps, ring main, deluge, foam system, other fire fighting equipment)
- Systems to prevent contaminated firewater runoff. This aspect has been highlighted especially since the experience of the Sandoz warehouse fire in Switzerland in 1986, and chemicals contaminated firewater runoff in to the Rhine
- Safe emergency assembly areas
- Design accidental blast load for structures from vapour cloud explosions (equipment support structures as well as control room)
- Structural failure from fire escalation (passive fire protection requirements, where appropriate). Use of PFP is more common in offshore oil and gas structures than in onshore process plants. PFP details are available in the documents by UK HSE (1992a, 1992b, 1998).
- Communication systems (public address, general alarm)
- Emergency power and lighting
- Flare system
- Signage in the plant (prohibition signs, mandatory action signs, warning signs, fire fighting equipment signs, information signs)

For offshore facilities, evacuation equipment in accordance with SOLAS requirements are to be specified (e.g. survival craft, self-inflating life rafts, life jackets, life buoys, rope ladders and knotted ropes, safety equipment on deck.

### *12.4.7.3 Occupational safety and hygiene*

While not directly related to process safety, the performance standards in this area include:

- Equipment and ambient noise levels
- Ergonomic design (control room, access to field instruments for calibration and repair, access to manual valves, ability to handle spectacle blinds etc.)
- Personal protection equipment
- Safety showers and eyewash locations
- Hot and cold surface insulation
- Minimising fugitive emissions
- Atmospheric monitoring at the workplace

## 12.5 PROCESS HAZARD ANALYSIS DURING DESIGN

### 12.5.1 Safety Studies

The studies associated with this item are also referred to as Formal Safety Assessment, or Safety Analysis studies. These are listed in Table 12-2, with cross references to chapters where these are treated in more detail.

TABLE 12-2 SUMMARY OF SAFETY ANALYSIS STUDIES

| Safety Study | Comments |
|---|---|
| Hazard identification (HAZID) | Systematic HAZID and incorporation of hazard prevention and control measures in design (Chapter 4) |
| Hazard Register development | This forms the basis for hazard assessment (Chapter 4) |
| Hazard and Operability Study (HAZOP) | To verify the adequacy of the hazard prevention and control of deviations from design operating conditions, and to ensure operability/maintainability of the facility (Chapter 4) |
| Fire analysis | Includes escalation analysis of structural response to fires (Chapters 6 and 7) |
| Explosion Analysis | Chapter 6 and 7 |
| Toxic gas exposure analysis | Chapters 6 and 7 |
| Essential systems survivability Analysis (ESSA) | Addresses the vulnerability of protection systems under emergency conditions (Chapter 13) |
| Escape, Evacuation and Rescue Analysis (EERA) | Escape routes from the plant to assembly area, integrity of emergency assembly area, alternatives. This study is particularly rigorous in offshore oil and gas facilities. Covered in Chapter 12. |
| Flare radiation study | For estimation of flare height and separation distance, to protect personnel at ground level, for normal operating conditions and emergency flaring conditions. |
| CFD study for blast analysis | To determine the design accidental load for structures - undertaken mainly for offshore oil and gas facilities |
| Dropped objects analysis | Detailed analysis for offshore oil and gas installations, as lifting is carried out routinely throughout the |

| Safety Study | Comments |
|---|---|
| | lifetime of the facility. For onshore facilities, the review covers procedures for crane operations, carried out under a permit to work. A specific job safety analysis is carried out for heavy lifts. |
| Gas turbine exhaust plume dispersion study | Mainly for offshore oil and gas installations - turbine exhaust plume impact on activities on board (e.g. ability of crane operator to access/egress from the crane, without being affected by hot gases, helicopter operations) |
| Collisions of supply vessels with structures | Carried out for offshore oil and gas facilities. Can be qualitative or quantitative. |

### 12.5.2 Plant and Equipment Integrity

Technical integrity is defined as follows (Bale and Edwards 2000):

> *Technical integrity is concerned with the development of the design such that it is carried out by well trained personnel, who have been assessed to be competent, in accordance with recognised, sound practices and procedures and such that there is adequate provision by way of reviews and audits, to ensure the design intent is unimpaired in any way that could cause undue risk or harm to people or damage to the environment.*

The main issues to address in this area are:

- Material selection for chemical compatibility
- Corrosion considerations (all types of corrosion - galvanic, stress corrosion, embrittlement etc.)
- Corrosion allowances in design
- Provision of corrosion coupons for inspection and monitoring
- Low point drains
- Inspection provisions for corrosion underneath insulation
- Protection against overpressure (PSVs, rupture discs, SIS for pressure protection)
- Access provision for external and internal inspections
- Safety equipment selection (the equipment itself should not be damaged by the process incident). An example for pipeline shutdown valves is discussed by Mahgerefteh et al. (1998)
- Competence and training of design personnel

### 12.5.3 Loss Prevention Systems Design

Using the data generated from the safety studies, a layer of protection model can be developed, specifying the protection layers necessary. The loss prevention systems can then be designed using applicable codes and standards. There is a significant amount of literature in this area, chief among them being Lees (2001).

The main parameters in the design are:

#### 12.5.3.1 Hazardous area classification

In systems storing or handling flammable gases and liquids, specified areas around potential release sources of these substances are classified as hazardous areas, and all electrical and electronic equipment within the classified areas are specially designed to ensure that they would not pose an ignition source.

There have been different ways of classifying hazardous areas, each country using its own national standard, albeit with much commonality. Since the publication of the standard IEC 60079-10 (2002), it has become the international standard for classification of hazardous areas. The petroleum industry continues to adopt the oil industry codes such as Institute of Petroleum IP15 (2002) or API 500 (1997).

The main considerations are:

- Selection of electrical equipment and electronic field instruments consistent with the hazard zone.
- Elimination of hot surfaces in hazardous areas. If it is not possible to eliminate hot surfaces, then the pipework should be insulated to ensure that the surface temperature is well below the auto-ignition temperature of the flammable material. Maintaining the integrity of the insulation comes under the SMS.

#### 12.5.3.2 Gas detection

Gas detection covers both flammable gas detection and toxic gas detection. The latter is substance-specific. The main considerations in selection and location of gas detectors are:

- type of detectors for the application (point head, line of sight, laser-based)
- prevailing wind direction
- specific release sources (e.g. pump seals, valve glands etc.)
- distances to specified threshold concentrations based on dispersion analysis
- avoiding spurious alarms and trips
- ability to detect gas in the plant environment
- properties of the gas (density relative to air)

#### 12.5.3.3 Control of static electricity

Even with careful control of all possible ignition sources, static electricity has remained a major cause of ignition in process plants. Therefore, it is necessary to identify all possible sources of static electricity, so that design measures may be implemented to eliminate or control them.

A review of all causes of electrostatic hazards is provided by Pavey (2004). In summary, electrostatic hazard arise from:

- Generation of charge due to relative movement between materials, at least one of which is not a good conductor
- Generated charge can accumulate in one or more of the materials involved

- Even if the conducting material is connected to earth, the second material can continue be charged
- Once electrostatic charge has accumulated, it is not possible to control its discharge, which becomes a source of ignition, if the energy dissipated is higher than the minimum ignition energy of the flammable material.

Therefore the objective is to prevent accumulation of charges as far as possible. Some methods suggested by Pavey (2004) include the following:

- Alter the charging materials to the process equipment where possible (inherent safety)
- Restrict velocity of low conductivity single phase liquids to 7 m/s and multi-phase liquids to less than 1m/s.
- Inert gas blanketing of flammable atmosphere in vessels
- Grounding of all equipment storing and handling flammable materials, including flammable/combustible dusts
- Glass lined vessels or insulated vessels handling flammable liquids to be earthed through the lining near the bottom of the vessel
- Ensuring that the earthing lead has the appropriate electrical resistance and required mechanical strength against physical damage
- Grounding of mobile and hand-held tools at point of use, preferably through the person using them
- Provide earthed dissipative or conductive surface for personnel to stand on, while working
- Avoid spray filling or splash filling of vessels with flammable liquids
- Avoid using type D flexible intermediate bulk container (FBIC) in flammable atmospheres (Statham 1999)

A number of other measures may be found in Britton (1999), NFPA 77 (2000), and British Standard (PD CLC/TR 50504 - 2003).

Sometimes deluge water applied to disperse a gas cloud as part of explosion suppression can generate static electricity in the droplets. Remedial measures are suggested in the offshore technology report by HSE (1995).

#### *12.5.3.4 Fire protection*

The requirements of fire detection are developed in the fire analysis. This information is fed back into the design of fire protection system. Some of the main aspects to consider are:

- Location of fire detectors
- Definition of fire zones
- Firewater requirements and pump sizing
- Hydraulic design of firewater distribution network using relevant software
- Firefighting foam systems
- Fire protection of enclosures such as equipment rooms, machinery rooms, gas turbine enclosures (gaseous fire suppressants, high pressure water spray mist, manually applied fire extinguishing media)

- Control room fire protection
- Passive fire protection to prevent escalation
- Smoke ventilation
- Water curtains
- Snuffing steam

#### *12.5.3.5 Explosion protection*

Structural failures from vapour cloud explosion are prevented by building adequate structural strength into equipment support and primary structures. This is part of inherently safer design. However should an initial explosion occur, mitigation of the consequences is difficult. Generally a VCE is associated with a subsequent fire and hence fire protection measures would assist, provided the fire protection system itself is not damaged in the explosion (Piper Alpha disaster is a classic example - see Chapter 9).

For potential open air explosions, the best means of risk management is still reduction in congestion in layout design, better ventilation, gas detection and inventory isolation, and prevention of ignition. Investigations have been carried out on water spray induced dispersion of gas clouds, but the results have been inconclusive.

For flammable mixtures in confined areas, protection against explosion can be provided through the following means:

- Inerting
- Complete elimination of ignition sources (not practical or possible)
- Fast-acting flame suppressors (Gardner 1994)
- Deflagration venting through vent panels or rupture discs
- Total containment (expensive, and may be warranted only if highly toxic substances are involved)
- Passive deflagration suppression with expanded metal products (Fauske 2001).

### 12.5.4 Design Verification for Integrity

In many countries, regulation requires verification of the design of safety critical items in offshore oil and gas installations. The intention is to have safety critical elements verified as suitable by an independent and competent person. Such verification is like a regulatory check, but without the regulator. The efficacy of such verification and the associated costs are still debated.

The safety critical systems design verification procedure has not been extended to onshore process facilities by regulation, but has remained a recommended practice. However, the duty implicitly lies on the part of the facility operator to ensure the integrity of the design, apart from contractual liability clauses, passed down the chain of subcontractors.

### 12.5.5 System Availability Analysis

The performance standard of design on-line time can be achieved only if the plant and equipment are of high reliability and the maintenance measures are effective. System availability is a measure of both reliability and maintainability and is defined as

$$\text{Availability (A)} = \text{Up time} / (\text{Up time} + \text{Down time}) \qquad (12.1)$$

alternatively,

$$\text{Average A} = \text{MTBF}/(\text{MTBF} + \text{MTTR}) \qquad (12.2)$$

where

MTBF = mean time between failures (reciprocal of failure rate) and
MTTR = mean time to repair, including lead time for delivery of spares, if not held in stock.

It takes considerable effort to calculate the overall plant availability, as the availability model for the plant has to be developed, and individual equipment/unit availability has to be calculated. Therefore, it is not common that an availability analysis is undertaken for all process plants. However, where a high on-line availability is required, such as in offshore oil and gas installations, and ethylene or ammonia plants, many corporations undertake such an analysis to identify contributors for non-availability, so that the design can accommodate the necessary requirements to maintain plant performance. An availability analysis can be undertaken at any time during the life cycle, either at the design phase, or during the operating life of the plant, especially as part of plant extensions (Khan and Kabir 1995).

One way to improve availability is to reduce the mean time to repair. It is a measure of maintainability, as opposed to reliability, which is a probability. Maintainability issues are discussed in a review by Whetton (1993).

The literature on availability analysis in the process industry is scattered. A comprehensive overview is provided by Lees (2001) and O'Connor (1991). Where operations data is available, it is best to fit probability distributions for failure time and repair times. As described in Chapter 8, the Gamma distribution and the 2-parameter Weibull distribution are popular for failure time and repair time distributions.

A number of software models have been developed (e.g. MAROS), using Monte Carlo simulation of failure time and repair time probability distributions.

The main advantages of the study are that it helps to:

- identify redundancy requirements at design stage
- develop maintenance strategy (inspection intervals, preventive maintenance)

- evaluate alternative process concepts at a high level during process synthesis. Very often, the focus at this stage is operability rather than maintainability.
- develop spare parts strategy
- optimise intermediate storage inventory requirements, balancing between availability and inherent safety (intensification)

**EXAMPLE 12-6 AVAILABILITY ANALYSIS CASE STUDY**

An offshore gas facility was designed to produce gas from subsea wells, manifolded and brought to shore by a trunk pipeline, and a gas processing plant onshore. The company had contracted to provide the demanded amount of gas by the user at 98% availability, excluding line pack which may give about 0.5% availability. The design had already incorporated a number of redundancy measures to meet the availability. An availability analysis was undertaken of the design, from subsea wellhead to the sales gas compressors, to verify that the design could provide the contracted availability. The main findings were:

- There was too much redundancy in some areas which could be rationalised. This could result in capital cost saving.
- A spare umbilical (flexible pipe encasing a number of utilities, hydraulic oil, instrument cables, chemical injection lines etc.) from offshore control module to subsea wellheads was necessary, or alternatively, some of the utility lines can be duplicated within the umbilical.
- One of the significant contributors to non-availability was the mobilisation time for a subsea remote operated vehicle (ROV) for maintenance interventions on subsea wellheads. Attention was focused on reducing this time where possible, as well as re-evaluating the subsea wellhead design to maximise MTBF.
- An additional gas well planned for drilling a few years later may have to be brought forward to meet the availability.

The study provided a number of management options to ensure that the overall availability would be achieved. True to the common adage, the last 3% was more difficult to achieve than the first 95%.

### 12.5.6 Life Cycle Costs

The relationship between life cycle costs and life cycle phases is shown in Figure 12-4 (Post et al. 2002). The figure shows how quickly the life cycle costs are determined from concept planning through detailed design phases. Therefore, it is imperative that inherently safe design decisions are made early in the project. Edwards and Lawrence (1993) have shown that inherently safer plants are cost effective in terms of both capital and production costs.

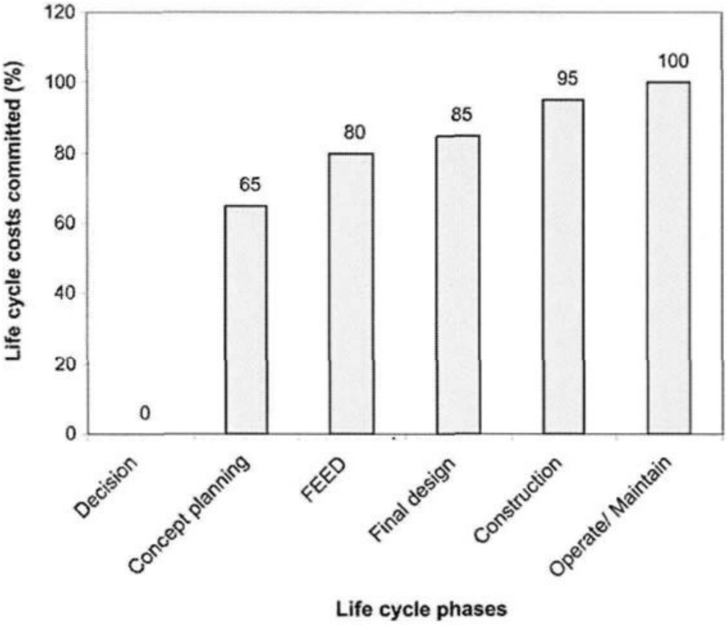


FIGURE 12-4 LIFE CYCLE COST COMMITMENT DURING LIFE CYCLE PHASES

## 12.6 CONSTRUCTION AND INSTALLATION

In a greenfield site, construction risk management essentially covers two aspects:

- Injury prevention to construction workers using traditional OH&S management practices
- Quality assurance of installation. This is critical for process safety. Some of the questions to review are:
  - Is the correct equipment installed in the correct location?
  - Are all the intrinsically safe barriers installed for all field terminations?
  - Are last minute modifications required to support the construction effort? How is this managed? These may mainly consist of piping route modifications.
  - Have lifting safety studies been conducted for heavy lifts of process equipment?
  - Is torque measurement of flange connection required to prevent overstressing, and how is this carried out?

- Is the approved lubricant used for piping connections? Lubricants may react with chemicals which may be discovered only during commissioning or even in the operational phase.
- Do all the equipment, especially minor equipment such as valves, meet the design specification?
- How do we manage human error as these activities are full of man-machine interactions?

A detailed checklist needs to be prepared based on a systematic hazard identification technique. Existing checklists may have to be built on, and facility specific.

### EXAMPLE 12-7 INSTALLATION ERRORS CAUSE SIGNIFICANT DELAYS

a) In a newly built ethylene plant, special low temperature duty materials are required in the cryogenic separation train. The piping was confirmed to meet the specifications, but the manual valves were not checked. During commissioning, all the manual valves in cryogenic services started leaking badly. Luckily ignition did not occur. The problem was traced back to a lapse in quality assurance. There was a month's delay in commissioning, as all the valves had to be replaced (lead time for delivery) and the system had to be fully pressure tested.

b) In a vinyl chloride monomer plant, a distillation column was replaced with a new larger column as part of planned plant capacity increase. The sieve trays in the new column had different hole sizes at different sections, for separation efficiency. No one checked during the installation that the correct trays had been fitted at the correct locations. The construction contractor was in no position to distinguish between the trays. When the plant was commissioned, the product was constantly out of specification. The buffer storage for rework inventory was full. The plant was shut down, flushed, purged and re-entered, when the fault was discovered. The entire column had to be re-trayed, causing significant loss of production.

■ ■ ■

Such examples abound in the industry and every experienced engineer has a wealth of tales to share. The question is: Have we learnt from past experience?

When it comes to brownfield developments (extension to existing operations, new plant adjacent to existing facility), the problems compound. In addition to the questions listed above for greenfield developments, additional issues to review are:

- What are the impacts of new construction and installation on existing operations, in terms of potential for loss of containment?
- What are the impacts of a process emergency in the existing plant on the construction activity?
- How are the interfaces managed (tie-in of new extension with existing facility, sharing of utilities such as steam, power, cooling water, instrument air etc. by the existing plant and new extensions)?

- Process isolations between the two sets of plants (spectacle blinds in correct positions, and if a slip plate is used, is its pressure rating consistent with the flange rating?)

The construction safety study guidelines for hazardous industries, issued by the New South Wales Government, Australia (1992) has a checklist that can be used in this regard. This checklist is not exhaustive, but can be used as a basis for further development that is facility specific.

## 12.7 COMMISSIONING

Any one who has walked through a process plant being commissioned would immediately notice the frenzy of activities that is hard to describe, and can only be experienced. The pressure to get the plant started is immense, once construction is completed. Those who have side-stepped some of the risk management measures in the preceding steps of the life cycle, or implemented them poorly, would find to their dismay that they have been amassing many potential problems for the commissioning stage.

Few really appreciate the fact that the commissioning phase is perhaps the most hazardous of the life cycle phases, as there are four activities occurring simultaneously:

- Commissioning of completed sections of plant
- Pre-commissioning of constructed sections of plant
- Completion of residual construction activities
- Existing plant operation (in the brownfield situation)

To compound this, there are a number of parties involved, each vendor of a package unit engaged in that unit's commissioning, and there are interfaces involved between packages.

### 12.7.1 Pre-Startup Safety Reviews

The OSHA PSM rule (1992) calls for a pre-startup safety review, but the Seveso II Directive does not explicitly mention this. The main aspects of pre-startup safety review are to ensure that:

- Construction has been undertaken according to design specifications (part of this is covered in the construction/installation risk management)
- Operating and maintenance procedures have been developed
- SMS in full has been implemented
- All actions arising out of HAZOP and other process hazard analysis studies have been implemented and closed out
- All changes subsequent to the final HAZOP have been subject to management of change procedure
- All safety critical systems are in place in the plant
- All safety instrumented systems are correctly configured in the programmable electronic system

- All personnel involved in operations and maintenance have been fully trained in the relevant procedures
- Any exemptions (design, statutory) have been adequately addressed and documented
- Isolations still required from other parts of the plant are in place, and those isolations to be removed for plant commissioning have been removed. This step is critical as personnel still completing construction could be inadvertently exposed to process material.
- A verification checklist has been prepared, and signed off by authorised personnel, giving approval for startup.
- Actions arising from the pre-startup review have been carried out and closed out.

### 12.7.2 Commissioning Safety Study

A commissioning safety study needs to be undertaken for the facility. This study takes the form an interactive workshop, aided by an experienced facilitator. The participants of the workshop are:

- Project contractor
- Project personnel
- Operations personnel
- Package equipment vendor representative (as needed)
- Operations management personnel from interfacing plants (adjacent process plants, utilities)

The workshop considers each step in the commissioning sequence in turn, and examines 'what if' scenarios. An initial brainstorming would be required to identify all the safety and operability issues. Some of the main issues are:

- Is the commissioning sequence correct?
- What actions to take if a vendor package has problems during commissioning? How does it affect other parts of the plant?
- If an adjacent plant supplies an intermediate to the facility being commissioned, how does a plant trip during commissioning affect the host plant? This is a major problem if the raw material supplied is gaseous, and there is no provision for buffer storage.
- Conversely, if the host plant trips, how does it affect the commissioning of the facility in question?
- If commissioning has to be abandoned due to loss of containment or other engineering problems, how does one recover from the situation, and restart the plant?
- What communication protocol is required among the various groups in the commissioning team, and is everyone aware of it?
- Given that a large number of people would be in the plant during commissioning, how are process emergencies handled?

**EXAMPLE 12-8 IF A COMMISSIONING SAFETY STUDY HAD NOT BEEN DONE ...**

A sulphuric acid plant was built by a company, adjacent to a copper smelter (operated by a different company) in a remote location. The raw material for the plant consisted of two sources:

- sulphur dioxide generated from a copper smelter (until that time the smelter gas was emitted to atmosphere through a very tall stack)
- burning of sulphur to supplement the smelter gas

A commissioning safety review was undertaken for the project, when the construction had been substantially complete. The acid plant contractor had not recognised the need for the study, having had extensive experience in this area.

During the review, the question was raised: What would the smelter operations do if the acid plant were to trip? Do they have provision for redirecting it to the stack automatically? No one could answer the questions. The question was deferred until the smelter operations personnel could be present in the workshop. It turned out that automatic redirection to stack had not been provided (an interface issue), and that in the event of an acid plant trip, smelter gases would be released at the work area where personnel are present, with potential for multiple fatalities.

The commissioning had to be deferred until this issue was resolved. It was also identified that the instrumentation to redirect the gas to the stack should be allocated a SIL value, and designed to that performance standard. Communication of information between the two plant control rooms were identified and established.

The whole issue arose at the commissioning study stage because this interface issue was not addressed in the HAZOP, due to a major error of omission. It was a case of better late than never.

## 12.8 OPERATION AND MAINTENANCE

### 12.8.1 Managing Operational Hazards

Operational hazards are normally identified and catered for through the process hazard analysis procedure, including layer of protection analysis. This aspect has been discussed earlier.

Managing risks during day-to-day plant operation essentially consists of recognising and managing abnormal situations, arising from process deviations. If left uncontrolled, the abnormal situation may lead to a process incident (overpressuring, runaway reaction, loss of containment etc.), through an escalating sequence.

The HAZOP procedure is routinely followed during the design phase, in which potential process deviations are identified, and remedial measures are incorporated, be it an alarm requiring operator intervention, or in the extreme, an interlock to trip the process. The main focus of HAZOP is on the design of protective measures to cope with process deviations.

What is not often carried out in a HAZOP is the identification of failure modes that initially cause the deviation. The causes are sometimes clustered into 'control loop failure'.

Once the plant is commissioned and handed over by the EPC contractor to plant operations, the control room operator is left with the task of identifying the causes of a process alarm, so that appropriate response can be initiated. In the absence of a documented FMEA specific to the process deviation in question, and operator awareness training on this, the operator may not be able to cope with the abnormal situation. Interviews with operators in operating facilities have provided mixed results, with experienced operators confident of their abilities and inexperienced operators feeling threatened. Even if a process trip occurs as a result of the deviation exceeding the safety envelope, without the knowledge of possible causes of the trip, re-starting the plant may not solve the abnormal situation. Should an incident occur, the subsequent investigation often attributes the incident to equipment failure and human error.

The area of abnormal situation management (ASM) has not been as well developed as some other areas of process safety, and is closely linked to human error management. One tool for management of abnormal situation is from information collected in an FMEA study and expected operator response that can be programmed into the DCS as an expert system diagnostic tool, and linked to the respective process alarm.

### 12.8.2 Managing Maintenance Safety

There are two major areas of maintenance management that relate to process safety:

1. Process isolation design for maintenance safety
2. Safe work procedures for maintenance

#### *12.8.2.1 Process isolation in design*

During the detailed design phase, the isolation philosophy should be clearly defined (single block valve, two block valves in series, double block and bleed arrangement, provision for positive isolation by providing spades or spectacle blind). The level of isolation can be a risk based decision, depending on line size, operating temperature and pressure, hazardous properties of material, and quantity of isolated inventory that may be released should a leak occur.

#### *12.8.2.2 Safe work procedures*

Safe work procedures are managed by the permit to work and isolation procedures in the SMS. Details are given in Chapter 11 and are not repeated here.

### 12.8.3 Mechanical Integrity

One of the critical aspects of managing risk is the assurance of integrity of an installation. This is a preventative measure, whereby accidents and unplanned down-time are avoided. This overlaps with the SMS to some degree in that a system should be 'fit for purpose' in order to be safe, and in order to operate efficiently. The OSHA rule (29 CFR 1910.119) specifically requires a program of mechanical integrity to be undertaken. Details of development and implementation of a program are described by Herrington (1996).

A brief outline of the tools available for managing and maintaining system integrity is given below.

### *12.8.3.1 System integrity inspections and monitoring*

The inspections and monitoring take many forms. Principal among them are:

**External Inspections:** Consist of mainly a visual inspection of the equipment for visible signs of degradation, corrosion, misalignment etc. This is not sufficient in itself and must be supplemented by other methods.

**Internal Inspections:** Apply to vessels and large size equipment. If the vessels were registered pressure vessels, then a statutory internal inspection would be required at specified intervals. For atmospheric vessels, such inspections are normally required by legislation if the product stored is a hazardous substance. The internal inspection may reveal faults not identifiable in the external inspection. For areas not readily accessible, inspection techniques use cameras and other inspection aids.

**Non-Destructive Testing (NDT):** Tests cover an array of methods including radiography of welds, magnetic particle testing for welds, ultrasonic thickness testing for corrosion/erosion, thermal imaging of refractory lined equipment etc. It is essential to maintain good documentation for all these tests, so that subsequent tests can be compared for progressive deterioration.

**Vibration/Bearing temperature Monitoring:** Applies to heavy rotating machinery. Any abnormal condition can be directly detected and alarmed for immediate attention.

**Corrosion Monitoring:** In systems where there is a potential for external corrosion (e.g. buried pipes and vessels), cathodic protection is provided by sacrificial anode, or impressed current. Monitoring these parameters is critical to the integrity of the system. In the case of buried long distance pipelines, 'intelligent pigging' is used to glean information on the pipeline status. A pig is a device used to clear blockages in a pipeline. The intelligent pig has built-in monitoring equipment for measuring pipeline thickness along its length.

The integrity management is complemented by a spare parts management philosophy whereby critical spares are carried to minimise down-time, and spares sourcing is planned to reduce lead-time.

### 12.8.3.2 Risk based inspection

In large installations, there are numerous mechanical components including many kilometres of piping. It is not possible to inspect all of them at the same fixed schedule. Therefore a risk-based inspection (RBI) regime is practised by many corporations. Plant equipment and components are given a risk rating based on a failure modes and effects criticality analysis and risk matrix. The inspection regime is based on the risk category (ASME 1991). Examples of risk based inspection and maintenance can be found for the petroleum industry in API (1995) and for cross-country pipelines in Dey (2001). Most risk based methods are qualitative.

RBI uses predictive trend analysis as a critical tool in system integrity management. All the information gathered from monitoring of operations and maintenance parameters are analysed using statistical distributions or time series analysis to predict future trends and time for failures. From the results, the preventative maintenance strategy is improved and failures at their incipient stages are attended to before a catastrophic failure occurs. An example as applied to erosion-corrosion risk in a piping system is discussed by Vinod et al. (2003).

### 12.8.3.3 Reliability Centred Maintenance

Reliability Centred Maintenance (RCM) is a powerful method of maintenance planning developed within the aviation industry and later adapted to several other industries including defence.

RCM is defined as (Rausand 1998) 'a systematic consideration of system functions, the way functions can fail, and a priority based consideration of safety and economics that identifies applicable and effective preventative maintenance (PM) tasks'. The main focus of RCM is therefore on the system functions and not on the system hardware.

A number of reports and textbooks on this subject are referenced by Rausand (1998), who describes 12 steps in a RCM analysis, listed in Table 12-3.

TABLE 12-3 STEPS IN RCM ANALYSIS

| Step | Description |
|---|---|
| 1 | Study preparation |
| 2 | System solutions definition |
| 3 | Functional failure analysis |
| 4 | Critical item selection |
| 5 | Date collections analysis |
| 6 | FMECA (See Chapter 4) |
| 7 | Selection of maintenance actions |
| 8 | Determination of maintenance intervals |
| 9 | Preventative maintenance comparison analysis |
| 10 | Treatment of non-critical items |
| 11 | Implementation |
| 12 | In-service data collection and updating |

The RCM analysis, according to Rausand (1998) basically provides answers to the following seven questions:

1. What are the functions and associated performance standards of the equipment in its present operating context?
2. In what ways does it fail to fulfil its functions?
3. What is the cause of each functional failure?
4. What happens when each failure occurs?
5. In what way does each failure matter?
6. What can be done to prevent such a failure?
7. What should be done if a suitable preventative task cannot be found?

The RCM task is too complex and large to be handled manually, and a good user-friendly software package is required to carry out the RCM analysis. Many corporations have developed in-house software to manage RCM.

RCM is focused on system function and not on hardware components, and tends to use in-house data and experience as much as possible, or if a wider database is used, data on similar equipment operating under similar environmental conditions are selected.

Khan and Haddara (2003) have proposed a new approach based on risk, referred to as risk based maintenance (RBM). A QRA is conducted on each unit of the system and where the risk of failure exceeds an acceptable criteria, the risk contributors are evaluated with a view to developing an improved maintenance strategy. The major difficulty in this approach is that in the use of generic failure data in the QRA, individual contributions of various failure modes to subsystem failure are rarely available. Further, not all failures are maintenance related. Unlike RBI, where predictive trend analysis is used to define inspection intervals before a major failure can occur, RBM has all the uncertainties associated with a risk assessment, as discussed in Chapter 10. In order to minimise such uncertainty, fuzzy logic systems for condition monitoring have been suggested (Harris 2002). A risk-matrix based risk assessment is still useful in prioritising maintenance activities, within the constraints of time and budget (Harnly 1998).

A major challenge confronting the industry is that the data collection on reliability is not effectively interfaced with critical maintenance, production and condition monitoring systems. An integrated strategy has been advocated by Beck (2003).

Huston (2002) has correlated the levels of efficiency with reliability and maintenance strategy for rotating equipment, which summarises the above concepts (see Table 12-4).

**TABLE 12-4 MAINTENANCE STRATEGY AND PROCESS EFFICIENCY (SOURCE: HUSTON 2002)**

| Strategy | Description | Efficiency |
|---|---|---|
| Reactive/corrective | Fix-it-if-it-breaks approach. Unplanned shutdowns occur | < 40% |
| Preventive maintenance | Planned shutdowns for equipment overhaul. Maintenance efforts not based on assessment or equipment condition | 40-60% |
| Predictive maintenance | Condition monitoring, planned shutdown schedules based on problem identification. Reduction in unplanned shutdowns | 60-80% |
| Proactive reliability | Identify root causes of equipment and process problems and take remedial measures. Increase in | > 80% |

| | | |
|---|---|---|
| maintenance | MTBF with virtually no unplanned shutdowns | |
| Operator-driven reliability | Front-line operators are allowed to 'own' the system. They identify, describe and assess problems and communicate information to plantwide team to keep equipment running. | > 90% |

### 12.8.4 Integrity of Safety Instrumented Systems

The integrity of safety instrumented systems (SIS) is achieved through the allocation of Safety Integrity Level (SIL) and verification of the instrument design that it meets the allocated SIL.

SIL allocation is based on IEC 61508 (1998) and BS IEC 61511.3-2003 (process systems), and described in Chapter 9. Additional information may be found in Dowell and Green (1998), Cohen (1999), Marszal and Scharpf (2002), and McDonald (2004).

## 12.9 DECOMMISSIONING AND SITE REMEDIATION

When a new facility is being designed, there is so much activity among the project and operations team that one tends to forget that the facility has a finite life at the end of which it has to be decommissioned and demolished, and this needs planning.

Decommissioning may be defined as the shutdown of a facility or part of a facility, to prepare for its complete demolition. The impacts of decommissioning operations are wide ranging (Hicks et al. 2000), and summarised in Table 12-5.

TABLE 12-5 IMPACTS OF PLANT DECOMMISSIONING

| No. | Impact Category | Description |
|---|---|---|
| 1 | Resource use | Energy requirements for decommissioning |
| 2 | Rehabilitation | Clean up of contaminated soil, surface water and groundwater, that may have occurred during the operational life |
| 3 | Residues | New solid and liquid wastes generated and their disposal and impact on environment. This includes marine environment in the case of offshore facilities |
| 4 | Hazards of decommissioning | Decontamination of equipment containing hazardous substances (draining, venting, purging, mechanical handling) |
| 5 | Social | Impact on local community, employment |
| 6 | Regulatory | Environmental regulations and their impact on decommissioning operations (approvals) |

The risk management tools described above can be used to address the end of life of process facilities, but this has not been widespread industry practice.

Hicks et al. (2000) have demonstrated the need for the integration of plant decommissioning issues with facility design - design the grave when you design the cradle. The objective is to reduce the life cycle costs as it has been shown that

4% to 8% of the project capital costs are required for decommissioning, and this needs to be taken into account in the process economics.

Examples of end of life considerations in design are:

- Prevention of soil contamination by appropriate floor surfacing of storage and plant areas
- Prevention of leakage from underground tanks by adequate surface protection, cathodic protection and monitoring systems
- Prevention of contaminated firewater runoff to surface water or groundwater
- Waste treatment and disposal strategy
- Policy of no onsite waste storage, rather than hoping for an environmentally acceptable disposal method to be developed in the future
- Trends in the regulatory environment, and potential changes in the regulations that may affect decommissioning

Systematic identification of the contributors to adverse impacts of plant decommissioning, greatly assists in the preparation of a robust decommissioning plan, and estimation of costs.

Major effort is necessary to decommission a plant if the operation involves hazardous materials. A detailed decommissioning plan needs to be prepared. Key considerations are (Phillips, 2002):

- Ensure there is adequate documentation on:
  - plant equipment
  - piping & instrumentation diagrams
  - underground storage tank and buried pipelines and power cables. If this information is not available, then it should be collected upfront.
- Identify inventories that need to be drained or blown down from equipment and piping, their hazardous properties, destination of drain and disposal methods
- Identify regulatory requirements and environmental approvals necessary for decommissioning, especially storage tanks above ground and underground.
- Define scope of work. What equipment will be decommissioned and mothballed, and what equipment will be demolished
- Identify interfaces with operating parts of the plant if partial decommissioning is required
- Identify procedures of work required to be in place and ensure that demolition contractors are trained. These include permit to work, lockout-tagout procedures and confined space entry procedures
- In older plants, asbestos may be present and this presents special safety, health and environmental problems.
- Ensure all activities are documented and signed off

A strong distinction must be made between equipment that has been drained, disconnected and in disuse (out of service), but not decontaminated. That equipment is not yet decommissioned, and should be assumed to contain hazardous material vapour inventory. Description of an accident occurring as a result of not decontaminating an out of service storage vessel is given in Example 14-7.

## 12.10 HUMAN FACTORS

In Table 12-1, we have seen that in almost every phase of the life cycle, managing human errors is featured. There are a number of activities in each phase, and decisions made in one phase can influence the subsequent phases.

While the approach and emphasis are different in the different life cycle phases, there are a number of common features and hence human factors and managing human error are summarised in this section.

Human errors can arise from two sources:

Type 1: Errors during the design and construction phase, made by project personnel, including contractors. This is the "latent" factor that lies dormant if left undetected and uncorrected, and has a propagatory effect during the operational phase.

Type 2: Errors by operations and maintenance personnel (including contractors) during the routine and non-routine tasks carried out in the operations phase of the facility.

The definition of human factors by HSE (1999) captures both the types:

*'Human factors refer to environmental, organisational and job factors, and human and individual characteristics, which influence behaviour at work in a way which can affect health and safety'.*

There is a vast amount of literature on the second type of errors. Since the early work of Reason (1990) and Kletz (1991), there has been a significant input to the process industry from behavioural sciences.

Table 12-6 gives a summary of risk related human factors that could have an impact over some of the principal life cycle phases of the product or process system.

TABLE 12-6 HUMAN FACTORS ACROSS SOME PROCESS LIFE CYCLE PHASES

| Life cycle phase | Important Human Factors |
|---|---|
| Strategic planning | Ignorance/lack of knowledge |
| Design | Knowledge/ignorance<br>Human-machine interface (HMI) issues |
| Operations | Adequate training<br>Process knowledge<br>Emergency response<br>Maintenance<br>Operating procedure<br>Shortcuts<br>Communications<br>Cognitive overload or lock<br>HMI Issues |

### 12.10.1 Human Factors in Design

Type 1 errors are conventionally managed by the following project management tools:

- Detailed project plan for design
- Project quality plan
- Awareness training of project personnel in project quality plan
- Vendors and contractors required to follow established quality plan
- Verification of design calculations, drawings through single discipline checks, inter-disciplinary checks, and independent checks by client's project team.

What is not conventionally done at this stage is to identify sources of error and eliminate them by training and by making the project quality plan more robust. This can be achieved by -

- Identify functions of project teams
- Conduct a functional analysis (input, output, resources)
- Conduct task analysis (identify activities associated with the functions)
- Conduct action error analysis on the tasks and prepare a checklist of possible errors (e.g. failing to undertake a task, use of wrong code or specification, failing to incorporate process safety design basis into one's own engineering discipline, conflicts between design basis among different disciplines, misunderstanding of objectives between Operator and Designer, different disciplines working with different versions of drawings, poor quality HAZOP, incomplete hazard identification etc. The list can be very long.)
- Develop preventative solutions to eliminate latent errors
- Incorporate the solutions into project procedures
- Communicate the findings to all project personnel and promote common understanding.

Failure to do the above has resulted in unnecessary re-work, with cost and schedule implications, and many projects unfortunately still prove the dictum that 'those who do not leant from their past mistakes are destined to repeat them'.

The major problem in Type 1 error is that they are latent, and may not be revealed until after an accident event, following a root cause tracing investigation. The onus is on the project team to get this right.

Type 2 errors can be forced on the operations team by the decisions made by the design team. Therefore, it requires the project team to evaluate the potential for human error during operations, and make sure that these can be prevented as much as possible. Examples of decisions are:

- Ergonomics of control room layout
- Ergonomics of visual display units
- Ergonomics of plant layout - access for process surveillance and maintenance, adequacy of lighting

- Decision on layer of protection - how much to leave to alarm and operator response, and how much to cover by SIS
- Assumptions on the ability of control room operator to manage abnormal situations
- Extent of process actions controlled or initiated remotely from control room and those that need to be done in the plant
- Communications
- Location and accessibility of personal protection equipment in plant (safety showers, eyewash, breathing apparatus etc.)

Once again a comprehensive checklist needs to be compiled, and the human factor implications of each decision must be reviewed at the design phase.

### 12.10.2 Human Factors in Operation and Maintenance

Most of the focus on human factors in the process industry has been on Type 2 human errors.

Three types of human failures have been identified (Anderson 2003).

- Errors - physical actions that were not as intended, e.g. pressing a wrong button.
- Mistakes - these are also errors, but errors of judgement or decision-making, e.g. making wrong diagnosis of an alarm and hence incorrect response
- Violations - These are intentional (though possibly well-meaning), such as taking short-cuts or non-compliance with procedures

Errors are often classified by behavioural scientists as errors of omission and errors of commission.

An error of omission is one that occurs as a result of the operator failing to perform a required task or omitting the step in the task. This could be due to intention, fatigue, or lack of awareness of the need for that action.

An error of commission is one in which the operator takes action but is the inappropriate action to take. Errors of commission are sub-classified into:

- Selection error - wrong object, wrong action. The 3-Mile Island incident is a classical example.
- Errors of sequence - execution of tasks in incorrect sequence.
- Time error - Operator executes the task too early or too late

Violations occur as a result of behavioural problems or over-confidence in one's capabilities. While human failures due to errors and mistakes may be occasionally tolerable due to their inevitability, human failure due to violation is unacceptable.

Wells (1996) has provided an extensive discussion on task analysis and human failure modes.

Human error can be managed by the following means:

- Promotion of attitudes and behavioural changes where appropriate. This is culture based and hence may have varying degree of success.
- Task analysis and identification of failure modes. Develop measures to minimise the failure modes. These include:
  - Measures to minimise fatigue and heat stress in the work place
  - Change in working environment and ergonomic design
  - Provision of expert systems information on the screen as a guide for abnormal situation management
  - Verify if an error is recoverable or not. If it is recoverable, identify what prompts are required for the operator to recover from the error. If it is non-recoverable, and the consequences are serious, then design an additional layer of protection (using layer of protection analysis) and do not entirely rely on correct human response

The concept of training, training and more training has been only partially effective in the past. It may address mistakes arising from lack of knowledge, but will not eliminate errors, which is inherent to human nature.

Human errors in reliability assessment can be conducted using human error evaluation techniques described in Chapter 8. Additional details may be found in CCPS (1994).

## 12.11 REVIEW

In this chapter, we have addressed concepts relating to managing risks during the entire life cycle of a facility, from concept design through to detailed design, operation and decommissioning. The hazard identification and risk assessment tools in Chapters 1 to 11 are interwoven with life cycle risk management, to present an integrated and holistic picture.

The concept of inherent safety has been described in some detail, as applying to all the phases of the life cycle, and confined to design alone. The major focus has been managing risks in the design phase, as this influences the plant operation the most. Process safety management in the operational phase is covered by the SMS, described in Chapter 11, and not repeated here. The need for maintaining plant integrity has been emphasized as a key to maintaining process safety performance.

Since human factors permeate the whole of life cycle activities, an overview of human factors is provided. This is a vast subject in itself and only an introductory review is provided, with appropriate references for further information.

The life cycle approach has indicated how decisions made at each phase of the life cycle can influence subsequent phases, and hence highlighted the need for the integrated approach. Much of what is described in this chapter is applicable to managing a major hazard facility, discussed in Chapter 13, but the concepts apply to all of the process industry, and are not restricted to major hazard facilities alone.

## 12.12 REFERENCES

American Petroleum Institute (API). *Best resource document on risk based inspection for API committee on refinery equipment*, American Petroleum Institute, Washington D.C. 1995.

American Petroleum Institute (API). *Recommended practice for classification of locations for electrical installations at petroleum facilities classified as Division 1 and Division 2*, American Petroleum Institute, Washington D.C. RP 500:1997.

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

American Petroleum Institute (API). *Recommended Practice for Design and Hazard Analysis for Offshore production Facilities,* American Petroleum Institute, Washington D.C. API RP 14J:2001.

American Society of Mechanical Engineers (ASME). *Research taskforce on risk based inspection guidelines, Risk based inspection: development of guidelines,* American Society of Mechanical Engineers, Washington, D.C. General document CRTD 20-1:1991.

Anderson, M. 2003, 'Human factors and COMAH: A regulator's perspective' in *Hazards XVII, Process Safety - Fulfilling our Responsibilities*, *Institution of Chemical Engineers Symposium Series No.149*, pp. 785-792.

Bale, E.A. and Edwards, D.W. 2000, 'Technical integrity - an engineer's view', *Transactions of Institution of Chemical Engineers*, Part B, Process safety and Environmental Protection, vol. 78, pp. 355-361.

Beck, R. 2003, 'Achieve best-in-class reliability', *Chemical Engineering Progress*, pp. 58-61, June.

Bollinger, R.E., Clark, D.G., Dowell III, A.M., Ewbank, R.M., Hendershot, D.C., Lutz, W.K., Meszaros, S.I., Park, D.E. and Wixom, E.E. 1996, *Inherently Safer Chemical Processes: A Life Cycle Approach*, (ed.) D.A. Crowl, American Institute of Chemical Engineers, New York, NY.

British Standard. *Petroleum and natural gas industries - Offshore production installations - Guidelines on tools and techniques for hazard identification and risk assessment.* BS EN ISO 17776:2002.

British Standard/IEC. *British Standard - Functional Safety - Safety instrumented systems for the process industry sector - Parts 1 to 3.* BS/IEC 61511: 2003.

British Standard Institution. *Electrostatic - Code of Practice for the avoidance of hazards due to static electricity*, PD CLC/TR 50404:2003.

Britton, L.G. 2000, 'Avoiding Static Ignition Hazards in Chemical Operations', *American Institute of Chemical Engineers*, January.

Busby, J.S. and P.W.S. Chung, 2003, 'In what ways are the designers' and the operators' reasonable-world assumptions not reasonable assumptions?', *Transactions of Institution of Chemical Engineers*, Part B, Process Safety and Environmental Protection, vol. 81, pp. 114-120.

CCPS, 1994, *Guidelines for Preventing Human Error in Process Safety,* Center for Chemical Process Safety, American Institute of Chemical Engineers, New York.

Chia, S., Walshe, K. and Corpuz, E. 2003, 'Application of Inherent Safety Challenge to an Offshore Platform Design for a new gas field development –

Approaches And Experiences', *Institution of Chemical Engineers (IChemE) Hazards XVII Conference*, United Kingdom.

Cohen, W. 1999, 'Application of ISA S84.01 to SIS in the chemical and petrochemical industries', *Process Safety Progress*, vol. 18, no. 4, pp. 221-224.

Dalzell, G. and Chesterman, A. 1997, 'Nothing is Safety Critical', *Institution of Chemical Engineers (IChemE) Hazards XIII Conference*, United Kingdom.

Dey, P.M. 2001, 'A risk-based model for inspection and maintenance of cross-country petroleum pipeline', *Journal of Quality in Maintenance Engineering*, vol. 7, no. 1, pp. 25-41.

Dowell III, A.M. and Green, D.L. 1998, 'Formulate emergency shutdown systems by cookbook', *Chemical Engineering Progress*, pp. 51-61, April.

Edwards, D.W. and Lawrence, D. 1993, 'Assessing the inherent safety of chemical process routes: is there a relation between plant costs and inherent safety?', *Transactions of Institution of Chemical Engineers*, Part B, Process Safety and Environmental Protection, vol. 71, pp. 252-258.

Edwards, V.H. and DeMichael, D.B. 1999, 'Properly isolate pressure relief devices', *Chemical Engineering Progress*, pp. 57-64, November.

Englund, S.M. 1991, 'Design and operate plants for inherent safety - Parts 1 and 2', *Chemical Engineering Progress*, vol. 87, no. 3, pp. 85 and vol. 87, no. 5, pp. 79.

Englund, S.M. 1996, 'Inherently safer plants: Practical applications', *Process Safety Progress,* vol. 14, no. 1, pp. 63-70.

Englund, S.M. 1990, 'Design and Operate Plants for Inherent Safety', *Advances in Chemical Engineering*, vol. 15, pp. 75-135.

Fauske, H.K. and Henry, R.E. 2001, 'Expanded metal networks: A safety net to thwart gas explosions', *Chemical Engineering Progress*, vol. 66, December.

Ferguson, D.J. 2004, 'Applying inherent safety to mitigate offsite impact of a toxic liquid release', *19th CCPS International Conference*, June 29-July 1, Orlando, Florida, pp. 167-170.

French, R.W., Williams, D.D. and Wixom, E.D. 1996, 'Inherent safety, health and environmental reviews', *Process Safety Progress*, vol. 15, no. 1, pp. 48-51.

Gardner, G. 1994, 'Explosion suppressions gain favour', *The Chemical Engineer*, 14 April, pp. 21-23.

Getz, R.C. 1996, 'Critical elements in the design of piping system for toxic fluids', *Process Safety Progress*, vol. 15, no. 1, pp. 26-31.

Gupta, J.P. and Edwards, D.W. 2002, 'Inherently Safer Design – Present and Future', *Transactions of Institution of Chemical Engineers*, Part B, Process Safety and Environmental Protection, vol. 80, pp. 115-125.

Harnly, J.A. 1998, 'Risk based prioritization of maintenance repair work', *Process Safety Progress*, vol. 17, no. 1, pp. 32-38.

Harris, J. 2002, 'On system condition auditing', *Transactions of Institution of Chemical Engineers*, Part B, Process Safety and Environmental Protection, vol. 80, pp. 197-203.

Health and Safety Executive (HSE) 1989, *Quantitative Risk Assessment: Its Input to Decision Making*, HMSO, London.

Health and Safety Executive (HSE) 1990, *Risk Criteria for Land-Use Planning in the Vicinity of Major Industrial Hazards*, HMSO, London.

Health and Safety Executive (HSE) 1992a, *Passive Fire Protection: Performance Requirements and Test Methods*, prepared by the Steel Construction Institute, Report No. OTI 92 606.

Health and Safety Executive (HSE) 1992b, *Availability and Properties of Passive and Active Fire Protection Systems*, prepared by the Steel Construction Institute, Report No. OTI 92 607.

Health and Safety Executive (HSE) 1995, *Electrostatic hazards associated with water deluge and explosion suppression systems offshore - Remedies suggested*, HSE Offshore Technology Report, OTO 95 026, September.

Health and Safety Executive (HSE) 1998, *Review of Test data on the Performance of PFP Materials in Jet Fires*, Offshore Technology report - OTO 97 078, May.

Health and Safety Executive (HSE) 1999, *Reducing Error and Influencing Human Behaviou*r, HSG48, HSE Books, UK.

Hendershot, D.C. 1995, 'Some thoughts on the difference between inherent safety and safety', *Process Safety Progress*, vol. 14, no. 4, pp. 227-228.

Hendershot, D.C. 2000, 'Process Minimisation: Making plants safer', *Chemical Engineering Progress*, pp. 35-40, January.

Herrington III, E.F. 1996, 'A team-based approach to mechanical integrity implementation', *Process Safety Progress*, vol. 15, no. 2, pp. 110-113.

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

Howell, A., Hanson, K., Dhole, V. and Sim, W. 2002, 'Engineering to business: Optimizing asset utilization through process engineering', *Chemical Engineering Progress*, pp. 54-59, 61-63, September.

Huston, E. 2002, 'Optimizing a chemical plant's physical assets', *Chemical Engineering Progress*, vol. 60, September.

Institute of Petroleum. *IP - Model Code of Safe Practice Part 15, Area Classification Code for Petroleum Installations*, London. 2002.

International Electrotechnical Commission. *Electrical apparatus for explosive gas atmospheres, Part 10 - Classification of hazardous areas,* International Electrotechnical Commission. IEC 60079-10:2002.

International Electrotechnical Commission. *Functional Safety of Electrical/ Electronic/Programmable Electronic Safety-Related Systems, Parts 1 to 7*, International Electrotechnical Commission. IEC 61508:1998.

International Electrotechnical Commission. *Systems Engineering-System Life Cycle Processes*, October. ISO/IEC 15288:2002.

Khan, F.I. and Amyotte, P.R. 2002, 'Inherent safety in offshore oil and gas activities: a review of the present status and future directions', *Journal of Loss Prevention in the Process Industries*, vol. 15, pp. 279-289.

Khan, F.I. and Amyotte, P.R. 2003, 'How to Make Inherent Safety Practice a Reality', *Canadian Journal of Chemical Engineering*, vol. 81, pp. 2-16.

Khan, F.I. and Haddara, M.M. 2003, 'Risk-based maintenance (RBM): a quantitative approach for maintenance/inspection scheduling and planning', *Journal of Loss Prevention in the Process Industries*, vol. 16, pp. 561-573.

Khan, F.I., Sadiq, R. and Amyotte, P.R. 2003, 'Evaluation of available indices for inherently safer deign options', *Process Safety Progress*, vol. 22, no. 2, pp. 83-97.

Khan, M.R.R. and Kabir, A.B.M.Z. 1995, 'Availability simulation of an ammonia plant', *Reliability Engineering and System Safety*, vol. 48, pp. 217-227.

Kletz, T.A. 1991, *An Engineers' View of Human Error*, 2nd edn, The Institution of Chemical Engineers, Rugby, England.

Kletz, T. A. 1994, *What Went Wrong*, Gulf Publication House, Houston, TX.

Kletz, T.A. 1984, *Cheaper, Safer Plants, or Wealth and Safety at Work*, Institution of Chemical Engineers, Rugby, UK.

Kletz, T.A. 1996, 'Inherently Safer Design - The Growth of an Idea', *Process Safety Progress*, vol. 15, pp. 5-8.

Kletz, T.A. 1985, 'Inherently Safer Plants', *Plant/Operations Progress*, vol. 4, pp. 164-167.

Kletz, T.A. 1991, *Plant Design for Safety*, Taylor & Francis, Bristol, PA.

Kletz, T.A. 1998, *Process Plants: A Handbook for Inherently Safer Design*, Taylor & Francis, Bristol, PA.

Kletz, T.A. 1978, 'What You Don't Have, Can't Leak', *Chemistry and Industry*, (May 6), pp. 287-292.

Lees, F.P. 2001, *Loss Prevention in the Process Industries*, 2nd edn, Butterworths-Heinemann, Oxford.

Lutz, W.K. 1997, 'Advancing inherent safety into methodology', *Process Safety Progress*, vol 16, no. 2, pp. 86-88.

Mahgerefteh, H., Saha, P. and Economou, I., 1998, 'Control valves for pipe rupture', *The Chemical Engineer*, 24 September, pp. 26-28.

Marszal, E.M. and Scharpf, E.W. 2002, *Safety Integrity Level Selection: Systematic Methods Including Layer of protection Analysis,* ISA - The Instrumentation, Systems and Automation Society, NC, USA.

National Fire Protection Association. *Recommended practice for static electricity*, National Fire Protection Association, Quincy, MA, USA. NFPA 77:2000.

New South Wales Government - Department of Planning, Infrastructure and Resources 1992. *Hazardous Industry Planning Advisory paper No.7 - Construction Safety Study Guidelines*, Sydney, Australia.

O'Connor, P.D.T. 1991, *Practical Reliability Engineering*, 3rd edn, John Wiley.

Occupational Health and Safety Administration (OSHA). *Process safety management of highly hazardous chemicals*. Federal Register, Washington DC. OSHA 29 CFR 1910.119:1992.

Pavey, I.D. 2004, 'Electrostatic hazards in the process industries', *Transactions of Institution of Chemical Engineers*, Part B2, Process Safety and Environmental Protection, vol. 82, pp.132-141.

Phillips, L.T. 2002, 'Decommissioning process plant facilities', *Chemical Engineering Progress*, December, pp. 60-73.

Post, R.L., Hendershot, D.C. and Kers, P. 2002, 'Synergistic Design Approach to Safety and Reliability Yields Great Benefits', *Chemical Engineering Progress*, vol. 98, pp. 60-66.

Preston, M.L. and Hawksley, J.L., 1997, 'Inherent SHE - 20 years of evolution' in *Hazards XIII - Process Safety, the Future, Institution of Chemical Engineers Symposium Series No.141*, pp. 11-23.

Rausad, M. 1998, 'Reliability Cantered Maintenance', *Reliability Engineering and System and Safety*, vol. 60, pp. 121-132.

Reason, J. 1990, *Human Error*, Cambridge University Press.

Rogers, R.L. and Hallam, S. 1991, 'A chemical approach to inherent safety', *Transactions of IChemE*, Part B, Process Safety and Environmental Protection, vol. 69, pp. 149-152.

Rushton, A.G., Edwards, D.W. and Lawrence, D. 1994, *Transactions of Institution of Chemical Engineers*, Part B, Process safety and Environmental Protection, vol. 72, pp. 83-87.

Senecal, J.A., Harry, L.D., Meltzer, J.S., Piccirilli, V., Pizzarello, C. and Slonski, S.J., 1999, 'Forestall fires with advanced technology', *Chemical Engineering Progress*, pp. 35-42, August.

Statham, B. 1999, 'Static spark debate', *The Chemical Engineer*, 29 April, pp. 23-24.

Summers, A.E. 2000, 'Consider an instrumented system for overpressure protection', *Chemical Engineering Progress*, pp. 65-68, November.

Vinod, G., Bidhar, S.K., Kushwaha, H.S., Verma, A.K. and Srividya, A. 2003, 'A comprehensive framework for evaluation of piping reliability due to erosion-corrosion for risk-informed service inspection', *Reliability Engineering and System Safety*, vol. 82, pp. 187-193.

Wells, G. 1996, *Hazard Identification and Risk Assessment*, Institution of Chemical Engineers, Rugby, England.

Whetton, C. 1993, 'Maintainability and its application to process plant', *Process Safety Progress*, vol. 12, no. 3, pp. 158-165.

## 12.13 NOTATION

| | |
|---|---|
| API | American Petroleum Institute |
| ASM | Abnormal Situations Management |
| ASME | American Society of Mechanical Engineers |
| BLEVE | Boiling Liquid Expanding Vapour Explosion |
| CCPS | Center for Chemical Process Safety |
| CEI | Chemical Exposure Index |
| CFD | Computational Fluid Dynamics |
| DCS | Distributed Control System |
| EERA | Escape Evacuation and Rescue Analysis |
| EMS | Environmental Management System |
| EPC | Engineering Procurement Construction |
| ESD | Emergency Shutdown |
| ESSA | Essential Systems Survivability Analysis |
| F&EI | Fire & Explosion Index |
| FEED | Front End Engineering Design |
| FIBC | Flexible Intermediate Bulk Container |
| FMEA | Failure Modes and Effects Analysis |
| FMECA | Failure Modes Effects and Citicality Analysis |
| HAZID | Hazard Identification |
| HAZOP | Hazard and Operability Study |
| HIPPS | High Integrity Pressure Protection System |
| HSE | Health and Safety Executive (UK) |
| HVAC | Heating Ventilation and Air-Conditioning |
| IEC | International Electrotechnical Commission |
| IP | Institute of Petroleum |

| | |
|---|---|
| IPF | Instrumented Protective Function |
| IS | Intrinsically Safe |
| ISD | Inherently Safer Design |
| ISO | International Organisation for Standardisation |
| ISIR | Individual Specific Individual Risk |
| km | kilometers |
| LPG | Liquefied Petroleum Gas |
| LSIR | Location Specific Individual Risk |
| mm | millimeters |
| MTBF | Mean Time Between Failures |
| MTTR | Mean Time To Repair |
| NDT | Non-Destructive Testing |
| NFPA | National Fire Protection Association (USA) |
| O&M | Operations & Maintenance |
| OH&S | Occupational Health & Safety |
| OSHA | Occupational Safety and Health Administration (USA) |
| PFP | Passive Fire protection |
| PSV | Pressure safety valve |
| QRA | Quantitative Risk Analysis |
| RBI | Risk Based Inspection |
| RBM | Risk Based Maintenance |
| RCM | Reliability Centred Maintenance |
| RTJ | Ring joint (to American National Standards Institute) |
| ROV | Remote Operated Vehicle |
| RP | Recommended Practice |
| SIL | Safety Integrity Level |
| SIS | Safety Instrumented System |
| SMS | Safety management System |
| SOLAS | Survival of Life At Sea |
| VCE | Vapour Cloud Explosion |

# 13 MANAGEMENT OF MAJOR HAZARD FACILITIES

*"The purpose of this legislation is to ensure that in the control of industrial major hazards, the ignorant seek knowledge, the wise think again, and the incompetent, never be in control."*

*Debate in the House of Lords on the CIMAH Regulations*

Major hazards and in particular, major hazard facilities (MHFs) have taken on a growing importance in international and national regulations. Accidents such as Flixborough (UK), Seveso (Italy), Bhopal (India) and Piper Alpha (North Sea) have led directly or indirectly to the current regulatory framework that exists worldwide.

Due to the potential of MHFs to cause major disasters if poorly designed, located or controlled, these comprehensive regulations and guidelines are aimed at the effective management of risk generated by such activities. Amongst the drivers for control of major hazards is the associated land use planning issues. This has been a major concern to national governments, where new activities are to be located nearby to sensitive land uses such as residential areas or high occupancy activities. Appropriate siting of new developments near to existing MHFs is also a major planning challenge. The other drivers include an increasing concern for environmental damage, injury or fatality to facility personnel and the loss of plant and equipment leading to major business interruption.

In this chapter we discuss the general regulatory framework surrounding risk management of major hazards, whilst in Chapter 16, the important issue of land use planning is considered in more detail. We set out the key factors in risk management of major hazard activities in what follows.

In summing up a training presentation in 1991 for ICI managers on lessons from the Piper Alpha disaster, Dr Brian Appleton said:

> *"Safety is not an intellectual exercise to keep safety managers in work. It is a matter of life and death. It is the sum total of everybody's contribution to safety management that determines whether the people we work with live or die."* (VEC 1991)

We need to keep these thoughts foremost in our minds as we practise process risk management for it is not just corporate personnel but the general public and the environment that can be so often affected by major hazard disasters.

## 13.1 MAJOR HAZARDS AND THEIR MANAGEMENT - PERSPECTIVES

In his book on "Managing Major Hazards", Andrew Hopkins (1999) discusses a number of perspectives often taken in order to explain disastrous accidents. These perspectives have a direct relation to managing major hazards. They include:

(i) The inevitability of socio-technical disasters.
This is the approach that says industrial accidents are simply bound to happen just as natural disasters occur. There is an inevitability to man-made disasters because of the failings of people and that technological development "bites back" (Tenner 1997; Greenhalgh 1994).

(ii) The production versus safety conflict.
Getting the product out the gate or to the destination is what counts! The production imperative versus safety is a constant challenge. In some cases, safety concerns have been sidelined for the sake of production - sometimes being able to sustain the risk but often not. The prevailing industrial and commercial safety culture is moving rapidly to prioritizing key safety issues above production. There are still those who think they can always "get away with it".

(iii) The normal accident theory of complex systems.
The "normal accident" theory espoused by Charles Perrow (1999) argues that modern complex, highly coupled industrial or commercial plant and processes have the seeds of accidents built into them. There is again an inevitability of failure due to so many potential pathways for accident propagation. These cannot be fully analyzed or predicted. He contrasts linear, loose systems with complex, highly coupled systems to illustrate the fundamental differences in system designs.
However, as Hopkins points out, no significant discussion is given to the advances in systems design and analysis methods that seek to provide insights into critical factors that can be effectively addressed to provide high reliability. It is when this level of synthesis and analysis remains superficial that potential disasters await the operator. Dőrner (1996) provides interesting insights into approaches to tackle some of these issues.

(iv) The misinformation paradigm.

"Disaster equals energy plus misinformation" (Turner 1978) captures some of the aspects of the importance of information and its use in major hazard operations. In many cases, misinformation is due to limited understanding of chemical and physical phenomena that directly affect designs and combines with the release of energy to create accident scenarios. In other cases lack of information at the appropriate time leads to false perceptions and incorrect actions by personnel. Each is a recipe for disaster.

(v) The latent errors and general failures framework.
James Reason (1997) shows convincingly that failures in management of systems and design lead to the existence of latent conditions that when activated allow propagation of accident sequences that potentially lead to disaster. This approach has been widely recognized as a key issue in safe system design and operation. It has led to the establishment of the Tripod Delta (section 13.7) approach that creates an integrated way of thinking about systems that helps address latent conditions and many related factors (Hudson et al. 1994).

(vi) The failure of organizational memory.
The lack of memory within corporations is often a major factor in further accident occurrence. The need to capture experiences from accidents is vital for organizations to ensure that lessons are learnt right across the organization. Kletz (1993, 2003), emphasizes the importance of this aspect through many case studies within the process industries.

Each of these perspectives adds vital components to a holistic view of the causes of major hazard disasters. Chiles (2001) provides a series of case studies illustrating many of these perspectives in major accidents across many industry sectors.

The over-riding point in all these perspectives is the pivotal role that management plays in assuring safety of major hazards operations.

## 13.2 THE REGULATORY FRAMEWORK AND REQUIREMENTS

Most modern expressions of the control of major hazards have their origins in the work of the UK Advisory Committee on Major Hazards (ACMH) that published 3 reports over the period 1976 to 1984. These reports were subsequent to the Flixborough disaster in 1974 which acted as a catalyst for those studies. Concurrently in continental Europe, the European Commission (EC) was considering the issue of major hazards following the release of trichlorophenol and other toxic compounds from a chemical factory in Seveso, Italy. The subsequent directive, 'Major Accident Hazards of certain industrial activities" (82/501/EEC) was issued in 1982 and commonly referred to as the "Seveso Directive". The updated and expanded Seveso II Directive (96/82/EEC) was enacted in 1997. These directives led to a raft of national regulations across the European Community (Lees and Ang 1989) as well as affecting regulatory arrangements in Australasia.

However, there is currently little commonality in individual approaches of member states across the European Community. Approaches range from risk based assessment and control in countries such as the UK, The Netherlands and

Denmark to prescriptive engineering controls in Germany. Other countries have a mixture of these approaches.

Similar developments in the USA led to federal legislation to handle accidental releases of hazardous substances. Key was the Superfund Amendments and Reauthorization Act (SARA) of 1986 with Title III being the Emergency Planning and Community Right-to-know Act (EPCRA). The federal legislation covers all states and facilities that have chemical substance inventories above certain stated threshold quantities. This is similar in concept to the EC and Australian directives. These regulations were supplemented by the OSHA rule on Process Safety Management (PSM) (1992) and the US EPA Risk Management Programs (RMP) for prevention of chemical releases (1996).

Within Australia, the federal government established the over-arching national standard on "Control of Major Hazard Facilities" (NOHSC 1996) in 1996, together with its code of practice. This standard was intended to be implemented in individual states through specific legislative arrangement such as the Occupational Health & Safety (Major Hazard Facilities) Regulations 2000 in Victoria or the Dangerous Goods Safety Management Act 2001 in Queensland.

These acts and regulations require formal treatment of hazards and risks from these designated operations. In particular, the production of a comprehensive safety report or safety case is normally a requirement of major hazards regulations for offshore and on-shore activities.

It is the content of such a report that is discussed in the following sections as well as the important management aspects of these activities. The focus of the Safety Case is primarily but not exclusively on the low frequency high consequence incidents such that a clear demonstration is given by the operator concerning the adequacy of the design and operation of the facility. The "adequacy" is often judged by means of the ALARP principle that ensures design and controls are suitable and effective in eliminating and reducing risks.

As emphasized in some regulations:

> *"The demonstration of adequacy of safe operation is the heart of the safety case, and a safety case that fails to achieve this in a transparent and robust manner consistent with the operational philosophy of the facility would not meet Regulatory requirements".* (Worksafe Victoria 2001)

## 13.3 THE SAFETY CASE/REPORT APPROACH

The use of a formal safety case preparation to help address the management of major hazards is now commonplace for both on-shore and off-shore operations. In many cases, such as the UK and Australasia, it is enshrined in relevant major hazards regulations such as:

(i) The UK Control of Major Accident Hazards (COMAH) Regulations, 1999.

(ii) The Dutch, Hazards and Major Accidents Regulations, 1999.

(iii) UK Off-shore Installations (Safety Case) Regulations, SCR, 1992, and subsequent amendments.

(iv) The Australian Government, Major Hazard Facilities Regulations, 1996/2002.

(v) The Australian Government, Petroleum (Submerged Lands) (Management of Safety on Offshore Facilities) Regulations, 1996.

(vi) Victorian State Government, Australia, Occupational Health and Safety (Major Hazard Facilities) Regulations, 2001.

(vii) Queensland State Government, Australia, Dangerous Goods Safety Management Act and Regulations, 2001.

(viii) OSHA, PSM for highly hazardous chemicals, 1992.

(ix) USEPA, Risk Management Program (RMP) under the Chemical Emergency Preparedness and Prevention Program, 1996.

These regulations, to varying extents, prescribe the development of a 'case' or 'report' that sets out a clear set of studies that demonstrates the operations are designed, constructed and operated in a safe manner where all risks have been eliminated or minimized. The following sections deal with the outcomes, critical success factors and dangers in the safety case regime.

In what follows, "safety case" and "safety report" are regarded as synonymous terms.

### 13.3.1 Planned Outcomes of Safety Reports

The safety report has the intent that the operator will demonstrate a range of competencies and actions in relation to the major hazard. These can include:

(i) A clearly established philosophy concerning the methods and actions that establish and maintain integrity of operations. The integrity will encompass aspects of engineering principles, standards and systems of work. It will also integrate operational practices and the form and development of a corporate culture based around system safety.

(ii) A demonstrated, in-depth understanding of all hazards associated with the activities and the risks to people, property, environment and related factors such as business reputation, cultural and heritage values.

(iii) A comprehensive and integrated plan to eliminate, contain, mitigate or control risks to a level as low as reasonably practicable (ALARP) or so far as is reasonably practicable (SFAIRP).

(iv) An established and exercised emergency plan to deal with all foreseeable incidents both on and off-site.

(v) The design and implementation of an on-going safety management system that addresses all relevant aspects of the operation.

(vi) An established training and education program for all employees involved in the operation.

(vii) An established and on-going dialogue with local communities that might be affected in some way by the operations.

(viii) A commitment to the continual improvement of safety in the operations and the maintenance of the safety report over the life cycle of the facility.

### 13.3.2 Factors that Lead to Successful Safety Reports

A number of critical factors should be noted in developing safety reports (Worksafe Victoria 2001). They include:

(i) A clear, concise corporate management philosophy that underlies the case being made.

(ii) A comprehensive presentation of the operations within their geographical, economic, technical and social framework. All dangerous goods and operations need to be discussed.

(iii) A full disclosure of all hazards associated with the operations that include substances, processes, human and management system aspects.

(iv) The design and construction basis for the operations and how engineered controls are addressed for major hazards and incidents.

(v) The basis on which safety management systems are developed, implemented and improved. This is particularly the case for safety critical management issues within the operation.

(vi) A convincing account of the consultation processes that were undertaken with all stakeholders as well as the on-going communication systems and protocols to be followed.

(vii) A credible demonstration of the systems in-place that maintain the "living" nature of the safety report–not forgotten on the shelf!

(viii) The way in which all aspects related to the safety report are integrated into a holistic approach to give integrity to the activity and its management.

In like manner it is relatively easy to identify key critical issues that can negate the effective development and use of safety reports.

### 13.3.3 Recurring Issues in Safety Report Preparation

One of the principal concerns for operators and regulators is that the safety report must demonstrate in a convincing way that all necessary controls are in place to address risks, and are effective. Britton (2003) provides a number of reasons for inadequate safety report preparation as:

(i) Inadequate links between the major accident scenarios and the measures provided to address them.

In many cases, safety reports did not clearly demonstrate that the measures taken to address accident scenarios were adequate. Descriptions of measures are often provided but the case for the effectiveness of those measures was deficient. Aspects of risk control such as inspections, maintenance and change management were missing or poorly developed.

(ii) Incomplete argumentation that all necessary measures have been taken to prevent or limit the consequences of a major accident.

Here it was found that operators failed to show a systematic risk assessment process that led to risks being ALARP. The process of risk minimization was deficient. The approach of asking "What more can be done?" or "What is not being done?" are crucial to the ALARP demonstration.

(iii) Inadequate information on the measures taken and their application.

Here the descriptions were often given in general terms, referencing corporate standards and practices. What was lacking was the relevance of the standards, what they covered and how they were related to the proposed measures. It is clear that the lack of information and argumentation in safety reports concerning links between the identified accident scenarios and the measures to effectively address them effectively is still a major challenge for operators. The underlying ALARP concept is often not addressed convincingly despite its central importance in managing major hazards.

### 13.3.4 Factors Neutralising the Benefits of Safety Reports

Some factors work against the intent of the safety report and tend to neutralise its positive contribution to process safety. Amongst some of the critical factors, we can identify the following:

(i) A corporate attitude that sees the safety report solely as a regulatory requirement to be endured and then "put to bed".

(ii) Over-reliance on consultants in performing significant amounts of the safety report with no clear technology transfer or learning outcomes to the corporation.

(iii) Lack of "live" systems that ensure the up-to-date maintenance of the safety report throughout the life cycle of the process or operation.

(iv) Poor change management processes over the operational life cycle such that corporate memory is lost, background arguments and assumptions misplaced and internal technical documentation remaining out-of-date.

(v) Lack of "buy in" by corporate personnel at all levels in developing, presenting and maintaining the safety report.

The challenge for the corporation is maintaining the "real-time" aspects of the safety report work over the complete life cycle of the process.

## 13.4 COMPONENTS OF A SAFETY REPORT

The components of the safety report cover all relevant analysis, assessment and control steps necessary to document the operation and in most cases to demonstrate that it achieves a risk that is low as reasonably practicable (ALARP). Figure 13-1 shows the principal components of a typical safety report.

The following sections give detail and commentary with examples of the principal safety report components.

### 13.4.1 Nature of Materials, Scale and Operations

Purpose: To set the context of the major hazard operations in terms of the materials, methods and processes as well as the spatial setting of the activities.

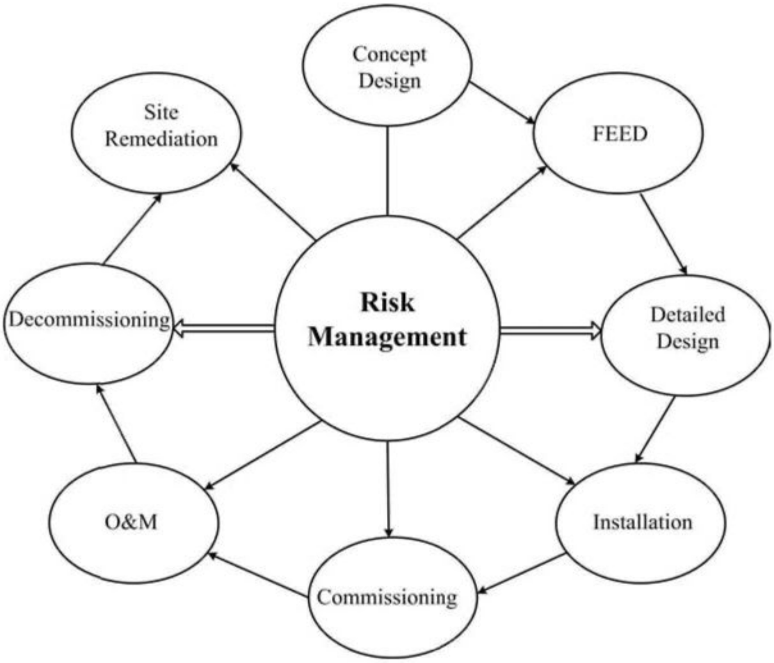


FIGURE 13-1 PRINCIPAL COMPONENTS IN A SAFETY REPORT

Table 13-1 sets out key aspects of the context of the major hazard operations.

TABLE 13-1 NATURE, SCALE AND CONTEXT OF ACTIVITIES

| Issues | Aspects |
|---|---|
| Nature of the study | • Objectives to be addressed<br>• Methodologies adopted<br>• Techniques and justification<br>• Dissemination of outcomes<br>• Personnel involved |
| Facility or activity | • Historical background<br>• Location and surrounding land uses<br>• Topology, geology and hydrology<br>• Facility purpose and processes<br>• Layout and key operations<br>• Access routes<br>• Design and construction criteria<br>• Standards, materials, fabrication<br>• Verification processes |

| Issues | Aspects |
|---|---|
| | • Commissioning<br>• Safety systems description<br>• Highlights of where inherent safety is incorporated in design |
| Key risk receptors | • Class of receptor (people, property, ... )<br>• Communities (population density, demography)<br>• Environmental receptors (land, water, ... ) |
| Prevailing meteorology | • Wind, storm, flood, atmospheric stability, ...<br>• River/water course flows, tides, ... |
| Materials | • Dangerous Goods Classes, inventories, form of substances<br>• Toxicity, flammability, explosive potential, reactivity<br>• Wastes and by-products of activities<br>• Production throughputs or transport quantities |

These aspects should set out in a comprehensive manner the principal data that helps describe the major hazard activities as well as physical, social and geographical context in which the activities take place.

### EXAMPLE 13-1 LPG TERMINAL LOCATION

Figure 13-2 shows a land use planning map overlaid on an aerial photograph, that illustrates a number of sensitive land uses surrounding the subject site. The major circles indicate distance from the centre of the site. Of special consideration here were nearby commercial operations to the immediate south and east of the site as well as established and planned residential areas to the east, within a 350 to 500m range. Other important features included a major highway to the west and relatively steep land sloping to the west of the site. These features were important aspects in the safety report outcomes.

Numbered locations were annotated to provide details of activity, occupancy, building type and possible location of other dangerous goods facilities such as fuel storage depots.

The land use survey provided vital information in decision making concerning impact of hazardous incidents, an input to emergency planning and to future land use planning issues.

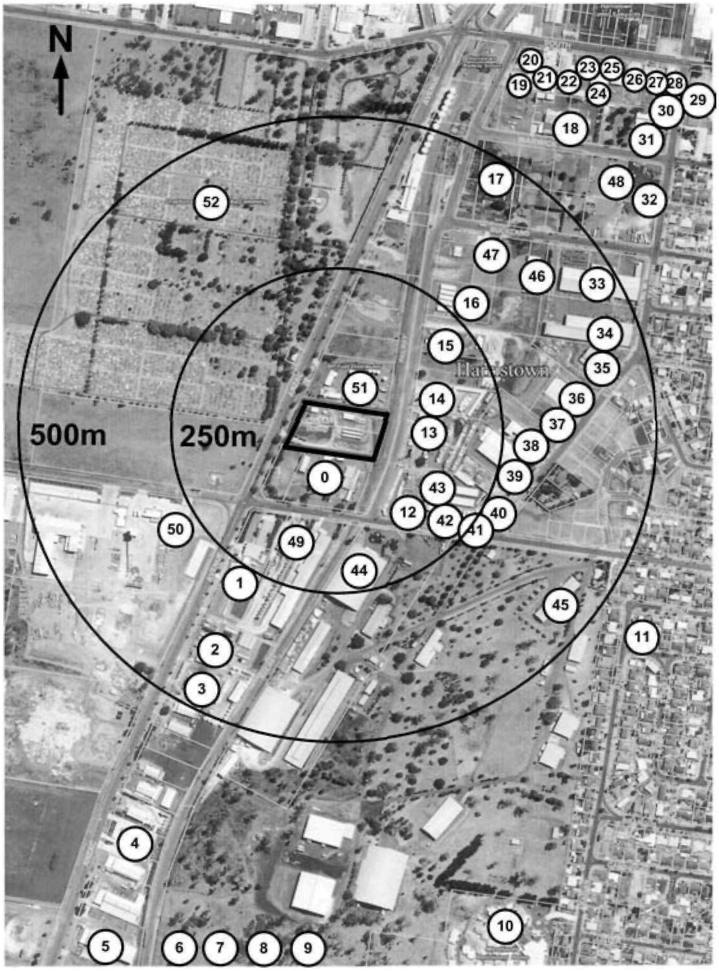


FIGURE 13-2 LPG TERMINAL LOCATION AND SENSITIVE LAND USES (ENERGEX LTD)

### 13.4.2 Comprehensive Risk Assessment

Purpose: To fully identify hazards, estimate consequences and likelihood of incidents ensuring that measures are taken to eliminate or mitigate risks.

The risk assessment addresses a number of important issues that have already been mentioned in Chapter 9. In Table 13-2 the key issues and aspects of this safety report component are summarized.

TABLE 13-2 COMPREHENSIVE RISK ASSESSMENT COMPONENTS

| Issues | Aspects |
|---|---|
| System definition | • Clear definition of study boundaries<br>• Context of study<br>• Study focus: safety, environment, business, heritage/cultural, legal. |
| Hazard identification | • Methods to be used and their justification<br>• Personnel and competency of staff involved<br>• Historical and/or industry databases used<br>• Focus on hardware, human and safety management failures, reactive systems, security and external factors (flood, cyclone, ...) |
| Consequence analysis | • Qualitative and/or quantitative methods used<br>• Models/software used and justification<br>• Estimates of uncertainty and their significance<br>• Physico-chemical properties of released materials<br>• Basic assumptions on size of release and duration<br>• Effect of mitigation systems |
| Likelihood analysis | • Basic failure rate data used in the analysis<br>• Uncertainty estimates and sensitivity studies<br>• Complex failure sequences (fault trees)<br>• Event tree analysis and mitigation systems<br>• Role of human factors in analysis |
| Risk evaluation | • Identifying major risk contributors<br>• Ranking of all risks and prioritization<br>• Estimates of uncertainty in risk estimates<br>• Use of appropriate screening tools such as qualitative risk matrices, LOPA or risk graphs |
| Risk assessment and treatment | • Appropriate tolerability criteria for risk categories<br>• Application of inherent safety principles for risk contributors<br>• Applying ALARP/SFAIRP principles to all major risk contributors<br>• Extension of ALARP to medium and low risk contributors<br>• Justification of decision process in the assessment phase |

### 13.4.3 Demonstration of Adequacy of Hazard Control Measures

The demonstration of adequacy of hazard control measures consists of two major components:

- To demonstrate that the hardware control measures adopted (inherent safety, prevention, detection and mitigation measures) can effectively control the major accident events identified; and
- To demonstrate that the Safety management System (SMS) provides a comprehensive and integrated system for all aspects of control measures adopted in relation to hazards and major incidents.

The bow-tie model described in Chapter 8 is a useful tool for demonstration of adequacy. Each major accident event is selected in turn, and the threats that could cause the accident event are identified. In the next tier, each threat is selected one at a time, and the barriers in place to prevent the threat occurring are listed. Similarly, the control measures to prevent the impact of loss of containment, and mitigate the effects are evaluated.

In order to evaluate the barriers and mitigation measures in terms of their adequacy to control the major accident events, a number of parameters are defined. The terms and definitions are given below:

1. Control Hierarchy

The specific hierarchical role played by the control measure. The specific functions are:

a) Elimination
b) Prevention
c) Detection
d) Prevention of ignition
e) Process isolation
f) Pressure relief
g) Depressuring
h) Fire protection
i) Prevention of escalation

Items (c) to (g) are collectively referred to as Process Safeguarding.

2. Effectiveness

Effectiveness is defined as the probability that the control measure will perform its function to control the threat or consequence, assuming 100% reliability, survivability and availability.

3. Reliability

Reliability is the probability that the control measure would operate on demand. For instrument systems, the unreliability is estimated as the Fractional Dead Time (FDT), depending on the frequency of function testing. For non-instrumented systems, e.g. integrity inspection procedures, the reliability may be defined as the probability that the inspection is carried out on schedule.

4. Survivability

The survivability is defined as the probability that the control measure remains unimpaired during the major incident (MI) until it has performed its function. For instance, if there is smoke ingress into the air intake of the diesel firewater pumps under certain wind direction/weather conditions, then the pumps would not perform their function and are said to be impaired. In such an event, the survivability of the control measure would be significantly less than 1.

5. Availability

Availability is the time over which the control measure is available to perform its function. The time to carry out repairs of faulty equipment, lead time for obtaining spare parts, and downtime during function testing are the times when the control measure is unavailable.

Performance targets are set for the above parameters, and the overall effectiveness of each barrier and control measure is examined in terms of the above parameters. Rule sets may be developed for rating the adequacy of the barriers and control measures. For instance, one rule set may be that each threat must have at least two *independent* barriers (sometimes 3, depending on the frequency of the threat), and that these barriers must have an overall effectiveness of more than 95% each.

The causes of a major accident event would vary from incident to incident, but there would be a number of common features. In the main, the causes of a loss of containment of hazardous materials consist of mechanical failure of hardware, instrument and control system failure, or human error. Similarly, the prevention barriers would be robustness of design, protection against corrosion, overpressuring and impact, skills and competency of personnel, and integrity inspections.

It is possible that the same threat may be present in more than one major accident event, and the same mitigation measure would be present to control more than one event. To the extent these influence multiple major accident events, their criticality increases, and hence the barriers and mitigation measures must meet the performance targets of the parameters.

Once it is established that a set of barriers and mitigation measures would control the hazards in the Terminal to adequate performance standards, the next step is to ensure that the integrity of these control measures are maintained. The processes for maintaining the integrity of these control measures are defined as Safety Critical Processes (SCP). Associated with each SCP is a set of safety critical activities (SCA), specifically targeted for controlling the major accident event.

The SCP and the associated SCA have a direct link with the SMS, and are controlled through the SMS. Thus, the SMS becomes the primary instrument in controlling the major accident events on a major hazards facility.

### 13.4.4 Emergency Planning Procedures

Purpose: To develop, implement and exercise emergency plans that address the required resources for minimizing adverse impacts on people, property and the environment.

Due to the very nature of major hazard activities, residual risks still exist due to the operations being undertaken. Emergencies, both on-site and off-site are feasible and the incidents that constitute emergency situations need to be addressed. Table 14-3 sets out the key issues for emergency planning activities (CHEM Unit 1998).

TABLE 13-3 EMERGENCY PLANNING ACTIVITIES

| Issues | Aspects |
|---|---|
| General considerations | • Aim and objectives of the plan<br>• Scope, emergency type of identification<br>• Emergency levels defined<br>• Key stakeholders (industry, community, external emergency services, ...) |

| Issues | Aspects |
|---|---|
| Hazards | • Materials and effects<br>• Locations<br>• Types of incidents (fire, release, explosion, ...)<br>• Consequence estimates |
| Emergencies | • Types and levels defined<br>• Emergency control (functions, duties, ... )<br>• Control zones (cold, warm, hot, hazard)<br>• Emergency procedures (alarm, contain, protect, ... )<br>• Emergency resources needed (equipment, people, ... )<br>• Reporting and terminating<br>• Recovery processes<br>• Communications (press, police, public, ... ) |
| Consultation | • Local community awareness<br>• Employee information<br>• Emergency services (police, fire, rescue, bomb squad, ...) |
| Plan management | • Training and education programs<br>• Exercising and testing plan<br>• Reviewing performance<br>• Auditing of plan for preparedness, effectiveness and responsiveness<br>• Updating and improving |

Emergency plans can often be written and never exercised. In many cases, when plans are activated during a real or simulated emergency severe problems can be encountered that lead to significant loss of control making the plan ineffective. Regular exercising of the plan and in-depth performance review is absolutely essential.

### EXAMPLE 13-2 EMERGENCY PLANNING MATRIX

A useful summary form for the developed emergency plan as presented within a safety report can take the form of an emergency planning matrix. Table 13-4 illustrates a number of emergency planning elements for a mining operation.

TABLE 13-4 EMERGENCY PLAN ELEMENTS FOR MINE-SITE RELATED EMERGENCIES

| Event | Level of emergency | Emergency services required | Resources needed | Organizational aspects | Damage control actions |
|---|---|---|---|---|---|
| Bush fire on mine site | Site wide<br>Potential external alert | Site fire fighting team.<br>Town fire crew or country fire authority | Fire fighting truck and water tankers | Evacuation of affected mine workers.<br>Roll call | Fire containment.<br>Shutdown of affected operations.<br>Evacuate near fire areas such as AN storage and explosives. |

| Event | Level of emergency | Emergency services required | Resources needed | Organizational aspects | Damage control actions |
|---|---|---|---|---|---|
| Ammonium nitrate (AN) fire | Site wide and external | Site fire crew<br>Local fire crews<br>Police and ambulance on alert | Fire fighting<br>Plans and maps | Communications<br>Evacuation notice | Fire spread<br>Evacuation downwind |
| Bulk diesel fuel fire | Local and site | Site fire fighting crew | Fire fighting water | Evacuation notice<br>Communication to fire and recovery crews | Evacuate from local area<br>Fire spread control<br>Adjacent cooling of tanks and/or structures |
| Explosives magazine incident | Site | Ambulance<br>Police<br>Site and town fire crews<br>Emergency airlift | Fire fighting equipment and water | Roll call<br>Search and rescue<br>Communications and Public relations/media liaison | Evacuation of area<br>Knock-on effects from fire and further explosions |

### 13.4.5 Safety Management System (SMS)

Purpose: To develop and implement systems that manage all major hazard risks and to continually seek improvement in performance.

The analysis of major hazard disasters inevitably points the finger at significant management failures as either root causes or significant contributing factors in those accidents. Hence, there is an appropriately important emphasis on the safety management systems for major hazards. Chapter 11 has dealt with many of the issues in significant depth and Table 13-5 provides a summary of some of the key issues (CHEM Unit 2002b) based around the management cycle of policy-planning-implementation-monitoring/evaluation-audit/review.

TABLE 13-5 MAJOR ISSUES IN SAFETY MANAGEMENT SYSTEMS

| Issues | Aspects |
|---|---|
| Commitment and Leadership | • Safety policy<br>• Resources<br>• Responsibility and accountability |

| | |
|---|---|
| | • Communication |
| Planning | • Objectives and targets<br>• Information requirements<br>• Safety plans |
| Implementation | • Hazard identification and risk assessment<br>• Safety assurance<br>• Systems of work<br>• Training<br>• Emergency preparedness<br>• Management of change |
| Monitoring, measurement and evaluation | • Performance criteria<br>• Inspection, monitoring and testing<br>• Incident reporting and investigation |
| Auditing and review | • Auditing<br>• Review and improvement |

Figure 13-3 shows the typical management cycle that is common to many approaches for establishing an SMS.

Clearly the importance of auditing, performance indicators and feedback for corrective actions is vital for the on-going improvement in the SMS. The effectiveness by which the SMS cycle is addressed will determine the real efficacy of the system. (Kelly and McDermid 2001; Santos-Reyes and Beard 2002)

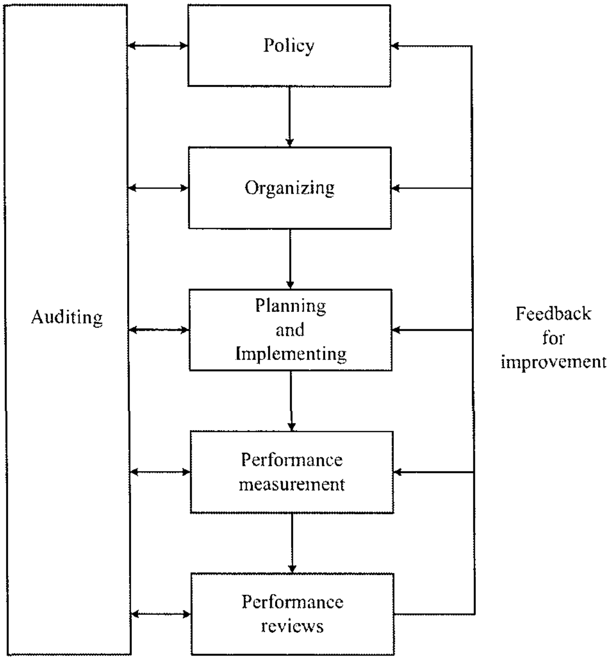


FIGURE 13-3 GENERIC SMS CYCLE

## 13.4.6 Education and Training Issues

Purpose: To provide appropriate information, supervision, training and education to all personnel so as to provide safe operational practices.

Education and training in any area of commerce and industry are vital ingredients for improvements in safe operations. Competency of personnel is paramount and that implies effective education and training. Inadequate or inappropriate training is a recipe for disaster and often a major factor in major hazard accidents.

EXAMPLE 13-3 PIPER ALPHA DISASTER - INDUCTIONS

Failure to induct personnel arriving on the North Sea Piper Alpha platform prior to the disaster in 1988 meant that one of the survivors knew virtually nothing of the layout and emergency procedures. In desperation, surrounded by flames he jumped from the platform unaware of his position or what was below. Providentially he landed in the sea and was rescued. A rather extreme example of failure to educate and train personnel.

Table 13-6 shows some of the principal issues and their aspects that relate to training and education.

TABLE 13-6 EDUCATION AND TRAINING ISSUES

| Issues | Aspects |
|---|---|
| Competency standards | • Generic competencies<br>• Specific competencies (task matrix) |
| Education and training | • The audience being addressed<br>• Content of programs<br>• Methods and presentation forms<br>• Evaluation - assessment and verification<br>• Continual education/improvement |
| Training/education records | • Induction<br>• Information/training/education |

A typical, specific competencies analysis for training can be represented in a task matrix as seen in Figure 13-4 (CHEM Unit 2002a).

| Competency | Workgroup/Roles | | | | |
|---|---|---|---|---|---|
| | Administration | Production | Maintenance | Warehouse | ... |
| SMS-general | ✓ | ✓ | ✓ | ✓ | |
| Permits to work | | ✓ | ✓ | ✓ | |
| Isolations | | ✓ | ✓ | | |
| Emergency plans | ✓ | ✓ | ✓ | ✓ | |
| Incident reporting | ✓ | ✓ | ✓ | ✓ | |
| Other ... | | | | | |

FIGURE 13-4 COMPETENCIES TASK MATRIX (CHEM UNIT 2002A)

### 13.4.7 Employee and Community Consultation

Purpose: To communicate over the life-time of the operations timely and relevant information to key stakeholders and receive feedback from those parties.

Employee and community consultation is one of the greatest challenges in managing major hazard operations. In most national regulations it is a requirement to be exercised by the operator. The key issues related to consultation are given in Table 13-7 (CHEM Unit 2001, 2002c).

TABLE 13-7 CONSULTATION ISSUES

| Issues | Aspects |
|---|---|
| Consultation details | • Operation details<br>• Hazards/major risk contributors<br>• Risk reduction being undertaken<br>• Major accident warning systems<br>• Community/employee safety measures<br>• Major accident over |
| Consultation process | • Consultation area for community<br>• Stakeholders (residents, business, schools, sports associations, ... )<br>• Interest groups (newspapers, action groups, ...)<br>• Plain English terms/language<br>• Clear technical explanations<br>• Liaison officers for stakeholder groups<br>• Consultation groups from community and interested parties |

Poor consultation with employees and especially the local community and interest groups can be a recipe for disaster. Mistrust and suspicion builds leading to community resentment and often hostility to the operations. In extreme cases, cessation of operations or abandonment of planned developments can occur.

EXAMPLE 13-4 COMMUNITY CONSULTATION FOR POOL CHLORINE STORAGE FACILITY

A major international chemical manufacturer and supplier of chlorine-based swimming pool chemicals established with the help of local authorities an effective community consultation process. A committee of local residents, nearby business operators and emergency services personnel met regularly with the operator to discuss, exchange information and consult on the design and operations of the facility. In this way, the local community was fully informed of the hazards, risks and controls associated with the operation. Suspicions were dispelled and harmonious relations between the stakeholders were sustained. Company credibility was secured by a committed Managing Director who acted responsively to any issues raised in the consultation process.

■ ■ ■

**EXAMPLE 13-5 COMMUNITY OUTRAGE AND ACTION AGAINST CORPORATION**

An international chemical company whose operations are located close to local communities suffered a significant continuous leak of chlorine that was eventually isolated by the plant personnel. It released a significant amount that fortunately did not adversely affect the local community. However, vociferous community reaction to the accident led to the shutdown of the plant for over 1 month by government authorities with subsequent investigations by international certifying organizations. The corporation eventually committed themselves to "... improving communications with the local community", something that had been long overdue.

Figure 13-5 provides an overview of the linkages between various components of the Safety Report.

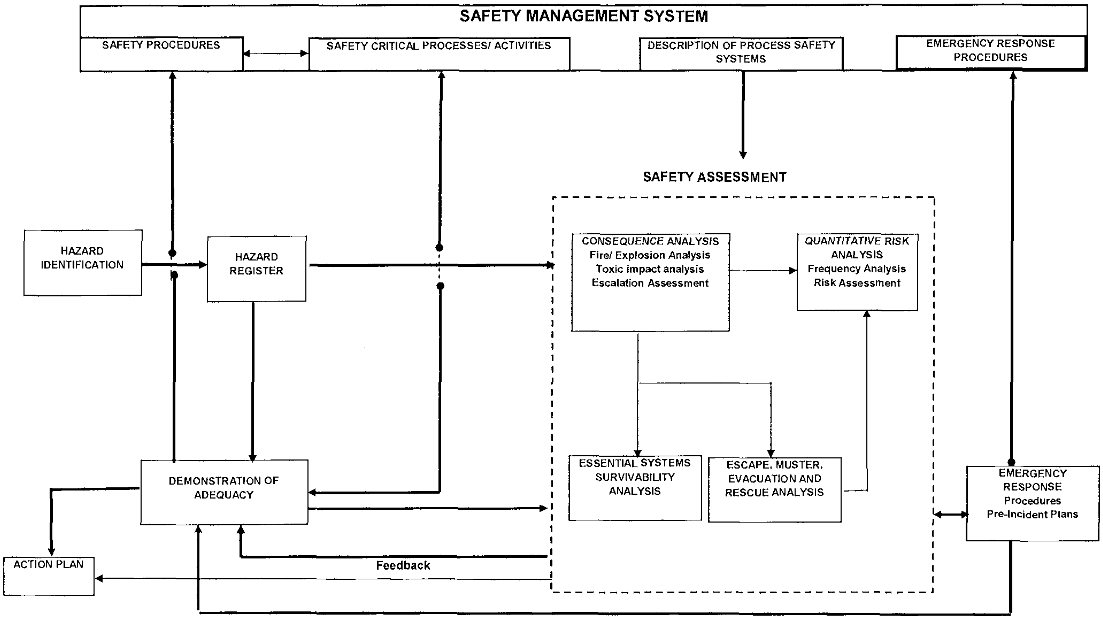


**FIGURE 13-5 PRINCIPAL LINKAGES BETWEEN SAFETY REPORT COMPONENTS**

### 13.4.8 Risk Communication Issues

Section 2.7 has already mentioned the importance of risk perception within risk management practice. Likewise risk communication is an area that needs serious consideration. It too has been the subject of much work over the last 30 years by numerous social scientists (see for example, Kasperson et al. 1988; Sandman 1991; RSSG 1992).

Developing effective risk communications strategies as part of the risk management process is vital and has been the emphasis in several legislative programs (CHEM Unit 2002c; EC1996; Government of Victoria 2000). Bier (2001a, 2001b) has emphasized two major areas of risk communication:

(i) Risk communication to decision-makers
(ii) Risk communication to the public

Both share common elements but in the first case emphasis is often on communicating technical results together with issues of uncertainty, variability and dependence. For the public, additional issues such as message format, use of risk comparisons, audience differences and the use of mental models play an important role.

These approaches emphasize a changing risk communication environment where a strongly educational focus has given way to a more consultative approach (Frewer 2004). The former view held that the public were essentially ignorant of the scientific truth about risk and probability, and hence the focus was on realignment of public views to those of experts in the field. Frewer notes that a changing approach is more prevalent in which the process is more transparent and inclusive across the risk management framework.

In developing some of the early communication strategies, Sandman (1986) outlined 10 common patterns of risk perception that should be considered in addressing effective approaches. These included:

(i) Unfamiliar risks are less acceptable than familiar risks
(ii) Involuntary risks are less acceptable than voluntary risks
(iii) Risks controlled by others are less acceptable than risks under one's own control
(iv) Undetectable risks are less acceptable than detectable risks
(v) Risks perceived as unfair are less acceptable than risk perceived as fair
(vi) Risk that do not permit individual protective action are less acceptable than risks that do
(vii) Dramatic and memorable risks are less acceptable than uninteresting and forgettable ones.
(viii) Uncertain risks are less acceptable than certain risks
(ix) Cross-hazard comparisons are seldom acceptable
(x) People are less interested in risk estimation than risk reduction and they are not interested in either one until their fear has been legitimized

In a similar manner Hance et al (1989) outlined some key issues which need to be considered when dealing with public risk communication. Agencies and industries need to give priority to:

a) Understanding the community's concerns and values
b) Involving people in risk decisions that affect their lives
c) Developing meaningful processes for explaining risks
d) Develop trust and credibility

In carrying out dialogue with a community it is important to:

a) Pay as much attention to perception of risk and concerns as to scientific variables.
   This is because of the importance of the identified patterns of risk perception already mentioned
b) To the extent possible, involve the local community in the decision-making process.
   Because:
   - People are entitled to be involved in issues that directly affect them
   - Involvement in the process creates better understanding
   - Input from those that bear the risk can lead to better policy decisions and solutions
   - Co-operation can improve credibility
c) Pay attention to "process" matters such as phone calls, literature, timing, meetings etc.
d) Release information early.
   Because:
   - People are entitled to it
   - It will leak anyway and can cause distrust and credibility problems
   - More likely to have good community involvement
   - People tend to overestimate risk when information is withheld
e) Address community concerns when explaining risk – don't ignore people or regard them as ignorant!
f) Put data into context
   - Use of comparisons is important, to avoid black and white polarization of issues
g) Choose risk comparisons carefully
   - Don't over or under emphasize risks
   - Need to allay fears in some communities and heighten fear in other cases
h) Acknowledge uncertainty
   - The ability to say "I don't know"
i) Remember that ultimately the communities, not the government or industry, must decide what is acceptable to them
j) Effective communication at all levels of involvement across the life cycle

Much of these concepts and approaches to risk communication are now routinely advocated in public guidelines and technical journals, yet lamentably, often absent in practice. This absence reaps its own rewards. Risk communications to the public by engineers and scientists is often a very difficult task mainly due to the professional training regime. As Lester (2000) comments:

*"Engineers and scientists working with communities need to learn to communicate their technical content in a way that connects with personal perceptions andfeelings"* (pg 80)

Professional training often works against effective public communication and many scientists and engineers are ill-equipped to tackle the task. In contentious situations professional advice from social scientists and communication experts can be advantageous.

Lester contrasts technical communication and persuasive communication. Table 13-8 summarises these concepts.

TABLE 13-8 CONTRASTING TECHNICAL AND PERSUASIVE COMMUNICATION

| Technical Communication | Persuasive Communication |
|---|---|
| Impersonal, objective | Personal, subjective |
| Intellectual response and focus | Emotional response and focus |
| Emphasis on process and content | Emphasis on benefits |
| Information driven | Influence driven |

The concepts in this section must be considered as part of the overall communication of risk assessment and risk management practice to regulatory authorities and local communities affected by the planned activities. Not to do so courts potential disaster.

## 13.5 PERFORMANCE MONITORING

The safety report sets out all the principal components relevant to the safe performance of the operations. Within the safety report a large number of issues are dealt with that impact directly or indirectly on safe operations. As a vital part of the safety report, performance indicators and safety performance measures are an integral part of a "healthy" operation. The challenge is in defining those indicators and obtaining the performance measures that give a true indication of the health of the system. Reliance on simplistic occupational health measures such as lost time injury rate (LTIR) can be very misleading since the measures only reflect one end of the incident spectrum (see section 1.4.1). They are however an indication of safety concern and culture.

Andrew Hopkins (1999), commenting on the Moura Mine disaster in Queensland, Australia, in which 11 men died, writes:

*"It is painfully obvious that a good LTIFR is at best an indication that the processes leading to lost time injuries are being well managed, not that the low frequency/high severity risks are being carefully controlled.*

*On the contrary, the danger is that a single-minded focus on reducing the LTIFR leads systematically to the neglect of catastrophic risk. Where there is potential for catastrophe, safety management must not be driven exclusively by a concern to reduce the lost time injury frequency rate. That way lies disaster, quite literally".* (page 89).

(The terms LTIR and LTIFR - frequency rate denote the same measure, the latter is tautological)

Safety performance raises several key questions that need to be addressed. These include (Mitchison and Papadakis 1999):

(i) How does the "safety culture" of an organization impact on overall performance?
(ii) What are the key aspects of safety performance and how are they to be evaluated?
(iii) What are the best means to identify weaknesses in the safety management system and how can they be addressed effectively?

In nearly all cases, the key mechanism of performance assessment is the audit - not just "hearing" what people say, as important as that is, but delving deeply into the structure, relationships and effectiveness of all systems that seek to address aspects of the corporate safety. In Chapter 15, we cover the auditing of systems and highlight a range of audits, their development and application.

Safety performance can be seen as a control issue for a particular system which has a defined structure. That structure consists of technical and human factors. Reason (1997) uses this view of human performance to analyze the role of people within technical systems. Suitable performance measures are needed to then compare against goals so as to provide the drivers for better performance.

The challenge is in defining and using the best set of performance indicators. This has been the concern of numerous authors in the last 10 years, where the safety report regime is dominant.

Good performance indicators have certain characteristics (NOHSC 2004) such that they are:

(i) controllable or able to be influenced
(ii) relevant
(iii) assessable or measurable
(iv) understandable and clear
(v) accepted as true indicators of performance
(vi) reliable, providing the same measures when assessed by different people, and
(vii) sufficient to provide accurate information but not too numerous

Suitable indicators need to address the principal areas within the safety report and especially within the safety management system. Hence the performance indicators need to be "targeted" to specific aspects of the safety report and hence operational system.

### 13.5.1 Performance Standards

Performance standards for plant equipment is often specified for purposes of plant availability. Section 11.4.2 provides a few indicative examples of performance standards. In the broader context of management of major hazards, however, a much wider range of performance standards need to be established.

Corporate performance standards are often expressed for the following areas of company policies:

(i) Financial

(ii) Environment

- land use
- waste minimization
- pollution control and remediation
- energy performance
- biodiversity

(iii) Safety and health

- safety management
- emergency management
- industrial hygiene
- responsible care
- construction safety
- fleet safety
- regulatory compliance

(iv) Social

- employees
- community
- philanthropy
- innovation

Such performance standards will normally lead to corporate commitments. In the area of health and safety these could be expressed in terms such as:

- No harm to people or the environment ever.
- A corporate culture with shared commitments to zero harm.
  A commitment to continual improvement and the prevention of pollution.

These types of general statements require firm measures or indicators in order to provide information for feedback into the corporation and a demonstration of these commitments. The next section discusses this in detail.

**EXAMPLE 13-6 CORPORATE STANDARDS**

In line with many major corporations, the Eastman Kodak Company sets HSE Performance Standards to establish best practice. In the case of Kodak, it specifies 29 corporate standards in the four key areas of Environment, Safety, Health and Medical. Many corporations set specific performance objectives over fixed timeframes such as 5 years to help tackle key concerns. In the case of Kodak the 2004-2009 environmental goals involve emission reductions of specific chemicals and Greenhouse gases (GHGs) by target amounts as well as set targets for conservation of resources such as energy and water use.

http://www.eastman.com

### 13.5.2 Key Performance Indicators (KPIs)

KPIs for major hazard operations have been the focus of much research and debate (Hurst et al. 1996; Bellamy and Brouwer 1999; Mitchison and Papadakis 1999;

Santos-Reyes and Beard 2002; Basso et al. 2004; OECD 2003). Much of this activity has been driven by the regulatory frameworks such as Seveso II, COMAH (UK) and OSHA (USA).

Much has been written about performance indicators as a vital measure of the "health" of safety report components and safety management systems. Earlier approaches led to tools such as:

(i) PRIMA (Process risk management audit), and
(ii) SAQ (Safety attitude survey questionnaire)
(iii) AVRIM2 (Arbeidsveiligheidsrapporten)

These were audit approaches derived from the European Community Project on Auditing and Safety Management for Safe Operation and Land Use Planning (CEC EV5V-CT92-0068) between 1993-1994.

Various direct and indirect measures were included in such tools including:

(i) Accident measures: Major, minor, near-miss, ...
(ii) Loss of containment measures: LOC and Lines of Defence,
(iii) Fatality and injury measures: FAR, LTIR, ...
(iv) Attitudinal measures: to safety, procedures, ...

In some cases, composite scores for particular aspects of the operation were computed. Weighting of raw scores was often used to prioritize audit aspects. All these approaches depend on targeted auditing by internal and external parties to ensure completeness and to help address quality issues (see Chapter 14).

One of the most important issues in performance monitoring is the capture of both *latent factors* as well as *immediate factors* for both *technical* and *human aspects* in the operation (Santos-Reyes and Beard 2002). This takes seriously the accident framework espoused by Reason (1997) where latent factors associated with the design and operation are often activated by an immediate or initiating event, such as a loss of containment. The latent factors play an important role in accident propagation.

Similar approaches have occurred in the nuclear industry (Khatib-Rahbar et al. 2000) where a hierarchical performance indicator (HPI) regime was developed to cluster PIs into groups that would aid in:

(i) predicting future performance
(ii) identifying aspects of the safety culture and organizational influences
(iii) signalling deteriorating performance.

The high level PI measures were related to safety indicators (SI) to ensure that the most meaningful PIs were tracked. PI measures were defined in 3 levels (high, medium and low) depending on the potential relative change in the SI. This led to the generation of risk increase factors (RIFs). This provides a framework for a "live" safety report.

One of the most comprehensive approaches to the issue of performance indicators is the work of the OECD Working Group on Chemical Accidents (OECD 2003). The study has provided guidelines on the development of safety performance indicators (SPIs) for three main stakeholder groups:

(i) Industry groups
(ii) Public authorities
(iii) Communities and the public

The important concept underlying this work is the use of 2 broad indicator groups:

a) Outcome indicators: being measures of the extent of improvement in performance given in terms of a percentage or ratio. It provides the basis for measurable improvements in the system.
Such general indicators could be:
- Reduction of chemical risks from the operation.
- Extent of interaction and collaboration with public authorities.
- Extent of communication with local community.
- Reduction in hazardous inventories.

b) Activities indicators: being the measures of actions taken that lead to improvements in safe operation.
Such activity indicators could be:
- Procedures for systematic risk reduction measures over the plant life cycle.
- Program and liaison personnel for public authority consultation.
- Resources available for facilitating community involvement.
- Mechanism to seek inventory reduction.

The SPIs cover a wide range of socio-technical aspects related to the safe operation of chemical and major hazard activities. They provide a comprehensive basis for assessing the "health" of an operation from 3 key perspectives.

Table 13-8 gives a summary of the SPIs relevant to Industry, Public authorities and Communities.

TABLE 13-9 SUMMARY OF SAFETY PERFORMANCE INDICATORS (SPI)

| Stakeholder | General SPI areas |
|---|---|
| Industry | • Policies and general management of safety (leadership, goals, ...)<br>• Administrative procedures (HAZID, management of change, ...)<br>• Technical aspects (design, engineering, inherently safer designs, ...)<br>• External co-operation (public, regulators, ...)<br>• Emergency preparedness (internal, external, ...)<br>• Accident, near-miss reporting and investigation |
| Public authorities | • Internal organization (personnel, goals, ...)<br>• Legal framework (land use planning, safety reports, permits, ...)<br>• External co-operation (co-ordination among authorities, non-government, industry, ...)<br>• Emergency preparedness (planning, co-ordination, response, ...)<br>• Accident reporting (near-miss, lessons, follow-up, ...) |
| Communities and the public | • Prevention of accidents (information acquisition, communication)<br>• Emergency preparedness (information, participation, ...)<br>• Response and follow-up (communication, participation, debriefing, ...) |

## 13.6 THE ROLE OF INHERENT SAFETY IN MANAGING RISKS

The concepts of inherent safety (IS) were dealt with in section 12.3. In the case of major hazards it is vital that the concepts are exercised from the very inception of a project. Failure to do so inevitably leads to sub-optimal designs and can impact on operational performance. It is also a costly exercise to implement significant process design changes well into the process life cycle.

In dealing with major hazards, the following areas remain major challenges for applying inherently safer practices over the process life cycle:

(i) Site or route selection
Where key considerations should be:

- available land
- external hazards (nearby industries, major port facilities, motorways)
- sensitive land uses near to transport routes or fixed sites

(ii) Research phase
Including:

- raw material choices (substitutes, green chemicals)
- chemical reaction pathways (pressure and temperature levels)
- materials (temperature limits, corrosion)
- reactor types (vapour, multiphase, liquid phase)

Each of these helps reduce latent failures in the system and mitigates impacts.

(iii) Process development phase
Includes the ISD pyramid shown in Figure 12-3

(iv) Detailed design
Including:

- specific equipment integrity
- control systems design (distributed control system, DCS integrity)
- fail-safe features
- environmentally tolerant systems
- passive vs. active protection systems
- minimizing leak potential in equipment and piping design (e.g. all welded systems)
- routing of control and power supplies
- minimizing sampling points and potential loss of containment points
- human factor considerations (ergonomic designs, human-machine-interface (HMI) concepts)

It is vital in the context of major hazards that each of the foregoing areas are seriously considered so as to reduce potential incidents. The reality in many commercial engineering environments is often otherwise, with little consideration of IS principles, but only a willingness to "tinker" with previous designs.

(i) Serious application of IS principles goes a long way to reducing major hazard risks.

## 13.7 BEHAVIOURAL ASPECTS OF MAJOR HAZARDS MANAGEMENT

Organizational effectiveness is a prime focus of many corporations in an attempt to improve the performance of all personnel at all levels in the organization. As Sellers and Marsh (2003) indicate, it is the effectiveness of connecting people to systems. The superlative performance of corporations in the area of system safety takes seriously the human factors as an integral aspect of design and operation.

The types of problems that Sellers and Marsh refer to in discussing behaviour-based approaches include:

(i) Increasing the likelihood that right behaviour will occur.
(ii) Engaging personnel in the improvement process.
(iii) Assuring upstream diagnosis of system deficiencies.
(iv) Relying on other than punitive actions as a means of improvement.
(v) Encouraging groups and individual to assume responsibility for improvement.
(vi) Making better use of positive feedback to aid performance of personnel.

These challenges and many others are often the focus of corporation-wide initiatives. For example the Tripod Delta approach adopted by Shell International (Hudson et al. 1994) focussed clearly on addressing "latent" failures within the organization with a special emphasis on human error. It relied heavily on the work of Reason (1990) who outlined key approaches to human error analysis and prevention. The approach has had significant benefits within Shell International.

In a similar manner the DuPont Safety Training Observation Program (STOP) aims at addressing many behavioural issues related to safety performance (DuPont 2004). It consists of a series of self-implemented programs focussing on supervision, employee behaviour, personnel interdependence and ergonomic issues. It is a widely adopted program by major international corporations. Other corporations have their own brand of systems, and other frameworks such as Human Error Risk Management for Engineering Systems (HERMES) or Technique for Human Error Rate Prediction (THERP) have been proposed and used (Cacciabue 2004; Swain 1983).

As a means of informing organizations in the UK of the importance of human factors in industrial safety, the HSE provided useful guidance notes on a range of issues (HSE, 1999). The principal, top 10 issues identified by UK COMAH assessments (Anderson, 2003) included:

(i) Organizational change and change management
(ii) Demanning and staff levels
(iii) Training, competence and supervision issues
(iv) Shift and overtime fatigue
(v) Handling process alarms

(vi) Compliance with safety critical procedures
(vii) The organizational culture in terms of safety
(viii) Communications
(ix) Ergonomics or human factors in design
(x) Maintenance error.

**EXAMPLE 13-7 PROCESS ALARMS**

It was recognized in the design of an industrial batch reactor that an emergency water quench system was required in case of reaction runaway. A system was installed that required manual activation by the operator.

On the first occasion that the activation was needed, the operator was busy with other tasks and unable to respond within an adequate timeframe. The reactor overpressured partially releasing its contents. Here there was inadequate analysis of human factors and an unreasonable demand on the operator. An automatically activated quench system would have been more appropriate.

These are the focus of many work systems that seek to improve performance. They are recurring themes in all industries. In a review of methods to tackle many of these issues Simpson et al. (2003) developed a series of guidelines aimed at assessing performance of systems in a number of the key areas. This provided scores for the five areas of:

- accident investigation
- emergency response
- procedures
- communications
- availability of information

The outcomes allowed refinement, correction and redevelopment of the relevant systems.

In commenting on the negative issues surrounding human factors and behaviour based approaches the UK COMAH personnel noted (Anderson 2003) a number of important deficiencies including:

(i) An almost exclusive focus on engineering and hardware issues.
This bias did not adequately consider human performance aspects. Can operators respond adequately to alarms? Is there time to respond? Is the task too complex? What information processing skills are needed for diagnosis? A few typical issues faced in this area.

(ii) A focus on occupational safety.
Here the issues relate to not adequately addressing human errors in maintenance but rather an exclusive concern on how maintenance can be safely carried out via adequate isolation, confined entry procedures and the like.
Given the fact that maintenance errors can lead to "latent" failures that could eventually play a role in a major accident, the need to focus on human factors is essential.

**EXAMPLE 13-8 SPRAY MAINTENANCE FAILURE**

During maintenance procedures on a spray system for an ammonia absorber, the spray head was incorrectly oriented when reinstalled. Over a period of months, the spray subsequently eroded an inner steel sleeve, releasing an acidic solution into downstream units. This eventually led to major blockages in other spray systems with a major emergency response required to avert a significant environmental accident. This is a case where human factor related to maintenance procedures and supervision were found wanting.

(iii) Focus on the short term
When some human factor issues are considered, they are often done so for compliance purposes rather than long term benefits. This is the "short sighted" management perspective.

(iv) Ownership
This relates to the use of outside agencies or consultants that provide specialist human factors advice but there is little or no transfer of ownership to the organization. This continues to be an issue in the whole area of risk management where outside agencies are involved.

**EXAMPLE 13-9 RISK ASSESSMENT PRACTICE**

A medium sized company required to do a risk assessment (RA) for a large mixed hydrocarbon storage terminal hires an external consultant to carry out the risk assessment for regulatory approvals. Little if any ownership occurs at the end of the development process, since the risk assessment is seen as an impost to be endured and submitted as just part of the paperwork.

(v) Realism
There is often a lack of realism in attributing performance levels to personnel, especially in emergency situations. In these cases, where significant events are taking place, substantial amounts of data are being generated and processed, the reliability of the best trained personnel dramatically reduces. This often needs to be acknowledged in assessments and in design of systems.

(vi) Failure in identifying safety critical issues
For MHF sites, there is often a lack of identifying and analyzing safety-critical tasks, roles, responsibilities and procedures. This is important in defining where human intervention plays a critical role in MHF operations, especially related to major hazard incidents.

It can be convincingly argued that organizational effectiveness demands that human factor and behavioural issues be comprehensively addressed in the management of MHFs. Without this, there is a vast range of latent factors lurking in the system, waiting to be unleashed and destined to cause potential disasters. Remember Bhopal, Piper Alpha or Longford as reminders.

## 13.8 REVIEW

In this chapter we have highlighted three major aspects of risk management applied to major hazard facilities. These have emphasized the role of the safety report as a comprehensive, "living" document that treats the MHF risk in a holistic manner.

Notwithstanding the importance of the safety report and the huge amount of learning acquired through such an exercise, the areas of inherently safer plant design and the vital role of behavioural aspects must be emphasized. They are often the forgotten ingredients in a holistic approach to MHF risk management.

Achieving integrity of all the components mentioned in this chapter is not an easy task. It requires a high level of organizational effectiveness, which in itself must be priority in the risk management process. We need to emphasize KPIs that actually target the right areas of MHF design and operation to ensure continually improvement. As seen in this chapter, occupational health and safety KPIs are simply not enough to address the key issues.

## 13.9 REFERENCES

Anderson, M. 2003, 'Human factors and COMAH: a regulator's perspective', Hazards XVII Process safety - fulfilling our responsibilities, *Institution of Chemical Engineers Symposium Series No.149*, Rugby, UK, pp. 785-792.

Basso, B., Carpegna, C., Dibitonto, C., Gaido, G., Robotto, A. and Zonato, C. 2004, 'Reviewing the safety management system by incident investigation and performance indicators', *Journal of Loss Prevention in the Process Industries*, vol. 17, pp. 225-231.

Bellamy, L.J. and Brouwer, W.G. 1999, 'AVRIM2, a Dutch major hazard assessment and inspection tool', *Journal of Hazardous Materials*, vol. 65, pp. 191-120.

Bier, V.M. 2001a, 'On the state of the art: risk communication to decision makers', *Reliability Engineering and System Safety*, vol. 71, pp. 151-157.

Bier, V.M. 2001b, 'On the state of the art: risk communication to the public', *Reliability Engineering and System Safety*, vol. 71, pp. 139-150.

Britton, T. 2003, 'Lessons learnt about preparing COMAH safety reports' in Hazards XVII Process safety - fulfilling our responsibilities, *Institution of Chemical Engineers Symposium Series No.149*, Rugby, UK.

Cacciabue, P.C. 2004, 'Human error risk management for engineering systems: a methodology for design, safety assessment, accident investigation and training', *Reliability Engineering and System Safety*, vol. 83, pp. 229-240.

CCPS 1994, *Guidelines for Implementing Process Safety Management Systems*, Center for Chemical Process Safety, AIChE, New York.

CHEM Unit 2001, *Community consultation and communication guidelines: The Dangerous Safety Management Act 2001*, Queensland Government, Department of Emergency Services, Australia.

CHEM Unit 2002a, *Guidelines for Major Hazard Facilities E: Education and Training*, CHEM Unit, Department of Emergency Services, Queensland Government, Australia, MHF-05-OGL-1.

CHEM Unit 2002b, *Safety Management Systems: Guidelines for major hazard facilities (F)*, CHEM Unit, Department of Emergency Services, Queensland Government, Australia, Available at: http://www.emergency.qld.gov.au/chem/ .

CHEM Unit 2002c, *Guidelines for Major Hazard Facilities G - Community Consultation*, CHEM Unit, Queensland Government, Australia, MHF-07-OGL-1.

CHEM Unit, 1998, *Emergency Planning: Guidelines for Hazardous Industry*, Chemical Hazards and Emergency Management Unit, Dept. Emergency Services, Queensland State Government, Australia, ISBN 0724293108.

Chiles, J.R. 2001, *Inviting disaster: Lessons from the edge of technology*, Harper Business, New York, USA.

Covello, V.T. and Allen, F.W. 1988, *Seven cardinal rules of risk communication*, OPA-87-020, US Environmental Protection Agency, Washington DC, USA.

Dőrner, D. 1996, *The Logic of failure: Recognizing and avoiding error in complex situations,* Perseus Books, Cambridge, USA.

DuPont 2004, 'DuPont Workplace Safety Training Materials, STOP Programs', Available at: http://www.dupont.com/stop/index.html .

EC 1996, 'Seveso II Directive (96/82/EEC) on the control of major accident hazards involving dangerous substances', *Official Journal of the European Communities*, L10/13-33.

Fleming, M. and Lardner, R. 1999, 'When is a risk not a risk?', *The Chemical Engineer*, pp. 12-16, July 8.

Frewer, L. 2004, 'The public and effective risk communication', *Toxicology Letters*, vol. 149, pp. 391-397.

Government of Victoria 2000, *Occupational Health and Safety (Major Hazard Facilities) Regulation*, Gazetted July 1, Melbourne, Australia.

Greenhalgh, G. 1994, *Expecting Disaster: Risk and impending disaster in a historical and social perspective*, Centre for Risk Research, Stockholm School of Economics, ISBN HHS-CFR-A-2-SE.

Hance, B.J., Chess, C. and Sandman, P. 1988, 'Improving Dialogue with Communities: A risk communication manual for government', Environmental Communication Research Program, Rutgers University, New Brunswick, New Jersey, USA.

Hopkins, A. 1999, *Managing major hazards: The lessons of the Moura Mine disaster*, Allen & Unwin, Sydney, Australia.

HSE 1997, *Successful health and safety management*, HS(G)65, Health and Safety Executive, Sudbury, UK.

HSE 1999, *Reducing error, influencing behaviour*, HS(G)48, 2nd edn, HSE Books, UK.

Hudson, P.T.W., Reason, J.T., Wagenaar, W.A., Bentley, P.D., Primrose, M. and Visser, J.P. 1994, 'Tripod Delta: Proactive Approach to Enhanced Safety', *Society of Petroleum Engineers*, pp. 58-62, January.

Hurst, N.W., Young, S., Donald, I., Gibson, H. and Muyselaar, Andre, 1996, 'Measures of safety management performance and attitudes to safety at major hazard sites', *Journal of Loss Prevention in the Process Industries*, vol. 9, no. 2, pp. 161-172.

Kasperson, R.E., Renn, O., Slovic, P., Brown, H.S., Emel, J., Goble, R., Kasperson, T.X. and Ratick, S. 1988, 'The Social Amplification of Risk: A Conceptual Framework', *Risk Analysis*, vol. 8, no. 2, pp. 177-187.

Kelly, T.P. and McDermid, J.A. 2001, 'A systematic approach to safety case maintenance', *Reliability Engineering and System Safety*, vol. 71, pp. 271-284.

Khatib-Rahbar, M., Erikson, H. and Sewell, R.T. 2000, 'A New Approach to Development of a Risk-based Safety Performance Monitoring System for Nuclear Power Plants', *Specialist Meeting on Safety Performance Indicators*, Madrid, Spain.

Kirchsteiger, C. 2000, 'Availability of Community level information on industrial risks in the EU', *Transactions of Institution of Chemical Engineers*, vol. 78, Part B, pp. 81-90.

Kletz, T. 1993, *Lessons from disasters: how organizations have no memory and accidents recur*, Institution of Chemical Engineers, Rugby, UK.

Kletz, T. 2003, *Still going wrong: case histories of process plant disasters and how they could have been avoided*, Gulf Professional Pub., Boston, USA.

Lees, F.P. and Ang, M.L. 1989, *Safety Cases within the CIMAH Regulations, 1984,* Butterworths, London, UK.

Lester, M. 2000, 'Communicate Risk Effectively', *Chemical Engineering Progress*, pp. 79-83, June.

Mitchison, N. and Papadakis, G.A. 1999, 'Safety Management Systems under Seveso II: Implementation and Assessment', *Journal of Loss Prevention in the Process Industries*, vol. 12, pp. 43-51.

MOLNZ 1994, *Managing Hazards to Prevent Major Industrial Accidents*, Dept. of Labour, Wellington, New Zealand.

NOHSC 2004, 'Positive Performance Indicators for OHS Part I National Occupational Health and Safety Commission, Worksafe Australia, ISBN 0644352663.

National Occupational Health and Safety Commission (NOHSC). *Control of Major Hazard Facilities*, National Occupational Health and Safety Commission, Commonwealth of Australia. NOHSC: 2016:1996.

NSWDOP, 1995, *Guidelines for the development of Safety Management Systems*, HIPAP 9, NSW Dept. of Urban Affairs, Australia.

OECD, 2003, *Guidance on Safety Performance Indicators: Companion to OECD Guiding Principles for Chemical Accident Prevention, Preparedness and Response*, OECD Environment, Health and Safety Publications no. 11, Paris, France.

Occupational Safety and Health Administration (OSHA). *Process safety management of highly hazardous chemicals*. Occupational Safety and Health Administration, Federal Register, Washington D.C., USA. OSHA 29 CFR 1910.119:1992.

Papadakis, G.A. and Amendola, A. 1997, 'Guidance on the Preparation of a Safety Report to Meet the Requirements of Council Directive 96/82/EC (Seveso II)', Joint Research Centre, EC, EUR17690EN, Luxembourg.

Perrow, C. 1999, *Normal accidents: Living with high risk technologies*, Princeton University Press, USA.

Reason, J. 1997, *Managing the risks of organizational accidents*, Ashgate, Aldershot, UK.

Rimington, J.D. 1995, 'Risk and the regulator: Puzzles and Predicaments', *Transactions of Institution of Chemical Engineers*, vol 73, Part B, pp. 173-181.

RSSG 1992, *Risk: analysis, perception and management*, Royal Society Study Group, The Royal Society London.

Sandman, P.M. 1986, 'Getting to Maybe: Some communications aspects of siting hazardous waste facilities', *Seton Hall Legislative Journal*, pp. 437-465, Spring.

Sandman, P. 1991, Environmental Communication Research Program, Ryders Lane, Rutgers University, New Brunswick, USA.

Santos-Reyes, J. and Beard, A.M. 2002, 'Assessing safety management systems', *Journal of Loss Prevention in the Process Industries*, vol. 15, pp. 77-95.

Sellers, G. and March, C. 2003, 'Using behaviour-based methods to improve organizational effectiveness', Hazards XVII, Process Safety - fulfilling our responsibilities, *Institution of Chemical Engineers Symposium Series No.149*, Rugby, UK, pp. 173-181.

Sorensen, J.M. 2002, 'Safety Culture: a survey of the state-of-the-art', *Reliability Engineering and System Safety*, vol. 76, pp.189-204.

Simpson, G., Tunley, C. and Burton, M. 2003, 'Development of human factor methods and associated standards for major hazard industries', HSE Research Report 081/2003, HMSO, Norwich, UK.

Swain, A.D. and Guttmann, H.E. 1983, *Handbook on human reliability analysis with emphasis on nuclear power plant application*, NUREG/CR-1278, Washington D.C., USA.

Tenner, E. 1997, *Why things bite back: Technology and the revenge of unintended consequences*, Vintage Books, USA.

Turner, B. 1978, *Man made disasters: the failure of foresight*, Wykeham.

US Environmental Protection Agency (EPA). *Risk management programs for chemical accidental release prevention*, US Environmental Protection Agency, Federal Register, Washington D.C., June, Final Rule, 40 CFR Part 68:1996.

VEC 1991, ' 'Learning from Accidents' the Piper Alpha oil platform disaster: messages for managing safety', VEC International Production for ICI Group Safety.

White, M.P., Pahl, S., Buehner, M. and Haye, A. 2003, 'Trust in risky messages: the role of prior attitudes', *Risk Analysis*, vol. 23, no. 4, pp. 717-725.

Worksafe Victoria 2001, 'An overview of the Safety Case Regime under the Occupational Health and Safety (Major Hazard Facilities) Regulations' Guidance Note MHD GN-3, Government of Victoria, Australia.

## 13.10 NOTATION

| | |
|---|---|
| ACMH | Advisory Committee on Major Hazards (UK) |
| ALARP | As low as reasonably practicable |
| AN | ammonium nitrate |
| AVRIM2 | Arbeidsveiligheidsrapporten (The Netherlands) |
| CHEM | Chemical Hazard and Emergency Management |
| CIMAH | Control of Industrial Major Accident Hazards (precursor to COMAH) |
| COMAH | Control of Major Accident Hazards |
| EC | European Commission |
| EPCRA | Emergency Planning and Community Right-to-know Act |
| FAR | Fatal accident rate |
| GHGs | Greenhouse gases |
| HAZID | Hazard identification |

| | |
|---|---|
| HERMES | Human error risk management for engineering systems |
| HPI | Hierarchical performance indicator |
| HSE | Health and Safety Executive (UK) |
| KPIs | Key performance indicators |
| LOC | Loss of containment |
| LOPA | Layer of protection analysis |
| LTIFR | Lost time injury frequency rate |
| LTIR | Lost Time Injury Rate |
| MI | Major incident |
| MHFs | Major hazard facilities |
| PI | Performance Indicator |
| PRIMA | Process Risk Management Audit |
| RIFs | Risk Increase Factors |
| SAQ | Safety Attitude Survey Questionnaire |
| SARA | Superfund Amendments and Reauthorization Act |
| SCA | Safety Critical Activities |
| SCP | Safety Critical Processes |
| SFAIRP | So far as is reasonably practicable |
| SI | Safety indicator |
| SMS | Safety management system |
| STOP | Safety Training Observation Program (DuPont, USA) |
| THERP | Technique for human error rate prediction |
| USEPA | United States Environmental Protection Agency |

# 14

# AUDITING PROCESS SAFETY MANAGEMENT SYSTEMS

*"No single measure can meet all of these properties (efficient, understandable, practicable, can be integrated into normal operational activities and promotes involvement), but it is useful to at least know what one should look for in a search of improved measures of safety performance"*

*W E Tarrants, 1980*

It has been recognised, especially after the Piper Alpha disaster that "... safety is crucially dependent on management and management systems" (Lord Cullen 1990). When we have a Safety Management System (SMS), we should be able to measure its performance. Two basic questions arise:

1. By what standards are we to assure that the integrity of a process facility is maintained through its life cycle?
2. How do we know that we are actually achieving the standards in practice?

Defining safety critical activities and setting performance standards for these activities provides the answer to the first question. Regular auditing of the SMS and comparing the audit findings against the performance standards answers the second question.

In this chapter, we shall describe how performance standards can be set, and review the principles and methods of auditing process safety management systems.

## 14.1 AN OVERVIEW OF SYSTEMS AUDITING

### 14.1.1 Maintaining SMS performance

In Chapter 11, we have seen that SMS functions require an interface with the auditing component at all stages of SMS development, implementation, and monitoring. In fact without effective auditing, and monitoring the key performance indicators (KPIs) that indicate the health of the system, one would never know how effective the SMS is, and where efforts and resources should be targeted for improving safety performance. Figure 11-1 reinforces the importance of auditing.

All systems of control tend to slip in their effectiveness over time, as changes occur in the facility and in the organisation. If this deterioration is not detected and corrective actions taken, the SMS is no longer as effective in hazard control. It has been said "nothing rusts faster than a procedure". Therefore, regular auditing of the system is necessary.

**EXAMPLE 14-1 SYSTEMS DETERIORATE OVER TIME**

A process facility, a subsidiary of a large corporation, stored and handled a number of hazardous materials. The site safety coordinator was an enthusiastic individual who ensured that the SMS procedures were followed effectively, and had implemented a number of improvements. The coordinator also organised regular internal audits.

A mandatory independent audit of the facility, required as part of licensing conditions, was undertaken and the site was judged to be one of the best-managed sites. After that audit, the safety coordinator had moved on, and the position had not been filled for some time. No internal audits were conducted. By the time a new coordinator was appointed, the effectiveness of the procedures had deteriorated significantly.

Two years later, the same auditor was invited to conduct another independent audit to comply with regulatory requirements. The auditor was disappointed that a well-managed site could be allowed to deteriorate so rapidly. Had the internal audits been conducted, the problems could have been identified and solved much earlier.

There are few important lessons in the above example:

- Systems do deteriorate over time due to changes
- Auditing is the best tool to identify the fall in standards and take corrective actions
- No performance standard was set in the SMS on the need for internal audits in between scheduled biennial regulatory audit.
- The blame does not rest with the facility management alone, but with the corporate management as well.
- Without the regulatory 'stick' to wield, some audits may not have been conducted at all.
- Systems should not be dependent on individuals. If this happens, then there is effectively no system in place.

The important aspects to note in the auditing regime are:

- Auditing applies to all aspects of SMS, from systems development, implementation and monitoring.
- Auditing applies to the entire life cycle of the facility through all the stages.
- Provisions for effective auditing should themselves form part of the SMS framework. Auditing is not external to the management system, but an integral part of it, though external parties may undertake the audit or audits from time to time.
- Without a set of performance standards (PS) and key performance indicators (KPI), an audit can only make general comments in relation to industry best practice, but will be unable to focus on specific remedial measures. An audit recommendation such as "Process Safety Management (PSM) performance must be improved" does not lead one anywhere.
- It is more important to ask "how well are we doing against industry best practice?" rather than, "have we complied with regulatory requirements?" which would follow as a matter of course, if industry best practice can be achieved.
- Where performance standards are set, the following issues are of relevance (Chia et al. 2004):
    - fit for purpose
    - easily measurable
    - appropriate mixture of reactive ('lag') and proactive ('lead') indicators have been developed
    - appropriately rationalised to a manageable set
    - accepted by all stakeholders

### 14.1.2 Levels of Safety Culture

Safety culture in organisations spans a wide spectrum. On the one hand there is a superlative safety program combining process safety, OH&S, and behavioural sciences for human error minimisation, and at the other end, there is no check against non-compliance with codes and regulations.

The range of safety cultures is illustrated in Figure 14-1.

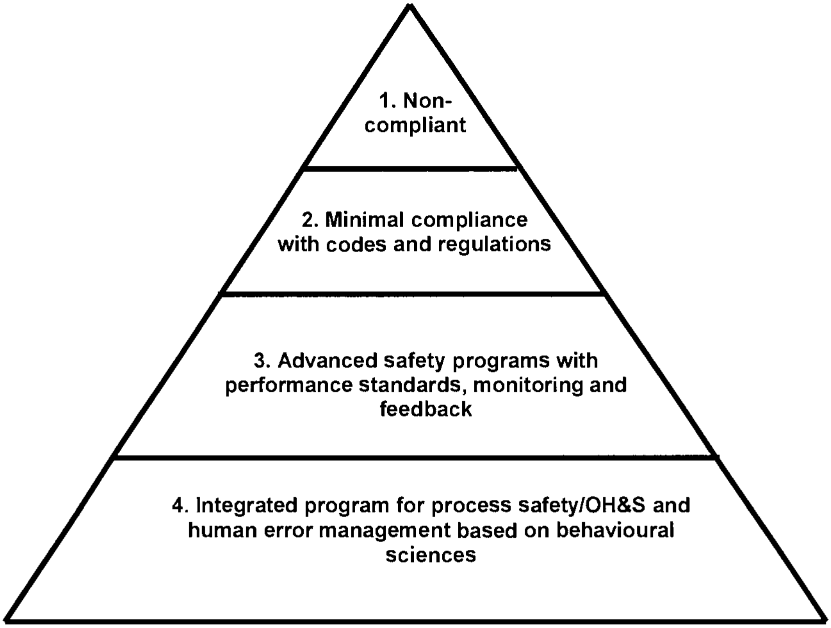

1. Non-compliant
2. Minimal compliance with codes and regulations
3. Advanced safety programs with performance standards, monitoring and feedback
4. Integrated program for process safety/OH&S and human error management based on behavioural sciences

FIGURE 14-1 RANGE OF SAFETY CULTURES

As part of the audit, it is necessary to undertake an evaluation of the prevailing safety culture. The principal objective is to move down the pyramid in Figure 14-1 as far as possible, aiming to perform progressively better than minimal compliance with codes and regulations. This does not always happen, where regulatory compliance is viewed as the last word in accident prevention. Most companies are expected to hover between Levels and 2 and 3.

In a survey of 100 companies following the introduction of OSHA Rule 1910.119 (OSHA 1992), Schweer et al. (2000) found that some companies who were "PSM leaders" from the inheritance of a strong safety culture before OSHA rule was introduced, had slipped into a mode of compliance. At the same time, non-compliant companies "PSM laggers" began to catch up with compliance (see Figure 14-2).

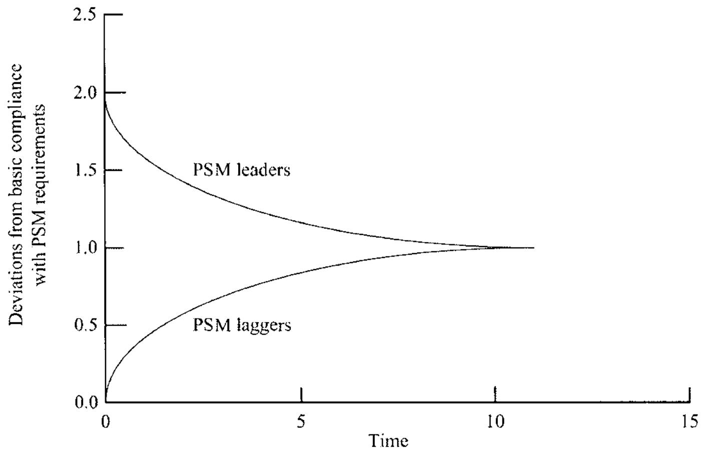


FIGURE 14-2 INDUSTRY COMPLIANCE PERFORMANCE WITH PSM

(Source: Schweer et al. 2000)

Tweeddale (2003) has described the measurement of safety culture and climate in detail.

### 14.1.3 Areas Covered by Audit

There are three basic areas of coverage of an audit for measuring safety performance (EPSC 1996):

- Systems and procedures
- Plant and equipment
- People

All the SMS elements described in Chapter 11 are subject to the audit. These can be divided into the three above areas as shown in Table 14-1.

TABLE 14-1 AUDIT ELEMENTS AND AREAS COVERED

| Area Covered | SMS Element |
|---|---|
| Systems and procedures | Major accident prevention policy (MAPP) |
| | Organisation |
| | Performance standards |
| | Hazard identification and assessment |
| | Documentation, safety report |
| | Management of change |
| | Systems of work |
| | Inventory management |
| | Emergency plans |
| | Investigation and reporting |
| | Periodic Review |
| | Improvement plans |
| Plant and equipment | Hazard prevention, mitigation measures |
| | Mechanical integrity |

| Area Covered | SMS Element |
|---|---|
| | Safety critical equipment |
| People | Staff selection and training |
| | Contractors |
| | Communications |
| | Competence |

Although the list in Table 14-1 shows single elements, in practice, auditing involves an integrated series of checklists that can overlap between the elements, with a large number of checklist items under each element.

## 14.2 THE PROCESS SAFETY MANAGEMENT AUDIT

### 14.2.1 Principal Objectives

The principal objective of an SMS audit is

*"to check and verify that the control measures for major hazard control in the facility are effective, in order to ensure continued safe operation of the facility."*

This principal objective leads to a number of activities:

- Review the SMS for its completeness and suitability to control the hazards in the facility
- Review the adequacy of procedures developed to implement the SMS
- Verify that performance standards and key performance indicators have been developed for the procedures for measuring actual performance
- Examine how the procedures are actually being applied in practice, and their effectiveness
- Measure safety performance of systems and procedures, plant and equipment, and people
- Identify non-conformances of procedures in actual practice to expected practice
- Identify deviations from performance standards
- Identify corrective actions to close the deviations. It is essential that the corrective actions identify root causes of the deviations and address them, and not just the immediate causes.
- Implement corrective actions and close out.

### 14.2.2 Benefits of Audit

There are a number of direct and indirect benefits that result from a sound audit process.

- Helps to identify problem areas, and areas of non-compliance and poor performance

- Direct involvement of both management and staff at all levels in the audit process reinforces the commitment to safety
- Independent audits help to identify problems experienced by the operators, which might not have otherwise been communicated to the management
- Helps to set priorities on safety improvement measures
- Provides feedback to management on improvements to policies, systems and procedures
- Ensures continued compliance with regulatory requirements
- Provides assurance on the quality and integrity of process safety in the facility
- Reduces the potential for process incidents
- Provides input to quantitative risk analysis, if management factors need to be integrated into the analysis. Depending on the prevailing safety culture, this may be one way of demonstrating to a complacent but self-assured management that all is not well.

### 14.2.3 Levels of Audit

An audit can be conducted at different levels, depending on the area of focus. The levels vary between organisations, but the general consensus for industry best practice is:

- Audits at different levels need to conducted
- The frequency of audits at these levels would vary, with lower level audits conducted at intervals more frequent than higher level audits
- At each level of audit, documentation and feedback to the management is an essential requirement
- It is essential that the auditors are independent of specific activity being audited, if in-house audits are conducted
- At each higher level of audit, the findings from previous lower levels of audit and the completeness of closeout of actions arising needs to be covered

Figure 14-3 summarises the various types of audit during the facility life cycle.

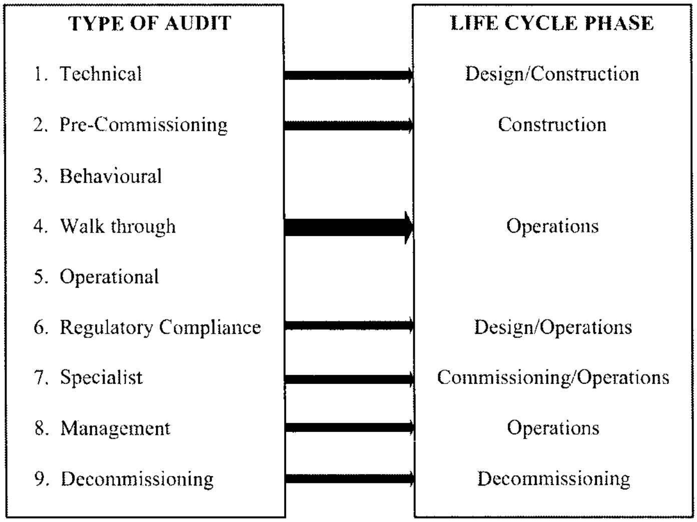


FIGURE 14-3 TYPES OF AUDITS DURING FACILITY LIFE CYCLE

A modular structure for audits has been suggested by McKeever and Lawrenson (1992).

Audits to suit different needs of the organisation, and techniques of auditing are reviewed in CCPS (1993).

### 14.2.3.1 Technical audit

*Are we meeting corporate and industry standards for design and construction?*

The technical audit reviews the design and construction standards of the equipment to ensure that the facility meets the corporate and industry standards, such as API or IP standards for the petroleum industry.

The technical audit is initially undertaken at the design stage of the facility life cycle. For plants in the chemical process industry, this review is updated during the operational phase if there have been:

- changes to the facility, as part of management of change (MOC)
- changes to operating conditions or feedstocks
- changes to codes and standards

For oil and gas offshore facilities and upstream onshore facilities, this review is undertaken at fixed intervals (generally on a 5 year cycle) as the reservoir conditions may have changed significantly over that period (Wallace 1990).

The main areas covered are:

- Compliance with codes and recommended practices (e.g. API RP 14C - 2001 for offshore installations)

- Safety instrumented systems
- Hazardous area classification
- Relief devices and flare capacity checks
- Equipment and piping capacities
- Operating limits for process variables and design limits of plant

Different areas of the audit can be carried by respective discipline engineers or managers, after consensus agreement by audit team, and lead auditor.

Repeat audits take the form of a gap analysis of changes and their impact on process safety.

**EXAMPLE 14-2 FAILURE TO CONDUCT TECHNICAL AUDIT AT DESIGN STAGE**

A mineral processing facility producing nickel uses solvent extraction to extract the desired metal from the ore leachate. The solvent extraction process uses ammonia as a reagent. The design consists of 3 x 100 tonne anhydrous ammonia tanks.

The process safety standards in mineral processing plants, located close to the mine in remote locations, is not the same as one would expect in the chemical process industry, located close to population centres. The design contractor did not undertake a technical audit of the design. As a result, one important standard (anhydrous ammonia code) was not applied to the design (incompetence of the designer), and another standard (pressure piping code) had been incorrectly applied (Schedule 40 piping used instead of Schedule 80 piping).

Fortunately, pre-commissioning checks were undertaken using a process safety specialist (appointed at the behest of the investment bank), who discovered a number of code non-conformances during the checks. The problem was rectified, but at considerable cost and commissioning delay.

### 14.2.3.2 Pre-Commissioning audit

*Is the plant ready for commissioning in terms of installed safety equipment, approvals, documentation, training, and interfaces with various parties involved?*

This is an important audit, and forms a separate element in process safety management (OSHA 1992). The main objective is to ensure that the installation meets all design and construction requirements.

Pre-commissioning is a vulnerable phase, as there is high pressure on the project to commission the plant and start operating. Failure to undertake a proper audit at this stage could result in extensive delays during commissioning.

Main features of the audit are:

- Licences and approvals
- Safety critical equipment been installed in correct locations
- Loop testing of all control loops and shutdown loops, and interlocks function correctly
- All signs and notices in place
- All equipment and instruments are tagged
- Commissioning procedure in place and commissioning crew trained

- SMS procedures in place and training has been completed
- Pressure testing/leak testing completed
- Rotating equipment checked for alignment and direction of rotation
- Hazardous area classification integrity intact (intrinsically safe barriers for terminations of all field instruments)
- Spades/blinds have been correctly installed for plant sections to be isolated, and spade pressure rating is compatible with line pressure rating
- Interfacing conflict between various vendor equipment/packages, other plants resolved
- Ergonomic issues are addressed
- All process documentation up to date

The audit is conducted by an experienced senior person or team from outside the project, not subject to the same project pressures.

**EXAMPLE 14-3 INTERFACE ISSUES MISSED**

1. Example 12-8 in Chapter 12 illustrates the importance of managing interfaces in a copper smelter.
2. An industrial complex consisted of a number of integrated process plants. Over a period of time, the ownership of the plants was split among three different companies. The common effluent treatment facility was under separate management, but shared by all the plants on site. The effluent treatment plant's new owners also received waste streams from outside the complex.

   When one of the plants in the complex was planning an extension, the question of whether the existing effluent treatment plant would be able to treat the additional waste generated was initially ignored, as the entire attention was focused on the interfaces between existing plant and the new extension under the same ownership. This omission was discovered only when the proposal was submitted for the approval of the environmental authority, which raised a number of questions on the effluents generated and their treatment.

■ ■ ■

### 14.2.3.3 Routine walk through audit

*Does the condition of plant and equipment and quality of housekeeping reflect what we say we do?*

This audit mainly focuses on the physical condition of the plant and equipment, housekeeping standards, and spot checks on systems of work and practices of activities that are being carried out during the audit. The audit is conducted during the operational phase of the facility life cycle.

This audit is useful in obtaining symptoms of problems in safety management, and carried out by auditors from another facility plant within the same organisation.

Important points to note are:

- Take the audit seriously, even though it is an internal audit, as it is part of continual improvement.
- Recognise that improving housekeeping in the plant to make it look good during the audit, and reverting back to where it was after the audit is self-deception.
- The person doing the audit may be a colleague. Do not take offence at adverse findings, but take them as constructive criticism. The same applies to the auditor - it is not a point scoring exercise against another plant.
- If the symptoms indicate that there could be problems in systems of work being implemented effectively, follow up with an investigation to ensure that corrective actions can be developed.

#### 14.2.3.4 Behavioural audit

*Does the level of understanding of, and commitment to process safety by the workforce meet the expectations in the safety policy?*

This is an informal audit involving personnel at all levels, generally carried out during the operational phase. The key aspect of the audit is to find answers for the following:

- Do personnel have the right attitude and aptitude to process safety?
- Are the systems of work being correctly followed by personnel?
- Is there a tendency to take short-cuts?
- Is there effective communication between area operators and control room, and between operators during shift change?
- To what extent there is a sense of complacency towards process safety during day to day activities?

A checklist of behavioural questions needs to be prepared as part of the audit. The audit outcome is a good reflection of the prevailing safety culture.

Page (1992) reports on a successful behavioural audit implemented as the first level of audit, as part of the environmental management system. A number of case study examples on human factors and behavioural issues are provided by Tweeddale (2003).

#### 14.2.3.5 Operational audit

*Do we do what we say we do? (Hawksley in EPSC 1994)*

Operational audit covers a check of local activities against local procedures.

**EXAMPLE 14-4 WE DO NOT ALWAYS DO WHAT WE SAY WE DO - 1**

An auditor was invited by a process facility to undertake a process safety audit. The auditor being new to the facility, had to undergo a safety induction before being allowed access to the site. The induction was a standard requirement for all contractors who would work on the site. When it came to work methods and line breaking for maintenance, the safety coordinator conducting the induction said to the auditor, "we induct the contractor personnel to be careful during line break, in case any hazardous material flows out". The auditor was surprised and wanted to know if there was a permit to work (PTW) system that covers process isolation, draining, purging or flushing before handover of a plant section to maintenance personnel. The facility had a PTW system, but process isolation and draining/depressuring before line break was not always practised. The management thought that the PTW covered all of these.

**EXAMPLE 14-5 WE DO NOT ALWAYS DO WHAT WE SAY WE DO - 2**

A process plant stored 98% sulphuric acid in two horizontal tanks of 40 tonnes each, within a bunded (diked) area. The tank had a local level gauge and an overflow pipe that flowed into a low point sump. Should an overflow occur, the acid would be pumped from the sump using a portable diaphragm pump to the effluent treatment area, via a PVC pipe. The effluent treatment was about 200m away and the PVC pipework passed along two pipe bridges. The operators were trained in the procedures for spill handling, especially the need to pump the spill out of the dike without dilution, or if diluted, wait for it to cool down. Unfortunately not all the operators were aware of the violent heat of reaction when water is added to 98% sulphuric acid.

On one occasion, when unloading from a bulk road tanker, an overflow occurred, as the level gauge was faulty, and the fault was not discovered until after the overflow. The operator thought that it would facilitate the pumping if he diluted the spill with water, and opened the water hose on top of the acid spill, and started pumping. The heat of reaction raised the temperature of the mixture above the design temperature of the PVC pipework, and acid started leaking from the pipework below the pipe bridges. Fortunately, no one was present on the road underneath the pipe bridges at that time, otherwise serious injury would have resulted.

The management was aware of this hazard, and thought that it had trained all the operators, and that the operators knew what they were doing, but this was not the case.

The main features of an operational audit are:

- the SMS procedures are accepted as given. This is often the case in internal audits. However, an external auditor may not accept this and question the adequacy of the SMS. This takes the audit to a higher level (see Section 14.2.3.6).
- an audit protocol checklist is developed before commencement of the audit. All aspects of the plant operation and maintenance are covered.
- all personnel are encouraged to speak openly to the auditor when questioned on the work methods.
- the activities on the plant are observed with respect to observance of the procedures, and personnel are interviewed and quizzed on the activities.
- the paperwork and documentation relating to the activities are reviewed. These may be a PTW form, a plant modification authorised by the management of change (MOC) procedure, or control room log book.

- the gaps between what is actually done and what should be done according to procedure are identified.
- the causes of the gaps are identified by the auditor - inadequate training, lack of understanding of the procedure, attitudinal problem etc. This is important for developing corrective actions, which may not be confined to counselling and re-training, but goes deeper into management accountability as well.
- the competency of the auditors is critical.

**EXAMPLE 14-6 AUDITOR COMPETENCY**

An oil company continued have minor problems in the bulk tanker load out of refined products and distribution to retail outlets. An operational audit conducted by the marketing and logistics department gave the operations a satisfactory safety performance rating. On one occasion, the bulk road tanker caught fire while discharging gasoline into underground tanks, and was gutted. One of the actions recommended by the investigation was that an operational safety audit be carried out, but this time, by an external auditor.

The external auditor found that the procedures were of industry acceptable standard, but there were gaps in the practices. Further, it was also revealed that the logistics department did not have the engineering expertise to carry out an operational safety audit, and the procedure that handed over the responsibility to the logistics department was incorrect. It should have been done by a trained auditor from operations or engineering.

### 14.2.3.6 Specialist audit

*Is what we say we do good enough? (Hawksley in EPSC 1994)*

The specialist audit is one level higher than the operational audit, and overlaps the operational audit. It checks the local procedures against 'good industry practice'. The specialist audit can also be undertaken at the commissioning stage to ensure that a robust SMS has been developed.

This audit is conducted by a process safety specialist. The main questions to ask are:

- Is there an SMS framework? Is it based on a recognised model?
- Does it cover all the elements of process safety?
- Have performance standards been developed for safety critical systems and activities?
- Have procedures been developed to cover all aspects of process safety?
- Have they been issued formally under a document control system?
- Are these procedures well written, comprehensive, and adequate?
- Does the system reflect 'good industry practice'?
- What are the gaps, and what is required to close the gaps?

### 14.2.3.7 Management audit

*How do we know that the SMS is functioning satisfactorily?*

*How does the management know whether or not the performance standards are being met?*
*What are the monitoring andfeedback mechanisms?*

This is a still higher level audit, and overlaps the specialist audit and operational audit. It covers the implementation of SMS standards and procedures, and an assessment of its effectiveness.

The main features of this audit are to evaluate the following:

1. SMS implementation strategy
2. Process safety organisation for the facility
3. Task matrix of responsibility and accountability
4. System of training and training records
5. Understanding of systems and procedures by personnel
6. Systems of work as they are understood and practised
7. Management of third party services
8. Emergency response plan
9. Records of emergency training and drills
10. Safety critical equipment register
11. Safety critical activities register
12. Performance standards for safety critical equipment and activities and their appropriateness
13. Process safety performance monitoring system and record keeping
14. Key performance indicators for performance monitoring
15. Gaps between PS and KPI and reasons for them (finding the causes is very important to develop root cause solutions)
16. Condition of plant and equipment and an evaluation of 'fitness for purpose'

A comprehensive SMS audit covers all the above levels, as well as regulatory compliance.

### *14.2.3.8 Regulatory compliance audits*

*How do we know that we are in compliance with regulatory requirements and licence conditions?*

Sometimes it may be necessary to undertake a targeted audit to check regulatory compliance. This audit is generally a subset of the overall SMS audit. The audit focuses on the following:

- List of safety related regulations applicable to the operation of the facility
- Conditions of licence issued by the regulatory agency. The conditions may cover a range of issues including safety related hardware and SMS procedures.
- Compliance with the regulation and licence conditions and identification of non-conformances

- Changes in the regulations or the codes referred to by the regulations since the original design of the facility, and identification of areas where upgrades are necessary for compliance. It may not be possible to achieve compliance of existing plant and equipment design to changed design codes, as the hardware was designed to the applicable codes at the time of initial design. Options to achieve an equivalent level of safety should then be explored and implemented.
- Changes in the plant hardware and operating conditions over a period of time that may be different to the requirements of regulatory codes.

While non-conformances raise some questions on the effectiveness of the SMS, achieving regulatory compliance alone does not provide the assurance as to the integrity of process safety.

### *14.2.3.9 Decommissioning audit*

*How do we know that equipment is fully decommissioned and does not contain hazardous materials, or would not create a hazardous situation?*

An audit is not normally undertaken for plant decommissioning, but is a necessary factor to ensure safety during the decommissioning process. Some of the features are:

- Completeness of depressuring, draining, purging
- Physical isolation of equipment from any part of the operating plant, and from energy sources (e.g. electrical equipment)
- Complete removal of hazardous materials from decommissioned equipment (atmosphere testing of vessels and tanks)
- Removal of equipment from site or moth-balling
- Management of contamination (soil, groundwater etc.), and remediation
- Communication and awareness of status by all personnel
- Approvals required for offsite disposal of material

**EXAMPLE 14-7 DECOMMISSIONED, BUT NOT DECONTAMINATED**

A hydrocarbon solvent tank in a process plant was to be decommissioned. The tank was emptied, physically isolated by disconnecting all pipework, but was not decontaminated. The tank was left in a disused state for a few years, and no one was aware that the tank had contained solvent vapour. The tank base had meanwhile heavily corroded.

During a partial plant turnaround, a heat exchanger tube bundle was removed to the repair yard, located close to the disused tank. Welding was to be conducted on the heat exchanger, and a PTW was issued, according to established practice. The contractor personnel started the hot work at the wrong end of the rather long heat exchanger. This end happened to be close to the disused tank. The spark ignited solvent vapour which flashed back to the tank causing an internal explosion. The tank took off like a rocket, fortunately missing an operating distillation column along its flight and landed about 50 metres away. There was no flame arrester on the tank. The incident resulted in 5 fatalities. ■ ■ ■

## 14.3 DEVELOPMENT OF AUDIT PROTOCOL

### 14.3.1 Need for a Protocol

An audit has to be well structured. While discussion can be open-ended, it is always necessary to keep to a structure to ensure that no details are missed during an audit.

An audit protocol provides such a structure. Experience has shown that an SMS framework is not necessarily suitable for the structure of an audit protocol, as there are considerable overlaps. Therefore, the audit structure, while following the SMS framework for convenience, must depart from this where necessary, especially to accommodate human factor issues permeating through every element of SMS. Further, each SMS element and related procedures can be audited at different levels as described in Section 14.2, resulting in overlaps.

A number of structured checklists, with cross-references for the overlaps where appropriate, provides for a useful audit protocol.

The advantages of a protocol are:

- Different auditors can audit different elements or different plant areas of the facility using the same protocol, and hence consistency is achieved.
- The protocol preparation forces the auditor to think through the entire set of SMS elements, their implementation, monitoring and effectiveness, and prepares for the audit.
- It allows for management review of the protocol (if this is agreed upon), to enable the facility management to prepare for the audit.
- It minimises subjectivity, at the same time is flexible enough to allow an investigative approach. It is not a question of giving a score if the answer is 'yes' and zero otherwise. The protocol should cover the line of questioning if the answer is 'no'.

  For example, take the question "Do you have a register of process interlocks, with their set points?"

  If the answer is 'yes', then the next question can be 'Do you have a schedule for function testing of interlocks?", and if the answer is 'yes' again, ask to see the schedule, and proof that the schedule is actually being observed. If the answer is 'no', then the next question modifies to, "How do you ensure function testing of the interlocks?"

### 14.3.2 Documents for Audit Review

An SMS audit of a process facility consists of three major steps:

- Facility inspection
- Review of documentation
- Interviews of personnel at all levels of the facility (operators, supervisors, engineers, department managers and site manager)

Additional facility inspections, specifically targeted to specific areas or equipment, may be carried out during the audit for verification.

The SMS audit is elaborate and time consuming. It requires a review of a range of documents by the auditor, even before interviews with personnel. A list of documentation associated with each element of the SMS is given in Table 14-2. The list is indicative and not exhaustive.

TABLE 14-2 DOCUMENTS REVIEWED IN A PROCESS SAFETY AUDIT

| SMS Element | Documents for Review |
|---|---|
| Overview | Current SMS manual |
| Major accident prevention policy (MAPP) | Current copy of policy (check signatory) |
| Facility details | Facility description<br>Process description<br>Flowsheets<br>P&IDs<br>Layout diagrams<br>List of hazardous materials<br>Location of hazardous materials in the plant and inventories (in process, storage) |
| Organisation | Process safety organisation diagram<br>Task matrix of responsibility and accountability |
| Communications | Communications protocol<br>Internal communications<br>External communications<br>Shift change procedures<br>Shift log<br>Communications with contractors |
| Staff selection and training | Job descriptions<br>Selection criteria<br>Training manual<br>Training register<br>Trainer qualifications<br>Training assessment procedure<br>Contractor selection criteria<br>Record of contractor personnel safety induction and training |
| Hazard identification and assessment | Hazard register<br>Previously conducted hazard and safety studies |
| Safety report | Safety report prepared for the site under a Major Hazard Facility regulation |
| Hazard prevention, mitigation measures | Safety critical equipment register<br>Safety critical activity register<br>Hazardous area classification diagrams<br>Fire protection systems layout diagram<br>Fire and Gas (F&G) detectors layout diagrams<br>Emergency shutdown system (ESD)<br>List of critical operating parameters, and operating limits<br>List of relief devices and set points<br>Pressure vessels register |

| SMS Element | Documents for Review |
|---|---|
| Management of change | MOC procedure<br>Register of changes carried out (hardware, software, procedures) |
| Systems of Work | Operating manual<br>Preparation for maintenance<br>PTW procedures<br>Register of PTW forms<br>Preventive maintenance program |
| Mechanical integrity | Records of preventive maintenance<br>F&G detectors calibration records<br>Records of interlocks function testing<br>Fire protection system inspection and maintenance records<br>Integrity inspection schedules<br>Integrity inspection records<br>Spare parts register |
| Inventory management | Inventory management procedure<br>Historic levels of inventory<br>Licence conditions |
| Emergency plans | Site emergency response plan<br>Pre-incident plans<br>Records of emergency drills and exercises |
| Investigation and reporting | Reporting procedure and forms<br>Record of actual incidents<br>Investigation procedure<br>Record of investigation carried out<br>Record of close out of actions arising from investigations |
| Performance standards | Documentation of performance standards for SMS procedures<br>Key performance indicators (KPI)<br>Record of monitoring performance against KPI |
| Periodic Review | Previous audit reports |
| Improvement plans | Documentation of closeout of previous audit actions |

### 14.3.3 Development of Checklist

Using the SMS elements described in Chapter 11, and the documentation listed for review in Table 14-2, a checklist needs to be developed for the audit. A generic checklist can be developed, which can be tailored to be site specific.

Checklists should not be rigid. They evolve over a period of time, with the growth of knowledge and experience of people. Examples of checklist can be found in DNV (1994) and Hessian and Rubin (1991). A structured audit technique has been developed by Hurst and Ratcliffe (1994).

## 14.4 REQUIREMENTS OF A SUCCESSFUL AUDIT

It is sad to read reports of accident investigations which state that only a month before the accident, an SMS audit gave the facility SMS in practice a clean bill of health.

Sir Arthur Eddington, in explaining the concept of the special theory of relativity and the Fitzgerald contraction, gave an analogy of financial auditing of a balance sheet. The first question about the balance sheet is "Is this true?" "Of course", one might add, "it *is* true; it has been duly audited and certified by an auditor." The next question is "Is this *really* true?"

The same can be said of SMS auditing. The facility is *safe* because the audit had not found anything adverse about the way safety was managed. The next question is "Is it *really* safe?"

There are a number of requirements for a successful SMS audit, which may not be met in all instances. Some of these are highlighted below.

### 14.4.1 Management Commitment

It is essential that management commitment to safety is *real.* The proof of this reality is action not words. Why does the senior management commission an audit? Is it really to know what the problems are so that they can be addressed as part of a continual improvement process, or is it just a regulatory compliance to keep the regulators at bay?

The auditor must be experienced enough to identify this single major issue, as it is the senior management commitment and leadership, or the lack of it, that flows down the management chain throughout the organisation.

### 14.4.2 Experience of Auditor

The auditor's experience is paramount in the successful outcome of an audit. Main requirements are:

- Experience in process safety
- Development and implementation of SMS
- Learning as a co-auditor working with experienced lead auditors
- People skills (putting the auditee at ease, at the same time maintaining a sense of formality - do not make it casual)
- Investigative approach
- Ability to grasp the organisation's *modus operandi,* so that solutions suggested would not be alien to the established culture.

It is not a question of using a checklist and filling in the boxes, but the ability to identify the root cause of identified problems, and suggest effective solutions.

### 14.4.3 Identification of Gaps in Audited Systems and Procedures

The main purpose of the audit is identifying the gaps between procedures and practices, and gaps in the procedures compared to industry best practice. Therefore, the auditor should have a clear idea of what the standards of expectation are, so that deviations can be identified.

Where key performance indicators have not been developed, the auditor can use industry standard practice to cover this issue, and make recommendations to the management.

### 14.4.4 Evaluation against Key Performance Indicators

Once the PS for the procedures are defined, the KPIs can be developed as a natural sequence. Some KPIs related to systems of work are listed below to provide an indication to the reader for the development of KPIs.

- Percentage of defective PTW forms in the number of forms audited
- Ratio of modifications carried out with proper MOC authorisation to total number of changes carried out
- Ratio of the number of interlocks actually function tested to number that should be tested according to schedule
- Percentage of number of interlocks that failed the function test
- Percentage of preventive maintenance items incomplete in a given period

KPIs can thus be developed for all safety critical systems and activities.

### 14.4.5 Structural Solutions versus Band-aid Solutions

One area where audit effectiveness could be undermined is when the root cause of a problem is not identified. This is illustrated by the following example.

**EXAMPLE 14-8 TRACING A PROBLEM TO ITS ROOT CAUSE**

Here is an example from an audit. The auditor is an independent specialist and the auditee is the maintenance manager.

*Auditor:* *"Please show me your function testing schedule for the emergency shutdown (ESD) system."*

Auditee shows the schedule. It shows quarterly testing requirements.

*Auditor:* *"Can you tell me when this system was last tested?"*

*Auditee:* *"Er..., you see ... the instrument technicians have been rather busy ... we missed the test in the last quarter."*

The problem is shifted to the instruments maintenance section.

If the auditor stops here, and makes a recommendation for function testing, the root cause is missed completely. This is a band-aid solution and the problem is bound to recur. Let us continue.

*Auditor:* *"Mm... when was the test previous to the missed one conducted, and can you show me the documentation?"*

*Auditee:* *"I am afraid I cannot. To be honest, this test has not been conducted for quite some time. But we did have an emergency that activated the ESD, so we know it works - I can't recall when."*

The plot thickens. The stop line does not end with the instruments maintenance section. It goes up the line to the maintenance manager.

*Auditor:* *Your procedure says that the performance of the ESD function is to be routinely monitored. Why did the failure to conduct function testing on such a critical safety function go unnoticed?*

*Auditee:* *"That is true, but we have all been too busy. The site manager is aware of this, but has not pressed ahead for its completion. We are having a plant turnaround in 3 months, and we hope to do all the function tests at that time.*

■ ■ ■

In the above example, the root cause has been lack of leadership and management commitment in practice, despite what the books say. The problem is structural, and cannot be solved by a quick fix.

By using a yes/no checklist alone, this investigation could not have been done effectively. If the problem is lack of site management commitment, then the question arises as to why this was missed in the corporate internal audits.

### 14.4.6 Rotation of Auditors in Internal Audits

It is useful to rotate the auditors in internal audits, so that any problem can be identified with a 'fresh pair of eyes' each time. If the same plant personnel do the audit, they may tend to skip over some items as having been satisfactory during the previous audit.

## 14.5 FOLLOW-UP AND CLOSE OUT OF AUDIT ACTIONS

One area where many organisations fail is in following up audit recommendations and closing them out. We have seen in many cases, rather frustratingly, that the actions from previous one or two audits are still outstanding when the next audit is undertaken.

In order for an audit to produce positive outcomes in improving the SMS in practice, the following points should be observed:

- Set target completion dates and responsibilities for all the action items arising from the audit.
- Set a PS for the task of closeout of audit actions. This can be, say, 90% of the actions shall be closed out be the target date, and the rest within 2 months after the target date.
- Set a KPI for closeout of actions as the percentage of actions completed by target date.
- Ensure that this KPI is reported by the safety coordinator in the monthly reports to senior management.
- Senior management should act on KPIs not meeting performance standards.

## 14.6 REVIEW

In Chapter 10, we have emphasized the importance of auditing and feedback to management at the very heart of an effective SMS in practice.

In this chapter, different types of audits to suit the facility life cycle stage have been described. Underlying all the audits is the development of a proper audit protocol, with sufficient flexibility to provide for an investigative approach. The audit requires a very large number of documents to be reviewed and assessed, together with interviews with plant personnel in all departments, at different levels.

The requirements of a successful audit have been described. The competency of the auditor, and the leadership and commitment of the management are the twin arms of a successful audit. The importance of identifying root causes to non-conformances and deviations is stressed, without which, the problems are most likely to recur.

The need to implement corrective actions arising from the audits within an agreed time frame is addressed. Some audit experiences have been shared in the form of examples.

## 14.7 REFERENCES

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

CCPS Center for Chemical Process Safety 1993, *Guidelines for Auditing Process Safety Management Systems*, American Institute of Chemical Engineers, New York.

Chia, S., Peach, G. and Duckworth, B. 2004, 'Measuring plant process safety performance for an onshore facility - the challenges', *11th International Symposium Loss Prevention*, Prague, pp. 1225-1231.

DNV Det Norske Veritas 1994, *International Safety Rating System*, 6th edn, DNV Industry Ltd, London.

EPSC European Process Safety Centre 1994, *Safety Management Systems: Sharing experiences in process safety*, European Process Safety Centre, published by the Institution of Chemical Engineers, Rugby, England.

EPSC European Process Safety Centre 1996, *Safety Performance Measurement*, (ed.) J. Van Steen, Published by the Institution of Chemical Engineers, Rugby, England.

Hessian, R.T. Jr. and Rubin, J.N. 1991, 'Checklist reviews' in *Risk Assessment and Risk Management for the Chemical Process Industry*, eds. H.R. Greenberg, and J.J. Cramer, van Nostrand Reinhold, New York, pp. 30-47.

Hurst, N.W. and Ratcliffe, K. 1994, 'Development and application of a structured audit technique for the assessment of safety management systems (STATAS)', Hazards XII - European Advances in Process Safety, *Institution of Chemical Engineers Symposium Series No. 134*, pp. 315-331.

Lord Cullen 1990, *The Public Inquiry into the Piper Alpha Disaster*, The Department of Energy, HMSO, London.

McKeever, D.J. and Lawrenson, R. 1992, 'Safety Management offshore - System requirements' in *Major Hazards Offshore and Onshore, Institution of Chemical Engineers Symposium Series No. 130*, pp. 149-169.

OSHA Occupational Health and Safety Administration. *Process safety management of highly hazardous chemicals*, Occupational Health and Safety Administration, Federal Register, Washington D.C., USA. OSHA 29 CFR 1910.119:1992.

OSHA Occupational Health and Safety Administration, *Process Safety Management*, Occupational Health and Safety Administration, Washington, D.C., USA. OSHA 3132:2000.

Page, S. 1995, 'Making Environmental Management Work' in *Environmental Management Systems,* Chapter 7, ed. P. Sharratt, Institution of Chemical Engineers, Rugby, England, pp. 83-93.

Schweer, D., Scholz, G. and Heisel, M. 2000, 'What are process safety management audits telling the operators?', *Hydrocarbon Processing*, October.

Tarrants, W.E. 1980, *The Measurement of Safety Performance*, Garland STPM Press, New York.

Tweeddale, M. 2003, *Managing risk and reliability in process plants*, Gulf Professional Publishing.

Wallace, I.G. 1990, 'Safety auditing in the offshore industry' in *Piper Alpha - Lessons for Life Cycle Safety Management, Institution of Chemical Engineers Symposium Series No. 122*, pp. 85-97.

## 14.8 NOTATION

| | |
|---|---|
| API | American Petroleum Institute |
| CCPS | Center for Chemical Process Safety |
| DNV | Det Norske Veritas |
| EPSC | European Process Safety Centre |
| ESD | Emergency Shutdown |
| F&G | Fire & Gas |
| HMSO | Her Majesty's Stationary Office |
| HSE | Health & Safety Executive (UK) |
| IChemE | The Institution of Chemical Engineers, UK |
| IP | Institute of Petroleum |
| ISRS | International Safety Rating System |
| KPI | Key Performance Indicator |
| MAPP | Major Accident Prevention Policy |
| MOC | Management of Change |
| OH&S | Occupational Health and Safety |
| OSHA | Occupational Safety and Health Administration, USA |
| P&ID | Piping and Instrumentation Diagram |
| PS | Performance Standard |
| PSM | Process Safety Management |
| PTW | Permit To Work |
| PVC | Poly Vinyl Chloride |
| RP | Recommended Practice |
| SMS | Safety Management System |

This page is intentionally left blank

# 15

# LAND USE PLANNING RISK MANAGEMENT

*"Engineers shall hold paramount the safety, health and welfare of the public in the performance of their professional duties."*

*- First canon of the Code of Professional Ethics of the AIChE*

Most major hazard disasters have had significant impacts on local communities near to major hazard facility (MHF) sites or along transport routes. Flixborough, Pemex, San Carlos de Rapita and Bhopal are obvious candidates that illustrate the point. Concern regarding land use planning (LUP) around MHFs and the development of appropriate dangerous goods transport routes have been pressing issues for governments, fuelled by vocal representations from the local communities affected by such operations. Much of the regulatory framework in the USA, Europe and Australasia is driven by concern for societal impacts that are reflected in planning decisions on new developments near major hazard operations as well as establishment of major hazard operations near to existing local communities.

Process risk management plays a vital role in the local overall planning issue. This chapter sets out the key factors in land use planning and in particular the role that risk management plays in that process.

## 15.1 THE NATURE OF OPERATIONS

The two major operational scenarios which are of key interest are:

- fixed site risks (e.g. storage, manufacturing facility)
- transport risks (e.g. bulk road or rail tankers of chemicals or petroleum products, gas pipelines or shipping)

Although there are significant differences in their characteristics they share many common elements of analysis, which include consequence analysis and event likelihood.

We consider the two major operational classes and see how these are dealt with in the context of land use planning.

### 15.1.1 Fixed Site Operations

These types of operations could be classified in a number of ways. One particular suggestion is based on the operations:

a) Storage facilities
b) Re-packaging facilities
c) Production/Manufacturing facilities.

These however say nothing concerning the amounts of materials present. In this respect it is necessary to have some classification scheme which reflects this factor.

Several governments have attempted such a classification based on three major components

a) the materials present (e.g. Dangerous Goods Codes Class 3 or 6.1)
b) the amount present (e.g. 600 tonnes of calcium hypochlorite)
c) the operations carried out (e.g. refining, tanning, minerals processing)

The main consideration in land use planning is whether or not an incident in a hazardous facility has the potential to cause an adverse impact on the operational site and on surrounding land uses. Since the impact distance is a function of the quantity of hazardous materials involved, planning requires certain "cut-off" or "threshold" values for hazardous substances to be nominated. This aspect is discussed later in considering the question of regulations. Several operational categories could be identified through these mechanisms which seek to generate a qualitative risk estimate. For instance:

Category 1: Minor Risk Sites

Here there are essentially occupational risks and negligible off-site impacts due either to the materials present, their quantities and the processing. These types of facilities would require minimal controls.

Category 2: Potential, Moderate Risk Sites

Here minimal off-site risks are expected, being tolerable to the local authority and community. Operations would be carried out subject to compliance with regulations.

Category 3: Potential, Major Risk Sites

These are called "major hazard facilities (MHFs)". They generate understandable risks. The activity is permitted by the relevant authority/community provided the risk is demonstrated to be at or below tolerable levels using the ALARP principle.

Category 4: Extreme Risk Sites

These are unacceptable and would be prohibited.

These categories as seen in Figure 15-1 where the various sectors cover regions of consequence and frequency of events. This generally relates back to a region on a risk matrix.

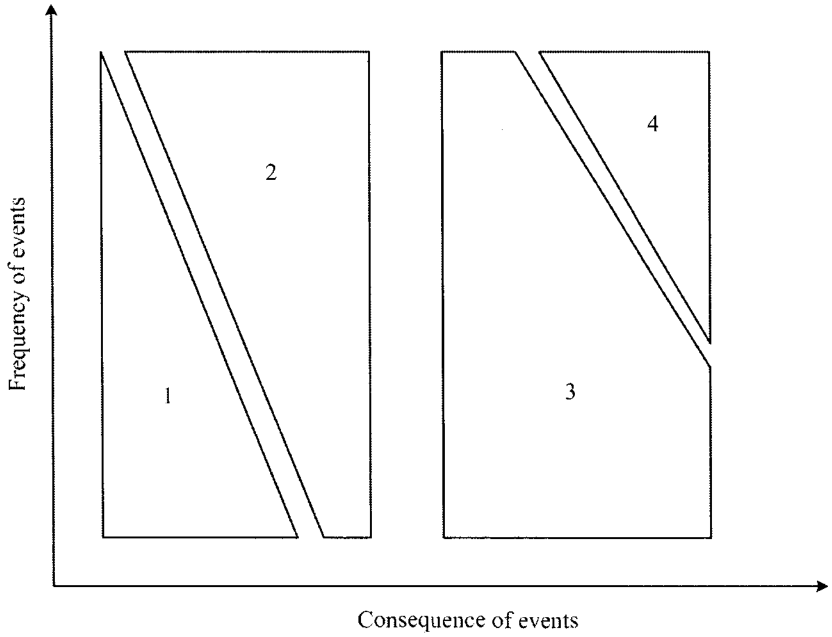


FIGURE 15-1 CATEGORIES OF ACTIVITIES

It must be emphasized that the same activity can have quite a different tolerability depending on its location. For example a munitions factory could be tolerated in a remote location but could be completely unacceptable if located near a population centre. Depending on national approaches, initial classification of operations can vary in the number of activity categories.

In dealing with the issue of activity classification, national governments have generally used threshold values of specific dangerous goods to aid classification. In the case of the EC 'Seveso II Directive' (96/82/EC), there exists a 2-tier approach that establishes two qualifying quantities of specified substances (Annex 1 of Directive) for MHFs. More obligations are imposed on 'upper tier' establishments than on 'lower tier' establishments. For example the quantities for acetylene for the two tiers are 5 and 50 tonnes. For substances not specifically named there is also a set of generic quantities based on characteristics of the substance, such as 'very toxic' (5 and 20 tonnes), oxidizing (50 and 200 tonnes) and 'flammable' (500 and 50000 tonnes).

In the case of the Victorian MHF regulations (2000) in Australia, the presence of a MHF is identified by a threshold value for specific named substances (e.g. acetylene being 50 tonnes) or for a dangerous goods class (e.g. Class 3 flammable liquid, packing group II or III being 50,000 tonnes). Similar approaches in the regulations for the State of Queensland in Australia (2002) led to a 3 level classification of (a) MHF, (b) 'large dangerous goods location' and (c) 'dangerous goods location'. Lesser obligations are imposed, depending on the lower potential hazard of the facility. Minor storage is also acknowledged in many planning provisions. This relates mainly to small businesses.

### 15.1.2 Transportation Operations

Consideration of the key transport activities include:

a) road transport
b) rail transport
c) air transport
d) marine transport
e) pipelines

International conventions cover regulations on the transport of dangerous goods (DG) such as the UN Recommendations on the Transport of Dangerous Goods (UNRMTG). This is commonly known as the 'Orange Book' (http://www.unece.org/trans/danger/ ).

Such regulations specifically target classification, packaging, labelling, placarding and documentation issues. They can also set-out restrictions on incompatible loading arrangements based on DG classes. These general considerations find specific manifestation in country regulations administered by such organizations as:

(i) US Department of Transport (USDOT)
(ii) Australian Government, Department of Transport and Regional Services (DOTARS)
(iii) UK, Department of Transport (DoT)

However, the regulations do not generally address the interaction of the transport of DGs with land use planning issues such as restricted transport routes for dangerous goods. This is often an important issue for local, regional and national governments. The following sections outline key issues and some of the actions governments have taken to manage risk to sensitive land uses. Air transport is not covered in this chapter.

#### 15.1.2.1 Road transport

Significant quantities of dangerous goods are transported by road each day. Gasoline, LPG, chemicals, herbicides and pesticides are common substances moved by road transport. In the UK, 100 million tonnes of petroleum and chemical substances were carried by road transport in 2002, this constituting 11.7 billion tonne-kilometres of transport activity (TSGB 2003). This represents 7% of all commodities transported in the UK.

In terms of DG related road accidents the initiating factors include:

a) the type of cargo and its inherent hazard (e.g. liquids, gases and their containment)
b) the transporter being used (e.g. 20 tonne LPG tanker, liquid fuels tanker, double road trailer or 'B double')
c) the operations carried out (e.g. loading, transfers, haulage)

The contributing factors for the hazardous impact can be quite different from fixed sites. In particular the following play a major role:

a) the changing population density along the route
b) the frequency of movements and the time of those movements
c) the initiating hazardous events
d) the changing meteorological conditions (e.g. windspeed, direction)
e) the probabilities of ignition, as sources vary along the route.

The term "linear risk" is used to describe these transport related processes, since the risk changes along the route. This is discussed in Chapter 9.

**EXAMPLE 15-1 ROAD TANKER INCIDENTS**

a) In September 1990 a road tanker carrying LPG crashed within the city of Bangkok, Thailand. The subsequent fire and explosion caused 63 deaths and over 90 people were injured. Inappropriate DG routes in heavily populated city areas contributed to the loss of life.
b) A double trailer (B double) ammonia road tanker suffered a single vehicle accident that resulted in the decoupling of the rear trailer from the prime mover. The decoupled tank trailer was subsequently holed as the rear tank collided with the support tray on the first trailer. The ammonia was released rapidly but due to wind direction and the remote location of the accident, ammonia was safely dispersed by the wind.

Example 15-1 emphasizes that transport route selection for dangerous goods is vital in protecting local communities. Many cities have established specific DG transport routes to ensure that large quantities of dangerous goods are not taken through city centres or close to major residential areas. Similarly, routes have been established for dangerous goods road transport from a number of major hazard storage facilities at Port Botany, Sydney, Australia.

### 15.1.2.2 Rail transport

Large volumes of flammable, corrosive and poisonous substances are routinely transported by rail systems. There is often little possibility of re-routing trains to avoid potential areas of environmental impact or high population density. However, new developments near existing rail lines can be controlled and new rail routes located to avoid unnecessary risk to sensitive land uses.

The principal initiating factors include:

a) type of cargo and the quantities involved
b) the train used (mixed goods, dedicated tank trains such as the US GATX)
c) the rolling stock and allowable speed on sections
d) the track conditions along the route.

Contributing factors to hazardous consequences are similar to road transport stated in section 15.1.2.1.

**EXAMPLE 15-2 RAIL RELATED INCIDENTS**

a) In April 2004, at least 154 people died and over 1300 were injured in North Korea when a train containing ammonium nitrate fertilizer collided with an oil tanker and subsequently exploded after ignition from electricity lines being brought down. The blast destroyed or damaged over 8,000 houses and completely destroyed all structures within a 150 metre radius of the blast centre. Included in the dead were 76 children in a local school. Densely populated areas surrounding the main rail junction at Ryongchan were severely affected.
b) In 1979 at Mississauga, Canada, a train derailment led to release of chlorine, styrene and propane. Fires and explosions ensued and eventually some 218,000 people were evacuated from the nearby area. Lost business and commercial productivity amounted to millions of dollars. No loss of life occurred in this instance due to emergency response and evacuation procedures.

The safety of infrastructure development in the railway air space over tracks carrying dangerous goods has become a focus of rail authorities in major cities in Australia.

### 15.1.2.3 Marine transport

Bulk shipment of commodity, chemicals, petroleum products and specialty dangerous goods occurs worldwide. The International Maritime Dangerous Goods (IMDG) code is a uniform code similar to the UNRMTG and sets standards for transport of DGs. The key issues for land use planning revolve around port facilities which include location of berths, associated bulk storage facilities and associated transport to and from the port.

Similar to sections 15.1.2.1 and 15.1.2.2, initiating factors and contributing factors are very similar. Other risk management issues relate to preferred navigation routes and control of environmental impacts, lessons clearly evident from the Exxon Valdez incident in Alaska. Compulsory pilotage is often required in sensitive environmental areas such as the Great Barrier Reef in Australia.

**EXAMPLE 15-3 MARITIME INCIDENTS**

a) One of the worst maritime incidents with major on-shore implications occurred on April 16, 1947, when the SS Grand Camp containing ammonium nitrate exploded in the harbour of Texas City, USA. Over 600 people died in the explosion, many never identified due to the horrific burns sustained. The initial blast caused domino effects in the nearby Monsanto chemical plants, destruction of grain storage facilities, oil and chemical storage tanks.
b) The bulk petroleum carrier Exxon Valdez, ran aground in Alaska in 1989 causing a major environmental spill of crude oil. The incident took several years of intense cleanup effort at enormous cost.

### 15.1.2.4 Pipeline transport

Major gas, oil and mining related pipelines are used across most countries to efficiently distribute or transport materials. Pipeline corridors for major gas distribution are often well defined by competent authorities and activities within the corridors strictly controlled. Inner city reticulation of gas is normally designed and controlled by gas supply corporations with appropriate approvals by local authorities.

The key factors in regard to risk include:

a) Proposed route of pipeline and the sensitive land uses bordering the route. These include residential areas, cultural and heritage areas, native land and title claims, sensitive environmental areas such as wetlands, rivers and habitat as well as adjoining industrial developments.
b) The material being transported, including its phase (vapour, liquid or dispersed solids), hazardous properties and its physico-chemical properties such as viscosity, density and surface tension.
c) Types of hazardous incidents including environmental damage, earthquake, fire, explosion and toxic impacts. Also the potential operations in the vicinity of the pipeline especially construction activities.
d) Design and operation of the pipeline including:
   - design standards for the line
   - burial and backfill designs
   - supervisory control (SCADA systems)
   - shutdown, monitoring and leak detection systems.

**EXAMPLE 15-4 PIPELINE INCIDENTS**

a) On June 3, 1989 in the Russian Ural Mountains, a leaking LPG pipeline near the town of Uta, 100 km east of Moscow, created a vapour cloud that exploded. The pipeline ran adjacent to the Trans-Siberian railway and the explosion was set off by passenger trains on the track. Over 500 people died and around 700 were injured in the accident. The combination of a major LPG leak with poor dispersion conditions and ignition sources provided by the trains generated a major disaster.

b) On June 9, 1994 in Allentown, USA, a compression coupling on a gas pipeline failed and gas then dispersed into the local neighbourhood. Gas penetrated into an 8 storey retirement home and subsequently exploded, killing 1 person and injuring 66 others. Over $5 million of damage was incurred. Loss of life was reduced because many of the residents were out of the building. Lack of gas detection systems and poor maintenance procedures were key contributing factors.

### 15.1.3 Interactions between Fixed Sites and Transport Routes

Not only do planners concern themselves with the issues of fixed site risks and transport risks but consideration of interactions between operations are often crucial. The following issues often arise:

(i) Impacts from fixed sites on nearby transport routes such as major highways where site events can have significant impacts on vehicular traffic. This includes fires, explosions and toxic gas releases.

(ii) Impacts from transport route accidents affecting and propagating onto fixed sites, e.g. a road tanker explosion or ship explosion in a port can cause major incidents on a fixed site.

(iii) The interaction between aircraft flight paths and major hazard facilities, especially in the case of large industrial areas near major airports. Issues of location of airports and flight paths need to be considered.

(iv) Interaction of pipeline incidents such as fire or explosion with road or rail transport as well as impact on fixed site operations.

Each combination, where applicable, requires consideration within the planning process leading to the allocation of specific transport corridors, pipeline easements, aircraft flight paths and runway orientations, as well as the appropriateness of fixed site locations. Lines (1998) discusses some of these issues in detail.

## 15.2 THE STAKEHOLDERS AND THE ISSUES

Industrial activities and transport of dangerous goods is essential in our society. The challenge is how these activities are integrated in a meaningful and rational way into the overall planning schemes.

Business and industry locations need to be considered in relation to:

a) residential precincts
b) business parks near residential precincts
c) businesses near residential precincts
d) low impact business and industry precincts
e) general impact business and industry precincts
f) special industry precincts

Within the realm of land use planning there are several key players. These include:

(i) State or Provincial Government

Issues at this level are broadly:

- strategic planning
- regional development
- development control

However the interface between a developer and the local community is generally devolved to local authorities. Hence the second main player is:

(ii) Local Government

Issues here can include:

- development control plans
- town planning schemes
- impacts
  - environmental (air, noise, water)
  - social (health, safety, consultation)
  - infrastructure (services, transport, effluent etc.)

Clearly the next stakeholder is the proponent of the project or activity.

(iii) The Proponent

Issues here can be:

- economic viability of the proposed operations
- on-site safety
- off-site safety
- communication with other stakeholders (community, authorities, action groups)
- access (markets, raw materials etc.)

Finally but not least is the general public as one of the major stakeholders

(iv) General Public

The issues and concerns can be extensive and varied. They could include:

- maintenance of amenity
- noise, odour, pollution, lighting issues
- transport corridors
- natural environment quality
- refuse and wastewater disposal and treatment
- hazard and risk
- information and communication (with governments and industry)
- risk perception by public and the outrage factor

In some circumstances, the National Government is also a major player, especially where there are proposals of "national interest". What is obvious is that the land use planning issue for hazardous industries or transport operations is very complex. Many stakeholders with their own agendas often seek an outcome which protects their sectional interests.

The implications of such a complex system are far reaching. It requires an approach which has, at least, the following characteristics shown in Table 15-1.

One of the major issues is to do with the appropriateness of the approach. It is absolutely necessary to identify those developments which are considered "major hazard sites" or major hazard activities such as vehicular transport and pipelines. These require significant analysis. Minor stores and the like require consideration but nothing like the degree of analysis needed for major hazards. This could be the difference between a qualitative analysis approach compared with a quantitative analysis approach, which is time-consuming and very expensive.

**TABLE 15-1 KEY IMPLICATIONS FOR LAND USE PLANNING**

- Comprehensive approach
  - all players considered and heard
  - environmental impact assessment (process risk assessment forms a component of this study)
- Co-ordinated approach
  - clearly defined goals and standards of performance
  - clear communications
  - continued involvement
- An appropriate approach
  - level of analysis versus level of potential impact
  - level of control versus level of hazard

To appreciate the concerns in land use planning we consider in the following sections some of the principal precincts and their potential interaction with hazardous operations.

### 15.2.1 Business and Industry Precincts

A useful picture of the interrelation of the 6 previously mentioned precincts is given in Figure 15-2 which seeks to place the precincts on a graph of amenity versus impact (Kinhill Cameron McNamara, 1994).

This shows how business and industry (B&I) precincts might interrelate, with residential areas being of high amenity with little or no direct impact from say special industry precincts (e.g. large scale chemical plants). They in turn create little impact from B&I activities (e.g. home-based activities) within the precinct. The six precincts are described as follows:

(i) Residential Precincts
Attached or detached housing, apartment buildings where B&I activities are essentially home-based with no undue interference to neighbouring residences.

(ii) Business Parks near Residences

A slightly lower level of amenity to that of residential areas with low levels of impact from B&I activities.

(iii) Business Parks

These describe local government or state government B&l environments specially created, catering for mutually apportive B&I activities. These are "clean and green" developments. These would have a range of impacts depending on occupants.

(iv) Low Impact and Industry Precincts

These refer to the majority of B&l activities (excluding retail operations). They are characterised by small to medium scale businesses using small to medium sized premises. They are the traditional "light" industry areas. They are likely to have medium to low levels of amenity and similar impacts. They could be adjacent to residential, business parks or general B&I developments.

(v) General Impact B&I Precincts

Characterised by low levels of amenity and medium to high levels of impact. Hazards are minimised through inherently safe designs and procedures. They are likely to be associated or adjacent to low impact B&I developments, business parks or special industries.

(vi) Special Industry Precincts

These are likely to have the highest impacts depending on the type of industry. These developments will generally be separated from other development areas due to their hazardous nature. They could be associated with general impact B&I precincts.

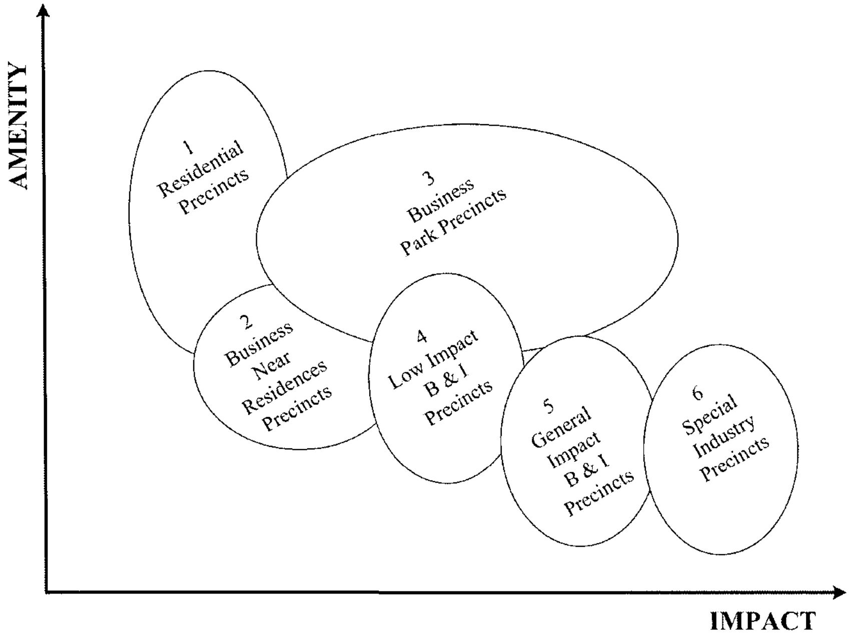

AMENITY
1 Residential Precincts
3 Business Park Precincts
2 Business Near Residences Precincts
4 Low Impact B & I Precincts
5 General Impact B & I Precincts
6 Special Industry Precincts
IMPACT

FIGURE 15-2 BUSINESS AND INDUSTRY PRECINCTS - A CONCEPTUAL FRAMEWORK

Each of these precincts can have associated with it a set of performance standards which address those characteristics. In deciding how this integration takes place, it is clear that certain performance standards are needed for a range of characteristics. These can include:

a) hazard and risk criteria
b) natural environmental values
c) transport impact standards
d) wastewater, surface water, refuse disposal
e) offensive odour and air pollution standards
f) noise at site boundary
g) lighting
h) visual amenity

In deciding on appropriate hazard and risk criteria we need realistic guidelines which reflect the acceptable impact on each of the locations discussed above. This is discussed further in section 15.4.

### 15.2.2 The Challenge for Planners and Proponents

The real challenge for planning is the appropriate integration of business and industry activities into a holistic planning approach that addresses all the issues in section 15.2.1. Industrial and transport risks play a role in the decision making - in some cases a subservient role.

Some of the key desired environmental outcomes (DEOs) for industrial areas include: (BCC 2004)

- a range of industries to provide employment and economic growth
- operational certainty for existing industries that maintain high environmental performance
- compatible, clustered industries to achieve synergies and economies
- heavy traffic and adverse impacts not to intrude into adjacent residential and community use areas
- level of risk is appropriate and compatible with surrounding land use areas
- location and operation of industries have minimal impact on the natural environment and biodiversity values
- industrial development design promotes personal sensitivity and safety.

### 15.2.3 Regulatory Frameworks

The Seveso II Directive (Article 12) is explicit in its requirement for land use planning with respect to major hazard sites - *"Member States shall ensure that their land-use and/or other relevant policies and the procedures for implementing those policies take account of the need, in the long term, to maintain appropriate distances between establishments covered by this Directive and residential areas, areas of public use and areas of particular natural sensitivity or interest, and, in the case of existing establishments, of the need for additional technical measures in accordance with Article 5, so as not to increase the risks to people."*

Not only the EC member countries but most other countries have over-arching planning provisions that set down the main principles for planning. In the UK, The Town and Country Planning Act (1990) is one such framework. In Australia, such regulations as the Integrated Planning Act (Queensland) 1996 and the Environmental Planning and Assessment Act (New South Wales) 1979, set out the parameters for planning.

The goals of such Acts are:

- reinforce local government roles in planning
- regional planning to be done at state/provincial level
- planning schemes to be developed at local level
- the establishment of Development Control Plans (DCPs)
- establishing integrated development approval schemes (IDAS) at local/state levels
- community consultation processes
- dispute resolution processes.

The DCPs must be formulated to address such issues as:

- the topology
- the natural or built environment, or both
- regional land use patterns
- public utility infrastructure systems and transport systems
- regional or local economic and employment factors
- the social and cultural features of the population including housing
- any constraints and opportunities in respect of the development, and
- in the case of a strategic plan, any reasonable development options available.

Acts often set out the composition of the DCP to include the following overall features:

- a map or series of maps indicating intentions for future development of designated parts or the whole of a planning scheme area
- statements of the intent of the DCP
- criteria for implementation of the plan

Part of the development control plans is the establishment of development zones and setting out the role that risk plays in the performance standards of industries wishing to establish in the appropriate zones such as light industry or special (hazardous) industry.

**EXAMPLE 15-5 PLANNING LAND USE AREAS IN THE VICINITY OF A REFINERY**

Figure 15-3 shows the area adjacent to a petroleum refinery (Heavy Industry) in Brisbane, Australia. Approximate areas of development are indicated under 4 key categories:

a) Greenspace

  - conservation areas
  - environmental protection areas
  - rural
  - parklands
  - sport and recreation

b) Residential
  - low density
  - low-medium density
  - medium density
  - high density
  - character areas

c) Industrial
  - future industry
  - light industry
  - general industry
  - heavy industry
  - extractive industry

d) Community areas that include such uses as educational activities.

Here, the refinery area, a MHF site and designated as a heavy industry area, is separated from low density residential areas by conservation and parkland areas on the south. To the west the general industry area is separated from the low density residential areas by the conservation precinct. This represents a typical application of precincts shown in Figure 15-2.

This is typical of DCPs where an integrated approach to planning exists. Tolerable risk provides one of many performance criteria for industrial or transport operations.

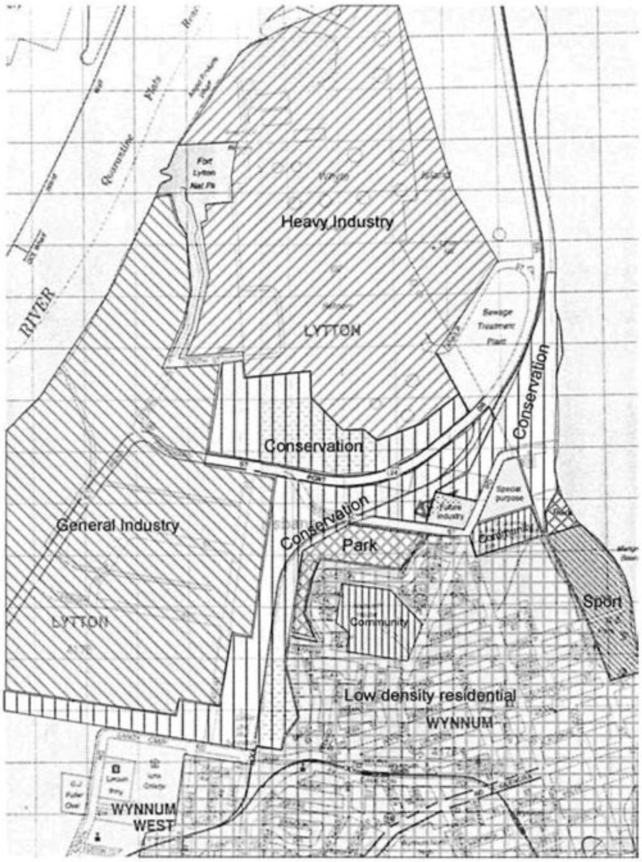
## 15.3 PLANNING AND MANAGEMENT ISSUES

For the development of potentially hazardous operations the following issues can be identified.

### 15.3.1 Land Use Planning Issues

Included are:

- siting
- corridors and access
- surrounding land uses/activities (existing and future)
- future development potential
- environmentally sensitive receptors
- "effect" oriented factors:
  - amenity, economic need
  - choice amongst options
  - separation (cordon sanitaire)
- management in relation to development
- potential future uses of any vacant land surrounding hazardous facilities



[redacted] FIGURE 15-3 GENERAL LAND USE PLANNING AREAS AROUND A REFINERY (Map, Courtesy of UBD, Australia)

### 15.3.2 Issues for Process Industry Management

Included are:

- life cycle of the proposal
- - potential for site contamination
- - responsibilities for bankrupts
- hazardous versus potentially hazardous operations
- cost-benefit analysis
- "source" oriented factors associated with the operations
- - risk management

A facility is considered “hazardous” if the risk from the operations exceeds the tolerability criteria either due to inadequate or lack of hazard control measures. It is “potentially hazardous” if the hazard control measures are sufficient to reduce the risk to tolerable levels are lower.

### 15.3.3 Communications Issues

Included are:

- effective processes
- encompassing community, government and proponents
- level of community involvement in decision making
- access to adequate resources/information
- honesty and openness

### 15.3.4 Control Issues

Included are:

- defining potentially hazardous operations
- categorization strategies for such operations (minor, moderate, major etc.)
- regulation of operations:
- land use (successors in title)
- development (holder)
- activity (licencing)
- on-going monitoring
- audits/reviews
- need to look at different client needs:
  - public safety and health
  - occupational health & safety
  - environmental protection

### 15.3.5 Route Selection for Transportation Risk Management

Transport and pipeline route selection is an important planning decision. Incidents such as those in Example 15-1 illustrate the need for DG transport route planning and the siting of key depots for storage and transfer operations.

Route selection of DG transport for existing roads and highways is done primarily on the basis of qualitative analysis with some quantitative consequence modelling based on standard scenarios. The factors that influence route selection include:

(i) imposed consequences of loss of containment and subsequent events such as fire, explosion and toxic impacts.
(ii) frequency and type of DG loads in an area
(iii) traffic density on routes and the presence of intersections, rail crossings and tunnels.
(iv) population density along prescribed route.
(v) adjacent land development zones.
(vi) time of transport operations (day versus night operations)
(vii) historical traffic accident rates in a given route

In cases of major transport of large quantities of dangerous goods such as explosives, ammonia, chlorine or special fuels it can often be necessary to assess societal risk levels and use these to generate alternative routing options. Assessment of linear risks is discussed in Chapter 9.

## 15.4 RISK MANAGEMENT FACTORS

In applying risk management practice to land use planning we need to define what factors affect the decision making process and what information is critical to that process.

Risks to life, property and the environment arise from hazardous materials and activities as well as their management. We need to identify these issues, determine the adequacy of the underlying design and the safety management systems in order to understand likely impacts. Chapters 4 to 11 address many of these issues.

How do we address the "residual" risk after we have implemented our design and procedures? It is done in two basic ways.

a) the in-situ or “source” oriented measures
b) the regulation of land use or “effect” oriented measures

We need both (Milburn and Cameron 1992). There are numerous examples where risk has been increased dramatically by failure at the “source” or process level as well as a failure in land use planning procedures which has compromised safety for local communities.

This is especially the case where 'cordon sanitaire' or buffer areas originally established around high risk operations are rezoned for residential development.

### EXAMPLE 15-5 RESIDENTIAL REZONING

a) In the mid 1950s the Lucas Heights (Australia) HIFAR research reactor for producing radio isotopes was built in isolated bushland southwest of Sydney, many kilometres from residential areas. Over the past 40 years development pressures on local authorities in the area have meant the rezoning of land to the east of the site for intensive suburban development. Now, residential homes are located within 900 metres of the facility and vocal opposition has been evident to the renewal of the reactor facilities.

b) Residential rezoning around the Caltex Refinery in the Brisbane (Australia) suburb of Wynnum North resulted in encroachment of high population densities around the refinery. Following the residential development, complaints regarding refinery noise levels and night lighting from the flares increased dramatically forcing significant investments by the operator to address such issues.

Further attempts to establish high density townhouse developments on nearby land were challenged by the refinery and several other parties in the Land and Environment Court. These challenges were successful in maintaining lower population densities, based mainly on planning arguments where risk was only one of many decision factors.

### 15.4.1 Approaches to Land Use Planning for Major Hazards

There are several key approaches to the land use planning issue - covering qualitative to quantitative approaches (HSE 1989; Christou et al. 1999; Christou and Porter 1999).

#### *15.4.1.1 Generic separation distances*

These set separation distances of residential areas from a range of industrial developments. These were mainly based on experience and on environmental emission impacts such as odour. Buffer distances serve three key purposes:

- they help control the impact of industrial emissions thus maintaining quality of life issues
- they protect amenity
- they help manage off-site risks from industrial operations (the "effect" oriented factor)

**EXAMPLE 15-6 GENERIC SEPARATION DISTANCES BETWEEN INDUSTRIAL AND SENSITIVE LAND USES**

The EPA in the State of Western Australia (EPAWA 2004) has proposed guidance for separation distances based principally on environmental grounds. Typical of these separation distances are:

| | | |
|---|---|---|
| aluminium production | : | 1500-2000 metres |
| cement manufacture | : | 1000-2000 metres |
| chemical fertilizers | : | 1000-2000 metres |
| chlor-alkali | : | 2000-3000 metres |
| power station | : | 3000-5000 metres |
| gas works to supply mains | : | 300 metres |
| pesticides manufacture | : | 300 - 1000 metres |

The quoted ranges quoted ranges cover different extents of activity. In many cases, individual studies using risk based methods are deemed necessary, rather than relying on crude separation distances.

The use of generic separation distances has a number of characteristics:

a) They seek to ensure essentially "zero" harm to sensitive land uses
b) They do not directly address the risk issue in terms of major hazards
c) They can lead to significant areas of land being embargoed from development, with significant cost to land owners and local authorities.

#### *15.4.1.2 Consequence based land use planning*

An initial step in using quantification is consideration of impacts from hazardous incidents at "source". This leads to concepts of hazard distances to specified threshold levels for a range of incidents such as explosion, fire and toxic releases.

Christou et al. (1999) discuss the idea of "reference scenarios" that a proponent must address as part of the approval process. These can be supplemented by other scenarios identified by the competent authority or proponent. This approach takes no account of scenario likelihood and is an application of the 1D risk management model of section 3.2.1.

Issues of what are "credible" or "worst conceivable" scenarios to consider as well as the appropriate threshold levels for assessment continue to be debatable aspects of this approach. Assessment criteria such as IDLH or ERPG levels for toxic exposures covered in section 7.4.1 or specific overpressures causing eardrum rupture can be used to establish the hazard range.

Reference scenarios currently used for example in France include such events as:

a) BLEVE incidents for liquefied gases
b) Total, instantaneous loss of containment for pressure vessels
c) Fire in largest storage tank
d) Explosion of storage tank vapour space

The consequence based approach generally leads to large areas of land being embargoed from development around major hazard operations. It tends towards significant conservatism in land use planning terms. However the approach is extensively used worldwide, especially in Europe.

The uncertainties associated with QRA have been discussed in detail in Chapters 9 and 10. Because of the large variance in the assessed risk, the risk based approach has not been used in Germany, but the focus has been on incident prevention and consequence minimisation. Graf et al. (2004) provide a good insight into handling the uncertainty in risk assessment for land use planning decisions.

An alternative approach is to generate vulnerability maps of land uses surrounding hazardous facilities, based on the nature of the incident and its physical effects, and the vulnerability of the target receptors. The information is captured on a large matrix, where the land uses are represented as area cells. Geographical Information System (GIS) tools are used for data processing and information and management (Tixier et al. 2004).

In France, the approach is essentially based on consequence assessment of postulated accident events, and reduction of the consequence impact through a number of engineering measures, using land use planning as complementary to onsite hazard control measures. The word 'risk' is used in this sense and not in the probabilistic sense (Salvi et al. 2004).

In a related issue of planning emergency response to industrial accidents the Province of South Holland in the Netherlands developed assessment tools based on consequence analysis from fire, explosion and toxic releases. These provided a structured and justifiable way of using simple consequence methods to provide useful inputs into decision making (Ham and Blom-Bruggeman 1998a, b). They were considered as giving conservative impact assessments.

#### *15.4.1.3 Risk based land use planning*

This approach uses the 2D risk management model of section 3.2.2 where both consequence and likelihood are considered in arriving at an imposed risk from an operation. Generating risk estimates is far more time consuming than the previous approaches and is only justified for operations that are deemed as major hazards.

As discussed in sections 2.2 and 2.3 both individual and societal risks are used in this form of land use planning. National and regional governments often adopt a range of tolerable risk levels for specific land uses such as residential, commercial and recreational uses. Such criteria are discussed in Chapter 9. Prominent in the application of risk based land use planning strategies are the UK, The Netherlands, Belgium, Hong Kong and Australia. Some key characteristics of selected countries are:

a) The Netherlands

- Maximum individual risk level of $10^{-5}$/yr for housing around existing sites
- For a single risk source, maximum tolerable individual risk of $10^{-6}$/yr
- Application of societal risk criterion of $10^{-3}/N^2$ for N or more fatalities
- Application of ALARP to all risks from operations

b) Australia

The State of New South Wales has adopted the following criteria for individual risk (DIPNR 2001):

- Maximum individual fatality risk of $10^{-6}$/yr in residential areas
- For other sensitive land uses, individual fatality risks are:

  $<$ $50 \times 10^{-6}$/yr for nearby industrial sites
  $<$ $10 \times 10^{-6}$/yr for recreation/sports areas
  $<$ $5 \times 10^{-6}$/yr for commercial developments
  $<$ $0.5 \times 10^{-6}$/yr for schools and hospitals

- Injury criteria are also used:

  $<$ $50 \times 10^{-6}$/yr chance of 4.7 kW/m$^2$ heat flux at residences or 7 kPa overpressure impacts
  $<$ $50 \times 10^{-6}$/yr chance of 23 kW/m$^2$ heat flux at industrial sites or 14 kPa overpressure impacts
  $<$ $10 \times 10^{-6}$/yr chance of serious injury from toxic exposure
  $<$ $50 \times 10^{-6}$/yr chance of acute responses from toxic exposure

Although no explicit societal risk criteria are considered, the variation in individual fatality criteria do take this into consideration. Other Australian states have similar risk criteria.

c) The United Kingdom

The UK HSE refers to a consultation distance based on postulated accident events to set limits, but decision making is essentially risk-based (HSE 1989).

The HSE makes use of individual risk criteria in land use planning decisions. In most cases these are applied to new developments in the vicinity of existing hazardous operations. The Health and Safety Executive (HSE) recommended (Jones, 1989) the use of the concept of "dangerous dose" to an individual to address the issue of differing susceptibilities to event impacts.

They seek to define a dose of toxic gas, thermal radiation or overpressure which gives the following effects:

- severe distress to everyone (substantial number needing medical attention)
- some seriously injured (requiring prolonged treatment)
- highly susceptible might be killed

Using this concept the HSE,

a) uses a lower bound of $1 \times 10^{-6}$ per year of receiving a 'dangerous' dose or worse. This equates to $1 \times 10^{-6}$ per year chance of fatality for those who are highly vulnerable.
b) uses ⅓ in a million per year of a ‘dangerous’ dose or worse for cases involving institutions or long stay hospitals.
c) uses an upper bound of 10 in a million per year of a 'dangerous' dose of worse for all development cases above a certain size.

In applying these criteria, the HSE would give the following advice:

(i) Indicate 'ALLOW' for any proposals below the lower bound as this is considered negligible (⅓ or 1 in a million)
(ii) Indicate 'REFUSE' for any development proposal involving 25 or more people where the upper bound (10 in a million) is exceeded.
(iii) Where the risk is in the intermediate zone the HSE considers if there are features which tend to justify more or less straight advice, CONSULT.

In terms of societal risk, the HSE is not prescriptive in its use of F-N graphs, although these risk representations are certainly used in large scale, fixed site and transport studies.

In dealing with developments near existing major hazards the HSE have classed developments into four categories. These are:

| | |
|---|---|
| Category A: | Housing, hotel, holiday accommodation |
| Category B: | Workplaces, car parks, warehouses etc. |
| Category C: | Retail, community, leisure |
| Category D: | Highly vulnerable (schools, hospitals etc.) |

Using these categories, the HSE has then combined these with the previous limits on risk to give a 3 zone planning concept, shown in Table 15-2.

TABLE 15-2 HSE ADVICE ZONES

| Category | Zone | | |
|---|---|---|---|
| | Inner | Middle | Outer |
| A | Refuse | Consult | Allow |
| B | Allow | Allow | Allow |
| C | Consult | Consult | Allow |
| D | Refuse | Consult | Consult |

The inner zone, middle zone and outer zone distances are based on levels of thermal radiation, overpressure and toxic dose. They clearly depend on the type of hazardous activity considered. This categorisation provides the basis for the "consultation" distances set by the HSE. Using these distances, it is necessary to consult with the HSE for new non-hazardous developments within the consultation zone, which generally coincides with the outer zone distance. In general, the distances to the zones are based on

(i) Inner zone: $\geq 10 \times 10^{-6}$ per year of at least 1000 thermal dose units (1000 $(kW/m^2)^{4/3}$ .s) or 14 kPa overpressure. The thermal dose is related to probit calculations.

(ii) Middle zone: $\geq 1 \times 10^{-6}$ per year of at least 1000 thermal dose units or 14 kPa overpressure.

(iii) Outer zone: $\geq ⅓ \times 10^{-6}$ per year of at least 1000 thermal dose units or 7 kPa overpressure.

These are considered conservative values. The above approach classifies development and then bases decision making on the 'dangerous' dose concept at various risk levels.

### 15.4.2 Assessing Source Oriented Factors

Here the onus is on the operator to ensure that good risk management is in place. The process relies on concepts covered in earlier chapters that include:

(i) hazard identification - systematically looking for potential hazard incidents which could harm;

(ii) consequence analysis - determining the release rates of substances and the subsequent physical effects;

(iii) frequency analysis - determining the likelihood that such specified events will occur;

(iv) risk analysis - combining consequences and frequencies to arrive at individual and societal (group) risk levels; and

(v) risk assessment - comparing identified risks with defined risk criteria for decision making and ensuring risks are ALARP.

At the present time, quantitative risk assessment provides the principal tool for informed land use safety planning.

### 15.4.3 Assessing Effect Oriented Factors

A proposal to introduce a hazardous establishment to a locality or to extend existing operations involves a number of effect oriented decisions. These include:

a) whether, on planning grounds such as amenity, access or economic need the activity should be permitted;
b) a choice amongst options - siting, alternate access routes, disposal systems;
c) the other land uses to be permitted nearby, for example, housing, shopping centres, sports facilities; and
d) the separation distances required between the plant and the adjoining sensitive land uses.

The basis of these decisions is whether the establishment is justifiable, in any one of its optional states, to the proponent, regulatory authorities and the public. The risks generated by the activity are usually only one of the factors which influence the final decision. Other factors such as operational, economic, social, political and environmental are usually of equal importance. However, when the risks are high, they may dominate the decision making.

### 15.4.4 Implementing Risk Management

Minimising the risk from hazardous industries should be central to any process of risk management. The key principles for this may be gleaned from experience within Australia and beyond. These principles are:

- classifying the hazardous establishments by magnitude of risk:
- setting thresholds of risk between each category;
- determining the appropriate mechanisms for risk estimation;
- determining the significance of risk in terms of sensitive land uses; and
- determining the mechanisms for controlling those risks.

#### *15.4.4.1 Classifying hazardous activities*

These have been mentioned briefly in section 15.1.1. It is possible to categorise hazardous industries by taking into account both frequency and consequence of incidents flowing from inventories of hazardous substances and on-site operations. In Categories 1 and 2, it is considered that the quantities of hazardous substances used on-site will cause no significant off-site impacts. Categories 3 and 4 are of key concern to land use safety planning. Because of the range of risk within categories, there are grey areas between categories which may require consultation to resolve key issues.

The action considered appropriate to each of the four categories is detailed below.

- Category 1: Minor risk sites - where only occupational risks having negligible off-site impacts are likely to arise. These establishments would contain minor amounts of hazardous substances, would be exempt from the need to placard, and could be exempted from the hazardous industry controls.
- Category 2: Potential moderate risk sites - where minimal off-site risks may be expected, which would be considered acceptable (tolerable from the public's viewpoint). The operation of such establishments would be allowed subject to compliance with prescriptive regulations, under the duty of care of the occupier. Those sites generating risks which bring them into the grey area with Category 3 may require special treatment.
- Category 3: Potential major risk sites (MHFs) - generating justifiable risks, which may be permitted at the discretion of the relevant authority provided the risk is reduced below an acceptable level.
- Category 4: Extreme risk sites - generating unacceptable risks which should be prohibited.

#### 15.4.4.2 Quantifying the thresholds

It is necessary to filter out those establishments which constitute minor risk to adjacent and adjoining land uses. It is important that the initial filtering method uses a simple technique based on potential hazard rather than the laborious and costly techniques in quantified risk assessment. A factoring method based on dangerous goods quantities is used in Australia, the USA and the European Communities.

Figure 15-4 shows an integrated approach for local authorities who need to deal with operations involving dangerous goods (Cameron 1997). This identifies several categories of activities dealing with dangerous goods with the initial classifications being made on quantities of classes of DGs. Once classification is made then the appropriate level of analysis can be made.

#### 15.4.4.3 Applying quantitative risk assessment

Using a self-regulation process, a proponent or occupier can categorise the establishment. Where it clearly lies within the higher risk Categories 3 and 4, the regulatory authority normally requires the submission of a risk assessment to support an application for approval to develop or expand the facility. Such a requirement is incorporated in the terms of reference of an environmental impact assessment.

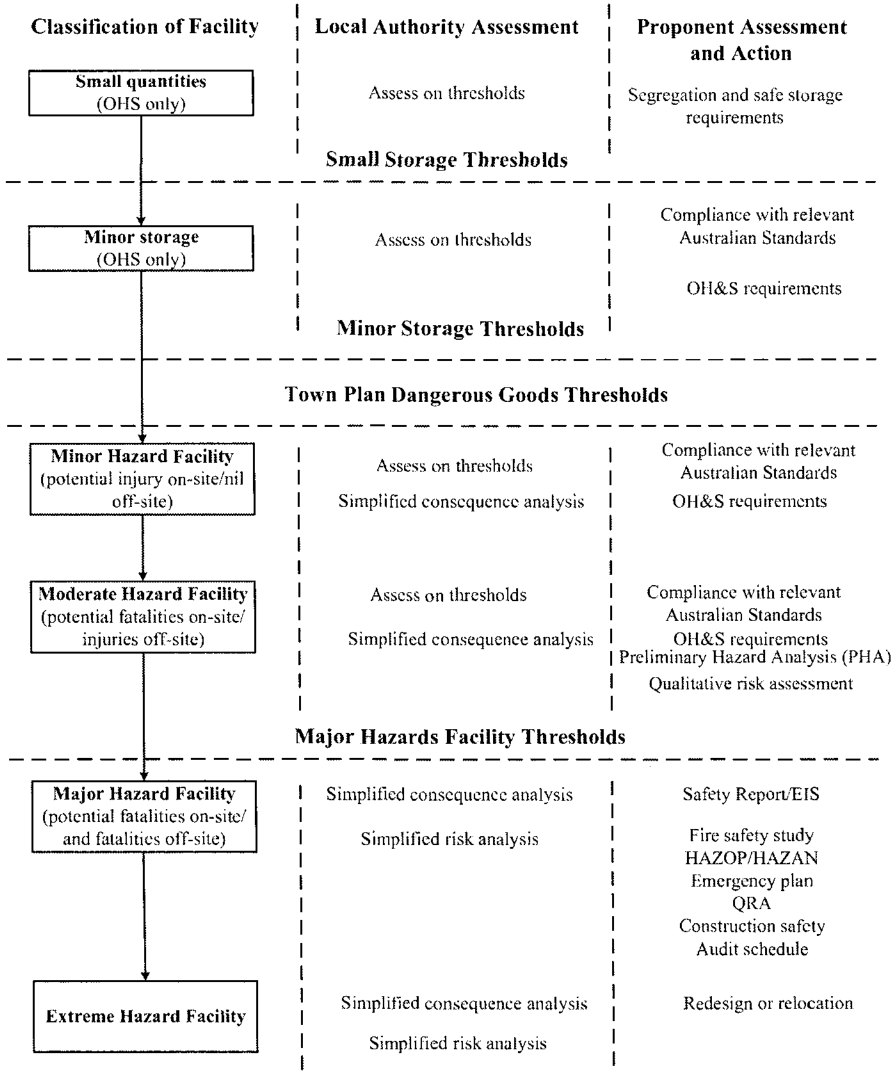
#### 15.4.4.4 Determining the significance of risk

The significance of the identified risks must be determined for those establishments which are in the higher risk categories.

Iso-risk contours on a land use or area map would indicate areas of concern. For establishments which impose intolerable risk on sensitive land uses, the res'ponsible authority can require further risk reduction. In cases where the risks are tolerable, the authority would still demand that the risks be reduced to as low as reasonably practicable (ALARP).

### 15.4.4.5 Mechanisms to control risk

The residual risk imposed by an operation can be reduced in two different ways, namely in-situ measures (technology and management), or by physical separation. Minimising risk implies control, either self-control or imposed control or a combination of both. In order to optimise the attributes of a particular establishment, it is necessary to impose both forms of risk reduction.



| Classification of Facility | Local Authority Assessment | Proponent Assessment and Action |
|---|---|---|
| Small quantities (OHS only) | Assess on thresholds | Segregation and safe storage requirements |
| | Small Storage Thresholds | |
| Minor storage (OHS only) | Assess on thresholds | Compliance with relevant Australian Standards<br>OH&S requirements |
| | Minor Storage Thresholds | |
| | Town Plan Dangerous Goods Thresholds | |
| Minor Hazard Facility (potential injury on-site/nil off-site) | Assess on thresholds<br>Simplified consequence analysis | Compliance with relevant Australian Standards<br>OH&S requirements |
| Moderate Hazard Facility (potential fatalities on-site/ injuries off-site) | Assess on thresholds<br>Simplified consequence analysis | Compliance with relevant Australian Standards<br>OH&S requirements<br>Preliminary Hazard Analysis (PHA)<br>Qualitative risk assessment |
| | Major Hazards Facility Thresholds | |
| Major Hazard Facility (potential fatalities on-site/ and fatalities off-site) | Simplified consequence analysis<br>Simplified risk analysis | Safety Report/EIS<br>Fire safety study<br>HAZOP/HAZAN<br>Emergency plan<br>QRA<br>Construction safety<br>Audit schedule |
| Extreme Hazard Facility | Simplified consequence analysis<br>Simplified risk analysis | Redesign or relocation |

FIGURE 15-4 A GRADED FRAMEWORK FOR ASSESSING DANGEROUS GOODS FACILITIES

## 15.4.5 Decision Making and Land Use Planning

What are the principal concerns and issues that make up the decision process? The following subsections give some ideas.

### *15.4.5.1 Nature of potential effects on people*

- How are they affected?
  - Is it injury or fatality which is predicted or is disease likely to occur?
- What is the agent of the harm inflicted?
  - This could include blast impact, fire radiation or toxic gases.
- What is the affected area if the incident were to occur?
  - This looks at the extent of the incident and seeks to quantify the effect distances. These could be quite variable depending on time of the year and operational modes.

### *15.4.5.2 Nature of effects on surrounding land use*

This seeks to identify clearly the sensitive land uses that could be involved in any incident. These include:

- residential areas
- business and industry sectors
- recreation and commercial areas
- sensitive land uses such as schools, aged housing and hospitals

### *15.4.5.3 Nature of the accompanying effects*

This looks at other associated issues of the operation and can include:

- wastewater, refuse disposal
- noise generation
- transport of raw materials, products (road, rail, pipeline etc.)
- lighting (external, flares etc.)
- visual amenity (buildings and structures)
- odour
- natural environment values

### *15.4.5.4 Economic benefits*

This issue considers what benefit the operation has to the local community, region or state. In some circumstances it is possible that the individuals who bear the risk do not benefit from the activity. This makes acceptance difficult. Economic issues include:

- employment generation
- what are the benefits to the exposed community

- are there other benefits such as support for community activities?
- what are the benefits to the general economy?

#### 15.4.5.5 The nature, purposes and limitation of risk assessment

The issues here can include:

- Purpose of the assessment
  (i) Justify a new operation
  (ii) Optimise an existing or new operation

- Nature of the assessment
  (i) Is it conservative in its approach?
  (ii) Is it a "cautious best estimate"?

- Role of uncertainties
  (i) in identifying likely scenarios
  (ii) in predicting consequences
  (iii) in estimating frequencies

#### 15.4.5.6 Other influencing economic factors

These can include:

- is it new plant or risk control measures on an existing operation?
- is it an extension of existing operation or new plant on a greenfield site?
- has the ALARP principle been applied?

#### 15.4.5.7 Dimensions of public concern and risk communication

An important aspect of decision making is the level of public concern and what affects this.

- is the risk familiar?
- is an existing plant regarded as well established and secure?
- is there a perception of associated benefits to the public?
- what unfavourable associations are in the public mind?
- has there been recent incidents involving this type of operation?
- is the public involvement adequate?
- if there is expert advice, is there any confidence in it?
- can the emergency services cope with any incidents?

The importance of risk communication has been emphasized in sections 2.7 and 13.4.8. Allen (1997) and Bier (2001) discuss many relevant issues surrounding communication of risk to the public amongst which the most important are:

- a recognition that the affected community is often strongly divided on risk issues with many not approving of the cost-safety trade-off approaches often used.
- the changing attitudes of the community who can readily amend views based on situational changes, either becoming more accepting or more resistant based on industry performance.
- the demand of local communities to be true participants in the decision making process. This typically through the environmental impact assessment (EIA) process.
- the growing sophistication of local community understanding of risk issues and their ability to articulate concerns regarding land use planning issues.
- the ever increasing standard of living that demands greater levels of amenity in residential zones.

All the above factors are important in the overall decision making process. It has been said often that this type of activity in land use planning is 'a social and economic decision making activity, accompanied by technical information'.

**EXAMPLE 15-7 RISK BASED ISSUES AROUND A REFINERY**

Figure 15-3 set out planning areas adjacent to a major petroleum refinery. This showed various separation zones between the residential areas and heavy industry to the north and lower risk general industry to the west.

A number of quantitative risk assessments had been carried out by the refinery operators to help assess potential off-site impacts from major accidents on the site. The off-site risk was dominated by hydrogen fluoride (HF) releases from the alkylation unit. Figure 15-5 shows the approximate regions for both $1\times10^{-6}$ and $1\times10^{-7}$ individual fatality risks per annum. The range reflects the uncertainty between the best estimate and a conservative estimate. Societal risks were also assessed.

On the basis of individual fatality risk, current residential areas are not significantly impacted by the events considered on the refinery site. However high density development at the northern end of the residential area was refused based on a number of considerations (Brabazon 2001). These included:

(i) That due to the risks from all sources, and not just HF incidents, the acceptability of the risk to proposed development was not demonstrated. These additional risks arose from other industries plus rail and road transport activities.

(ii) Further encroachment of high population density developments would further compromise the operations at the refinery.

(iii) The community need for residential development in the proposed area could not be demonstrated since alternative sites were available and the establishment of residential developments has far more flexibility than relocating industrial operations.

(iv) The development was incompatible with the provisions of the City Plan which sought to avoid small allotment areas and maintain population densities to low levels.

This situation clearly illustrates that "risk" in planning terms is a multifaceted concept not restricted to safety risks but encompassing both the acute and chronic aspects from industrial and transport activities. Land use planning decisions require authorities to consider the totality of risk and the provisions enshrined in planning precincts that seeks to balance a range of different land use precincts.

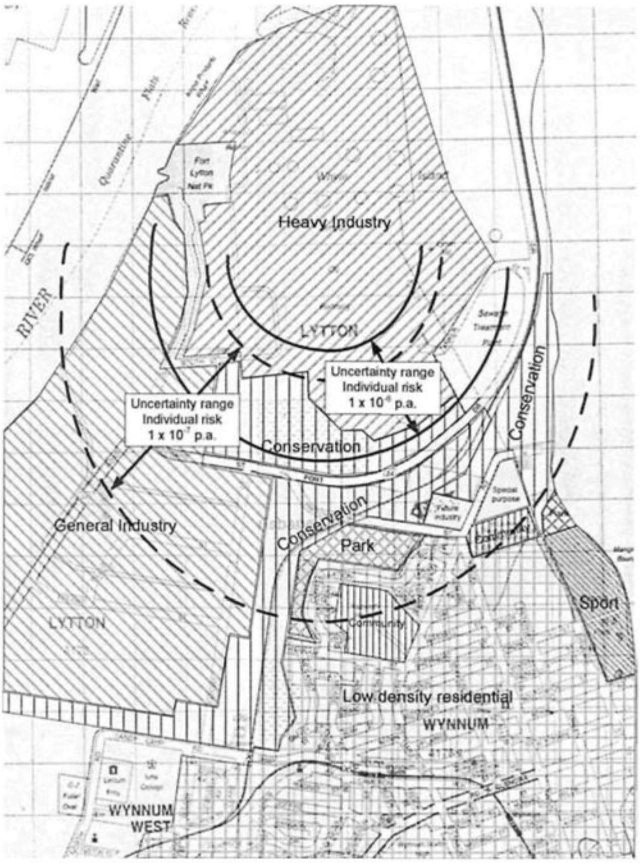


FIGURE 15-5 RISK CONSIDERATIONS AROUND A REFINERY SITE (Map, Courtesy of UBD, Australia)

## 15.5 REVIEW

Hazards, risks and planning is a multi-faceted problem and one that is certainly non-trivial. However there are key issues which can be addressed effectively provided that all affected parties are involved in the consultations.

Risk management is the real concern of planners when hazardous operations are to be considered. Decisions must take into account not just technical issues of hazard and risk but also community needs, social justice, economic viability and a range of other performance measures.

Land use planning is essentially an economic and social activity informed technically by risk assessment.

## 15.6 REFERENCES

Allen, P.T. 1997, 'Trading Cost against Safety: The structure of people's beliefs', *Process Safety Progress*, vol. 16, no. 2, pp. 89-93.

Bier, V.M. 2001, 'On the state of the art: risk communication to the public', *Reliability Engineering and System Safety*, vol. 71, pp. 139-150.

Brabazon 2001, 'Edgarange Pty Ltd. v. Brisbane City Council and Ors', Planning and Environment Court, Brisbane, QPEC 01.062, September 21, Queensland, Australia.

Cameron, I.T. 1997, *Definition and Assessment Procedures for Dangerous Goods, Facilities: Brisbane City Council,* Research Report, Uniquest Ltd., The University of Queensland, Australia, December.

Cassidy, K. and Pantony, M. 1988, 'Major Industrial Risks - A Technical and Predictive Basis for On and Off-site Emergency Planning in the Context of UK Legislation', *Institution of Chemical Engineers Symposium Series, No. 110*, pp. 75-94.

Christou, M.D. and Porter, S. 1999, *Guidance on Land Use Planning as required by Council Directive 96/82/EC (Seveso II)*, Institute for Systems Informatics and Safety, Report EUR 18695 EN, Italy.

Christou, M.D., Amendola, A. and Smeder, M. 1999, 'The control of major accident hazards: The land-use planning issue', *Journal of Hazardous Materials*, vol. 65, pp. 151-178.

Dept. Tourism, Small Business and Industry 1996, *Risk Assessment, Hazard Analysis and Planning for Difficult to Locate Activities*, Info. Paper, Qld Govt.

DIPNR 2001, *Hazardous Industry Planning Advisory Paper No 4: Risk Criteria for land use safety planning*, Dept. of Infrastructure, Planning and Natural Resources, NSW State Government, Australia.

EPAWA 2004, *Guidance for the Assessment of Environmental Factors: Separation distances between industrial and sensitive land uses*, No. 3 Draft, EPA Western Australia, Australia.

Government of Victoria 2000, *Occupational Health and Safety (Major Hazards) Regulations*, Melbourne, Australia.

Graf, H., Klein, T. and Schmid, O. 2004, 'Explicit Offsite Risk Analysis Methods: Weaknesses and Current Work', *11th International Symposium Loss Prevention*, Prague, pp. 1117-1125.

Ham, J.M., and Blom-Bruggeman, J.M. 1998a, *Guide to hazardous industrial activities*, Fire Service Directorate of the Ministry of Home Affairs, The Province of South Holland, The Netherlands.

Ham, J.M. and Blom-Bruggeman, J.M. 1988a, *Enclosures to be used in conjunction with the Guide to hazardous industrial activities*, Fire Service Directorate, Ministry of Home Affairs, The Province of South Holland, The Netherlands.

HSE, Health and Safety Executive, UK 1986, *The Control of Major Accident Hazards Regulations 1984 (CIMAH): further guidance on emergency plans*, HMSO, London, ISBN 0-11-883831-8.

HSE, Health and Safety Executive, UK 1989, *Quantitative Risk Assessment: Its Input to Decision Making*, HMSO, London.

HSE, Health and Safety Executive, UK 1990, *Risk Criteria for Land-Use Planning in the vicinity of Major Industrial Hazards,* HMSO, London.

Jones, D.A. 1989, 'Acceptable risk - The use of HSE risk criteria for the siting of public development near major hazards', *6th International Symposium on Loss Prevention and Safety Promotion in Process Industries*, June 22.

Kinhill Cameron McNamara 1994, *Planning for Employment, Industry and Business Development, DCP Implementation Provisions for Business and Industry Precincts*, Reports BC4609-503-Rev0, July.

Laheij, G.M.H., Post, J.G. and Ale, B.J.M. 2000, 'Standard methods for land-use planning to determine the effects on societal risk', *Journal of Hazardous Materials*, vol. 71, pp. 269-282.

Lines, I.G. 1998, *The implications of major hazard sites in close proximity to major transport routes*, HSE Contract Research Report 163/1998, HMSO, St. Clements House, Norwich, UK.

Milburn, M. and Cameron, I.T. 1992, *Planning for Hazardous Industrial Activities in Queensland*, AIUS, Queensland, ISBN 0-86419-814-0.

Miller, C. and Fricker, C. 1993, *Planning and Hazard in Progress in Planning*, Pergamon Press, December.

OECD 1990, *Role of Public Authorities in Preventing Major Accidents and in Major Accident Hazard Land use Planning*, Discussion document, OECD Workshop, 19-22 February.

Queensland Emergency Services 1995, *Review of Hazardous Substances Management in Queensland*, CHEM Unit, Qld Emergency Services, December.

Salvi, O., Rodrigues, N., Descouriérre, S., and D. Gaston, D. 2004, 'Risk assessment and decision making related to Land Use Planning in France', *11th International Symposium Loss Prevention*, Prague, pp. 1304-1311.

Tixier, J., Dandriuex, A., Dusserre, G., Bubbico, R., Luccone, L.G., Mazzarotta, B., Silvetti, B., Hubert, E., Rodrigues, N., Salvi. O. and Gaston, D. 2004, 'Vulnerability of the environment in the proximity of an industrial site', *11th International Symposium Loss Prevention*, Prague, pp. 1260-1267.

TSGB 2003, *Transport Statistics for Great Britain (TSGB), Chapter 4, Road traffic, freight and accidents and motor vehicle offences*, UK Department of Transport, United Kingdom.

Versteeg, M.F. 1989, 'The Practice of Zoning: How PRAs can be used as a Decision-Making Tool in City and Regional Planning', *Reliability Engineering and System Safety*, vol. 26, pp. 107-118.

## 15.7 NOTATION

| | |
|---|---|
| ALARP | As Low As Reasonably Practicable |
| B&I | Business and Industry |
| BLEVE | Boiling Liquid Expanding Vapour Explosion |
| DCP | Development Control Plans |
| DG | Dangerous Goods |
| DIPNR | Department of Infrastructure, Planning and Natural Resources, NSW, Australia |
| DoT | UK Department of Transport |
| DOTARS | Australian Government, Dept. of Transport, Regional Services |
| EC | European Community |
| EIA | Environmental Impact Assessment |
| EPA | Environment Protection Agency |
| EPAWA | Environment Protection Authority of Western Australia |
| ERPG | Emergency Response Planning Guidelines |
| GIS | Geographical Information Systems |
| HSE | Health & Safety Executive, UK |
| IDAS | Integrated Development Approval Schemes |
| IDLH | Immediately Dangerous to Life and Health |
| IMDG | International Maritime Dangerous Goods |
| km | kilometres |
| kPa | kilo-Pascals |
| kW/m$^2$ | kilo-Watts per square metre |
| LPG | Liquefied Petroleum Gas |
| LUP | Land Use Planning |
| MHF | Major Hazard Facility |
| N | Number of fatalities |
| OH&S | Occupational Health & Safety |
| PHA | Preliminary Hazard Analysis |
| PRA | Probabilistic Risk Analysis (alternate term for QRA) |
| QRA | Quantified Risk Assessment |
| SCADA | Supervisory Control and Data Acquisition |
| TSGB | Transport Statistics for Great Britain |
| UNRMTG | UN Recommendations on the Transport of Dangerous Goods |
| USDOT | US Department of Transport |

# Index

This page is intentionally left blank