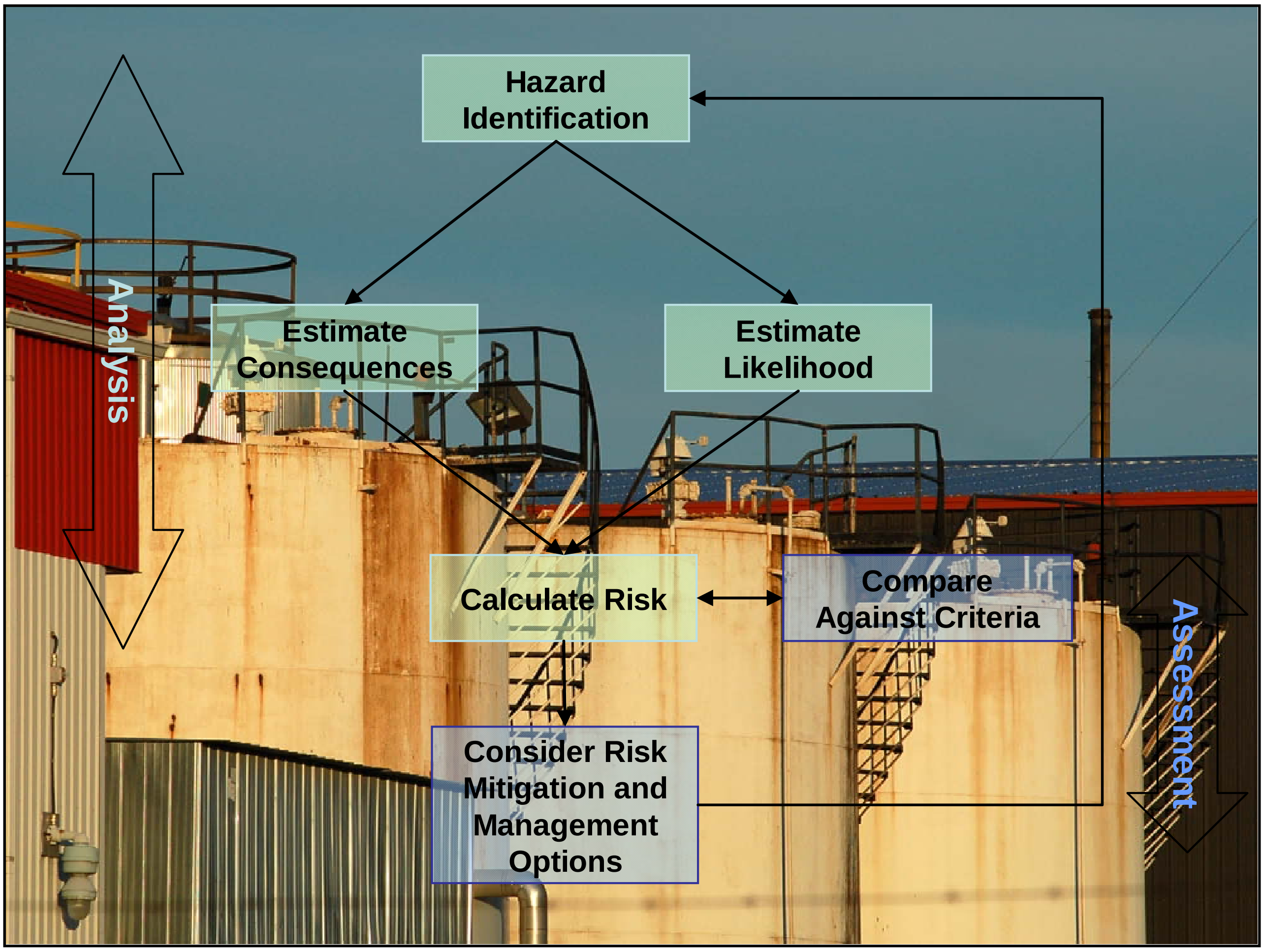
NSW GOVERNMENT | Planning

Hazardous Industry Planning Advisory
Paper No 6

Hazard Analysis



January 2011

HIPAP 6: Hazard Analysis

23–33 Bridge Street
Sydney NSW Australia 2000
www.planning.nsw.gov.au

ISBN 978-0-73475-862-0
DOP HAZ_009

Foreword

Since the 1980s, the New South Wales Department of Planning has promoted and implemented an integrated approach to the assessment and control of potentially hazardous development. The approach has been designed to ensure that safety issues are thoroughly assessed during the planning and design phases of a facility and that controls are put in place to give assurance that it can be operated safely throughout its life.

Over the years, a number of Hazardous Industry Advisory Papers and other guidelines have been issued by the Department to assist stakeholders in implementing this integrated assessment process. With the passing of time there have been a number of developments in risk assessment and management techniques, land use safety planning and industrial best practice.

In recognition of these changes, new guidelines have been introduced and all of the earlier guidelines have been updated and reissued in a common format.

I am pleased to be associated with the publication of this new series of Hazardous Industry Advisory Papers and associated guidelines. I am confident that the guidelines will be of value to developers, consultants, decision-makers and the community and that they will contribute to the protection of the people of New South Wales and their environment.

SHaddad

Director General

Contents

List of Figures and Tables

Executive Summary

Background

The orderly development of industry and the protection of community safety necessitate the assessment of hazards and risks. The Department of Planning has formulated and implemented risk assessment and land use safety planning processes that account for both the technical and the broader locational safety aspects of potentially hazardous industry. These processes are implemented as part of the environmental impact assessment procedures under the Environmental Planning and Assessment Act 1979.

The Department has developed an integrated assessment process for safety assurance of development proposals, which are potentially hazardous. The integrated hazards-related assessment process comprises:

- a preliminary hazard analysis undertaken to support the development application by demonstrating that risk levels do not preclude approval;
- a hazard and operability study, fire safety study, emergency plan and an updated hazard analysis undertaken during the design phase of the project;
- a construction safety study carried out to ensure facility safety during construction and commissioning, particularly when there is interaction with existing operations;
- implementation of a safety management system to give safety assurance during ongoing operation; and
- regular independent hazard audits to verify the integrity of the safety systems and that the facility is being operated in accordance with its hazards-related conditions of consent.

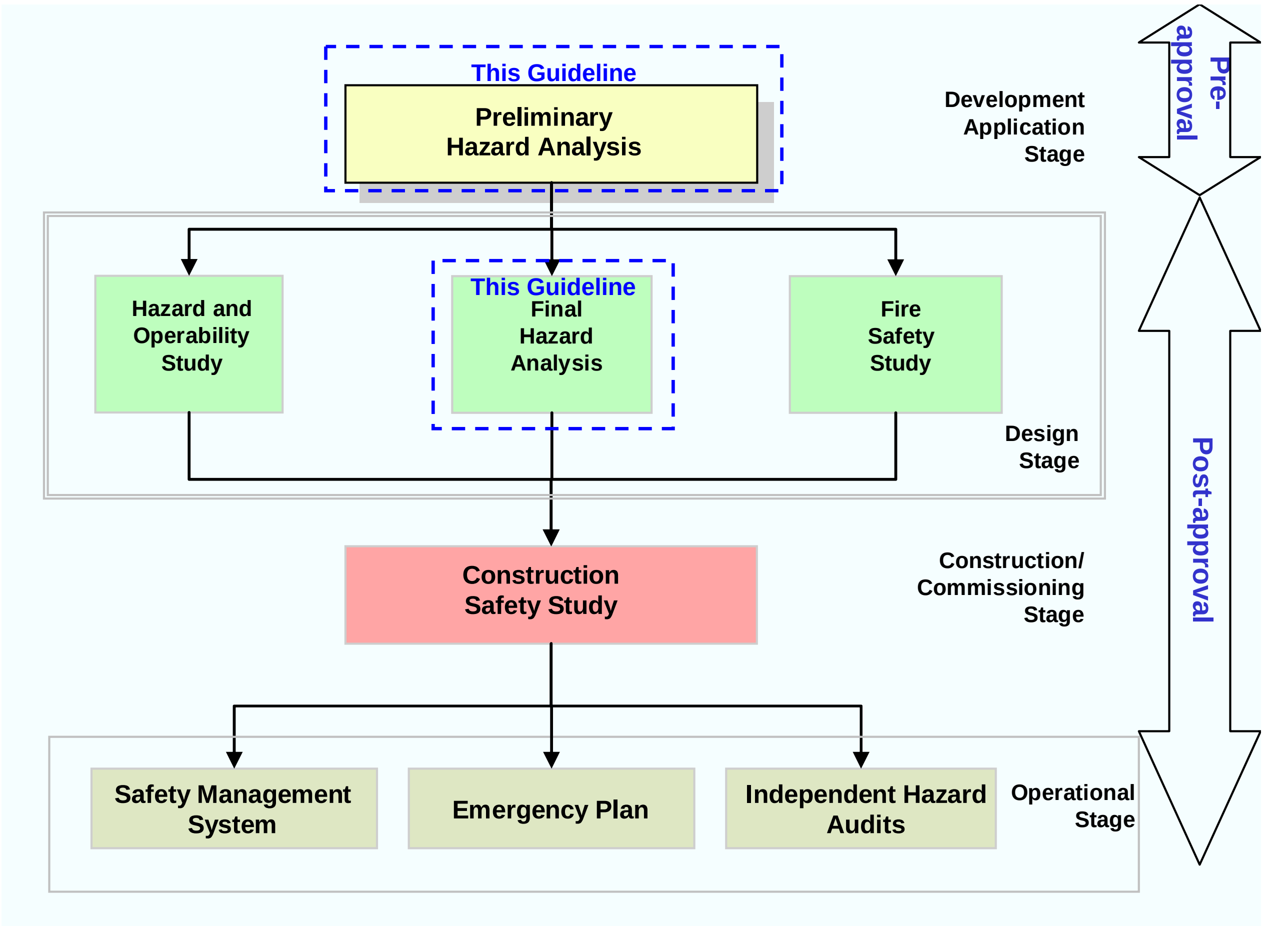
The process is shown diagrammatically in Figure 1.

A number *of Hazardous Industry Advisory Papers (HIPAPS)* and other guidelines have been published by the Department to assist stakeholders in implementing the process. All existing HIPAPs have been updated or completely rewritten and three new titles (HIPAPs 10 to12) have been added.

A full list of HIPAPs is found at the back of this document.

The part of the process covered by this guideline is highlighted in Figure 1.

Figure 1: The Hazards-Related Assessment Process



Hazard Analysis

In assessing development proposals (for new facilities and substantial modifications to existing ones), the emphasis is on preventing or minimising major hazardous incidents on-site, such as fire and explosion or the release of significant quantities of toxic or biologically harmful chemicals, that could result in significant off-site effects.

The assessment of the suitability of a site to accommodate an existing or proposed development of a potentially hazardous nature must be based on consideration of:

- the nature and quantities of hazardous materials stored and processed on the site;
- the type of plant and equipment in use;
- the adequacy of proposed technical, operational and organisational safeguards;
- the surrounding land uses or likely future land uses; and
- the interactions of these factors.

This information is incorporated into the hazard analysis. The objective of hazard analysis is to develop a comprehensive understanding of the hazards and risks associated with an operation or facility and of the adequacy of safeguards. Without such analysis it is difficult to be confident that design and operation can be carried out with an adequate level of safety.

The hazard analysis process encompasses qualitative and quantitative methods. However, neither quantified nor qualitative analysis should be pursued for its own sake.

The quality of the hazard analysis depends on the ability of the analyst to understand the plant and processes at the facility and assess what might go wrong. The analyst should draw upon specialised technical expertise to provide guidance as necessary.

This document provides guidance on the general approach recommended for hazard analysis and details the requirements for reports to be submitted to government authorities.

1 Introduction

SECTION SUMMARY

This section briefly introduces the document, which provides general guidance on conducting a hazard analysis. While it is particularly focused on the NSW assessment requirements for potentially hazardous industry, it is also useful as a broad introduction to the techniques of hazard analysis.

A hazard analysis may be produced at an early stage of a project to support an application for approval or after the detailed design studies have been completed.

The paper is divided into three parts. General principles of hazard analysis are first outlined, followed by a description of the components of hazard analysis. The final part details the suggested form and content of hazard analysis reports. Further information is provided in the appendices.

This document provides guidance on the general approach recommended for hazard analysis and details the requirements for reports to be submitted to government authorities. In addition to studies carried out for the assessment of development proposals, hazard analyses may be carried out for existing developments. Analysis of existing sites may be carried out, for example, at the volition of site operators, as required following hazard audits or for other regulatory processes. The approach and methodology outlined in this paper is applicable to hazard analyses carried out for all such purposes.

For proposed new development, a distinction is made between a preliminary hazard analysis (PHA) and a final hazard analysis (FHA). The PHA is required at an early stage of the project and a report on the PHA is typically required with the development application. A PHA may be based on limited information since complete data on the design and precise safeguards may not be available at the initial stage. The PHA should be as final and comprehensive as the available information allows. An outcome of the PHA may be the selection of technology or the site for the development. The results of the PHA form an input to the later stages of the project development.

The final hazard analysis extends and updates the PHA with design information that becomes available as the project progresses. It also draws upon and feeds into the results of other studies carried out as part of the development approval process, including the hazard and operability study (HAZOP), fire safety study and emergency planning. The approach and methodology for the PHA and FHA should be the same and therefore no distinction is made in this document between the two.

This guideline provides development proponents, consultants, engineers, safety officers, government officers and interested members of the community with the basis for an understanding of the various elements of hazard analysis and the standards of analysis and reporting required.

It is not intended that it provide the basis for a person or group without prior knowledge or experience to carry out a hazard analysis.

The paper is divided into three parts. Some general principles of hazard analysis are outlined in sections 2 and 3. Sections 4 to 8 describe the components of hazard analysis. The final part, commencing at page 27, details the suggested form and content of reports prepared to present the results of the hazard analysis process. Further information is provided in the appendices.

A list of reference material for further reading is included at the end of this document. The list is not exhaustive and additional specialised material may be required, depending on the nature of the particular development and the associated hazards.

2 Purpose and Principles of Hazard Analysis

SECTION SUMMARY

Hazard analysis is a tool for systematically identifying and assessing the hazards and risks associated with a facility and, on the basis of agreed criteria, forming judgements about the acceptability of those risks to the surrounding locality.

Basic principles are that hazard analysis should:

- be comprehensive, holistic and systematic;
- be qualitative, quantitative and site-specific;
- be complementary to other safety studies;
- use consistent and well-documented methods and data;
- review the adequacy of safeguards; and
- utilise all opportunities for risk reduction.

KEY MESSAGE

- The greatest benefit of hazard analysis is not the numerical outputs but rather the insight into the risks and their implications provided by the analytical process.

2.1 The Purpose of Hazard Analysis

The objective of hazard analysis is to develop a comprehensive understanding of the hazards and risks associated with an operation or facility and of the adequacy of safeguards. Without such analysis, it is difficult to be confident that design and operation can be carried out with an adequate level of safety.

Whilst hazard analysis reports play a role in providing information to government authorities to enable informed decisions on the acceptability of new or existing activities, the principal output of hazard analysis is the achievement of improved safety and the contribution to safety assurance.

The hazard analysis process encompasses qualitative and quantitative methods. The techniques provide mechanisms for:

- formal identification of hazards;
- analysis of the magnitude and likelihood of possible hazardous incidents; and
- consideration of the relevance and adequacy of proposed safeguards.

Levels of risk may also be quantified and used to form a basis for judgment of the acceptability of the risks imposed by the development and consideration of opportunities for risk reduction.

It is important that the quantification of risk be seen as only one output of the hazard analysis. Quantification of all dimensions of risk is not always possible or necessary to enable judgments to be made on sound hazard management. The results of the various elements of the analytical process — hazard identification, consequence analysis, probability/frequency analysis and risk estimation and analysis — can, and should, be used for 'avoiding avoidable risk', emergency planning, plant modification, etc.

Quantified risk results can be very powerful in:

- assisting the identification of cost-effective risk reduction measures;
- aiding choices between technologies and locations; and
- assisting judgments as to the acceptability of particular facilities and operations in particular locations.

They should not be seen, however, as absolute or objective measures nor as the most significant output of the analytical process. Throughout the analysis, the qualitative aspects need to be given due attention alongside the quantitative aspects. Analysts must understand the limitations and uncertainties of the analytical methods. Quantification should be avoided where it will not aid rigour in the analysis or it is clearly entirely arbitrary.

Furthermore, neither quantified nor qualitative analysis should be pursued for its own sake. For example, if the earlier steps in the analysis show there to be no hazards of concern, no significant consequences, or frequencies so low as to be considered non-credible, then proceeding with the analysis beyond such points may well be fruitless. However, due regard must be given to cumulative impacts.

Hazard analysis is a dynamic process. For new plants it should be integral to design. Recommendations and decisions arising out of an analysis performed early in the life of the project should form the basis of choices and decisions made in later stages. These may include the choice of location for a facility; the consideration of feasible alternative technologies; or further improvement in safeguards incorporated into equipment and operating procedures.

The quality of the hazard analysis depends on the ability of the hazard analyst to understand the plant and processes at the facility and assess what might go wrong. The hazard analyst should draw upon specialised technical expertise to provide guidance where necessary. It is usually appropriate to involve the plant designers and operational personnel in the hazard analysis. An improved understanding amongst company personnel of the hazards associated with their facility, and the resultant improvements in safety, can be an important benefit of a hazard analysis.

2.2 General Principles

The hazard analysis process should be based on the following principles. It should:

- **be comprehensive, holistic and systematic**

  The analysis should provide a comprehensive assessment of the nature of hazards at the facility as a whole. A systematic approach should be used to ensure that all parts of the plant and operations are covered and that interactions between different operations have been considered even where specific equipment or process units comply with applicable codes and standards. Judgment should be used on the appropriate level of detail.

  The analysis should consider, for example, whether natural disasters, deliberate acts or hazardous events in neighbouring sites pose a threat and the potential for the discharge of hazardous materials in waste streams. The study should also cover associated operations such as the transportation of hazardous materials.

  The analysis should apply to atypical and abnormal events and conditions. It is not intended to apply to continuous or normal operating emissions to air or water.

- **be qualitative, quantitative and site-specific**

  The hazard analysis approach combines qualitative and quantitative methods specifically tailored to address technical controls, operational and organisational issues and locational issues of a particular facility or operation. Judgment is required on the appropriate methodology and depth of analysis required based on the nature and scale of the development, the type of operations being carried out, the location of the facility and external influences. The analysis should utilise up-to-date assessment tools and techniques.

- **be complementary to other safety studies**

  The hazard analysis should be complementary to other safety studies and integral to the plant design process. Ideally, at least for new development, the hazard analysis and other safety studies should be carried out concurrently and interactively so that the output of one study can be used as an input into another, and all in turn as inputs to the refinement of the design and operating arrangements.

- **use consistent and well-documented methods and data**

  Data collection and its use should be consistent throughout the analysis. All steps taken in the process should be traceable and the information gathered as part of the analysis should be well documented to permit an adequate technical review of the work to ensure reproducibility, understanding of the assumptions made and valid interpretation of the results.

- **review adequacy of safeguards**

  Throughout the analysis, the adequacy and relevance of safeguards need to be kept under review. An important output of the analysis is the identification of appropriate additional or alternative safeguards.

  The types of safeguards which should be considered are:

  – operational safeguards such as safety related operating procedures, emergency response procedures, safety monitoring and maintenance arrangements and permit-to-work systems;

  – organisational safeguards such as overall safety management systems, training programs and systems for the assessment and documentation of modifications; and

  – physical safeguards such as plant hardware, site and plant layout, and separation from neighbouring uses.

  Procedures for the documentation and review of operational and organisational safeguards should also be assessed for their adequacy.

- **utilise all opportunities for risk reduction**

  The principle of `avoiding avoidable risk' should underlie the analyst's approach. Even where other risk criteria are met, both the consequences and likelihood of hazardous incidents should be reduced wherever technically feasible alternatives can be implemented without jeopardising the financial or technical viability of the operation or facility.

3 Elements of Hazard Analysis

SECTION SUMMARY

There are two main components of hazard analysis:

1. analysis, in which hazards are identified leading to an estimation of the risk based on the consequences of credible accidents and their likelihood; and
2. assessment, in which the risks are compared against relevant criteria and risk mitigation and management options are evaluated.

While the use of sound methods and data for consequence and likelihood estimation are very important, the most fundamental component of the process is hazard identification. The success of this step relies heavily on the qualifications and experience of the study team.

KEY MESSAGE

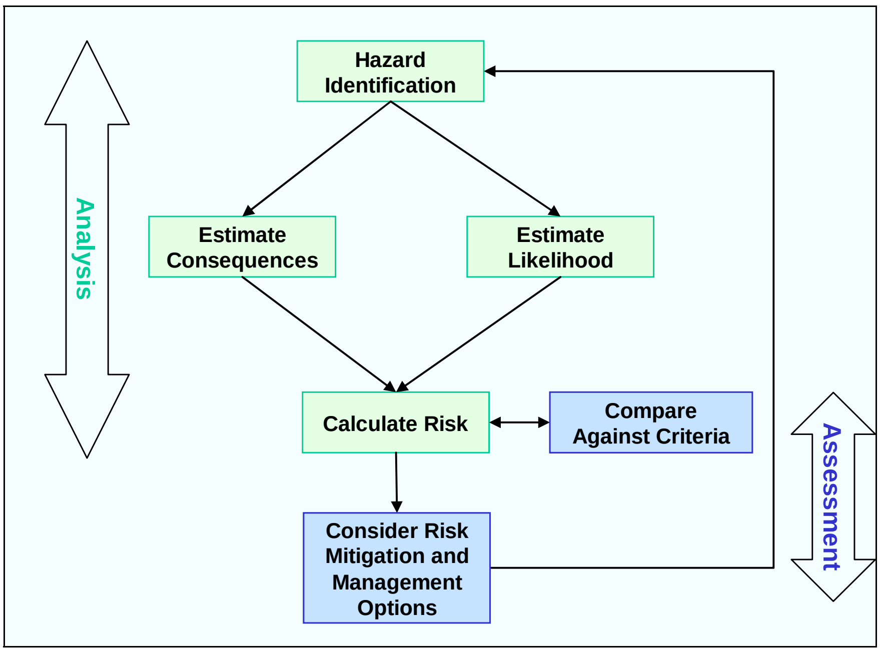
- An overlooked hazard can be a risk understated.

The main elements of hazard analysis are:

- identification of the nature and scale of all hazards at the facility, and the selection of representative incident scenarios;
- analysis of the consequences of these incidents on people, property and the biophysical environment;
- evaluation of the likelihood of such events occurring and the adequacy of safeguards;
- calculation of the resulting risk levels of the facility; and
- comparison of these risk levels with established risk criteria and identification of opportunities for risk reduction.

A schematic of the hazard analysis process is included below.

Figure 2: Basic Methodology for Hazard Analysis



A hazard is any thing or situation with a potential for causing damage to people, property or the biophysical environment. A hazard may be obvious or may require a detailed examination of a number of system components to reveal a shortcoming.

Hazard identification is a very critical step in the hazard analysis process. It involves the systematic identification of possible hazards, both on-site and off-site. In identifying hazards, operational and organisational safeguards designed to prevent or mitigate the effects of hazardous incidents should be taken into consideration.

Since there are usually numerous ways in which a hazardous incident may be initiated, if quantification of risk is required, it will usually be necessary to select discrete failure scenarios which can be used to represent the range of possible initiating events. Having defined the representative initiating incidents to be analysed, it is then necessary to methodically consider the various ways in which incidents may develop, and to identify the possible final outcomes.

As part of the hazard identification process, the analyst should review the adequacy of proposed or existing safety related hardware, and operational and organisational safeguards. This review should be continued throughout the course of the hazard analysis such that at the conclusion of the study, the analyst is satisfied that all appropriate safeguards have been identified and are or will be in place and effective. Any shortcomings in safeguards should be commented upon in the report findings and recommendations. Applicability of standards and codes should be reviewed and commented upon. For the case of existing facilities, compliance with standards should be reviewed.

Consequence analysis involves the analysis and quantification of the effect of the various incident outcomes. Mathematical models and computerised tools are often used to calculate the impact of such incidents as fires, explosions or the release of toxic substances and their effect on people, buildings and the biophysical environment.

It is also necessary to estimate the likelihood of the representative initiating incidents occurring and hence the likelihood of the particular outcomes should those incidents occur, having regard to all the proposed technical, organisational and operational safety controls.

Risk is the likelihood of a defined adverse outcome. For instance, one may wish to consider the risk of fatality, injury or environmental damage. In order to calculate risk, it is necessary to consider the likelihood and the consequences of each of the hazardous scenarios identified.

In terms of public health and safety, risk is usually expressed as individual risk or as societal risk. Individual risk is a measure of the risk to an individual at a specific location within the effect zone of a hazardous incident. The consideration of societal risk provides a mechanism by which the number of people exposed can be taken into account as well as the magnitude of the individual risk to each of those people. It is often expressed as the likelihoods of specified numbers of fatalities.

For land use safety planning purposes, assessment of individual risk levels can be used to ensure that no particular individual is exposed to unduly high levels of risk, and societal risk can be used to ensure that the risk impact on the community as a whole is not excessive.

The analysis should reveal all major risk contributors, the relevance of proposed or existing safeguards and their adequacy in mitigating effects to people, property and the biophysical environment. It should also indicate the extent of compliance with the qualitative and quantitative risk criteria set out in Hazardous Industry Planning Advisory Paper No. 4, *Risk Criteria for Land Use Safety Planning.*

Even where the facility complies with numerical risk criteria, recommendations for reducing the likelihood and consequences of hazardous events on people, property and the biophysical environment should be made where technically feasible solutions will not adversely affect the economic viability of the project. Depending on the purpose of the hazard analysis, these might include:

- the use of alternative locations or technologies;
- improving plant operability, safety systems and operating procedures;
- improving site layout and vessel design;
- reducing inventories of hazardous materials; and
- considering less hazardous alternatives for process materials and operating conditions.

Where such recommendations are to be implemented, it may be appropriate to recalculate the likelihood and consequences of the relevant incident to present results showing the risk reduction that has been achieved.

4 Hazard Identification

SECTION SUMMARY

The identification of all significant hazards is essential to a successful hazard analysis. There are a number of useful hazard identification techniques (see Appendix 1). The choice of method(s) will depend on the type of facility being studied, information availability and the expertise of the analyst. In all cases, the objective is to build up a picture of:

- hazards intrinsic to the facility, including material and process hazards and system failures, including human error and instrumentation and equipment failures;
- external hazards, both natural and of human origin;
- possible accident scenarios, their initiating events and consequences; and
- technical and procedural safeguards.

Once all significant hazards have been identified, representative events and accident scenarios are carried forward for further study. This should consider potential impacts on people, property and the biophysical environment. In particular, careful attention should be given to identifying worst case scenarios.

KEY MESSAGE

- Accident scenarios should not be dismissed because they are thought to be unlikely. All credible accidents with off-site consequences should be carried forward for further analysis.

4.1 The Identification Process

Hazard identification is the first and most important step in any hazard analysis and involves the identification of all possible conditions that could lead to a hazardous incident. The comprehensive and systematic identification of all hazards is critical to the success of the hazard analysis as a hazard not identified at this stage is excluded from further analysis.

There is no single definitive method of hazard identification. The methods adopted depend on the preferences of the analyst, the purpose of the hazard analysis and the information available at the time. Some of the more frequently used techniques are described briefly in Appendix 1.

The important thing is that a good understanding is gained of the way in which incidents may be initiated, and how they might develop to the point of inflicting harm on people, property or the biophysical environment. It is essential that the analyst be experienced in hazard identification, and that, where possible, plant designers and company personnel with relevant operating experience are involved in the identification process.

Hazard identification requires the consideration of all the relevant available information regarding the facility. This might typically include:

- site and plant layout;
- detailed process information in the form of engineering diagrams and operating conditions;
- the nature and quantities of materials being handled;
- operational, organisational and physical safeguards; and
- design standards.

For existing facilities, a site inspection should be carried out, preferably as part of a comprehensive hazard audit in accordance with Hazardous Industry Planning Advisory Paper No. 5, *Hazard Audit Guidelines*.

If the analysis is being performed at the early stages of a project, much of this information may not be available in any detail. The analyst will have to use judgment and experience to compensate for information not yet available.

The identification process should not be limited to the activities at the facility, but should also consider:

- natural events such as floods, cyclones, earthquakes or lightning strikes;
- technological events such as vehicle impact on a support structure or impact of aircraft;
- malicious acts; and
- hazardous events on neighbouring sites.

Hazards associated with waste and transportation should be included in the analysis.

The identification of possible sources of accidental emissions which may be hazardous to the environment requires systematic analysis. The hazard identification process should take into account:

- environmental properties of the site such as soil characteristics;
- proximity to environmentally sensitive areas, such as wetlands or water courses;
- the environmental compartment, such as air, soil or water into which a material may be released; and
- the physical and chemical properties and degradation rate of the material.

The results of the hazard identification can be conveniently presented in tables indicating:

- the plant or system studied;
- the item description and identification;
- failure modes identified;
- the types of hazardous incidents that could occur;
- possible consequences; and
- optionally, criticality ranking.

Opportunities for improving operational and organisational safeguards should be indicated. Appendix 4 illustrates such a presentation.

4.2 Selection of Representative Initiating Events

Having identified the types of hazardous incidents which might occur, the next step, if quantification is to be undertaken, is to define discrete initiating events to be used to represent the range of possible incidents. This is necessary since there are usually a large number of variations in the way in which an incident can be initiated.

For example, pipework failures could occur with leak sizes varying from pin-hole leaks to full bore ruptures. Since it would be impractical to analyse the infinite number of possible leak sizes in detail, it is usual to select a limited number of hole sizes to represent the full range.

This process will involve a certain degree of screening, in that decisions may have to be made to omit certain events, on the basis that they ultimately will prove to be insignificant contributors to risk. In making these decisions, expertise in risk analysis is essential, since the inclusion of events which are not significant will make the analysis overly time-consuming.

However, it is extremely important that no significant events are omitted. For this screening process, the analyst will need to have a good appreciation of the likely magnitude of the risks of each event, prior to undertaking detailed analysis.

4.3 Scenario Development

The next step towards the quantification of risk involves taking each of the identified initiating events and systematically determining how the incident will develop. Usually there will be a number of possible final outcomes arising from each initiating event, depending on factors such as the behaviour of personnel and equipment, location of ignition sources, meteorological conditions etc. All possibilities need to be considered in creating a set of scenarios arising from each incident. The analyst should also consider propagation or domino effects where one incident may initiate others in nearby plant and equipment.

An attention should be paid in defining the worst case scenario. The worst case scenario (also termed the bounding case scenario) defines the upper boundary for the range of credible hazardous scenarios that must be considered. It must not be limited to the largest event within the capacity of existing protection systems, on the basis that events worse than this cannot be managed. A number of factors need to be considered in identifying the “worst event” and the potential effects of this event on people, plant and the environment should be taken into account. All available information, including historical incident records, should be considered in deriving the worst case scenario. The worst case scenario should reflect any foreseeable factors that could exacerbate the severity of an accident, including abnormal process conditions, out of hours manning levels, and the potential for control measures to be disabled or rendered inoperable by the accident

Analysis of the various possible event sequences is usually undertaken using event trees. These are logic diagrams which enable the various event sequences to be detailed. An event tree begins with the initiating event, and the various subsequent event sequence possibilities are determined, resulting in a set of possible final outcomes. The event trees for each of the initiating events can then be used for the subsequent quantification of consequences and likelihoods and hence the calculation of risk. Further detail on event tree analysis is included in Appendix 1.

5 Consequence Analysis

SECTION SUMMARY

Consequence analysis considers the impact of possible accidents in terms of injury or fatalities, damage to property or damage to the biophysical environment. The most common events considered are fires, explosions and toxic releases. Two aspects need to be considered:

1. the direct consequences (e.g. explosion overpressure, thermal radiation intensity or toxic concentration); and
2. the effects of those consequences on people, property and the biophysical environment.

Typically, once the accident scenarios have been established through hazard identification, mathematical models are used to estimate the consequences of the various types of incident. The use of various types of models is discussed, with particular emphasis on the need to understand their limitations.

When using computer software to carry out the calculations, it is especially important to avoid a “black-box” approach.

Consequence analysis is valuable in leading to a better understanding of a facility’s hazards and may be used as a basis for identifying ways of reducing or eliminating those hazards. A sound understanding of the consequences of possible accidents can also feed into other safety studies, such as safety management, emergency planning and fire safety.

KEY MESSAGE

- Consequence calculations should be realistic as possible. Where simplifying assumptions are used, they should err on the side of conservatism.

Consequence analysis involves the analysis and quantification of the potential of hazardous incidents for causing injury or fatalities, damage to property or damage to the biophysical environment. The consequence of an incident is estimated independently of its likelihood.

Consequence analysis should be undertaken separately for each of the selected incident scenarios to estimate the effects of each outcome on people, property and the biophysical environment. However, resource limitations may not permit detailed analysis of all possible cases. Judgment is required to select those cases that would provide a satisfactory indication of the consequences of the incident. The analysis should attempt to be as accurate and realistic as possible; however, simplifying assumptions will sometimes have to be made. Where this is the case, it is usually appropriate to employ a degree of conservatism.

The types of hazardous incidents most commonly encountered are fires, explosions and toxic releases. The consequences of these can be estimated quantitatively in terms of thermal effects, explosion overpressures and toxic effects. In some cases, the dispersion and effects of hazardous materials of other types such as polluting substances, radioactive materials and infectious materials will also need to be considered.

Since, in general, consequences become less severe with increasing distance from the source, it is usual to express consequences as the distance to a specified consequence level. For example, the results of a consequence calculation might be the distance to the thermal radiation intensity likely to cause fatality, or the distance to the level of explosion overpressure which would produce building damage.

A large number of mathematical models have been developed to estimate the consequences of various types of incidents. These models require inputs of the conditions preceding the release such as:

- physical and chemical properties of the released material;
- storage or operating conditions prior to the release;

- size of the release orifice; and
- assumptions regarding factors such as meteorological conditions and ignition sources.

Given the large number of computations required and the range of mathematical models in use, computerised techniques have been used increasingly for consequence analysis. Care should be exercised in selecting and using software. The suitability of particular software will vary from case to case. Where hazard analyses are carried out for submission to government authorities, it may be appropriate to seek advice on the acceptability of the particular software from that authority.

Some of the major types of models are discussed in the following sections. Depending on the type of incidents to be modelled, the analyst would need to use a selection of, or possibly all of, the types of models described. A more detailed discussion, with references which provide further information, is presented in Appendix 2.

The accuracy and usefulness of computer model outputs depend heavily on the knowledge and skill of the user. Software should not be used as a 'black box'. The analyst must be able to understand the suitability and limitations of the software and to challenge the outputs.

In the consequence analysis and throughout the hazard analysis, the analyst must be conscious of the uncertainties associated with the assumptions made. Assumptions should usually be made on a 'conservative best estimate' basis. That is, wherever possible the assumptions should closely reflect reality. However, where there is a substantial degree of uncertainty, assumptions should be made which err on the side of conservatism.

5.1 Discharge Models

Most hazardous incidents of concern are the result of hazardous material escaping from containment. This may, for example, be from a crack or hole in a vessel or pipework, or it may be due to complete failure of a vessel. It may also be from a relief valve or a valve which has failed or been left open. There are a large number of mathematical discharge models which can be used to estimate the rate of release of hazardous gases, liquids or a mix of both, and the amount released.

5.2 Dispersion Models

Dispersion models are used to estimate concentration/time profiles of flammable or toxic gases at various distances downwind from the point of release. In some instances, it may be necessary to model the dispersion of a mixture of particulates and gases (e.g. smoke).

Vapour cloud behaviour is determined by a variety of factors including:

- the density of the gas relative to air;
- the rate of release over time;
- the amount of air entrainment at source;
- wind speed; and
- weather stability.

Clouds which are lighter than air tend to rise, limiting the harm they can inflict. Dense clouds stay at low levels for a considerable distance downwind and pose a much greater hazard. Many hazardous substances are either denser than air (e.g. LPG or chlorine) or behave as if they are much denser due to their low temperature on release (e.g. LNG or ammonia).

It is also necessary to consider whether the release will be an instantaneous puff, a continuous plume or a time-varying release as this will have a significant effect on the concentration profile over time. Weather conditions such as wind velocity and stability affect the extent of dilution with air, and the cloud velocity.

The mathematics of dispersion modelling is sufficiently complex to require computer software to assist in the calculations. However, caution must always be exercised in using computer models to ensure that the situations simulated by the models are realistic.

5.3 Consequence Models

In the following two sections, a distinction is drawn between the consequences of events and their effects. Consequences are the physical phenomena associated with the incident, for example thermal radiation intensity, explosion overpressure or toxic concentration/dose. Effects describe the impact of consequences upon people, property and the biophysical environment.

5.3.1 Fires

Industrial facilities may contain a number of sources of ignition such as:

- hot surfaces of pipelines or vessels;
- electrical equipment;
- welding activities;
- naked flames; or
- static electricity.

If a release of hazardous material is ignited, a fire or explosion will result.

Depending on the physical properties of the hazardous material, the mode of release and the time of ignition, the types of fires of greatest concern are pool fires, jet fires, flash fires, fireballs and warehouse fires. These can give rise to high levels of thermal radiation and blast overpressures. In addition, the potential for the evolution of toxic combustion products or toxic fumes due to thermal decomposition may need to be addressed.

Thermal radiation intensity is determined by factors such as:

- the rate and efficiency of burning;
- the heat of combustion;
- the size and orientation of the flame; and
- the fraction of radiation transmitted through the atmosphere.

Pool Fires

A pool fire occurs if a flammable or combustible liquid accumulates in a pool on the ground and vapours caused by evaporation are subsequently ignited. The resultant fire covers the whole pool area.

The thermal radiation from pool fires tends to attenuate rapidly with distance from the flame surface, and so thermal effects are relatively localised. There is often significant potential, however, for escalation to incidents with more severe consequences. Combustion products are often toxic.

A variation on pool fires which may need to be considered is fires involving flowing flammable liquids. In such cases, both thermal radiation and direct involvement in the fire may result.

Jet Fires

A jet fire occurs when a flammable liquid or gas, under some degree of pressure, is ignited after release, resulting in the formation of a long stable flame. Jet flames can be very intense and can impose high heat loads on nearby plant and equipment.

Consideration of jet fires often leads to recommendations regarding spacing within and external to the site to limit heat radiation incident on critical plant and equipment. Where appropriate separation is not possible, special protection systems can be recommended.

Flash Fires

A flash fire occurs when a cloud of flammable gas mixed with air is ignited. If the cloud is sufficiently large, it is also possible that the flame may accelerate to a sufficiently high velocity for a vapour cloud explosion (VCE) to occur. Though very brief, a flash fire can seriously injure or kill anyone in the burning cloud. Its effects are confined almost entirely to the area covered by the burning cloud. Incident propagation, sometimes called domino effects, can occur through ignition of materials or structures within the cloud.

Fireballs

Fireballs can occur when large quantities of flammable gases are released violently and ignited, resulting in a rising ball of flame. The thermal radiation intensity at the surface tends to be very high, and although the duration is short, dangerous levels of thermal radiation can be experienced at considerable distances from the fire.

BLEVE

Many fireballs are due to the phenomenon known as a 'boiling liquid expanding vapour explosion' or BLEVE. These mostly involve liquefied flammable gases stored under pressure.

Most BLEVEs occur due to a storage vessel being subjected to flame impingement above the liquid level. Hot spots can develop resulting in substantial weakening of the metal to such an extent that it is no longer capable of containing the internal pressure. Internal pressures would also typically be higher than usual during such events due to the high temperatures.

If the vessel fails, the pressurised contents escape rapidly and expand forming a large cloud of vapour and entrained liquid. If ignited, a large fireball may result. Casualties can be due to thermal radiation, blast effects and projectiles. The most significant impact is usually thermal radiation.

Warehouse Fires

The possibility of fires in stores containing dangerous goods should also be considered as part of the hazard analysis. The consequences of such fires may be complex due to the variety of goods often stored in the same building. Of particular concern is the possibility of the evolution of toxic fumes, although explosions, fire and pollution of the biophysical environment may also be important.

The nature of possible consequences needs to be considered carefully with particular regard given to interactions between the various substances present. Such analysis will often lead to recommendations for the segregation of incompatible materials.

5.3.2 Explosions

Explosions can occur through a variety of mechanisms, but in each case damage or injury is caused by a pressure wave which in turn is created by rapid expansion of gases. The magnitude of the pressure wave is usually expressed in terms of blast overpressure. However, in order to properly predict the destructive capacity, it is necessary to consider the rate of increase/decrease in pressure as the wave passes.

Explosions involving flammable gases are of particular concern in industrial facilities. These can occur if a mixture of flammable gas and air within the flammable range is ignited. The magnitude of overpressure developed is strongly influenced by factors such as:

- degree of confinement;
- the size of the cloud;

- degree of turbulence;
- the combustion properties of the gas; and
- the location of the ignition source relative to the cloud.

Explosions may also occur as a result of catastrophic rupture of a pressurised vessel, ignition of dust clouds, thermal decompositions, runaway reactions and detonation of high explosives such as TNT. Both blast waves and projectile fragments may result.

5.3.3 Toxic Releases

The release and dispersion of toxic material can adversely affect people and the biophysical environment.

The greatest potential for far field effects is generally associated with the evolution of toxic gas. However, toxic concentrations in the air can also result from:

- vapours from toxic liquids;
- reactions of materials giving off toxic vapours or gases;
- the evolution of toxic combustion products or
  toxic products of thermal decomposition;
- liquid spills entering watercourses or contaminating land and ground water; and
- spills of solids (particularly powders and dusts) being blown or washed into water or onto land.

The consequences of such toxic releases may be particularly significant for sensitive areas of the biophysical environment.

Complex dispersion models are available to estimate the concentration/time profiles of airborne toxics, as discussed in section 5.2. There is also a variety of methodologies available for understanding the behaviour of hazardous materials in the soil or in water bodies.

5.4 Effects of Hazardous incidents

In order to quantify risk, it is necessary to convert the physical consequences of a hazardous incident into information relating to what effect those consequences have upon people, property and the environment. This can be done in a number of ways.

The most easily understood method involves the selection of a particular consequence level to represent an adverse outcome. For instance, it may be proposed that a specific thermal or toxic dose represents fatality, in which case any person receiving the specified dose or greater is assumed to be killed, whilst those receiving a smaller dose are assumed to survive.

However, this method is somewhat limited in that it does not take into account the varying susceptibility of people. Also, the technique is not applicable in certain circumstances, especially if one is considering either very long or very short periods of exposure.

To overcome this, a more sophisticated approach can be adopted, such as a probit method which allows the prediction of the probability of an adverse outcome (usually fatality) given knowledge of exposure conditions. This approach takes account of the variations in human susceptibility, but also has some limitations and it is more difficult to use.

In particular, the data used to derive probit equations is subject to a degree of uncertainty. Reliable data on the effect on humans is rarely available, and so data based on experiments on animals is often used, especially for toxic exposures.

In making a decision on the most appropriate method, it is essential that the analyst has a good understanding of the relationships between dose and effects, and that the limitations are also recognised.

5.4.1 Heat Radiation Effects

A large amount of information exists and a number of charts and tables are available to provide an estimate of the effects of exposure to thermal radiation. Most of these charts and models refer to exposure of bare skin. The effects can be modified for the presence of clothing and the effects of sheltering or running away.

Fire damage estimates for the various types of fires are based upon correlations with recorded incident radiation flux and damage levels. A table of radiation effects is included in Appendix 2.

5.4.2 Explosion Effects

Explosion effect models predict the impact of blast overpressure on people and structures. Explosions are hazardous to people due to blast overpressure, collapsing buildings and projectiles.

Explosion effects are determined by correlating damage produced with the overpressure resulting from the explosion. A table of the effects of overpressure resulting from explosions is also included in Appendix 2.

5.4.3 Projectiles

In addition to overpressure, explosion incidents can also produce a significant hazard in the form of high momentum projectiles. Their consideration is particularly important with regard to the potential for incident propagation, and in the prediction of maximum effect distances, since fragments are often projected well beyond the thermal radiation or blast overpressure effect zones.

5.4.4 Toxic Effects

The analysis of the effects of exposure to toxic substances is an extremely complex and developing science. Toxic substances can affect people in may different ways and the seriousness of the exposure will be highly dependent on the sensitivity of the individual and on the duration of the exposure. The analysis of effects on other species and on ecosystems is even more complex than for humans, and knowledge is often even more limited.

Effects can range from fatality or injury (e.g. damage to respiratory or nervous system, emphysema, etc.) to irritation of eyes, throat or skin, through to a nuisance effect. Effects can also be classified as acute, chronic or delayed. The toxic effects are frequently specific to conditions at the time of release.

The estimated dose to which an organism is exposed must be translated into an effect. This should be done using quantitative dose–effect functions relating the level of exposure to probability of fatality, injury etc. However, these functions are only available for relatively few chemicals and usually relate to short-term effects of acute exposures. Detailed information on the long-term effects of acute exposures is very limited.

For non-carcinogenic chemicals, it is generally accepted that adverse effects will arise only when a threshold value or level of concern is exceeded. However, very little information on dose-effect relationships is available. Consequence analysis, even in the absence of detailed dose-effect information for these chemicals, can provide insight into whether particular threshold values may be exceeded.

There are a number of comprehensive sources of toxicological data which cover a large range of chemicals. Information on the concentrations of hazardous substances that can cause serious injury or death has been published in sources such as AIChE (1988) and Sax and Lewis (1989). Electronic databases are also available.

The analysis of toxic material effects is particularly difficult in the case of smoke from fires which may involve multiple and uncertain components. It is difficult to assess what effects such combinations of toxins might have. In such cases, conservative assumptions about the toxins involved and their concentration may be appropriate.

A probit approach may be used where information exists for specific substances. Such an approach enables the number of fatalities/injuries to be estimated through the consideration of both toxic gas concentration and the duration of exposure. However, the results need to be used with caution as probit equations are largely based on data derived from animal population responses and the extrapolation to human response is not straightforward.

For both human and other species exposures, where data are limited, end effect calculations may be difficult or of little value. In such cases, estimation of the duration and exposure to defined levels of concern such as threshold limit value (TLV), immediately dangerous to life and health (IDLH), short-term exposure limit (STEL) etc. may be appropriate.

5.5 Effects on the Biophysical Environment

The assessment of risks to the biophysical environment must take into account both acute and chronic effects. It is concerned with both short and long time scales. The geographic dimensions within which the impact of a released material manifests itself may extend a considerable distance beyond the immediate environs of a facility through, for example, the contamination of a river.

Analysis of the consequences and effects of hazardous materials releases on the environment should be integrated into the analysis as far as possible. However, both in terms of dispersion and concentration mechanisms and effects on particular species and ecosystems, separate treatment is sometimes warranted. The analysis should consider such factors as the vulnerability of an ecosystem or species, the soil type and tidal flushing. Degradation of the chemical(s) may also need to be taken into account. Full quantification may not be possible or warranted in some cases. Judgment should be used as to the extent of qualitative and quantitative analysis which should be carried out.

As with human toxins where data are inadequate, the analysis may be appropriately focused on threshold or criteria concentrations in the air, water or soil.

Analysis of effects on the biophysical environment should also consider the possibility of impact on people through materials entering the human food chain or contaminating soil or water used for drinking or swimming.

5.6 Results of Consequence Analysis

Consequence analysis results can be used in a number of ways. Firstly, they provide an extension of the hazard identification process in that it leads to a better understanding of the potential hazards at the facility.

Secondly, consequence analysis may lead to recommendations for the elimination of hazards or the reduction of consequences. It may also lead to the conclusion that the likelihood of particular events needs to be minimised, due to their severity. Opportunities should always be taken where there are technically feasible alternatives which will not adversely affect the economic viability of the project.

Depending on the purpose of the hazard analysis, these recommendations may cover issues such as:

- the choice of the location of the facility;
- the technology in use;
- plant layout;
- vessel design and operating conditions;
- the use of alternative less hazardous materials; or
- reduction of inventories.

The capacity and adequacy of drainage and containment systems may also be addressed. The consequence analysis may then be repeated to estimate the impact of the implementation of the recommendations.

The results of the consequence analysis should also be used as inputs into other safety studies being prepared for the site. For instance, the consequence analysis should identify incident scenarios where an emergency response is required and consider whether emergency plans provide protection to people both off-site and on-site, and to the biophysical environment.

Guidance on the formulation of emergency plans is given in Hazardous Industry Planning Advisory Paper No. 1, *Emergency Planning*.

Fire system design should also draw on the consequence analysis, including analysis of contaminated fire fighting water run-off and containment. Hazardous Industry Planning Advisory Paper No. 2, *Fire Safety Study Guidelines*, provides guidance on such studies.

The event trees developed as part of the hazard identification and consequence analysis processes are also used for subsequent parts of the study. They form an essential basis for the analysis of likelihoods and estimation of risk.

6 Estimation of the Likelihood of Hazardous Incidents

SECTION SUMMARY

Because the historical frequency of major accidents is very low, it is seldom possible to obtain statistically significant historical information on the frequency of individual failure scenarios.

For this reason, logic models are typically used to estimate the likelihood of the identified final outcomes, using failure data for individual components and subsystems. Examples are the use of fault trees and event trees. Other methods are summarised in Appendix 3.

The section discusses the use and sources of generic failure data for both individual components and systems. Local information, such as meteorological conditions and the frequency of natural events, such as fires and floods, may also be required.

KEY MESSAGE

- Estimates of accident likelihood must be soundly based. Where generic failure data are used, care must be taken to ensure that the information is from systems comparable to the systems under study.

A prerequisite for the analysis of the likelihood of hazardous incidents and their effects is a proper understanding of the terms probability, likelihood and frequency.

A 'probability' is dimensionless and is a representation of the chance of something occurring. No time period is specified. For example, given that a flammable release has occurred, one may be interested in the probability of ignition. Wherever a number of outcomes are possible, the sum of the probabilities of each outcome must be equal to one.

'Likelihood' is an expression of the chance of something occurring in the future. It must be expressed in terms of a specific time period. For example, it might be estimated that the likelihood of catastrophic vessel failure is one chance in a million per year (or 1 x 10-6/year). The selection of the time period is arbitrary, but likelihoods are most often expressed per year or per hour of operation.

‘Frequency’ is similar to likelihood, but refers to historical data on actual occurrences. For instance, incident records may indicate that the frequency of failure of a particular item of equipment was twice per year. Failure frequency data are often used as a basis for predicting the likelihood of similar occurrences in the future.

In order to estimate the likelihood of particular outcomes of hazardous incidents there are usually two types of information which need to be considered. First is the likelihood of the initiating event. The second is the probabilities of the initiating event developing via the various event sequences identified in the earlier stages of the analysis.

The initiating event likelihood might be estimated directly through the consideration of historical failure data or, if this is unavailable, it may need to be derived through the consideration of the failure of subcomponents using logic models such as fault trees or event trees. The latter approach allows for the consideration of:

- specific operating conditions;
- organisational factors;
- maintenance programs;
- operator capabilities;
- manual/automatic intervention systems; and

- other technical, organisational and operational safety controls.

In order to quantify the likelihoods of each of the identified final outcomes, the initiating event likelihood can be combined with the various probabilities associated with each branching of the event tree. If event tree probabilities cannot be estimated directly, fault trees may be required to derive an estimate through analysis of subsystem failure.

As an example, to estimate the likelihood of a release of flammable material, the analyst may have to estimate the likelihood of loss of coolant to a reactor, which may lead to:

- a runaway exothermic reaction;
- the probability that safety interlocks fail to shut down the reactor;
- the probability of failure of emergency protection systems; and
- the probability that the operator fails to appropriately intervene.

Subsequent to the release, other probabilities which may need to be determined in order to estimate the likelihoods of the various outcomes are meteorological condition probabilities, ignition probabilities for releases in various directions, and the probability of explosion upon ignition, rather than flash fire.

6.1 Logic Models

Event Trees

An event tree starts with a single initiating event and the subsequent event sequence possibilities are represented by branching of the tree, leading to a number of possible final outcomes.

A likelihood can be established for the initiating event. Any point in the tree can be characterised by a particular consequence and an associated likelihood. Hence, event trees are important for both consequence and frequency analysis. To obtain likelihoods within the tree, conditional probabilities need to be determined wherever branching occurs. These probabilities may be available directly, or they may need to be estimated using an analytical method such as a fault tree.

Fault Trees

One of the most commonly used logic models for the estimation of the likelihood of a hazardous incident and scenarios which result is fault tree analysis.

Fault trees use logic similar to that of event tree analysis. However, the starting point is the final event of interest and the analyst works backwards in order to identify the sequences of events required to produce that final event. The technique is useful both for the quantification of particular likelihoods or probabilities, and as a method for identifying which event sequences and causal factors could lead to a hazardous incident.

An example of the use of fault trees is the case where a failure likelihood of a particular system is required and no specific failure data are available directly. The failure modes can be broken down into combinations of failures of smaller components for which failure data are available. Hence, the system failure likelihood can be estimated using a fault tree approach.

Fault tree and event tree examples are presented in Appendix 1. There is a further discussion of techniques for estimating failure likelihood (including human error) in Appendix 3.

6.2 Sources of Failure Data

The likelihood of potentially hazardous incidents arising out of hazards previously identified may be determined either from generic or specific historical plant failure data, or using an analytical technique such as fault tree analysis.

There is no simple way of specifying which sources of failure data are the most appropriate for a given hazard analysis. However, the quality of the data, the statistical significance of errors in the data used and the appropriateness of the circumstances to which the data are applied is crucial to the validity of the conclusions of the analysis. These aspects in particular should be well understood and should be discussed in the hazard analysis report.

Failure data are usually presented in one of two forms, depending on the nature of the equipment and the way it is used. For equipment in continuous use, it is usually expressed as failures per unit time (e.g. failures per million hours). Systems or components which are not normally in use, but which are called upon to act infrequently (e.g. protective systems) may have their failure rates expressed as probability of failure upon demand. In order to predict such probabilities, knowledge of testing and maintenance schedules is essential.

Generic failure data are those which have been collected from a wide range of sources representing many item-years of operation. Most generic failure data are available at the component level. However, data may be available for subsystems such as pump-motor combinations, closed control loops, gas detection systems, refrigeration systems etc.

Because of the large population of items included of any particular type, generic data can give a good first estimate of the likelihood of failure of similar items. However, generic data may not provide enough information for a complete analysis of a specific plant operating under specific circumstances.

The use of specific plant failure data derived from an organisation's own records would usually be preferable to generic data, provided that the item population and time period of data collection are sufficiently large. If applied to other plant within the organisation or extrapolated to other similar plants, these may still be better than other data because such data reflect design, construction, operation, maintenance and other management practices. Unfortunately, such data are rarely available.

In cases where plant specific data are not available, it may be appropriate to modify the best data available in order to reflect the operational and organisational practices of the company concerned. The analyst may have to use a degree of judgment in these cases, although more formal techniques are available to assess a company's overall safety performance and may be appropriate in some circumstances.

6.3 Other Data Requirements

Other data which may be required for the development of risk results are as follows:

- meteorological data, such as the probabilities of the occurrence of particular wind and weather conditions;
- natural event data, such as the likelihood of flooding, earthquakes, cyclones, etc;
- external events data, such as the likelihood of aircraft impact or events on neighbouring sites;
- susceptibility data, for example, if a probit approach is used to estimate fatality probability given a particular dose; and
- population presence data, if societal risk calculations are to be undertaken.

Much of these data are specific to the location of the facility and can be obtained from local sources.

7 Risk Analysis

SECTION SUMMARY

Risk is the likelihood of any defined adverse outcome. The risk of a particular outcome (e.g. fatality to an individual) at a specific location can be estimated by summing the likelihood of all events that could lead to that outcome at that location. This is known as *individual risk*.

In addition to individual risk, it is also possible to estimate the total number of people affected by each possible accident. This leads to an estimation of *societal risk*.

Individual risk results are commonly presented as contours which connect points of equal individual risk around the facility. Using this presentation, areas of high exposure can be readily identified.

Societal risk can be presented as a graph, called an F–N curve, which is a plot of cumulative frequency versus consequences, measured as fatalities.

In some cases, such as when dealing with damage to ecosystems, a numerical presentation may not be possible and a more descriptive approach may be warranted.

KEY MESSAGE

- The greatest benefit from the risk analysis is the insight it gives into the main risk contributors, providing a focus for risk reduction. This is more important than the absolute values of the numerical results, the significance of which is influenced by the accuracy of the input assumptions and calculation methods.

7.1 Risk Estimation

Risk is the likelihood of any defined adverse outcome. Risk can be defined for any of the final outcomes of an event tree by the effect of the consequences coupled with the associated likelihood. As the adverse outcome can take many forms, particularly in the case of effects on the biophysical environment, risks can be expressed in a number of different ways.

In some cases, such as human fatality risk from fire and explosion, the risk from each event can be identified at any point in the affected area. For each point in the area affected, the risk from each final like outcome (e.g. fatality, injury, irritation) can be calculated and, by summation, the total risk at each point can be determined. Hence, the distribution of risk around the facility can be calculated.

Similarly, the total risk at a particular location due to a number of facilities can be calculated by the summation of the risks from each individual facility. If the population in the affected areas is combined with the likelihood and consequence information for particular points, estimations of societal risk can be made.

For other cases, the defined adverse outcome could be a toxic concentration, a system failure or an impact on an ecosystem or species. Where a number of events contribute to the same outcome, summation is possible. For any facility or activity, however, there may be a number of risks which need to be analysed, understood and managed. It is not always possible or appropriate to try to reduce all risks to simplified comparable measures.

Throughout the hazard analysis process, it is necessary for the analyst to be aware of the uncertainties involved in each of the calculation steps. At the risk estimation stage it should be possible to estimate the uncertainty in the final results and to understand the sensitivity of the results to various critical assumptions.

7.2 Risk Presentation

The large amount of information on the likelihood and consequences of various hazardous events must be integrated into a presentation that reflects the goal of the hazard analysis and the measures of risk that are of interest. Risk measures may be presented as quantitative measures such as indices, tables, graphs or risk contour plots, or as qualitative indicators.

Among the more common forms of risk measure are individual risk and societal risk.

Individual fatality or injury risk measures represent the likelihood of a specified level of harm at a specified location. No account is taken of whether or not anyone is actually present at that location. It includes the likelihood of the injury or fatality occurring in a specified time period and the type of injury likely to occur, e.g. individual fatality risk at a certain location might be one chance in a million per year.

Individual risk is commonly presented as contours which connect points of equal individual risk around the facility. Using this presentation, areas of high exposure can be readily identified. Individual risk levels should, as far as possible, include all contributors to injury and fatality from fires, explosion and toxicity, even where there are uncertainties in correlating some consequences such as exposure to toxic concentrations.

In many instances, it is appropriate in the analysis to account for variations in the duration of exposure to that risk. It may also be appropriate to account for variations in people's vulnerability to the hazard and their ability to take evasive action when exposed to the hazard. By convention, and as a conservative measure, risk contours are usually plotted on the basis that the individual is exposed for the full duration of the hazardous incident and no account is taken of evasive action or protection by clothing, buildings etc. It is essential that the analyst understands the basis of the risk calculations and that assumptions used are internally consistent. It is also essential that these assumptions are clearly stated in the report.

Societal risk is a measure of risk to a group of people that could be affected, in terms of injury or fatality.

It takes account of the number of people in the affected area, the nature and scale of incidents which contribute to particular risk levels at particular points and the outcomes of these incidents in terms of injury and fatality. It is often expressed as the likelihoods of specified numbers of fatalities or the expected number of fatalities per unit of time.

Societal risk can be presented as a graph, called an F–N curve, which is a plot of cumulative frequency versus consequences, measured as fatalities. Other qualitative and quantitative risk indicators can also be used. Societal risk, in particular, has potential for a lack of clarity of meaning and the analyst must ensure that the indicator used is meaningful and understood and assumptions explicit.

Property damage risk indicators show the potential of incidents to cause damage to buildings and structures on-site and off-site, usually as a result of fire, explosions and missiles. This is usually expressed as the likelihood and intensity of heat flux or explosion overpressure incident at various points around the facility.

The risk of property damage may be presented as tables or risk contours of heat flux or explosion overpressure. Other property damage risk such as contamination or corrosion generally requires case-specific indicators with qualitative and quantitative components.

The results should provide an indication of the extent of the potential for accident propagation following an incident and should indicate whether there is adequate separation between major vessels and critical plant areas.

The assessment of the ultimate effects from toxic releases into natural ecosystems is difficult, particularly for atypical accidental releases. In many cases it may be impracticable to establish the final impact. For risk to the biophysical environment, generally the focus is on toxicity impacts on whole systems or populations rather than on individual plants and animals. Data are often limited and factors affecting the outcome variable and complex. There may be no immediate loss of plants or animals or other observable effects from a single release, but there may be cumulative and synergistic effects. The form of presentation of risk to the biophysical environment must necessarily be selected on a case-specific basis. In many cases, the likelihood of identified concentrations occurring in the air, water or soil may be the appropriate risk indicator. Qualitative indicators may also be appropriate in certain circumstances.

Risk levels may be presented for parts of the facility separately and for the whole facility on a cumulative basis. It may also often be necessary to present comparisons of the results of the study with other risk assessments. This type of presentation may show, for example, the effect of alternative processes or technologies in reducing risk or the effect of other risk reduction measures.

8 Assessment of Risk Results

SECTION SUMMARY

Risk results, in isolation are of limited value. Whether or not a particular level of risk is acceptable depends on both the nature of the risk (e.g. human injury or fatality, property damage), the sensitivity of the affected environment and the benefits provided by the activity giving rise to the risk.

The Department has developed a number of qualitative and quantitative risk criteria, which take these factors into consideration (see HIPAP 4). Risk results should be compared against all relevant criteria and the effectiveness of the various risk reduction strategies evaluated.

While the risk criteria should not be regarded as absolute, exceedences should only be permitted where there are overriding economic or social benefits from the facility under study.

KEY MESSAGE

- Every opportunity should be taken to identify ways of eliminating or reducing risk, even when all risk criteria are met.

Risk assessment is the process by which the results of the hazard analysis are used in decision-making through comparison with qualitative and quantitative risk criteria or comparison with the risk profiles of alternatives.

8.1 Assessment against Risk Criteria

In the case of land use safety planning decisions, the results of the hazard analysis should be assessed against the qualitative and quantitative risk criteria set out in Hazardous Industry Planning Advisory Paper No. 4, Risk Criteria for Land Use Safety Planning.

As emphasised in that paper, because of the probabilistic nature and uncertainties of the risk analysis, there needs to be a degree of flexibility in the implementation and interpretation of the risk criteria. The assessment should consider, among other things:

- qualitative as well as quantitative outputs of the analysis;
- the consequences and likelihoods of hazardous events;
- the vulnerability of people in the area;
- the sensitivity of the affected environment;
- the potential benefits of the development;
- variations in local conditions;
- existing risk exposures; and
- likely future use of surrounding lands.

The quantitative risk criteria should not be used as absolute levels. Where the risk levels exceed the established criteria, the acceptability of the facility may nevertheless be justifiable in terms of expected economic or social benefits.

Quantitative risk measures can also be used to demonstrate the benefits of risk reduction that can be achieved if recommendations arising out of the hazard analysis are implemented.

The implementation of the risk criteria should differentiate between existing land use situations and new situations where stricter locational and technological standards would usually apply.

The complexities of assessing risk to the biophysical environment and case-to-case differences render it inappropriate to specify precise risk criteria in these cases. The acceptability of the risk will ultimately depend on the value of the potentially affected area or system to the local community and wider society. Relevant factors in the capacity of the population or ecosystem to recover should be considered, including the extent of other stresses and the possibility of repopulation of affected areas.

8.2 Recommendations for Risk Reduction

By inspection of risk results, the contribution of each of the initiating events can also be identified and used for the development of risk reduction strategies.

The analysis should identify and preferably rank the individual contributors to risk of each of the initiating events identified. This then provides a basis for the development of appropriate risk reduction strategies. Through inspection of the major risk contributors and an understanding of the cost associated with particular risk reduction measures, cost-effective risk reduction strategies can be developed.

Even where a facility complies with established risk criteria, the implementation of technically feasible recommendations which reduce risk levels without significantly adversely affecting the economic viability of the project is desirable.

Recommendations to minimise the likelihood and consequences of a hazardous incident might include, for example:

- alternative technology or location;
- reduction of inventories;
- modification of process and storage conditions;
- early detection, control and clean-up of any releases and upgrading of containment and collections systems to ensure that they are capable of holding a spill of hazardous material;
- changes to site layout if large process or storage vessels or load-bearing structures are exposed to possible heat radiation, explosion damage or missiles;
- the siting of critical parts of the plant, such as control rooms, to ensure that they are not unduly exposed to the consequences of a hazardous event;
- improvements in plant operability;
- upgrading of operational and organisational safeguards (including training);
- improvements in emergency planning;
- land use controls; and
- improvements in fire safety systems.

The hazard analysis may also recommend particular detailed or specialist studies or investigations where appropriate, e.g. hazard and operability studies or the development of monitoring and maintenance programs.

9 The Hazard Analysis Report

SECTION SUMMARY

This section provides guidance on the content and structure of the hazard analysis report. The guidance is written from the perspective of the needs of a regulator requiring evidence that the facility being studied does not pose a significant risk to the surrounding community.

The Executive Summary and the Findings and Recommendations should focus on those aspects of particular relevance to the decision-making process.

This is supported by detailed information in the body of the report covering:

- a description of the facility, its operations and its location;
- processes employed and hazardous materials handled and stored;
- results of the hazard identification, consequence analysis and the likelihood estimation; and
- presentation of the risk results, their assessment against relevant criteria and the conclusions of the assessment.

The section concludes with suggestions about additional information that should be included in the report appendices.

KEY MESSAGE

- The hazard analysis report provides a basis for an informed judgment to be made on the acceptability of a facility. It should focus on key issues, rather than providing a high level of unnecessary detail.

The underlying principle for the hazard analysis report is that it should provide a reasonable basis for an informed judgment to be made on the acceptability of a facility. It should provide people with relevant expertise with sufficient information to be able to reconstruct and verify the analysis.

It is a recognised and important feature of hazard analysis that follow-up contact between the analyst and the regulatory authority may be necessary. This should not, however, be used as a justification for providing insufficient detail — expert judgment is required in this regard.

It must also be stressed that it is not beneficial to produce unduly lengthy or 'glossy' reports. A simple analysis of a simple site or system will only require a brief report.

The following paragraphs provide guidance on the information to be provided in the hazard analysis report.

9.1 Title Page

The hazard analysis report should have a title page which should be shown clearly on the cover and on a separate title sheet. The title page should clearly and unambiguously identify the facility covered by the hazard analysis and the location of the facility. The title sheet should also show who performed the hazard analysis, and the date of the report.

9.2 Table of Contents

The report should include a table of contents with page numbers. The table of contents should include a list of figures and appendixes.

9.3 Executive Summary

The purpose of the hazard analysis, along with an overview of the approach used, should be clearly stated.

The summary should highlight major findings of the hazard analysis. It is important to demonstrate a good understanding of the risks at the facility with major risk contributors identified. A brief comment on data limitations, assumptions and other uncertainties that could affect the conclusions of the analysis should also be included. The interaction between the hazard analysis and other safety studies that have been carried out for the facility should be highlighted.

The major recommendations should be summarised.

9.4 Findings and Recommendations

Findings

The results of the hazard analysis should be discussed in this section. The findings should demonstrate that the hazard analysis has comprehensively:

- identified all hazards at the facility;
- analysed the possible incident scenarios that could result from a hazardous incident and the consequences of these to people, property and the biophysical environment;
- estimated the likelihood of hazardous incidents that have the potential to result in significant consequences;
- demonstrated the extent to which the facility complies with qualitative and quantitative risk criteria described in Hazardous Industry Planning Advisory Paper No. 4, Risk Criteria for Land Use Safety Planning; and
- utilised all opportunities for recommending risk reduction using cost-effective, technically feasible measures to limit the consequences and likelihood of potentially hazardous incidents.

This section should indicate what steps have been taken to present the findings of the analysis to plant designers, construction engineers, operations management and other appropriate personnel to ensure that they have a full appreciation of the critical safety issues at their facility.

Recommendations

Recommendations that limit the consequences of major incidents could cover:

- choice of technology;
- layout of storage and process vessels;
- design of vessels and ancillary equipment; and
- mitigating systems.

Recommendations that limit the likelihood of hazardous events include improvement to control systems, operating practices and safety management procedures.

For a preliminary hazard analysis (PHA), the results should be used as inputs into other safety studies required as part of the development approval process. For example, the consequences of major incidents can be limited by appropriate protection and mitigating measures incorporated in emergency and fire prevention systems. The results of the consequence analysis can be used to develop appropriate emergency responses to be incorporated in the emergency plan. Protection systems that would mitigate the consequences of a major fire should be incorporated in the fire safety study.

Based on the results of the consequence analyses, an emergency plan, fire safety study, or other studies may be recommended for a facility already in operation, if these have not been carried out or if previous studies have been inadequate.

9.5 Site Description

This section should present an overview of the location of the site and operations carried out. It should present all relevant factual information available on the site, its activities and surroundings.

9.6 Location

The report should provide a description and evaluation of the site location and layout, and any inherent hazards, including off-site and natural hazards.

The report should describe surrounding land uses, population densities, sensitive natural environmental areas in the vicinity and current plans for development of the surrounding area. Maps and sketches of the facility and of surrounding land should be included.

A compilation of topographical, meteorological, seismological and other relevant information may be included as appendixes where appropriate.

The report should also indicate the number of people on site at various times and describe site security arrangements.

Where detailed descriptive information has been provided in other studies, clear cross-references to these documents would suffice.

9.7 Process

A brief process description should summarise all the processing steps and operations being carried out, with references to documents containing more detailed information cited where appropriate. The description should be accompanied by engineering information such as process flow diagrams and/or piping and instrumentation diagrams (if available). Access to proprietary process or technology information may need to be provided to the relevant authority on a confidential basis.

Hazardous Materials

This section should include a list of all materials (including their UN number) being handled, stored or processed at the facility, with maximum and average quantities shown. Full chemical names should be used rather than trade names or common names. Vessel and packaging size and type should also be shown. A scale plan of the site showing locations and quantities of significant inventories of hazardous materials and indications of normal operating or storage conditions should be provided. Material safety data sheets may be included as appendixes where appropriate, e.g. unusual materials.

9.8 Hazard Identification

This section presents the results of hazard identification procedures. The various methods of hazard identification used and some justification for their appropriateness in each case should be provided.

The results of the hazard identification should be listed for each major process or storage unit or area, with a brief description of possible incident initiating events, possible consequences and proposed or existing safeguards. Word diagram format such as set out in Appendix 4 may be useful in presenting this information. The report should comment on the adequacy of hardware and software safeguards, present or proposed, for each hazard identified.

Departures from relevant regulations and standards and deviations from licence and consent conditions that have occurred should be detailed.

For a final hazard analysis, the report should comment on the extent to which the results of the hazard and operability study (HAZOP), where required as part of the development approval process, have been used as inputs into the analysis.

Findings that will reduce or eliminate hazards should be included where appropriate. This may include, for example, the choice of location of the facility or technology, changes to design and operating parameters and reduction of inventories of hazardous materials on site.

Details of representative initiating events should be provided along with a description of the postulated scenario developments, usually in the form of event trees. If event trees are numerous or complex, they may be more appropriately presented in an appendix. It may also be appropriate for representative examples only to be included in the report. In such cases, the analyst must be able to provide such further trees as and when requested by relevant authorities.

9.9 Consequence Analysis

Consequence analysis results should be presented in sufficient detail to provide a good appreciation of the consequences of the hazardous incidents identified for further analysis.

The extent to which detail should be provided requires judgment on behalf of the analyst, and will vary from case to case. Where a small number of cases has been analysed, a full presentation of consequence results would be appropriate, whereas for large facilities a complete presentation may be unduly onerous and a summary of representative results may suffice. All relevant calculations should, however, be available to regulatory bodies upon request. In all cases, worst credible case scenarios should be identified.

Information regarding inputs and relevant assumptions should also be presented in sufficient detail to allow regulatory bodies to assess and validate calculations.

Mathematical models used in the calculations should be described briefly. Names of any computer software or other models used in the calculations should also be provided. All software and analytical tools used, including proprietary software, should be accessible to the approving authority on request. Sample calculations might be appropriately included as appendixes, particularly when unusual mathematical models or calculation techniques have been utilised.

The implications of the consequence results with regard to local populations and ecosystems should be commented upon. Risk reduction possibilities involving the reduction of consequences should also be discussed in this section.

9.10 Estimation of the Likelihood of Hazardous Events

This section should present the results of the analysis of the likelihood of hazardous incidents and their final outcomes. Sufficient information on assumptions relevant to the calculations and analysis should be provided to facilitate an understanding and enable reproducibility if required. It should include:

- the various methods of frequency and probability assessment used;
- all failure data and sources;
- sources and assumption for probabilities used;
- relevant fault trees and event trees;
- details of wind, weather, topographical, population, hydrological and other data used;
- the details of all other assumptions; and
- names and purposes of computer software used in the calculations.

Access to software, even when it is proprietary, must be allowed where hazard analysis reports are submitted to an authority for approval.

In the case of complex analyses, representative information, such as sample fault trees, may be included in the report provided that full information is available to relevant authorities on request.

The report should discuss the adequacy of measures taken or proposed to minimise the likelihood of a significant incidents occurring and make recommendations where further improvement is warranted.

9.11 Presentation of Risk Results

Risk results should be presented so as to enable assessment against all relevant qualitative and quantitative criteria for risk to people, property and the biophysical environment. Both individual and societal risk results should be included. Hazardous Industry Planning Advisory Paper No. 4, Risk Criteria for Land Use Safety Planning, should be consulted for guidance on risk criteria and presentation.

Usually, individual risk and risk to property should be presented in the form of risk contours. Societal risk F-N curves should be included where possible. Other forms of presentation may be appropriate, however, depending on the circumstances.

Risk to the biophysical environment may be presented in a number of ways, depending on the kind of impact under consideration. Often, an estimation of the likelihood of specified levels of damage or concentrations will suffice, although in some circumstances more sophisticated presentations may be appropriate.

In presenting these results, it is essential that the potential extent of uncertainty and the sensitivity of the results to changes in assumptions be discussed and, if possible, quantified. It is also important to highlight the major risk contributors.

Where risk reduction measures have been identified as options, their effect upon risk results should be documented and risk results with and without recommended risk reduction measures shown where appropriate.

The ranking of contributors to risk should be shown in tabular form and explained in the text.

9.12 Risk Assessment

The risk results should be compared with the qualitative and quantitative risk criteria.

Comparison with quantitative criteria may be relatively straightforward. However, comparison with qualitative criteria is likely to be more problematic and may require more detailed discussion.

Compliance with qualitative criteria (in particular those concerning environmental risk, avoidable risk and societal risk) should be discussed in the text, bearing in mind the comments in Hazardous Industry Planning Advisory Paper No. 4, *Risk Criteria for Land Use Safety Planning*.

It will often be appropriate, and will usually facilitate assessment, to supply additional information such as the risks of using alternative locations or technologies, background risk levels and the cost implications of risk reduction options.

Where the hazard analysis is carried out to aid selection of least risk options, the alternatives should be assessed against each other. It may also be appropriate to assess them against the general risk criteria as, in practice, risk profiles may be different and superficial comparison may not adequately account for all aspects which should be considered.

The risk reduction requirements, measures and strategies arising from the analysis should be detailed here. However, the specific and detailed recommendations can be covered under Findings and Recommendations.

9.13 Conclusions

The overall conclusions on acceptability and on hazard and risk management from the analysis should be presented in this section.

9.14 Appendixes

The following information should also be provided:

- a list of materials collected as part of the study; and
- the qualifications and experience of the hazard analysis team.

Other information which may, where appropriate, be supplied in appendix form includes:

- description of calculation methods used and some sample calculations;
- meteorological data for the site;
- description of computer software used in the various computations and sample output from the various models used;
- process and instrumentation diagrams, and other relevant drawings; and
- fault trees and event trees.

9.15 Glossary and Abbreviations

To ensure that the hazard analysis report is understood, a glossary of special terms, titles, names of parts of the facility and a list of abbreviations may also be appropriate.

Appendix 1

Hazard Identification Methods

This appendix provides a brief outline of some of the more frequently used formal hazard identification methods. Readily available references for further reading are also provided. Parry (1986), AIChE (1989c) and Warren Centre (1986) provide good overviews of the range of techniques available as well as some detail on each of the individual methods.

Different methods are better at identifying different types of hazard. Techniques such as HAZOP and FMECA are best at identifying process hazards such as process upsets and equipment failures, but may be weak in identifying other types of hazards such as human errors or external effects and influences. Techniques such as What-If tend to be broader, and are useful for identifying hazards associated with natural and man made external effects and influences. Task Analysis is a Human Factors Hazard Identification tool that is focussed on identifying hazards that result from human errors.

Hazard and Operability Study (HAZOP)

This technique uses a multidisciplinary team to methodically analyse each part of a plant to determine how deviations from the design intention can occur which may lead to hazardous situations or operational problems.

Where there is no realistic cause or the effects are unimportant, the cases are quickly passed over. Where the causes are credible and the effects significant, design changes may be required to eliminate the cause or a more detailed reliability study recommended. The combined results of such investigations are usually presented in a table or word diagram. The word diagram should identify the line or equipment analysed, the guide words applied, the problem identified, possible events and consequences, and recommended action.

Detailed description of this method is provided in Chemical Industries Association (1977) and Kletz (1986). Summary guidance on this technique is provided in HIPAP No 8 *Hazard and Operability Studies.*

Failure Modes and Effect Analysis (FMEA)

FMEA is a tabulation of each piece of equipment, its failure modes and their effect on the system or plant. FMEA identifies single failure modes that play a significant part in an accident. It is not efficient in identifying combinations of equipment failures that lead to accidents. Human error is not considered explicitly in FMEA, even though human error may result in equipment failure.

The FMEA may be limited to a part of the plant by applying system or plant boundaries to the area being analysed. All failure modes are identified for each plant, and the immediate effects and expected outcomes are recorded.

Fault Tree Analysis

Fault tree analysis is useful in identifying combinations of equipment failures and human error that can lead to an incident. It uses a logic diagram which starts with an undesirable event and works downwards until the range of possible causes have been identified. The end result of a fault tree is a list of combinations of equipment and procedural failures, for which appropriate failure rate data exist or can be generated, that are sufficient to result in the ‘top event'. The fault tree can be used to estimate the likelihood or probability of the top event occurring, as well as being a useful hazard identification tool.

This method is further described in Rasmussen (1975) and AIChE (1985).

Event Tree Analysis

Event tree analysis is usually an integral part of a hazard analysis. It is useful for consequence analysis, frequency analysis and risk summation, but can also be valuable in the hazard identification process, both in giving the analyst an appreciation of the way in which incidents may develop, and in allowing the adequacy of protective equipment and procedures to be assessed.

The technique begins with an initiating event and analyses the various event sequences which may develop. As an incident develops, various routes may be taken depending on the behaviour of personnel and equipment, as well as natural alternative routes such as wind direction and weather conditions. The end result is a list of final outcomes and the event sequences required to produce them.

Examples of event trees and fault trees follow.

Figure 3: Example Fault Tree

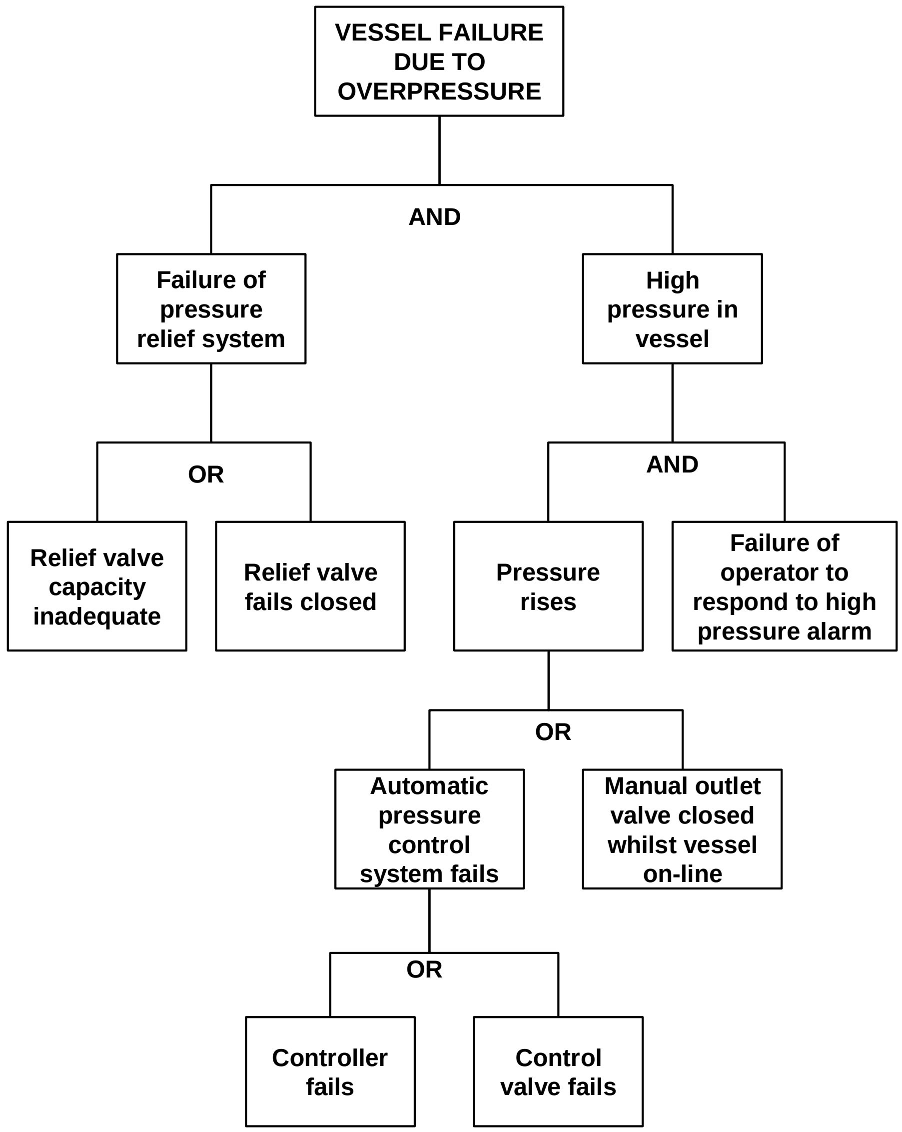
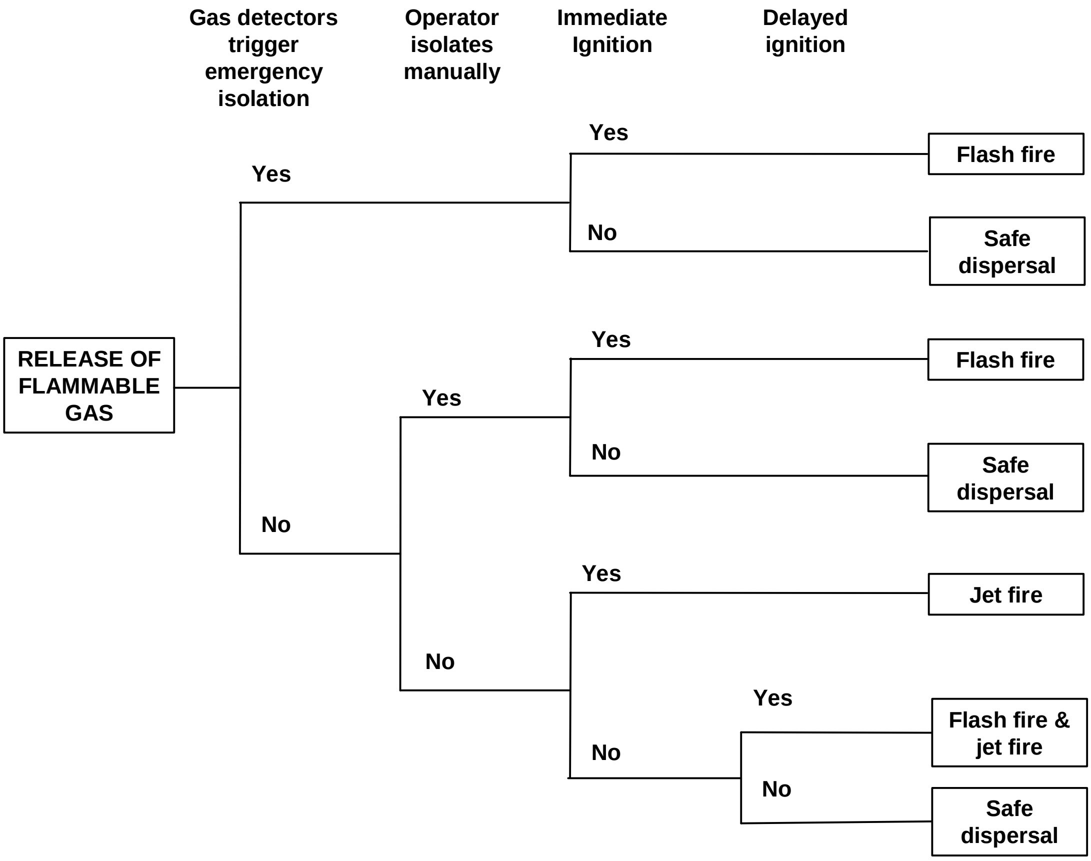


Figure 4: Example Event Tree



Appendix 2

Models for Consequence Analysis

The modelling of the consequences of hazardous incidents is a complex field requiring a substantial degree of expertise. The intention of this appendix is to provide a basic understanding of the range of issues involved and to direct those interested towards more detailed reference material. The references included have been selected because they are authoritative and widely available. They do not necessarily cover specialised detail nor do they necessarily represent the latest developments or techniques.

AIChE (2000) provides a good overview of the range of consequence models available. The TNO Yellow Book (1997) provides more detailed descriptions of some of the models.

Discharge Models

Discharge models are often the first stage in developing consequence estimates. Their purpose is to allow the rate of release and the amount released to be estimated.

It is important to correctly determine the phase of the discharge as this affects the flow rate. The release could be in the form of a gas, liquid or two-phase mixture. The behaviour of the contents of the vessel and the discharge rate depend on a number of factors such as the properties of the material and the temperature and pressure within the vessel immediately before release.

Some examples of discharge phenomena are as follows:

a) vapour discharges may result from:
   - a hole in equipment containing gas under pressure;
   - a valve discharge of vapour only;
   - evaporation or boil-off from a liquid pool.

b) liquid discharges may result from:
   - holes in atmospheric storage tanks or other atmospheric storage vessel or pipes under liquid head;
   - holes in process equipment containing pressurised liquids below their normal boiling point.

c) two-phase discharges may result from:
   - a hole in equipment in the region of a gas/ liquid interface;
   - a hole in pressurised process equipment containing a liquid above its normal boiling point;
   - a relief valve discharge under certain conditions (possibly a foaming liquid, a runaway reaction or because the vessel it relieves has been moved and the valve is no longer at the top of the vessel).

Gas and liquid discharge calculations are well understood and are readily available from standard references such as Perry et al. (1997) and Coulson et al. (1999). Further information is available from TNO (1997), Cremer and Warner (1982), and AIChE (1996).

The total amount of material released is usually determined by the amount of material stored in any single vessel or interconnected vessels plus the net ingress of material into the system, for instance, due to fluids being pumped from elsewhere.

In many situations, it is necessary to estimate the flash fraction of an initial liquid discharge, and the extent of entrainment of liquid droplets, for instance from pressurised liquefied gases. Methods for estimating flash fractions are presented in the TNO Yellow Book (1997), Lees (1996) and AIChE (1996).

Dispersion Models

The analysis of the dispersion of gases and particulates in air and contaminants in water bodies often plays a central role in consequence calculations. Because the effects of hazardous materials on people and the environment are dependent upon the concentration/time exposure profiles, these profiles must be considered in order to properly estimate effects.

In order to make the calculations manageable, however, rather than calculating the exact concentration/time profiles, it is often appropriate to make simplifying assumptions. For instance, the maximum ground level concentration of a toxic gas might be assumed to exist throughout the duration of the event instead of more rigorously analysing the time varying concentration. For flammable clouds, it may be sufficient to estimate the maximum dimensions of the cloud which is within flammability limits.

The exact methodology adopted will depend upon the needs of the particular circumstances and judgement will have to be exercised by the analyst in order to decide upon the appropriate degree of detail.

Vapour cloud behaviour is determined predominantly by the density of the gas relative to air, the rate of release over time and weather conditions. It is convenient to classify the clouds according to whether they are heavier than, the same density as or lighter than air (negative, neutral or positive buoyancy).

Clouds with positive buoyancy tend to rise. In most circumstances, this tends to limit the harm they can inflict.

Dense clouds stay at low levels for a considerable distance downwind and pose a much greater hazard. In some instances, dense clouds can travel upwind because of a combination of topographical features and gravitational forces.

Gases with Neutral or Positive Buoyancy

Gases of neutral or positive buoyancy may be assumed for dispersion calculations under a number of circumstances:

- for gases with density similar to that of air;
- for small puffs of dense gas that dilute rapidly at the point of release to a neutral buoyancy; and
- in a dense gas dispersion model after neutral buoyancy of the dispersing cloud has been achieved.

The Pasquill-Gifford model is the commonly used model for dispersion estimates. The model is described in Pasquill and Smith (1983), TNO (1997) and Lees (1996).

In cases where the release is a high velocity turbulent jet rather than a plume, more sophisticated analysis is required. The dispersion of a neutral, buoyant or dense jet is discussed in AIChE (2000).

Dense Gases

Substances included in the dense gas category include those with molecular weight heavier than air, liquefied gases at cryogenic temperatures and liquefied gases stored under pressure and which become denser than air due to a fall in temperature upon release.

The behaviour of dense gas clouds is characterised by an initial slumping and horizontal spreading due to the force of gravity.

A number of models have been developed for consequence modelling of dense gas dispersion. The mathematics which describes the dispersion process is complex and hence the models are usually incorporated into computer programs. Reviews of some models for dense gas dispersion are provided in AIChE (1996) and Daish et al. (1998).

Particulates

The dispersion characteristics of particulates such as toxic dusts or smoke may also need to be analysed. Lees (1996) provides a list of further references on the dispersion of particulates in air.

Fires

The thermal radiation incident at various points away from the fire is governed by the heat flux at the flame surface and the flame geometry. The surface heat flux is in turn governed by the burning characteristics of the particular material under the particular physical conditions. The heat flux at any particular point can be estimated using the 'view factor method' which is described in TNO (1997). The various types of fires are described briefly in Section 5.3.1 with further information available in TNO (1997).

Fire damage estimates are based upon correlations with recorded incident radiation flux and damage levels. A table of radiation effects is included in Table 1.

Explosions

The modelling of explosions is a complex and rapidly developing science. In terms of calculating risk, blast overpressures are the most important consequences, although projected fragments should also be considered.

The simplest and most often used technique of calculating overpressures is the well documented TNT Equivalence Model, described in Lees (1996). However, more sophisticated models are available, some of which are detailed in AIChE (2000). Information on explosion fragments is presented in TNO (1997) and Holden (1988).

More detailed information on explosion characteristics and modelling is contained in Lewis and von Elbe (1987) and Vinnem (1999).

A list of effects of explosion overpressure is included in Table 2.

Table 1: Effects of Heat Radiation

Heat Radiation [kW/m^2]	Effect
1.2	Received from the sun at noon in summer
2.1	Minimum to cause pain after 1 minute
4.7	Will cause pain in 15-20 seconds and injury after 30 seconds exposure (at least second degree burns will result)
12.6	Significant chance of fatality for extended exposure. High chance of injury After long exposure, causes the temperature of wood to rise to a point where it can be readily ignited by a naked flame Thin steel with insulation on the side away from the fire may reach a thermal stress level high enough to cause structural failure.
23	Likely fatality for extended exposure and chance of fatality for instantaneous exposure Spontaneous ignition of wood after long exposure Unprotected steel will reach thermal stress temperatures which can cause failures Pressure vessel needs to be relieved or failure will occur
35	Cellulosic material will pilot ignite within one minute's exposure Significant chance of fatality for people exposed instantaneously

Table 2: Effects of Explosion Overpressure

Explosion Overpressure	Effect
3.5 kPa (0.5 psi)	90% glass breakage No fatality and very low probability of injury from overpressure.
7 kPa (1 psi)	Damage to internal partitions and joinery, but can be repaired Probability of injury is 10%. No fatality
14 kPa (2 psi)	House uninhabitable and badly cracked
21 kPa (3 psi)	Reinforced structures distort Storage tanks fail 20% chance of fatality to a person in a building
35 kPa (5 psi)	House damaged beyond repair Wagons and plant items overturned Threshold of eardrum damage 50% chance of fatality for a person in a building and 15% chance of fatality for a person in the open
70 kPa (10 psi)	Threshold of lung damage 100% chance of fatality for a person in a building or in the open Complete demolition of houses

Environmental Effects

The effect of a release of hazardous material on the environment depends on a number of factors, including:

- the quantity and nature of materials released;
- the environmental pathways by which the contaminant may be transported;
- the fate of the contaminant in the environment;

- the concentration of the contaminant in the environment; and
- the species and populations at risk.

The assessment of risk to the biophysical environment must take into account the fact that the chemistry of contaminants is affected by many factors and must be evaluated on a site-specific and substance-specific basis. It is necessary to determine which aspect of the natural ecosystem is at risk and whether available data are adequate to estimate exposure and effects of concern.

Predicting an ecosystem's response to pollutant stress is difficult because of the large number of dependent and independent variables constituting and inherent to a natural ecosystem. These include population-level factors such as density, immigration, growth and mortality and community-level factors such as diversity, relative dominance and distribution. There are ways however, to simplify the complex structure of an ecosystem. For example, determination and analysis of key species may facilitate prediction of the effect of pollutant stress on dependent species. In addition, knowledge of physio-chemical parameters of pollutants may make possible the analysis of pollutant fate and transport. Nevertheless, ecosystem-level analysis is an inherently complex undertaking.

Similarly, the analysis of the physical and chemical processes involved can also be complex. For example, land contamination may result from many different activities and incidents including spills, fugitive emissions, waste disposal, mining spoil and tailings, industrial slag etc. A release into the soil can affect humans and animals by ingestion of contaminated dust transported in air, consumption of water from sources in contaminated areas or consumption of vegetables grown in contaminated soil. A pollutant may be subject to different processes in the same soil under different meteorological conditions. In arid areas, transportation through the air is more likely than in rainy areas where the flow of water through the soil may be sufficient to make transport by leaching and run-off more important. The physical properties of the soil are also important including permeability, organic carbon content and depth of groundwater table. Finally, the properties of the hazardous material, such as solubility in water, are important.

Various models can be used to evaluate ecosystem risk. These include models of fate, transport, exposure and effects as well as integrative models. However, the applicability of the models is usually restricted to specific conditions and, in many cases, the quantification by models of the transport and fate of some contaminants in the environment is not yet possible. A review of available models is given in Swann and Eschenroeder (1983) and Ricci (1985). The understanding of these matters is, however, developing rapidly and reference should be made to the relevant scientific literature when undertaking analysis of risk to the biophysical environment.

Other ecosystem models focus on population density, food chains, bioenergetics and toxicokinetics. The diverse models for both individual species and population groups have advantages and disadvantages that must be defined and tailored to meet specific circumstances. It is essential to use an orderly and justifiable approach in developing and selecting an appropriate ecosystem model. Refining and improving available models are critical aspects of developing precise models for each particular situation in nature. Models should not be used for situations where they have questionable validity or to predict impacts for conditions appreciably different from those for which the models were originally developed.

The transport and fate of contaminants over several environmental compartments are extremely complex. Fugacity models may aid assessment in this regard. These models are based on the principle that when released in a specific environmental compartment, the contaminant has a tendency to be distributed over other environmental compartments until equilibrium is reached. Such models have been developed by Mackay et al. (1983). However, the fugacity models only quantify the distribution over the basic environmental compartments - air, water, soil, sediment and biota rather than the concentration gradients within each of these compartments. Consequently, these models are only useful for analyses covering large regions.

Resilience and resistance are also appropriate response variables for impact assessment. Factors that affect the recovery of an ecosystem from environmental stress include:

- the severity of the stress;
- reversibility of effects;
- rate of effectiveness of stress removal;
- frequency and duration of ecosystem disturbance;
- resilience of ecosystems structure and function;
- extent of alteration;
- compensatory interaction of multiple species;
- kinetic balance of the system;
- complexity of the system;
- temporal and spatial variability;
- availability of regenerating units; and
- rate of re-establishment of the biological and physical habitat.

Appendix 3

Methods for Estimating the Likelihood of Hazardous Events

The likelihood of accidents and their consequences can be estimated using generic or specific failure data, either directly, or as input into logic sequence models.

Open literature is the most common source of generic failure data. However, detail is often lacking and important information such as failure mode and process conditions are often missing, and it is often possible to find data that varies widely due to this. Much of the data have been generated in the nuclear and aerospace industries and the conditions of operation may be different from, for example, process industries. Examples of failure data sources are Lees (1996), CCPS (1989), Committee for the Prevention of Disasters (1999) and IAEA (1988a).

Data are also available from published Risk Assessments of Major Hazard Facilities, such as sections of Environmental Impact Statements and Land Use Safety Studies.

Where specific failure data are not available, the likelihood of particular equipment failures or hazardous incidents may be estimated using logical sequence models. These techniques analyse the modes of failure and sequence of events that lead to hazardous incidents. The most commonly used methods are fault tree analysis and event tree analysis.

Random number techniques, such as Monte Carlo simulation, use a fault tree or similar logic model as a basis. The probability of each contributing failure is expressed as a range of probabilities. The severity of the 'top event' is expressed as a function of the probability of various events. In this way it is possible to differentiate the effect of each contributing factor to the top event.

Common cause failure (CCF) analysis is particularly useful in assessing the causes of dependent failures in plants where system redundancy has been increased to improve reliability. CCF investigates the factors that create dependencies among components and identifies those most likely to lead to a CCF. A quantitative CCF evaluates the probability of occurrence of each postulated CCF event. The method has been described in Mosleh (1988) and AIChE (1992).

External events analysis estimates the frequency of external events that can trigger a major incident. In evaluating external initiating events, the likelihood of the triggering event must be combined with the probability of failure associated with that event. Flood zone maps, earthquake zones,

The likelihood of people making mistakes is referred to as Human Error. Some examples are provided in Table 3. For more details see Kletz (1991) and CCPS (1994).

Table 3: Example Human Error Potential Values (based on Hunns and Daniels 1980 and Kletz 1991)

Type Of Behaviour	Human Error Probability
Extraordinary errors: of the type difficult to conceive how they could occur: stress free, powerful cues initiating for success.	10^{-5} (1 in 100,000)
Error in regularly performed, commonplace, simple tasks with minimum stress (e.g. Selection of a key-operated switch rather than a non key-operated switch).	10^{-4} (1 in 10,000)
Errors of commission[1] such as operating wrong button or reading wrong display. More complex task, less time available, some cues necessary (e.g. selection of a large-handled switch rather than a small switch).	10^{-3} (1 in 1,000)

Type Of Behaviour	Human Error Probability
Errors of omission[2] where dependence is placed on situation cues and memory. Complex, unfamiliar task with little feedback and some distractions (e.g. failure to return manually operated test valve to proper configuration after maintenance).	10^{-2} (1 in 100)
Highly complex task, considerable stress, little time to perform it. e.g. during abnormal operating conditions, the operator reaching for a switch to shut off an operating pump fails to realise from the indicator display that the switch is already in the desired state and merely changes the status of the switch.	10^{-1} (1 in 10)
Process involving creative thinking; unfamiliar complex operation where time is short, stress is high.	Greater than 10^{-1}

1 Errors of commission are errors in which the person performs extra steps that are incorrect or performs a step incorrectly. They also include errors where a person performs a sequence of steps in the wrong order or performs a step too quickly or too slowly. Errors of commission often reflect inadequate training and/or procedures, poor instruction or job aids, or a person being unaware of the risks/hazards associated with equipment or the environment.

2 Errors of omission are instances where a person fails to perform one or more steps in a procedure. They can be caused by people being confused or having communication problems. Distraction or diversion of attention is also often the source of these errors. An inadequate mental model of a complex system can lead to errors of omission when the system experiences a malfunction. They are particularly prevalent in maintenance tasks.

It is important that the generic nature of these values is recognised. As with all assumptions made during Risk Assessment, HEP values should be chosen conservatively, and where risk levels exceed relevant criteria, more detailed methods of analysis may be required.

Appendix 4

Sample Hazard Identification Word Diagram

Facility/Event	Cause/Comment	Possible Results/ Consequences	Prevention/Detection Protection Required
TANK FARM			
Petroleum tank fire	Static electricity build up and spark due to fast filling. Pressure vent valve fails, tank roof fails and ignition.	Tank roof may fail, fire of entire roof area. If not controlled or extinguished may involve other tanks in same compound	Pressure vent valves checked prior to fill/ discharge. Foam injection system in al class 3(a) tanks. Water cooling system on each tank.
Petroleum bund fire	Corrosion tank base/ floor. Pipeline/ pump leakage/ rupture. Tank overfilled.	Leakage of tank contents into bund. If ignited may result in pool or bund fire.	Tanks cleaned, inspected, integrity tested annually. Adequate foam stocks on site. High level alarms to be provided on all storage tanks. Foam/ monitors to be provided in and around bund compound.
Petro-chemical tank(s) (cool fire)	Adjacent tank fire or bund fire heating tank contents to decomposition.	Emission of toxic products or vapours. Downwind effects depend on toxicant released and wind/ stability conditions.	Tanks placed in separate bund. Cooling system on all tanks.
LPG ROAD TANKER FACILITY			
Flexible hose failure	Road tanker drives away while still connected. Third party damage or excessive wear.	Gas disperses. If ignited may result in flash fire. Impact local.	Fixed deluge system at road tanker bay. Scully system on tanker loading.
Pipe failure	Mechanical impact. Corrosion.		Area drained. Gas detectors around perimeter of LPG area.

Facility/Event	Cause/Comment	Possible Results/ Consequences	Prevention/Detection Protection Required
WAREHOUSE DANGEROUS GOODS STORE			
Warehouse fire	Wiring not flameproof. Handling equipment not intrinsically safe. Shrink wrapping fired by LPG, undertaken on site. Arson. Lighting not intrinsically safe. Unsafe storage of drums.	Fire involving warehouse contents. Exploding drums/ packets depending on material stored. Toxic combustion products evolved.	All products segregated by class. Thermal/ smoke detectors provided, linked to alarm and local fire station. Warehouse sprinkler system provided. Area bunded. Flameproof wiring used in dangerous goods store. Diesel forklifts only. Security firm employed after hours. All lighting intrinsically safe. Drum storage racked or drum height restricted.
LPG STORAGE			
Catastrophic vessel failure	Direct flame impingement on tank, from pipes, tank fittings or pump failure and ignition.	Pressure inside tank rises, if fire not extinguished, vessel may weaken and fail resulting in a BLEVE/ fireball. Damage widespread.	Vessel fitted with pressure relief valves, discharge vertical to atmosphere. Deluge system. Isolation valves fitted to all main liquid lines. Pump shut-off at two locations.
Large leak	Mechanical impact. Corrosion. Failure of tank or associated fittings, pump or pipework and ignition.	On dispersion, vapour may form a gas cloud. If ignited, may result in UVCE or flash fire.	Isolation valves on all main liquid lines. Pump shut-offs at two locations, local and remote. Gas detection on perimeter of LPG area. Fog nozzles provided. Crash barriers provided around tank.

Technical References

1. American Institute of Chemical Engineers /CCPS 1988, *Guidelines for Safe Storage and Handling of High Toxic Hazard Materials,* Centre for Chemical Process Safety, AIChE, New York.
2. American Institute of Chemical Engineers 1996, *Guidelines for Use of Vapour Cloud Dispersion Models*, 2nd ed, Center for Chemical Process Safety AIChE, New York.
3. Australian and New Zealand Environment and Conservation Council 2000, *Australian and New Zealand Guidelines for Fresh and Marine Water Quality,* Australian and New Zealand Environment and Conservation Council.
4. Center for Chemical Process Safety (CCPS) 1989, *Process Equipment Reliability Data*, AIChE, New York.
5. Center for Chemical Process Safety (CCPS) 1992, *Guidelines for Hazard Evaluation Procedures*, 2nd ed, AIChE, New York.
6. Center for Chemical Process Safety (CCPS) 1994, *Guidelines for Preventing Human Error in Process Safety,* AIChE, New York.
7. Center for Chemical Process Safety (CCPS) 2000, *Chemical Process Quantitative Risk Analysis*, 2nd ed, AIChE, New York.
8. Committee for the Prevention of Disasters 1999, *Guidelines for Quantitative Risk Assessment "Purple Book",* CPR 18E, Sdu Uitgevers, Den Haag.
9. CONCAWE Ad-Hoc Risk Assessment Group 1984, *Methodologies for Hazard Analysis and Risk Assessment in the Petroleum Refining and Storage Industry*, *Fire Technology*, vol. 20, no. 3.
10. Cremer & Warner 1979, *Risk Analysis of Six Potentially Hazardous Objects in the Rijnmond Area*: *A Pilot Study*, report to Rijnmond Public Authority.
11. Daish, N.C., Carissimo, B., Jagger, S.F., Linden, P.F., Britter, R.E. 1998, 'SMEDIS: Scientific model evaluation of dense gas dispersion models', *Proceedings of the 5th International Conference on Harmonisation within Atmospheric Dispersion Modelling for Regulatory Purposes*, Rhodes, May 1998. pp. 54-61.
12. Dutch Directorate of Labour 1997, *Methods for the Calculation of the Physical Effects of the Escape of Dangerous Liquids and Gases (TNO Yellow Book),* 3rd Ed, Dutch Directorate of Labour, Ministry of Social Affairs.
13. Eisenberg N.A., Lynch C.J. and Breeding R.J. 1975, *Vulnerability Model: A Simulation System for Assessing Damage Resulting from Marine Spills*, Enviro Control Inc., US Coast Guard Report CG-D-B5-75.
14. Embrey, D.E. 1986, 'SHERPA – A Systematic Human Error Reduction and Prediction Approach', *International Topical Meeting on Advances in Human Factors in Nuclear Power Systems*, USA.
15. Frank, W.L. & Whittle, D.K. 2001, *Revalidating Process Hazard Analyses,* CCPS, AIChE, New York.
16. Haddad S., Mullins D., Maltz A., *Ecological Risk Assessment and the Planning Process*.
17. Health and Safety Executive 1978, *Canvey: An Investigation of Potential Hazards from Operations in the Canvey Island/Thurrock Area*, HSE, HMSO, UK.

18. Health and Safety Executive 1981, *Canvey: A Second Report: A Review of Hazards from Operations in the Canvey Island/Thurrock Area Three Years after,* HSE, HMSO, UK.
19. Health and Safety Executive 1992, *The Tolerability of Risk from Nuclear Power Stations,* .HSE Books.
20. Health and Safety Executive 2001, *Reducing Risks, Protecting People*, HSE Books.
21. International Atomic Energy Agency December 1993 and December 1996 (Rev.1), *Manual for the Classification and Prioritisation of Risks Due to Major Accidents in Process and Related Industries*, International Atomic Energy Agency, Inter-Agency Program on the Assessment and Management of Health and Environmental Risks from Energy and Other complex Industrial Systems, IAEA-TECDOC-727 and IAEA-TECDOC-727 (Rev.1), Vienna.
22. Kletz, T. 1991, *An Engineer's View of Human Error*, 2nd ed, IChemE.
23. Lees, F.P. 1996, *Loss Prevention in the Process Industries*, 2nd ed, Butterworth-Heinemann.
24. Lewis, B. & von Elbe, G. 1987, *Combustion, flames and explosions of gases,* Academic Press.
25. Middleton, M. and Franks, A. 2001, *Using Risk Matrices*, The Chemical Engineer.
26. Mosleh, A. 1988, *Procedures for Treating Common Cause Failures in Safety and Reliability Studies*, US Nuclear Regulatory Commission, NUREG/CR-4780, Washington DC.
27. New South Wales Department of Planning 1994, *Best Practice Guidelines for Contaminated Water Retention and Treatment Systems*, Sydney.
28. Pasquill, F. & Smith, F.B. 1983, *Atmospheric Diffusion,* Ellis Horwood, London.
29. Pastorok, R.A., Bartell, S.M., Ferson, S. & Ginzburg, L.R. 2001, *Ecological Modelling in Risk Assessment: Chemical Effects on Populations, Ecosystems, and Landscapes,* Lewis Publishers.
30. Sax, N.I. and Lewis, D.J. 1989, *Dangerous Properties of Materials*, 7th Ed, van Nostrand Reinhold.
31. Schüller, J.C.H., Brinkman, J.L., van Gestel, P.J. and van Otterloo, R.W. 1997, *Methods for Determining and Processing Probabilities,* CPR12E, 2nd ed.
32. Standards Australia 1999, *Risk Management*, AS/NZS 4360:1999, ISBN 0 7337 2647 X.
33. van den Bosch, C.J.H. and Weterings, R.A.P.M. 1997, *Methods for the Calculation of Physical Effects,* CPR14E (parts 1 and 2), 3rd edition.
34. Vinnem, J.E. 1999, *Offshore Risk Assessment / Principles, Modelling and Applications of QRA Studies*, Dordrecht ; Boston : Kluwer Academic Publishers.
35. Williams, J.C. 1988, *A Data-Based Method for Assessing and Reducing Human Error to Improve Operational Performance*, Proceedings of the IEEE 4th Conference on Human Factors and Power Plants, pp. 436-450.
36. Wong W. 2002, *How Did That Happen? – Engineering Safety and Reliability*, Professional Engineering Publishing, UK.
37. Wright N.H., 1993, *Development of Environmental Risk Assessment (ERA) in Norway*, Norske Shell Exploration and Production.

Additional Information

Relevant DoP Publications

Hazardous Industry Planning Advisory Papers (HIPAPs):

No. 1 - Emergency Planning

No. 2 - Fire Safety Study Guidelines

No. 3 - Risk Assessment

No. 4 - Risk Criteria for Land Use Safety Planning

No. 5 - Hazard Audit Guidelines

No. 6 - Hazard Analysis

No. 7 - Construction Safety

No. 8 - HAZOP Guidelines

No. 9 - Safety Management

No. 10 - Land Use Safety Planning

No. 11 - Route Selection

No. 12 - Hazards-Related Conditions of Consent

Other Publications:

Applying SEPP 33: Hazardous and Offensive Development Application Guidelines

Multi-level Risk Assessment

Locational Guideline: Liquefied Petroleum Gas Automotive Retail Outlets

Locational Guideline: Development in the Vicinity of Operating Coal Seam Methane Wells

Electronic copies of some of these publications are available at:
www.planning.nsw.gov.au