Guidance Note

Safety Assessment for a major hazard facility

Advice for operators of major hazard facilities on conducting and documenting a Safety Assessment.

May 2011

1. Introduction

The major hazard facility parts of the Occupational Health and Safety Regulations 2007 (OHS Regulations) set out legal duties for control of risks from operating a major hazard facility (MHF). They apply to the operator of a facility who is the employer with management or control of the facility.

To obtain a licence to operate an MHF in Victoria, operators are required to submit a Safety Case which sets out how the facility will be operated safely.

This guidance note will assist the operator through the process of conducting and documenting a Safety Assessment which forms part of the Safety Case.

1.1. What is a Safety Assessment?

The purpose of a Safety Assessment is to help the operator understand all aspects of the risks to health and safety associated with potential major incidents and demonstrate how those risks will be reduced so far as is reasonably practicable. Any deficiency in the Safety Assessment process may make it difficult to demonstrate the adequacy of risk control measures and that the risk has been reduced so far as is reasonably practicable.

The Safety Assessment process is consistent with international standards on risk assessment including the process within AS/NZS ISO 31000:2009 – *Risk Assessment*. Reg 5.2.7 requires the Safety Assessment

to involve an investigation and analysis of:

(a) the nature of each major incident hazard and major incident

(b) the likelihood of each major incident hazard causing a major incident

(c) in the event of a major incident occurring –

  (i) its magnitude and

  (ii) the severity of its consequences to persons both on-site and off-site

(d) the range of risk control measures considered.

A Safety Assessment generally follows the hazard identification process although some iteration between the two processes may be required. Hazard identification processes will determine the hazards and causes of major incidents and most likely will have started identifying the range of risk control measures that provide protection against a major incident occurring.

The outcomes of the Safety Assessment are to:

- provide the operator and facility workers with sufficient knowledge, awareness and understanding of the risks from major incidents to be able to prevent and deal with dangerous occurrences
- identify major risk contributors
- provide a basis for identifying, evaluating, defining and justifying the selection (or rejection) of risk control measures for eliminating or reducing risk
- lay the foundations for demonstrating the adequacy of the controls necessary to assure the safety of the facility
- show clear links between risk control measures and the potential major incidents
- identify areas of concern for community consultation, critical Safety Management System controls and emergency plan
- achieve an acceptable level of on-site and off-site risk ie to demonstrate that risks are reduced so far as is reasonably practicable.

1.2. Features of a Safety Assessment

The Safety Assessment must be comprehensive and systematic.

A comprehensive Safety Assessment must:

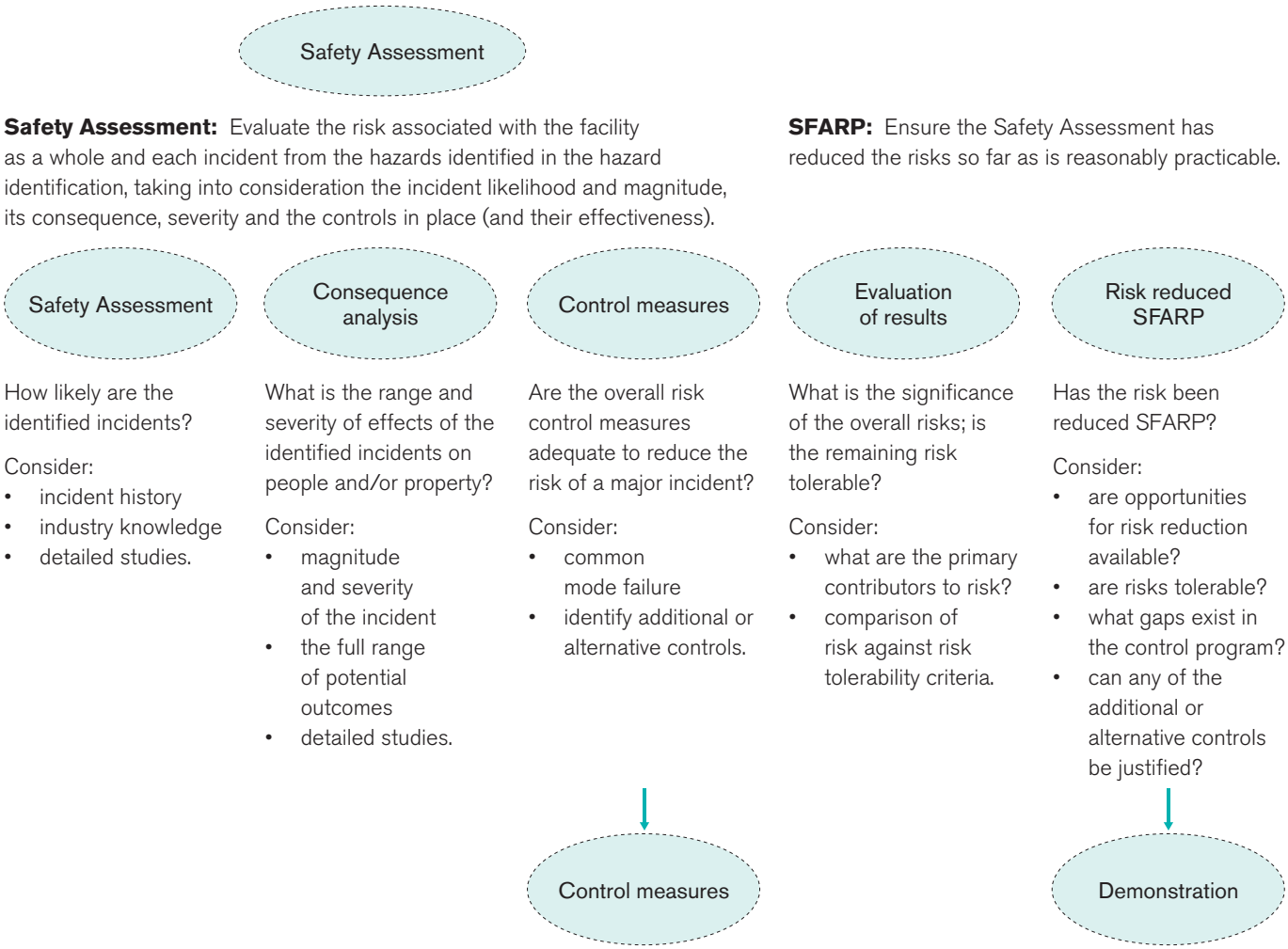
- cover all hazards, potential major incidents and associated parts of the facility
- address all of the aspects of risk for each hazard and incident (nature, likelihood etc)
- cover all areas and phases of operation of the facility including start-up, shutdown etc.

A systematic Safety Assessment must employ a logical, transparent and reproducible process which enables the operator to compare the range of incidents and identify which are the most important contributors to the overall risk profile of the facility. The following factors lead to a successful Safety Assessment:

- The Safety Assessment should be workable and relevant to the facility.
- A fresh view should be taken of any existing knowledge and it should not be automatically assumed that no new knowledge is required.
- The information is provided to persons who require it to work safely.
- An appropriate group of workers is actively involved and consultation occurs.
- Uncertainties are explicitly identified and reduced to an acceptable level.
- All methods, results, assumptions and data are documented.
- Risk control measures and their affects on risk are explicitly addressed.
- The Safety Assessment is used as a basis for adopting risk control measures, including improvements to the Safety Management System and emergency planning.
- The Safety Assessment is regularly maintained and used as a ‘live’ document.

Knowledge of hazards and their implications is necessary for Safety Assessment but is only worthwhile if it informs and improves decision-making and seeks to reduce risk so far as is reasonably practicable. Figure 1.1 shows the key steps in achieving an effective and compliant Safety Assessment.

Figure 1.1 – Key steps of a Safety Assessment



1.3. Key definitions

Control measure (control): Any system, procedure, process, device or other means of eliminating, preventing, reducing or mitigating the risk of major incidents arising at an MHF. Controls can include physical equipment, process control systems, management processes, operating or maintenance procedures, the emergency plan, and key personnel and their actions.

Hazard (major incident hazard, related to an MHF): Any activity, procedure, plant, process, substance, situation or any other circumstance that could cause, or contribute to causing, a major incident.

Hazard identification: The process of identifying hazards as described in the WorkSafe guidance note – *Hazard identification*.

Major incident: An uncontrolled incident, including an emission, loss of containment, escape, fire, explosion or release of energy, that –

(a) involves Schedule 9 materials, and

(b) poses a serious and immediate risk to health and safety.

Safety Assessment: A Safety Assessment process consistent with international risk assessment standards including AS/NZS ISO 31000 – *Risk Management*. A Safety Assessment involves an investigation and analysis of the major incident hazards and major incidents to provide the operator with a detailed understanding of all aspects of risk to health and safety associated with major incidents, including –

(a) the nature of each hazard and major incident

(b) the likelihood of each hazard causing a major incident

(c) in the event of a major incident occurring –

  (i) its magnitude and

  (ii) the severity of its consequences to persons both on-site and off-site

(d) the range of risk control measures considered.

So far as is reasonably practicable: To reduce risk to a level so far as is reasonably practicable involves balancing reduction in risk against the time, trouble, difficulty and cost of achieving it. This requires consideration of:

(a) the likelihood of the hazard or risk concerned eventuating

(b) the degree of harm that would result if the hazard or risk eventuated

(c) what the person concerned knows, or ought reasonably to know, about the hazard or risk and any ways of eliminating or reducing the hazard or risk

(d) the availability and suitability of ways to eliminate or reduce the hazard or risk

(e) the cost of eliminating or reducing the hazard or risk.

The guidance note – *Requirements for demonstration* provides further information on so far as is reasonably practicable as applied to major incident risk. More information on key terms is found in other MHF guidance material available from the WorkSafe website and in the definitions of the OHS Regulations (reg 1.1.5).

2. Planning and preparation

The Safety Assessment required by the MHF regulations is a distinct, formal exercise where the operator and workers stand back from routine activities and take stock of how well risk for the whole facility is understood and managed, and identify where fundamental improvements are needed. Safety Assessment provides an important link between the identified hazards, the adopted risk control measures and the demonstration of adequacy within the Safety Case.

To obtain a useful outcome with minimal rework, the operator must ensure that the Safety Assessment is planned and resourced appropriately. The Safety Assessment should be a living document and it should be easily maintained and updated.

2.1. Selecting the Safety Assessment technique

The operator must select appropriate techniques for identifying the hazards and assessing the risk for the facility. There is a range of techniques available for conducting a Safety Assessment. Some of these techniques are briefly described in the Appendices and additional information can be found in ISO/IEC 31010 *Risk management – Risk assessment techniques*. The major considerations that must be taken into account when selecting the Safety Assessment technique are that it:

- is suitable for the type and complexity of the facility and the nature of the hazards present
- assists in understanding and selecting the risk control measures
- is adequate to differentiate between hazards on a risk basis (ie likelihood and consequence)
- is capable of managing the assessment of cumulative risk and the potential effect of risk reduction measures on the risk
- is not overly complicated for the facility's needs
- is consistent with the facility's general approach to safety.

Depending on the different types of hazards and their potential outcomes, the operator may need to employ several techniques to develop a complete understanding of the hazards on a site. This is because all tools have limitations and weaknesses and no single tool will meet all the requirements for Safety Assessment. Some of the decisions that the operator will have to make in planning the Safety Assessment are:

- technique/s to be used eg layers of protection analysis (LOPA), quantitative risk assessment (QRA), risk matrix
- the level of detail required
- the resources available
- any risk criteria to be used (eg qualitative, semi-quantitative or quantitative).

2.1.1. Qualitative or quantitative risk analysis

Risk analysis may be done using qualitative, semi-quantitative and/or quantitative approaches. In selecting a risk assessment process, the operator should consider the objective of the risk assessment and the level of risk, as well as the detail needed in the assessment results. All three approaches involve the same steps and a variety of Safety Assessment techniques may be applied that correspond with these approaches. The common Safety Assessment techniques and the key points of each approach are listed in Table 2.1.

Table 2.1 – Risk analysis techniques – key aspects

Technique	Safety Assessment techniques	Key aspects of the risk analysis technique
Qualitative	Risk matrix method	• Low cost. • Likelihood and consequence expressed on a scale described in words. • Risk output is not expressed as a numerical value. • Emphasis is placed on relative ranking of hazards eg from highest to lowest. • Conducted via workshop. Participants estimate the risk resulting in greater ownership of the risk results. Site specific. • Based on subjective judgement so a higher potential for uncertainty. • Coarse level of risk assessment in general with little risk ranking capacity. • Difficult to calculate cumulative risk. • Often used as a preliminary risk assessment or screening tool. • Often used for operations or task-based risk assessments. • Suitable for simple facilities or where the exposure of the workforce, public etc is low. • Rapid assessment of risk. • Relatively easy to use. • Can take into account intangible issues such as public outrage and company reputation.
Semi-quantitative	Risk matrix method Risk nomogram Risk graph Layers of protection analysis (LOPA)	• Generates a numerical risk value (although this value is not an absolute value of risk). • Provides greater capacity to discriminate between hazards on the basis of risk. • Better for assessing cumulative risk although still coarse and difficult for large sites. Caution is required to ensure combining like data. • Some methods provide a more structured technique for understanding the effectiveness of controls.
Quantitative	LOPA Fault tree Event tree	• Based on calculated estimates of consequence (usually software modelling) and likelihood (estimates based on failure rate data – site or industry). • Provides a calculated value of risk. • Better suited to more complex decision-making or where risks are relatively high. • Some quantitative techniques (ie fault and event trees) can provide a more detailed knowledge of the causal chain of events and the influence of controls. • More rigorous, detailed and objective than other methods and can better assist choice between different control options. • More time intensive and expensive than other methods. • QRA can provide risk contours if necessary for demonstrating off-site risk and for land use planning. Does not necessarily provide a full understanding of the impact of controls.

When the operator selects a Safety Assessment technique, it is appropriate that the time and resources spent on the risk assessment are proportional to the hazard present and the risk arising from that hazard. Resources are frequently limited and spending excess time on low risks may take resources away from the risks and hazards that are more important.

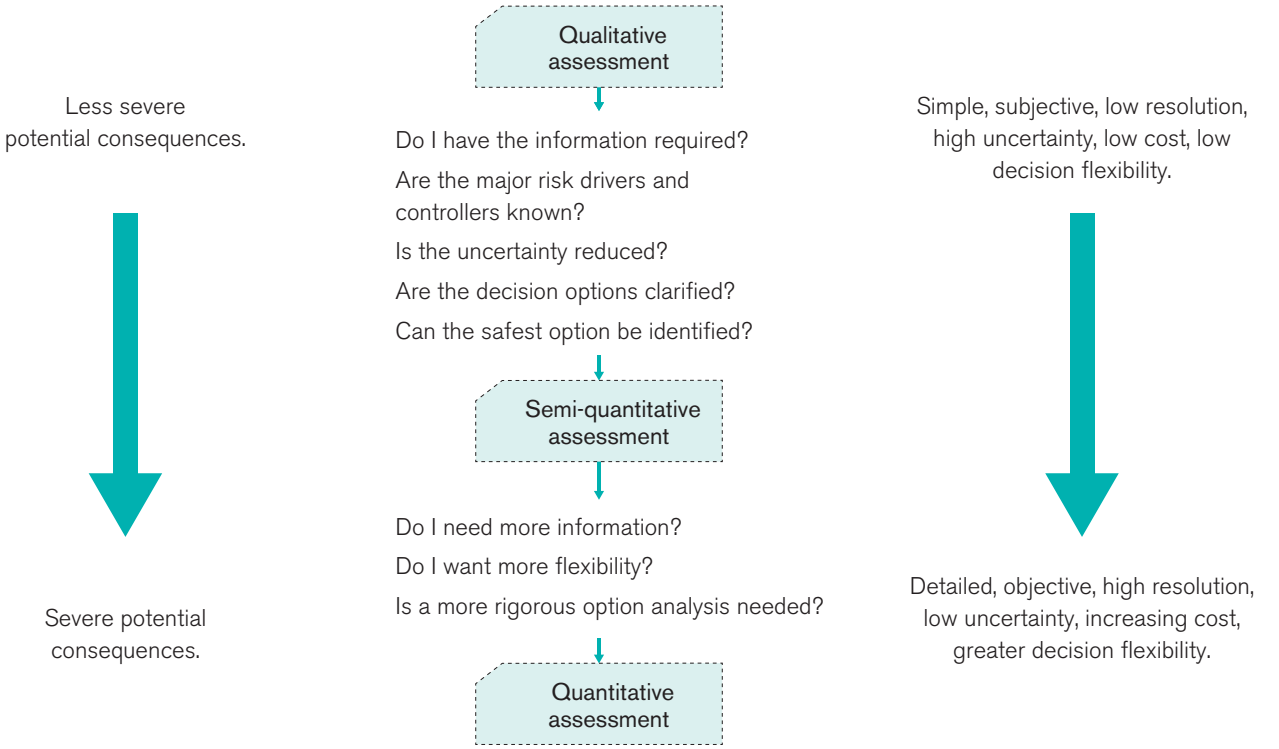
2.1.2. Use of a tiered approach

The tiered or multi-level approach to Safety Assessment may see relatively simple techniques initially used to assess all identified incidents and hazards eg a qualitative or semi-quantitative approach. Once this has been done, the areas of high risk or uncertainty may be subjected to more detailed and specific assessment.

It is possible that a combination of approaches may be required. For example, quantitative consequence modelling may be used to justify the consequence analysis category selected in a risk matrix approach. Alternatively, QRA may be employed for higher risks or more complex processes, while qualitative assessment is used for simpler processes. Some guidance is provided in Figure 2.1 and the following section.

The results of the preliminary hazard evaluation should provide guidance towards the types of detailed studies required. The greatest attention should be directed towards those areas where there are gaps in knowledge, and where the risks may be high. For example, if a qualitative risk assessment shows a high level of risk, then further analysis may be required, including a QRA, to examine the hazard in more detail.

Figure 2.1 – Selection of the risk analysis approach



Example

For an ammonia storage example:

- ABC Chemical Company regularly uses a qualitative matrix method for risk assessment.
- The facility is not complex and the operating personnel are familiar with the matrix method.
- The facility is very stable with changes to the facility occurring rarely.
- While the hazard of ammonia is well known, there is little appreciation of the magnitude of the consequences of a loss of containment.
- Generally the risk assessment is done on more day to day risks.

The company recognises that other techniques may provide some benefit but elects to use the matrix method for the following reasons:

- The operators are comfortable with the matrix method and changes to the facility are so infrequent that use of another technique is not justified on an ongoing basis.
- There are not many hazards so the risk matrix can provide sufficient differentiation of risk between hazards. Quantification, while difficult, is possible.

However, ABC recognises that by using consequence modelling as well it will be able to allocate the hazard to a consequence category more accurately.

The Safety Assessment tool must be able to manage/incorporate cumulative risk and assessment of risk reduction measures. Risk matrices or risk nomograms have a limited ability to achieve these objectives.

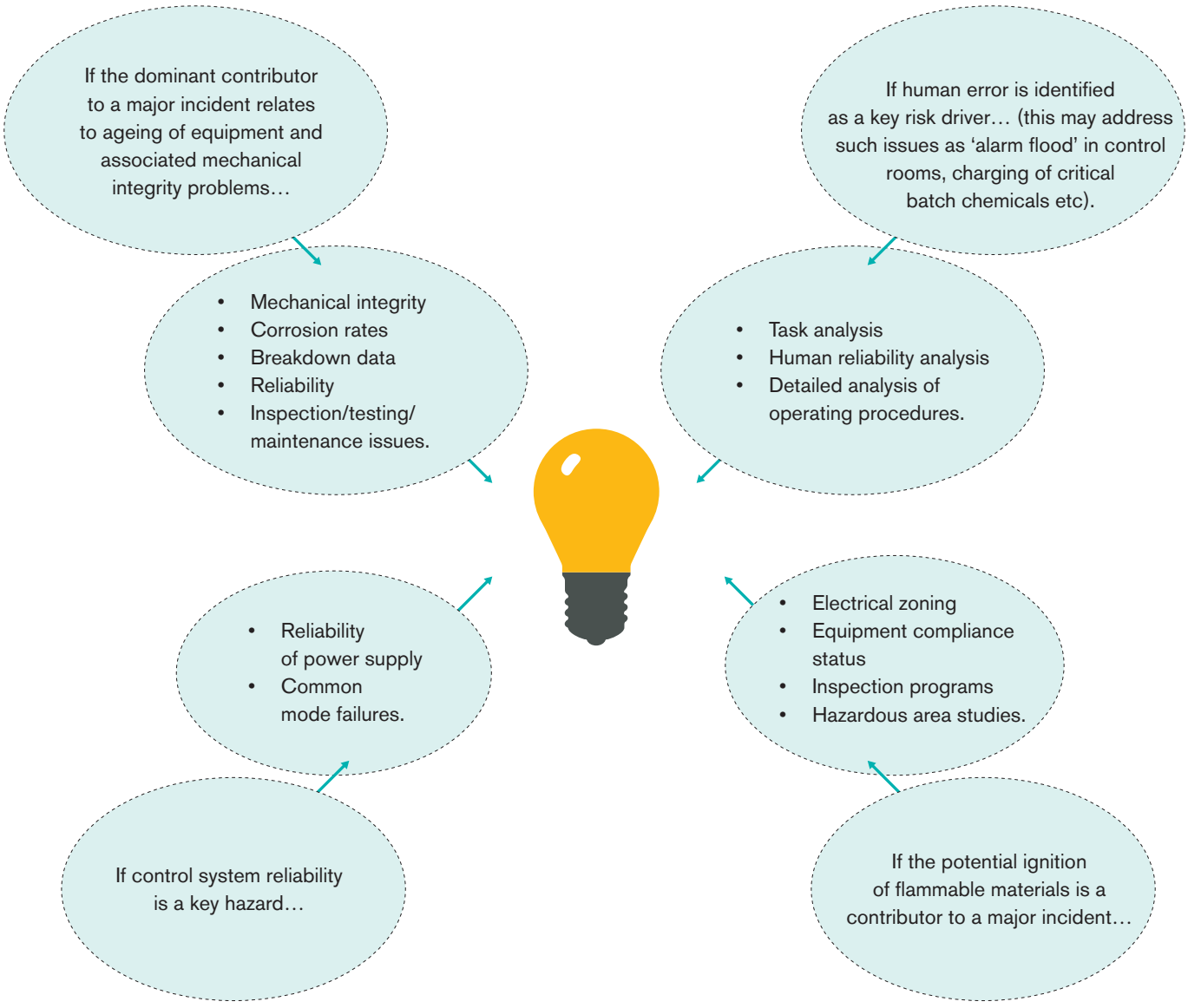
It is difficult to change approaches later in the Safety Assessment, so the operator should carefully consider the choices before making a final decision on which approach best suits the facility.

2.1.3. Detailed Safety Assessment studies

Detailed analyses of the facility and/or process may be required to better understand the mechanisms by which a major incident may occur and the controls in place to prevent this occurrence. These analyses supplement the chosen risk assessment technique and may be required to accurately assess the risk at the facility.

Detailed assessments may involve the application of more quantitative techniques such as fault tree technique or fire safety studies. However, there are other types of detailed studies that may be appropriate to fully investigate and understand a hazard. Some of these are shown in Figure 2.2.

Figure 2.2 – Potential studies for investigation and understanding of a hazard



Where the operator feels there is insufficient knowledge of causes, likelihoods etc in key areas, more detailed studies should be considered to reduce this uncertainty. The operator should choose appropriately detailed studies to investigate high risk/impact hazards. The level of effort required to complete the studies should be proportional to the risk of the hazards under investigation. The operator also needs to select an appropriate risk ranking methodology to allow accurate ranking of the hazards at the facility.

To make the process as efficient as possible, the operator should clearly identify what types of detailed study are required (if any), before conducting each stage of the risk assessment. This may not always be possible and some studies will only be able to be done after the risk assessment has identified a need. However, some detailed studies can readily be identified as being required prior to conducting any risk assessment activity. As some studies (asset integrity studies, hazardous area studies) can take time, it makes sense to identify the required studies and plan their implementation as early as possible.

Example

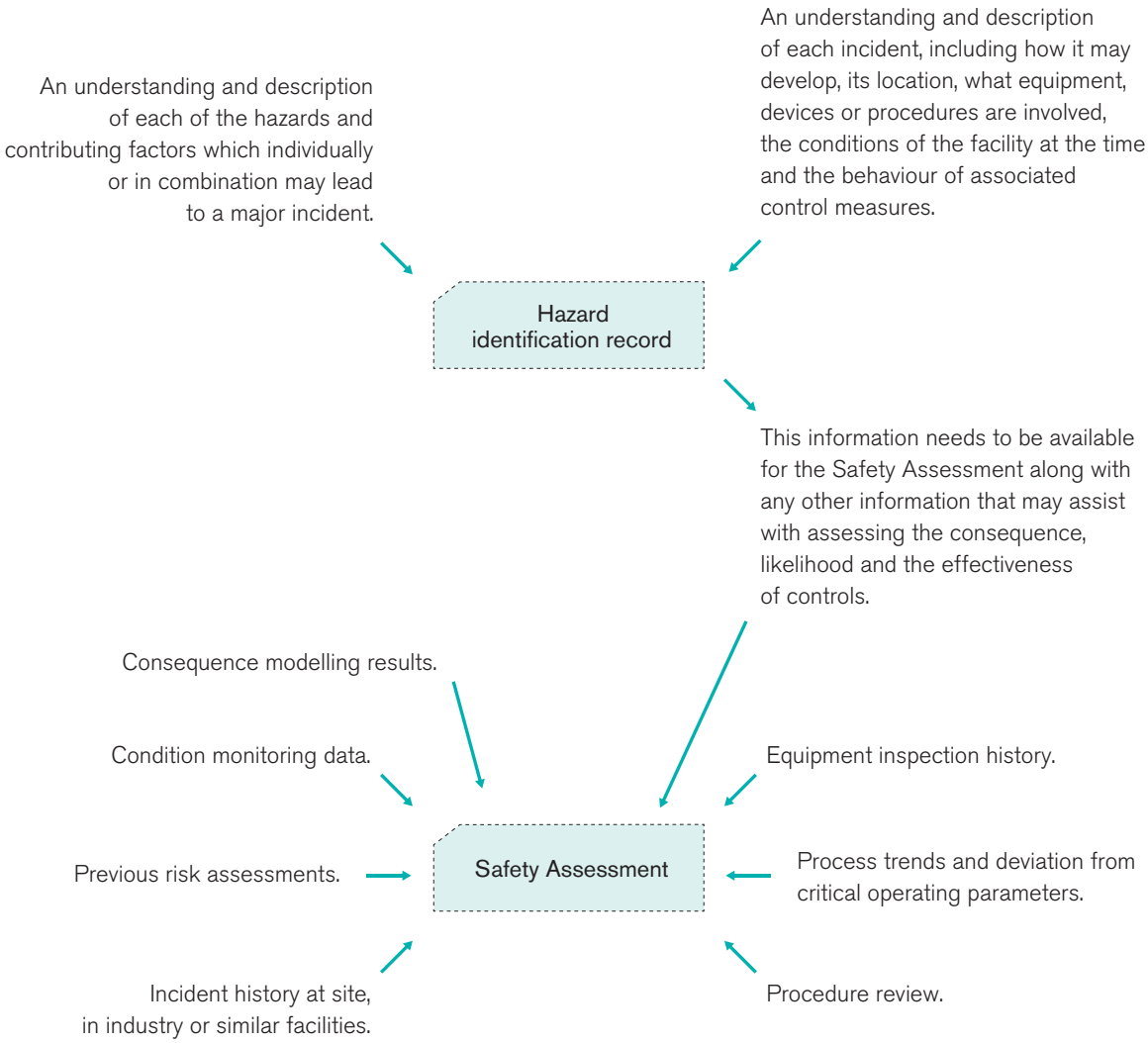
For the ammonia example, an ABC Chemical Company workshop identified that ammonia tanker unloading is a significant hazard. In moving towards driver-only unloading of the tanker, there is uncertainty about the likelihood of an incident arising from this activity.

ABC decides to conduct a task analysis and a human reliability study to quantify the likelihood of something going wrong. This figure is then used to allocate the frequency category on the risk matrix.

2.2. Preparing the information for the Safety Assessment

The hazard identification process should result in a comprehensive list of all potential major incidents and hazards (including underlying causes), together with the risk control measures and the linkages between hazards, controls and incidents. It should provide a description of the nature of the hazard and of each potential incident. However, a more detailed analysis of the controls is usually required for the Safety Assessment. Figure 2.3 shows the type and flow of information through the hazard identification process and into the Safety Assessment.

Figure 2.3 – Type and flow of information into the Safety Assessment



If a workshop is used for Safety Assessment, it is worthwhile to provide the information (in particular the results from the hazard identification) in a way that aids understanding amongst the workshop participants. Some methods of achieving this are:

- linking risk control measures to those hazards and causes to which they apply. If not already done during the hazard identification then it should be done prior to the Safety Assessment
- ensure that sufficient information on the risk control measures identified in the hazard identification is available to achieve a proper understanding of the level of risk reduction that each control provides
- grouping some site-wide hazards, such as utility failure, natural disaster, for reviewing only once rather than several times across several major incidents. This may be beneficial for some hazards (such as sabotage) that may be difficult to assess in terms of likelihood. The operator should ensure that the consequence assessment still considers the potential concerns present from site-wide hazards in each area to determine worst-case events.

Example

ABC Chemical Company identified that the following information will be necessary for its ammonia storage vessel and unloading facility:

- hazard identification records
- equipment design data
- vessel inspection records for the storage vessel
- test records for pressure relief valves and instrumentation
- the tanker unloading procedure as this is likely to be a key influence on risk
- incident history on-site (frequency and consequence)
- incident history for industry (frequency and consequence)
- relevant Material Safety Data Sheets (MSDS)
- exposure levels eg Immediately Dangerous to Life and Health (IDLH), Short Term Exposure Limit, Emergency Response Planning Guidelines.
- any consequence information available eg modelling.

2.3. Workforce requirements

Safety Assessment requires a large commitment from site personnel because ownership of the process is the shared through of the whole organisation from management to shop floor and also due to the amount of work required to demonstrate risk has been reduced so far as is reasonably practicable.

Safety Assessment is generally a team-based process requiring the assembly of an appropriate team. It is recommended that the operator involve representatives from management, supervisors, operators, maintenance and relevant technical personnel. The operator may also need to employ a third party to provide guidance on the way forward (ie a workshop facilitator) or technical expertise in a specific area.

The operator should also develop a role for all workers in the Safety Assessment process that allows them to contribute and gain an understanding of the hazards and controls present at the facility. Widespread awareness of these issues is essential for safe operation of the facility and is also an essential part of the consultation requirements.

The following points provide some guidance for the knowledge and skills required in the Safety Assessment process, to assist in the selection of the Safety Assessment team:

- include all relevant work groups. Each work group will tend to bring a different experience base and perspective to the process
- include representatives from both operations and maintenance who have a thorough and detailed knowledge of the facility and its history
- include a mix of operations, management and engineering disciplines. Hazards not evident to individual work groups may be identified due to the interaction between the various disciplines
- involve contractors and suppliers as necessary eg truck drivers provide a different perspective on loading/unloading operations.

Selection of personnel should take into account their ability to provide quality input in the following areas:

- determination of consequence, likelihood and risk
- assessment of the effectiveness of controls
- knowledge of historical incidents.

Like any workshop process, it is not possible to involve everyone in the Safety Assessment workshops. Therefore, it is important that feedback is provided to other workers. This feedback should take the form of communicating the hazards that are present, the risks associated with those hazards, the controls in place and any recommendations arising. Workers should also be provided with an opportunity to review and comment on the Safety Assessment output. This is both an important quality control activity and the mandatory consultation involvement. It also fosters a feeling of ownership among personnel not directly involved in the Safety Assessment process.

An example of typical resource requirements for the Safety Assessment process is provided in Table 2.2. It shows the estimated site commitment for a medium-sized site which identified 20 major incident scenarios with most information gathered using a workshop format.

Table 2.2 – Site commitment for Safety Assessment

Process	Personnel	Time commitment	Notes
Planning and preparation	Safety Case coordinator HSR.	Two weeks Two days	This would be carried out at the same time as planning for other steps in the Safety Case.
Risk assessment workshops	Workshop participants (6–8 people) Facilitator and scribe.	Three days (simple matrix) 10 days (LOPA) QRA (site specific)	This estimate is based on full day workshops. An alternative is to have part day workshops over a longer period of time. More time may be required depending on the complexity of the hazard scenarios. A QRA (the most quantitative method) has little workforce involvement. If done by others, there may only be one site representative required as a contact person to provide information.
Risk control measures			Review adequacy (see the guidance note – *Control measures* for details).
Detailed studies	Safety Case coordinator Study specific resources.	Weeks – months	Personnel and time commitments depend on the type of study, age of plant, availability of information etc. These studies need to be identified early to ensure that they can be completed in time. Some studies, such as additional asset integrity assessment (eg vessel inspections), if required, may require a facility shutdown. These need to be planned.
SFARP workshop	Workshop participants (6–8 people) Facilitator and scribe.	2–5 days	This workshop is to select improvements to be implemented. The goal is to demonstrate that risks have been reduced SFARP. The timeframe for this workshop depends on the age of the plant, the level of risk, the number of improvement opportunities etc. This estimate is based on full day workshops. An alternative is to have part day workshops over a longer period of time. This timeframe also depends on the initial risk assessment method used.

2.4. Health and safety representatives

The operator should develop a role for all workers in the Safety Case process that allows them to contribute and gain knowledge in relation to identification and selection of risk control measures, assessment of their adequacy, selection of ongoing management criteria and identification of improvement actions. Decision-making should be transparent and based on the same principles.

Health and safety representatives (HSR) should be involved in the process to the extent that they can ensure appropriate workforce involvement. WorkSafe recommends that the HSR is involved in:

- development of the Safety Assessment process
- selection of personnel and scheduling
- some workshops (particularly those where decision-making processes are involved)
- reviewing the workshop results
- process for implementing any recommendations arising from the workshop.

As elected representatives of workgroups, HSR are ideally placed to comment on issues such as personnel for workshops and the means for feeding back results.

2.5. Preparing an implementation plan

The operator needs to prepare a detailed implementation plan and relevant methodology documents. The methodology documents should detail not only the approach to the Safety Assessment but also the expectations of it.

Defining Safety Assessment methodology is critical to success. A lack of clear direction can waste time and resources, causing the team to examine issues of relatively minor concern. Once the operator has established the scope, selected personnel and gathered relevant information, the team leader can schedule any Safety Assessment workshops.

These workshops should be conducted as soon as possible. This allows enough time to complete the Safety Case. The operator must allow sufficient time to complete the detailed assessment of controls and any other more detailed studies that may be required as a result of the Safety Assessment.

Factors that should be considered in scheduling the Safety Assessment include the availability of key personnel and the needs to maintain production and maintain mental alertness.

Safety Assessment workshops should not normally exceed four to six hours per day. This reduces the likelihood of fatigue and associated loss of concentration that can affect the quality of the assessment. This may not always be possible, due to considerations such as the most efficient use of resources and inconvenience to personnel. If full day workshops are to be used then the workshop participants should be provided with frequent breaks.

Operators have found it useful to have time outside workshops to gather information or to have personnel working in the background. This provides the opportunity to:

- gather information for the next workshop
- search for information needed to clarify uncertainty in the previous workshop
- allow information to be obtained for control measure assessment
- do some alignment of controls (ie recognise where the same controls are applicable to similar hazards across the site).

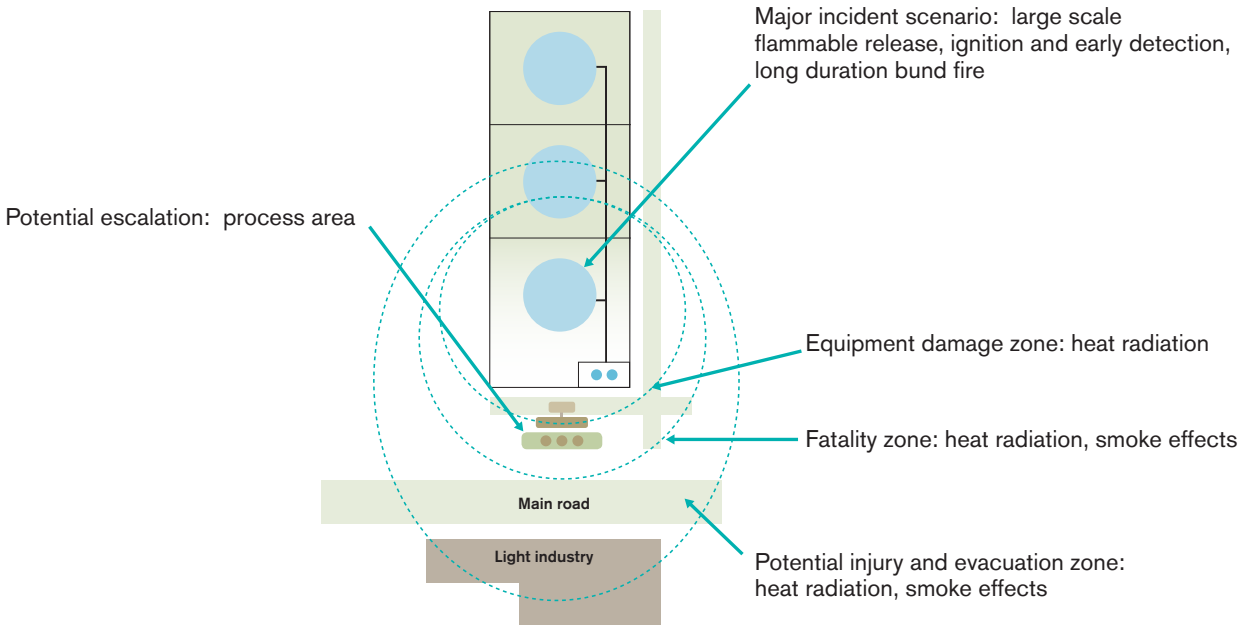
3. The safety assessment process

3.1. Consequence analysis

The Safety Assessment needs to assess the consequences of each major incident in terms of the magnitude as well as the severity of the incident. The magnitude of the incident is the size or scale of the effect zone created by the incident, within which a number of injuries or fatalities or extent of property damage could arise. The severity of the consequences is the actual level of injury incurred (including fatal or non-fatal injury) or damage caused. This depends on whether or not people are present, if there is active/passive fire protection etc.

To illustrate these aspects a fire incident is presented in Figure 3.1. Three consequence zones (the magnitude) are provided for three different levels of severity (equipment damage, fatality, injury).

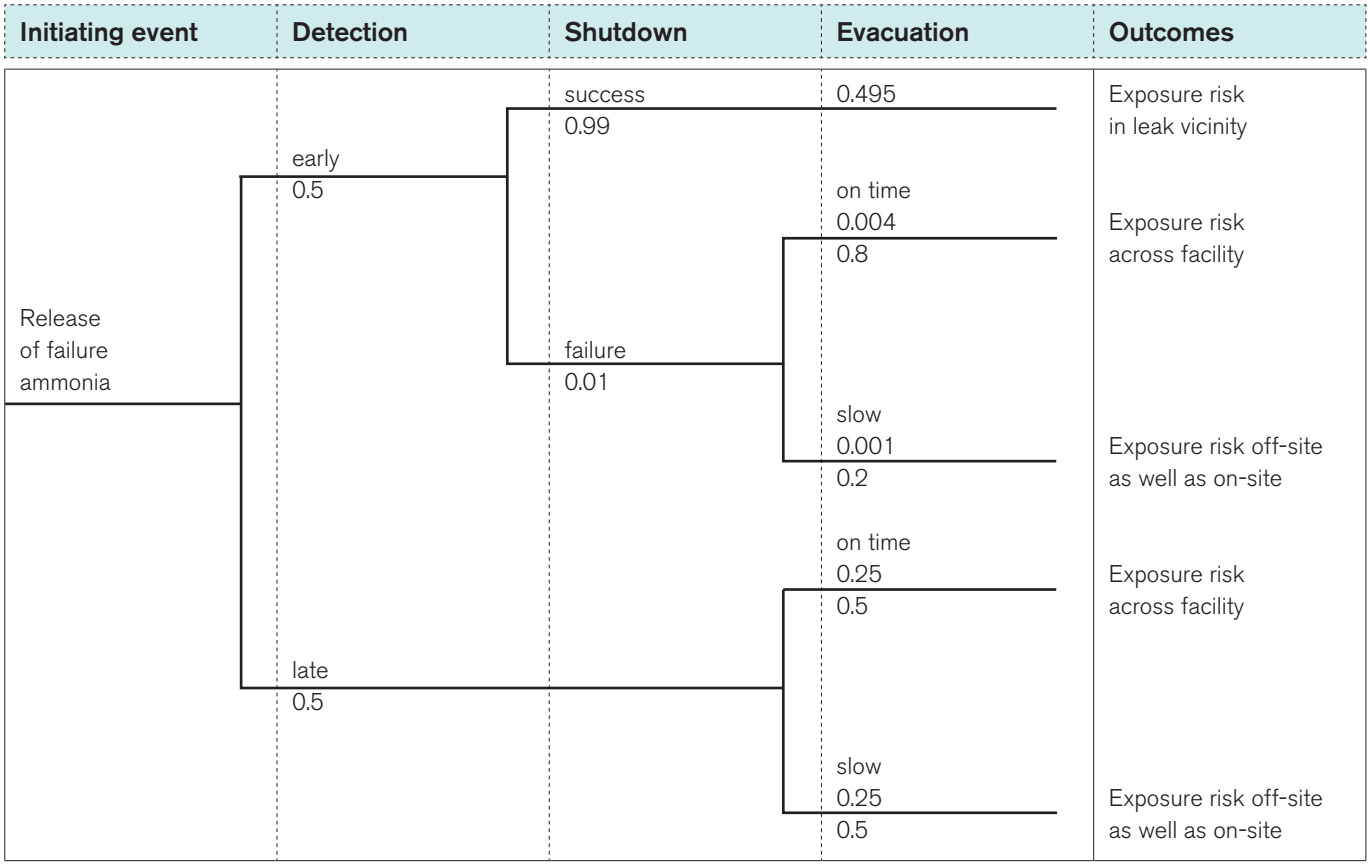
Figure 3.1 – Consequence zones



The main aim of this stage of the Safety Assessment is to understand the types of hazardous events that could occur based on the properties of the material released. The consequence assessment should provide an indication of the potential rate and duration of any release of hazardous material, the conditions and amount of material released, nature of associated hazards etc.

The operator also needs to consider the full range of possible consequence outcomes. Figure 3.2 demonstrates the range of potential outcomes for an ammonia release in the form of an event tree.

Figure 3.2 – Consequence outcomes – event tree



Assessment of the possible outcomes needs to include consideration of what may go wrong if measures to eliminate or prevent incidents are not present, are wrongly implemented or fail to function. The Safety Assessment must consider worst case outcomes as well as the most likely scenarios as this may affect the adequacy of risk control measures which are in place eg while most consequence outcomes affect the site itself, there may be worst case scenarios that affect off-site populations such as office blocks, schools or nursing homes. Consideration of worst case scenarios is particularly important when assessing the adequacy of the emergency response arrangements.

In determining the worst case events, the operator needs to consider the potential for one event to potentially trigger another larger event ie escalation. Escalation encompasses such scenarios as:

- a small jet fire impinging on an LPG vessel causing a BLEVE
- ignition of a drum fallen from a pallet in a flammable liquid store. While a minor incident, the fire may cause other drums to overheat and fail, leading to a large number of drums (and even a whole warehouse) being involved.

Usually a major incident scenario (eg loss of containment) may be characterised by a small number of representative outcomes. For complex situations it may be appropriate for an event tree analysis (such as Figure 3.2) to show the range of potential effects and the key factors influencing the outcome.

Whatever consequence analysis is conducted must be done to a level both sufficient for the estimation of risk and which is meaningful to the organisation.

Example

Ammonia is a pungent and suffocating gas which is corrosive to the eyes, skin and respiratory tract. The IDLH concentration for ammonia is 300 ppm, which is the highest concentration a healthy worker could receive in a 30 minute period and still escape with no permanent health effects (NIOSH, 2006). Exposure to relatively high concentrations could be fatal.

Ammonia is flammable but has a flammability limit of 16 vol % in air and an explosion or fire is unlikely in the absence of a high energy ignition source. The upper flammability level is 26 vol % (CHRIS, 2006 and Lewis, 2000). Therefore, it is a more serious toxic hazard than a flammability hazard.

Based on this information, and the fact that more hazardous flammable materials exist at this site, only toxic release scenarios from the ammonia storage system need to be assessed in detail. However, a nearby LPG storage tank could potentially impact the ammonia tank (escalation) and result in a catastrophic failure. This scenario is therefore included in the assessment.

Sensitive population areas were defined as an office block on the site, residential properties north of the facility and a hospital that could potentially be impacted by a low frequency, high consequence event. Sufficient modelling will be conducted to define the level of concern with respect to these populations.

3.1.1. Consequence estimation

Consequence analysis assesses the severity or impact of a potential hazard. Qualitative estimates of consequence tend to be based on incident history and workforce experience and estimation. For qualitative risk evaluation this requires selecting a consequence category eg on a risk matrix such as 'lost time injury', 'single fatality' or 'multiple fatalities'.

Quantitative estimates of consequence are done by consequence modelling. More detailed analysis of consequences can be achieved with complex computerised modelling techniques. Successful application requires the models to be used by personnel with adequate training and experience. Some examples of consequences that can be modelled include:

- pool fires
- jet fires
- confined and partially confined explosions
- flash fires
- toxic releases and their effects
- gas dispersion (flammable or toxic)
- BLEVE.

The results of consequence modelling typically show the area of impact of an event and the severity in terms of likelihood of fatality or injury within the impact area. The results can be used in conjunction with qualitative or semi-quantitative risk analysis to justify the consequence categories selected. In a QRA, consequence modelling is used in conjunction with event tree analysis to determine the risk of fatality or injury.

3.2. Likelihood analysis

Risk analysis also requires an estimate of the likelihood of the scenario occurring. For qualitative risk analysis this may simply require the selection of a category on the risk matrix. This selection is based on the experience and judgement of those conducting the assessment but can be justified if necessary with historical incident data.

In more complex quantitative assessment, the estimated frequency of a scenario occurring may be determined by using historical incident or failure databases. Event tree analysis is often used to determine the likely probability of escalating events, such as fires or explosions, following a major incident.

3.2.1. Likelihood estimation

To ensure consistency across the risk analysis, WorkSafe recommends standard guidance material is developed used for likelihood estimation. It is also suggested that risk matrix likelihood categories are assigned to quantitative frequencies (eg at least once per year, 1 in 10 years, 1 in 100 years) so they can be correlated with incident history and failure databases. It can be difficult, and unreliable, for persons to estimate very low frequency events. Options to help a site estimate the likelihood of occurrence for extremely low frequency events include:

- stating the frequencies in terms of experience on-site, within the company, within the industry, in all industries etc (see the Appendices).
- referring to industry guidance material or failure frequency databases
- use of fault trees to analyse the combination of

contributing factors that may lead to a potential major incident. Fault trees are described in more detail in the Appendices.

The operator should always record the basis, including relevant references, for determining likelihood, including all the assumptions that have been made. This helps ensure a robust analysis and will be beneficial for future reviews. The operator should also be careful that it is determining likelihood on the basis of the hazard and not based on the reliability of the controls that are in place. The likelihood may then be low due to an assumption that the control is very reliable when in fact it may not always be.

3.3. Screening of hazards

Screening of hazards during the hazard identification phase is not desirable (see the guidance note – *Hazard identification*) as there is a need to transparently demonstrate that all potential hazards resulting in a major incident are identified. However, it is possible to screen out hazards based on their consequences, such as those with minor consequences and no potential to escalate to a major incident.

During Safety Assessment the operator may also screen out those hazards that do not have the potential to result in a major incident. It may be tempting to do this using a crude qualitative risk assessment and screening out the hazards based on risk. This is undesirable as it is likely that assumptions will be made about the effectiveness and reliability of risk control measures without any actual assessment of those controls. The risk may be considered to be low due to the perceived effectiveness of the risk control measures while a considered assessment of the risk control measures may show them to be inadequate. The same applies for a screening based on likelihood, as many of the incidents will have a very low likelihood. Any screening of hazards should therefore only be on the basis of consequence and not risk or likelihood.

It should be noted that some consequence assessment may be conducted prior to or at the same time as the hazard identification process (see guidance note – *Hazard identification*). This may allow some early screening to occur (eg based on the consequences of a pipeline leak, where a small hole may not lead to a major incident but a large hole or rupture could).

All other hazards require some analysis of the risk control measures. This does not mean that they all need to be assessed to the same level of detail. The extent of analysis should be proportional to the consequence, the level of inherent risk and the reliance placed on risk control measures to be effective. This can provide an opportunity for a further screening process.

The operator should only screen out hazards using clear and justifiable guidelines. The screening of hazards should be a transparent process that is repeatable by others when using the same criteria.

Example

ABC Chemical Company's criteria for screening out incidents involving ammonia is that it only regards an incident as a major incident if:

- the IDLH impact zone exceeds a distance of 'x' metres
- the release of ammonia exceeds 50 kg.

The operator may need to support the chosen criteria using consequence modelling results. As a minimum, the operator should describe the reasons for selecting the criteria.

3.4. Control measure assessment

Throughout the Safety Assessment process the operator will be recording existing and/or potential new risk control measures when determining causes, likelihood, consequence etc. It is essential to be explicit about what risk control measures are being included and how they are considered to influence risk levels. The operator also needs to be aware of the potential for risk control measures to experience common mode failures.

Risk control measures are the means of reducing the risk associated with major incidents. They eliminate, prevent, reduce or mitigate the hazards and/or consequences. The hazard identification process assists the operator in the identification of risk control measures. Risk control measures may also be identified during the risk estimation and assessment processes. The Safety Assessment process should provide the operator with the following in relation to risk control measures:

- identification or clarification of existing and potential control measure options
- evaluation of control measure influence on risk levels
- basis for selection or rejection of risk control measures and the associated demonstration of adequacy
- basis for defining performance indicators for selected risk control measures.

Through the Safety Assessment process the operator should gain an understanding of which controls have the most influence on reducing risk. These need to be assessed in greater detail.

When conducting the Safety Assessment, the operator needs to consider each control measure eg how reliable is it or how effective might it be in a particular situation (ie during an incident)? This is intended as general

guidance only; detailed guidance is provided in the guidance note – *Control measures,* on assessing viability and effectiveness.

An operator would assess the risk for the facility as it exists currently, usually referred to as the base case. The risk for the facility can then be assessed for proposed additional risk control measures, either singly or as a group. Each of the alternative options needs to be clearly identified.

If the site has a large numbers of controls, a complete and in depth assessment of every control would be prohibitive. It is important that operators focus on the areas of greatest benefit. It may help to identify 'critical' controls and concentrate attention on those; however this is not required by the MHF regulations and WorkSafe makes no distinction between critical controls and other controls.

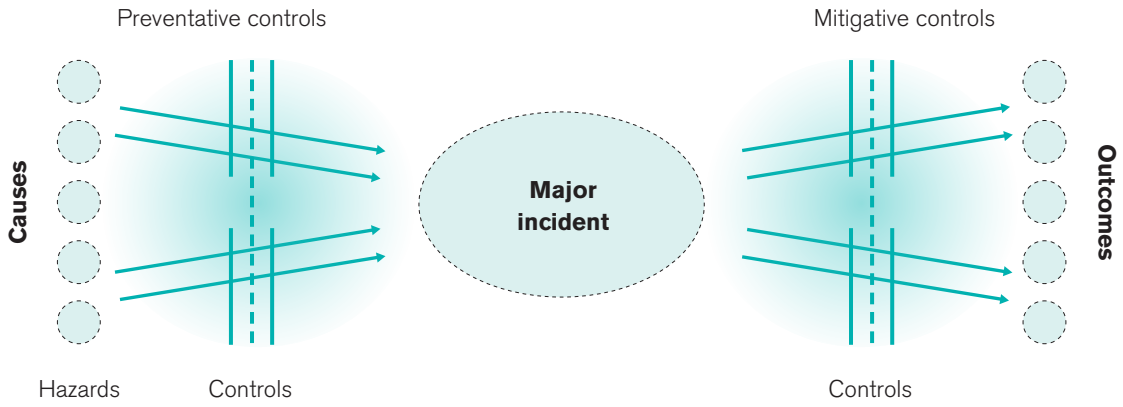
3.4.1. Bow tie diagram

An aid commonly used in MHF Safety Assessments is the 'bow tie' diagram (see Figure 3.3). It allows a range of prevention layers to be examined which may eliminate or minimise the likelihood of specific cases that may reduce the consequence of an event after a loss of control has occurred. The bow tie is an output of a (LOPA) as described in the Appendices but can be derived by other means.

The bow tie model:

- examines potential major incidents by describing the hazards and causes that may lead to an 'event' (loss of control that has the potential to result in a significant impact) and then describes a number of potential outcomes, or consequences that may result.
- provides an effective method of communicating the hazards that could lead to major incidents and the linkages to risk control measures. It also facilitates focussed monitoring and auditing of controls.
- allows a range of prevention layers to be examined, which may eliminate or minimise the likelihood of specific causes that may lead to an event. It also highlights mitigation layers that may reduce the consequence of an event, after a loss of control has occurred.

Figure 3.3 – Bow tie diagram



3.4.2. Performance indicators

The Safety Assessment should also generate information useful to the setting of performance indicators for risk control measures (refer to guidance note – *Control measures* for further details). Typical considerations that might come from the Safety Assessment are:

- risk control measures associated with high risk hazards may require rigorous performance standards
- control measure functionality should reflect the scale of incidents being controlled
- the required reliability or number of risk control measures should reflect the likelihood of the corresponding incidents.

For some types of risk control measures, the assessment may lead directly to performance requirements, eg performance indicators and standards for instrument control systems such as a high pressure trip or a gas detector may be determined directly. The performance indicators and standards generated from the Safety Assessment could include a probability of failure on demand (PFD) of less than 0.05 or a Safety Integrity Level (SIL) of greater than or equal to 2.

3.5. Risk assessment

3.5.1. Determining and interpreting the risk results

After the operator has analysed the consequences and likelihood of a potential major incident, the risk must be determined. This information must then be evaluated to determine the acceptability of the risk and whether further improvements should be considered. This requires the operator to provide a comprehensive risk profile for the facility.

The operator needs to determine both the **highest risk incidents** and the **overall profile of risks** from all of these incidents to understand the most important overall contributors to the risk profile, and to determine whether overall risks are adequately controlled.

Risks and hazard must be analysed and evaluated both individually and cumulatively. If there are a large number of different hazards and potential incidents at the facility, the total risk may be significant even if the risk arising from each individual hazard is low.

Without considering the hazards or risks cumulatively, the most significant incidents cannot be determined. Furthermore, some risk control measures may often only be recognised as critical or justified because of their cumulative impacts on several hazards.

For any incident there may be several independent hazards or combinations of hazards, each of which could lead to that incident, as well as several risk control measures which may be particularly critical because they may impact on one or more of those hazards. The Safety Assessment should give an understanding of the **total likelihood of each incident and the relative importance of each separate hazard and control measure**. Determining performance standards for the risk control measures can assist in demonstrating their importance (see section 3.4.2).

3.5.2. Managing risk uncertainty

The operator must clearly understand and describe the uncertainty present in the assessment. Uncertainty cannot be eliminated, and it will be necessary to make assumptions in some areas. The presence of uncertainty can be due to any of the following reasons (refer to Wells, 1997):

- invalid assumptions
- incomplete hazard or consequence identification and analysis
- inappropriate or inadequate models or methods used eg model not within its validity range
- incomplete, inadequate or irrelevant data.

It should be noted that reasons for uncertainty are different to reasons for error. Some examples of error are:

- out of date documentation (eg drawings)
- poor knowledge of changes in equipment or operations
- limited understanding of the effectiveness, performance or identity of control measures
- lack of awareness of hazards and associated control measures
- lack of information on the underlying reasons for specific procedures or process steps.

The key to understanding uncertainty and potential for error and managing these, in the context of the safety case, is to:

- record any assumptions made and the basis for the assumption
- explicitly recognise where the main gaps or uncertainties exist
- seek to reduce the level of uncertainty so far as is reasonably practicable by testing assumptions, conducting more detailed studies as required etc.

Where the level of uncertainty is high, the operator should consider using sensitivity analysis to test the robustness of the Safety Assessment results against variations within the key areas of uncertainty.

Example

ABC Chemical Company personnel have difficulty assessing the likelihood of operator error during the ammonia unloading operation and cannot come to an agreement.

As a result two actions are taken to minimise this uncertainty:

(a) The preparation of a task analysis and application of human error reliability data to arrive at a more structured risk value.

(b) An analysis of industry incidents to assess whether their risk value is in the ball park of industry data.

3.6. Demonstrating risks are reduced

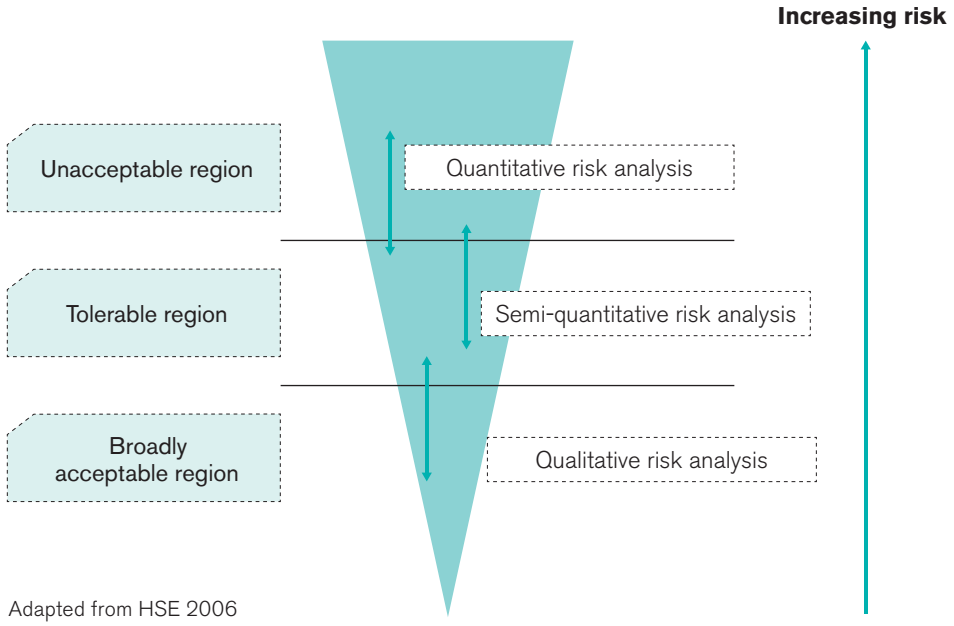
The goal of the Safety Case is to improve the safety of a facility and to demonstrate that risks have been reduced so far as is reasonably practicable. This means that the operator has taken steps to identify additional or alternative controls and has taken all reasonable steps to reduce the risk so far as is reasonably practicable. Further information on reasonably practicable as applied to major incident risk is in the guidance note – *Requirements for demonstration*.

3.6.1. Use of risk criteria

Risk criteria can provide a basis for judging the tolerability of risks that have been analysed, and for deciding the urgency or priority with which any identified hazard or risk should be addressed. Risk criteria can be applied for assessing the overall risk tolerability (eg as in a QRA) or used for assessing the adequacy of controls for a specific hazard scenario eg using a LOPA approach.

However, risk analysis is subject to uncertainty and therefore rigid criteria may be inappropriate. A common approach for overall risk criteria is to define three broad risk levels rather than fixed and rigid criteria, as illustrated in Figure 3.4 which has a different approach to risk reduction applied to each region.

Figure 3.4 – Risk triangle with types of risk analysis



Adapted from HSE 2006

In the 'unacceptable region' of Figure 3.4, the risk cannot be justified and risk reduction measures must be adopted. The middle region, between the 'unacceptable' and 'broadly acceptable' regions, is typically broad (eg several orders of magnitude). This middle region is 'tolerable', when appropriate risk control measures are in place and so far as is reasonably practicable has been achieved, with regular review necessary to assess whether additional controls are needed. Further risk reduction is not required if the cost is disproportionate to the improvement gained or is clearly not possible for other reasons. Many incidents are likely to fall into the middle band and therefore risk criteria on their own are likely to be insufficient to demonstrate the adequacy of controls. Operators should note that satisfying or achieving specific criteria may not necessarily demonstrate that risk has been reduced so far as is reasonably practicable. The risk associated with the broadly acceptable region is generally considered as insignificant or adequately controlled. However, even if a potential incident falls into the broadly acceptable region, some additional controls may still be justifiable to demonstrate risks have been reduced so far as is reasonably practicable, and the MHF regulations also require that this be considered.

A more detailed discussion on risk criteria is contained in the guidance note – *Requirements for demonstration*. If risk criteria are used as part of demonstrating adequacy, the operator will need to justify the selection of the risk criteria and show a clear linkage between the criteria and the demonstration that controls are adequate.

3.6.2. Risk reduction

While risk criteria may be used as part of the demonstration that risks have been reduced so far as is reasonably practicable, the criteria alone are not enough. To demonstrate that risks have been reduced so far as is reasonably practicable, the operator needs to demonstrate that it has taken all reasonable steps to reduce risk have been taken.

A reduction in risk can be achieved by:

- eliminating the causes of the incident
- reducing the likelihood of the incident or
- reducing the severity of the consequences.

The need for additional, or alternative, risk control measures may be indicated where:

- the risk assessment has shown the risks to be unacceptable
- it is necessary to demonstrate that risks have been reduced so far as is reasonably practicable
- there is evidence that an existing control is not performing as well as required
- a deficiency has been identified in the existing control regime eg an identified hazard with no identified control measure
- change is proposed for the facility
- the operator becomes aware of improved technology for managing pre-existing hazards.

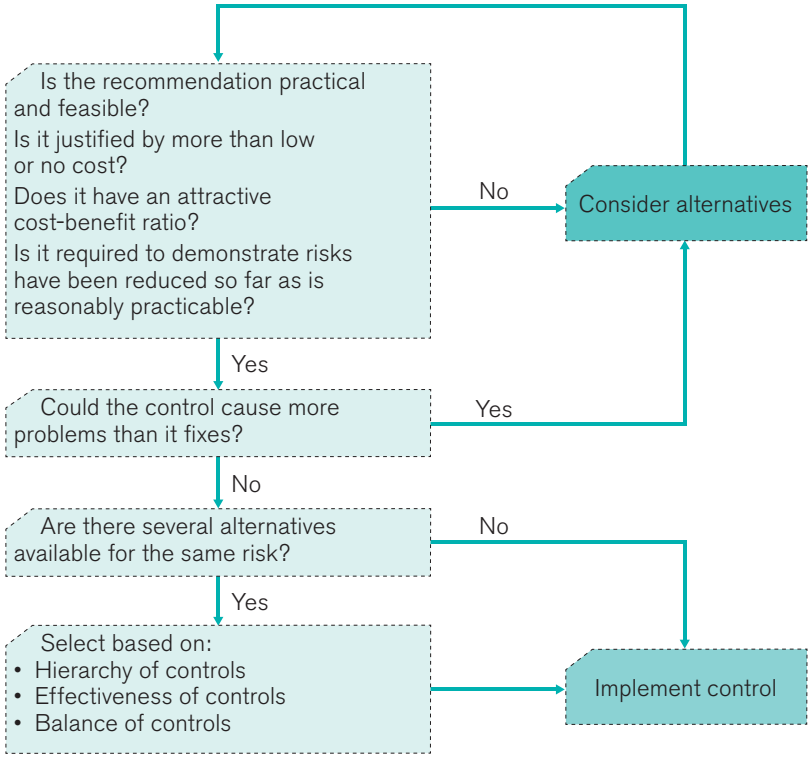
The Safety Assessment should ensure that alternatives are considered for all these situations. By evaluating options for risk control measures within the Safety Assessment, the operator should be able to determine what additional benefit (if any) is gained from introducing additional or alternative risk control measures.

The Safety Assessment should consider a range of risk control measures, and provide a basis for the selection or rejection of risk control measures as appropriate to the nature of the facility and its hazards (refer to Figure 3.5). It is important that the operator explains the reason for selecting or rejecting alternatives for the benefit of corporate knowledge. This is particularly important for the rejection of controls.

The reasons for rejection or selection should be derived from the findings of the Safety Assessment, in particular findings regarding effectiveness and viability. These reasons have a direct bearing on the ability to demonstrate the adequacy of risk control measures.

If a facility is an existing one, there will often be little knowledge of what alternatives have been considered in the past and the reasons for selection or rejection of controls. For an existing plant it is not very practicable to replace controls with other controls unless there are clear benefits but new or additional controls can be discussed on their own merits. Therefore, for new or alternative controls, it is important to provide the reasons for their selection or rejection.

Figure 3.5 – Control measure selection



Example

During the control measure assessment (refer to the guidance note – *Control measures*) ABC Chemical Company identified that an additional control measure (high level trip) should be considered to protect against overfilling the storage vessel.

The risk of overfilling was considered high during the risk assessment. This additional control was selected on the basis that:

- it was considered essential to provide protection given that manual control is insufficient
- the control had a significant risk reduction potential
- the proposed solution is known and of reliable technology
- it is higher on the hierarchy of controls than alternative controls.

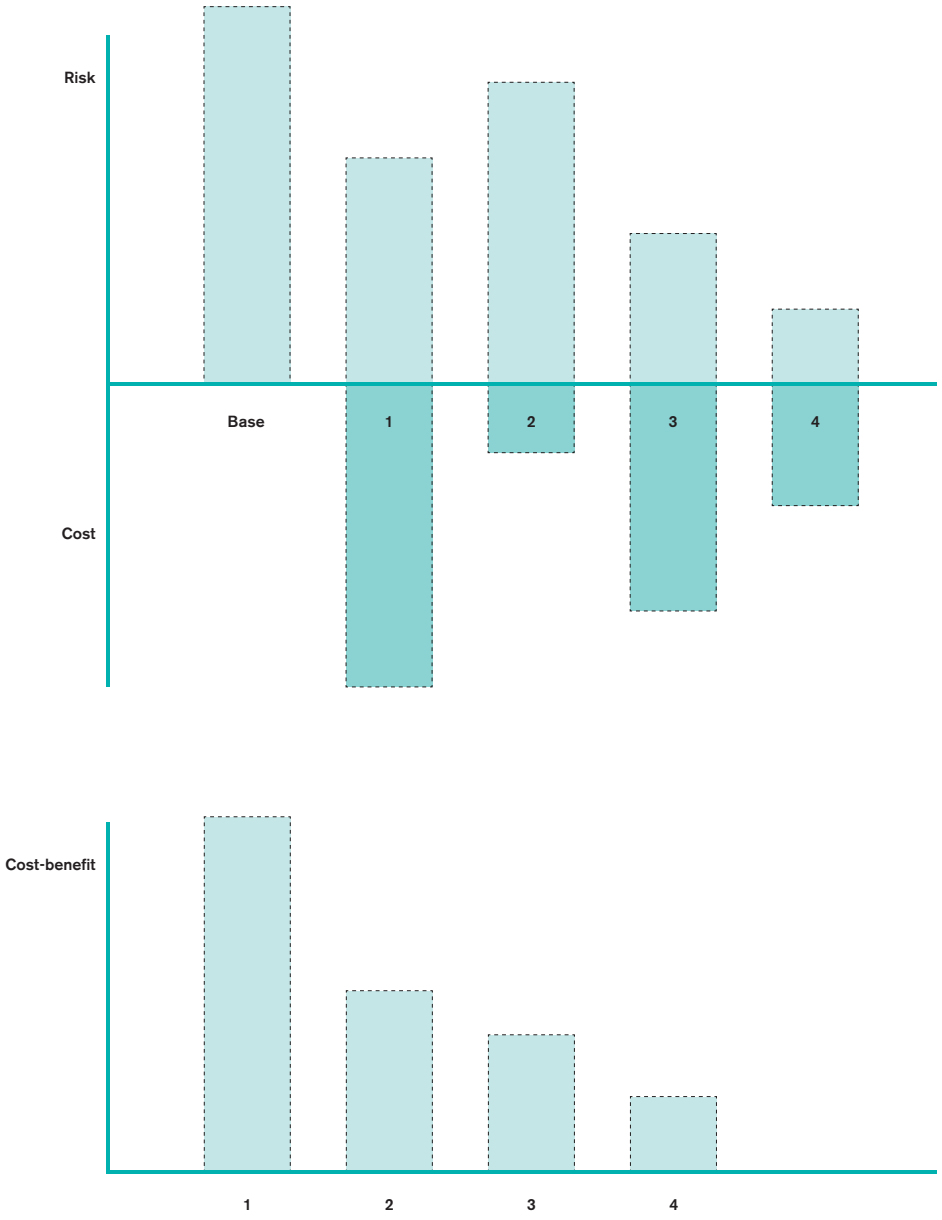
An alternative control was a proposal to use a smaller tanker and have the supervisor check that sufficient volume was available in the vessel before unloading. This was rejected on the basis that:

- it is lower on the hierarchy of controls (refer to the guidance note – *Control measures*) than the high level trip
- it was likely to be ineffective and possibly subject to human error
- even though lower cost, the cost-benefit ratio was higher.

There will be a limit on the resources for implementing additional controls and some prioritisation will be necessary. Operators must provide a justifiable basis for any prioritisation.

One method of doing this is to prioritise on the basis of cost-benefit. Priority should be given to those controls with the lowest cost-benefit ratio. The operator should avoid applying this methodology too rigidly as other factors may also be relevant in making this decision. This approach is illustrated in Figure 3.6.

Figure 3.6 – Cost-benefit ratio for alternative controls



Option

1 High cost and low risk reduction
2 Low cost and low risk reduction
3 Moderate cost and moderate risk reduction
4 Low cost and large risk reduction

Ranking

4 Implement
3 Consider further
2 Defer
1 Reject

4. Outputs

4.1. Safety Assessment outputs

At the end of the Safety Assessment the operator will have the following information for incorporating into the Safety Case:

- an understanding of the factors that influence risk and the controls that are critical to controlling risk
- the likelihood of potential major incidents
- the magnitude and severity of the consequences arising from major incidents for the range of possible outcomes
- clear linkages between hazards, the major incidents, risk control measures and the associated consequences and risk
- a prioritised list of actions to further reduce risks so far as is reasonably practicable.

The operator should also consider providing some examples of the Safety Assessment process for a specific major incident, and perhaps specific hazard, to help WorkSafe understand the process taken and any linkages that are present. This will also help any others who want to understand the Safety Assessment process for the facility.

4.2. Uses of Safety Assessment outputs

The ongoing management and use of the information developed during hazard identification and Safety Assessment is of fundamental importance to ongoing safe operation. The operator can use the outputs of the Safety Assessment in the following ways:

- to ensure that all workers understand the hazards and risks associated with the facility, the risk control measures in place to manage these risks, and their role in the prevention of major incidents
- to demonstrate risks are reduced so far as is reasonably practicable (refer to the guidance note – *Requirements for demonstration*)
- to assist in the development of the emergency response plans (refer to the guidance note – *Emergency planning*)
- to enable priorities and resource allocations to be based on appropriate information and assessment, resulting in a cost-effective improvement of safety
- to assist in the improvement of procedures and management systems
- as an input to 'training needs' analyses
- to assist with other processes such as management of change and incident investigation.

5. Review and revision

It is important that the operator keeps the Safety Assessment and the knowledge contained within it up-to-date. The Safety Assessment should be reviewed as changes occur. The operator also has an ongoing responsibility to understand and control the risks so far as is reasonably practicable at the facility, which includes any new risks that arise as a result of changes. This involves learning from plant experience, including improved standards, where community expectations have changed or new technology has become available, and looking for new ways to reduce the risk profile. The example below shows some of the triggers for Safety Assessment review. There are also additional review and revise requirements associated with MHF licence renewal and Safety Case update (refer to the guidance note – *Renewal of an MHF Licence*).

Example

Changes which could trigger a review of the Safety Assessment include:

- changes in the workforce which could lead to changes in working practices or in knowledge of the facility
- physical modification to facility or changes to operations eg hardware, software or process changes or new chemicals as these could introduce new hazards and thus change risk
- where new hazards are identified or periodically as part of the Safety Case review
- further information is now available which could help refine the risk assessment eg areas of previous uncertainty
- industry developments have occurred relating to technology or systems of work that may be applied to reduce risk
- incident or near miss investigations identify further hazards or indicate the risk may be higher than previously thought. Reports of incidents or near misses at other facilities should also be reviewed.

6. Quality assurance

The following table outlines the key activities and checks that should be undertaken to ensure quality in the Safety Assessment process.

Table 6.1 – Key activities and checks for quality assurance

Activity	Check
Validate hazards/major incidents	Check incident and near miss history on-site.
	Check industry incident history.
Validate likelihood and risk control measures	Verify that risk control measures are as reliable as thought. Inspection records for protective equipment should be reviewed.
	Ask personnel not present at the meeting to verify that assumptions make sense.
	Verify protective system reliability versus industry data and maintenance records.
	Verify that procedural controls exist and contain guidance to avoid the specific hazard/cause in question.
Validate consequence	If not already done, verify consequences by conducting consequence modelling.
	Conduct consequence modelling using modelling software for significant scenarios or a representative set of scenarios.
	Have impact criteria been linked back to authoritative sources?
Risk analysis	Sort the various major incidents in order of risk. Does the order look correct? If not, then consider why.
	Ask personnel to provide an indication of which hazards they perceive to be most likely to cause each incident. Compare this with the risk results.
	Have an independent person not involved in the Safety Assessment read the output from the risk assessment. The person should review the risk assessment including the assumptions and ask: • Do I agree with the basis for the risk evaluation? • Does each assumption and its basis make sense? If assumptions do not make sense to the person, it may be difficult for WorkSafe or others to understand.

7. Compliance checklist

The following checklist contains information on the MHF regulations as they relate to Safety Assessment.

Table 7.1 – MHF regulations relating to Safety Assessment

Section	Requirement
Reg 5.2.7(1)	The operator of an MHF must conduct a comprehensive and systematic Safety Assessment, in accordance with this regulation, in relation to all potential major incidents and all major incident hazards.
Reg 5.2.7(2)	A Safety Assessment must involve an investigation and analysis of the major incident hazards and major incidents so as to provide the operator with a detailed understanding of all aspects of risk to health and safety associated with major incidents, including: (a) the nature of each major incident hazard and major incident (b) the likelihood of each major incident hazard causing a major incident (c) in the event of a major incident occurring, (i) its magnitude and (ii) the severity of consequences to persons both on-site and off-site (d) the range of risk control measures considered.
Reg 5.2.7(3)	In conducting a Safety Assessment, the operator must: (a) consider major incident hazards and major incidents cumulatively as well as individually, and (b) use assessment methods (whether quantitative or qualitative, or both) that are appropriate to the major incident hazards being considered.
Reg 5.2.7(4)	The operator must document all aspects of the Safety Assessment, and the documentation must: (a) describe the methods used in the investigation and analysis (b) state all the matters specified in subregulations (2) (a) to (2) (d) (c) contain reasons for decisions as to the matters specified in subregulations (2) (b) and (2) (c) (d) contain, in relation to the range of risk control measures considered, (i) statements as to their viability and effectiveness, and (ii) reasons for selecting certain risk control measures and rejecting others (e) be kept available for inspection on request under the OHS Act.
Reg 5.2.12(1)	The operator of a major hazard facility who has ….(b) conducted a Safety Assessment under regulation 5.2.7 … must review, and if necessary, revise those matters to ensure that the risk control measures adopted are such that the operator continues to comply with regulation 5.2.8.
Reg 5.2.12(2)	A review and revision under this regulation must be conducted: (a) at the direction of the Authority, or (b) before a modification is made to the major hazard facility, or (c) after a major incident occurs at the major hazard facility, or (d) when an effectiveness test indicates a deficiency in a risk control measure, or (e) if there has been any change to the circumstances that formed part of the initial Property Protection Assessment under regulation 5.2.36, or (f) if a health and safety representative requests the operator to conduct a review and in any event at least once every five years.

Section	Requirement
Reg 5.2.13	(1) The operator of a major hazard facility must develop a role for the operator's employees, including the specific procedures they are required to follow to assist the operator to … (b) conduct or review a Safety Assessment under regulations 5.2.7 and 5.2.12 … (2) The operator must review the role for employees developed under this regulation if there is a change of circumstances, including a modification to a major hazard facility that would require additional or different knowledge and skills on the part of the employees to perform the role.
Reg 5.2.15(1)	A Safety Case prepared or revised under this part must … (b) contain a summary of the documentation prepared under regulations 5.2.6 and 5.2.7…
Reg 5.2.18	The operator of a major hazard facility must consult in relation to … (b) conducting or reviewing a Safety Assessment under regulations 5.2.7 and 5.2.12.
Reg 5.2.19	The operator of a major hazard facility must provide information, instruction and training to employees of the operator in relation to: (a) the kind of major incidents that could occur at the major hazard facility (b) all major incident hazards (c) the implementation of risk control measures …
Reg 6.1.44	WorkSafe may suspend or cancel a licence if it is satisfied … (e) in the case of a major hazard facility licence … (iv) that the licence holder no longer understands the content of the Safety Assessment conducted under regulation 5.2.7.
Schedule 10 (4.1)	(The SMS document must include) in relation to each part of the documented Safety Management System that describes the means of compliance with division 3 of part 5.2, an annotation or cross-reference identifying the specific provision of that division being complied with.

8. Further reading

General reference

Australian/New Zealand Standard, AS/NZS ISO 31000 – *Risk Management*, Standards Australia, 2009.

International Standard, ISO/IEC 31010, *Risk Management – Risk assessment techniques*, 2009.

Wells, G., *Hazard Identification and Risk Assessment*, Institution of Chemical Engineers, Rugby, 1997.

Center for Chemical Process Safety, *Guidelines for Hazard Evaluation Procedures*, 2nd edition, American Institute of Chemical Engineers, New York, 1992.

Montague, D. F., *Process Risk Evaluation – What Method to Use?* Reliability Engineering and System Safety, Vol. 29, No. 1, Elsevier Science, England, 1990, p27-53.

CONCAWE Ad-Hoc Risk Assessment Group, *Methodologies for Hazard Analysis and Risk Assessment in the Petroleum Refining and Storage Industry*, Fire Technology, Vol. 20, No. 3, 1984.

Health and Safety Executive, *Reducing Risks, Protecting People – HSE's Decision-making Process* (R2P2), Health and Safety Executive, UK, 2001.

Lees, F. P., *Loss Prevention in the Process Industries*, 2nd edition, Butterworth-Heinemann, UK, 1996.

Health and Safety Executive (HSE), *Guidance on 'as low as reasonably practicable' (ALARP) decisions in control of major accident hazards (COMAH).*

NSW Department of Urban Affairs and Planning, *Hazard Identification, Risk Assessment and Risk Control*, Major Industrial Hazards Advisory Paper (MIHAP) No. 3, Planning NSW, May 2003.

National Institute for Occupational Safety and Health, *Documentation for Immediately Dangerous to Life or Health Concentrations (IDLH)*: *NIOSH Chemical Listing and Documentation of Revised IDLH Values* (as at 3/1/95), US Department of Health and Human Services.

Chemical Hazards Response Information System (CHRIS), *Ammonia, Anhydrous (AMA)*: Fire Hazards, US Department of Transportation.

Lewis, R. J. Sr, *Sax's Dangerous Properties of Industrial Materials*, 10th edition, van Nostrand Reinhold, 2000.

Specific topics

Risk matrix

Australian/New Zealand Standard, AS/NZS 4360 – *Risk Management*, Standards Australia, 2004.

Middleton, M. and Franks, A., *Using Risk Matrices*, The Chemical Engineer, 2001.

Layers of Protection Analysis

Center for Chemical Process Safety, *Layer of Protection Analysis: Simplified Process Risk Assessment*, American Institute of Chemical Engineers, New York, 2000.

Fault and event trees

Center for Chemical Process Safety, *Guidelines for Hazard Evaluation Procedures*, 2nd edition, American Institute of Chemical Engineers, New York, 1992.

Vesely, W. E., Goldberg, F. F., Roberts, N. H. and Haasl, D. F., *Fault Tree Handbook*, NUREG-0492, US Nuclear Regulatory Commission, Washington DC, 1981.

QRA

DNV Technica for Altona Petrochemical Complex and Victorian WorkCover Authority, *Risk Assessment Guidelines for Victoria*, 1995.

Center for Chemical Process Safety, *Guidelines for Chemical Process Quantitative Risk Analysis*, 2nd edition, American Institute of Chemical Engineers, New York, 2000.

Committee for the Prevention of Disasters, *Guidelines for Quantitative Risk Assessment 'Purple Book'*, CPR 18E, Sdu Uitgevers, Den Haag, 1999.

Human factors

Center for Chemical Process Safety, *Guidelines for Preventing Human Error in Process Safety*, American Institute of Chemical Engineers, New York, 1994.

Kletz, T., *An Engineer's View of Human Error*, 2nd edition, Institution of Chemical Engineers (IChemE), Rugby, 1991.

Dougherty, E. M. Jr and Fragola, J. R., *Human Reliability Analysis: A Systems Engineering Approach with Nuclear Power Plant Applications*, Wiley Interscience, New York, 1988.

Reason, J. T., *Generic Error-Modelling System (GEMS)*, *A Cognitive Framework for Locating Common Human Error Forms*, New Technology and Human Error, ed. J. Rasmussen, K. Duncan and J. Leplat, 1987.

9. Appendices

Risk estimation techniques

These appendices are not intended to be a detailed or comprehensive description of Safety Assessment techniques. The methods and figures shown below are selected examples to illustrate different approaches. However, other approaches may be taken. Refer to Table 2.1 for discussion of the advantages and disadvantages of each technique. The further reading listed in this guidance note provides some of the significant references on this subject.

9.1. Risk matrix

A risk matrix is the most common approach used for qualitative Safety Assessment. The risk matrix is used to assess individual incidents in terms of categories (eg 'low', 'moderate', 'significant' or 'high' risk) based on their expected consequences and likelihood. AS/NZS ISO 31000 – *Risk Management* provides information on the risk matrix approach. An example of a risk matrix is shown in Figure 9.1. A basic risk matrix approach places each of the hazards considered into a region of the matrix. In the matrix below, risks are classified as low, moderate, significant or high risk as indicated by the shaded areas.

Figure 9.1 – Example risk matrix

			Consequence				
			Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
			1	2	3	4	5
Health and safety			Near miss First Aid Injury (FAI) or one or more Medical Treatment Injuries	One or more Lost Time Injuries (LTI)	One or more significant Lost Time Injuries (LTI)	One or more fatalities	Significant number of fatalities
Environmental			No impact	No or low impact	Medium impact (within facility boundary)	Medium impact (outside facility boundary)	Major impact
Financial loss			Loss below $5,000	Loss $5,000 to $50,000	Loss $50,000 to $1 million	Loss $1 million to $10 million	Loss above $10 million
Likelihood	5	Possibility of repeated events (1×10^{-1} per year)	Significant risk	Significant risk	High risk	High risk	High risk
	4	Possibility of isolated incidents (1×10^{-2} per year)	Moderate risk	Significant risk	High risk	High risk	High risk Incident 1
	3	Possibility of occurring sometimes (1×10^{-3} per year)	Low risk	Moderate risk	Significant risk	High risk	High risk
	2	Not likely to occur (1×10^{-4} per year)	Low risk	Low risk	Moderate risk	Significant risk	High risk
	1	Rare occurrence (1×10^{-5} per year)	Low risk	Low risk	Moderate risk	Significant risk	Significant risk

The risk matrix can also be used in a semi-quantitative format by placing numbers in each box of the matrix. This can provide greater resolution in risk ranking. In the risk matrix example in Figure 9.1, a simple scoring system can be introduced to represent the combined result of likelihood and consequence. The risk score or risk index can be calculated by multiplying the numbers in the likelihood rows and consequence columns. Note that these numbers increase with increasing likelihood and consequence severity eg incident 1 in Figure 9.1 has a likelihood 'score' of 4 and a consequence 'score' of 5. This equates to a risk score (or risk index) of 20 (ie 4 x 5).

Another benefit of the semi-quantitative approach is that the assessment of cumulative risk can be easier than a purely qualitative approach. One method for assessing overall risk is to use the sum of the risk indices for all incidents; hence the contribution of an incident is its risk index divided by the total risk. Caution should be used when using the sum of the risk indices to determine the overall risk as the number of incidents and incident grouping can significantly impact on the cumulative assessment. For example, three similar scenarios all ranked the same as incident 1, and a fourth scenario with a risk index of 10, have a total risk of 70. However, if the three scenarios were grouped as one incident because they involved similar pieces of equipment (eg an ammonia release from one of three identical tanks), the total risk would only be 30. Therefore, with a larger number of incidents the risk contribution per incident will be lower.

Corporate risk matrices may need to be tailored to the requirements for assessing major incidents to segregate the risks into the categories. Corporate risk matrices will often result in all analyses involving death being located in the 'high risk' category due to a limitation in the number of frequency categories. Additional lower frequency categories are frequently needed.

If a risk matrix is chosen to assess the risk at a facility, the operator needs to ensure that it provides sufficient differentiation between risks. For simpler sites, a risk matrix may provide sufficient differentiation. It is important that the attention given to hazards is proportional to the risk.

The operator should keep in mind that categories often differ by orders of magnitude. Therefore hazards may exist within the same box of the matrix and have substantially different frequencies. Where a large number of hazards exist, too many events may be ranked in one square to enable priorities on risk reduction opportunities to be made, so there may need to be some differentiation within each square. Examples:

- For each hazard (except low risk categories) a risk index could be generated based on a mix of criteria such as frequency, complexity, chemical hazard rating etc.
- Use another approach, such as LOPA (see section 9.3) and use the risk matrix only as a method of displaying risk.

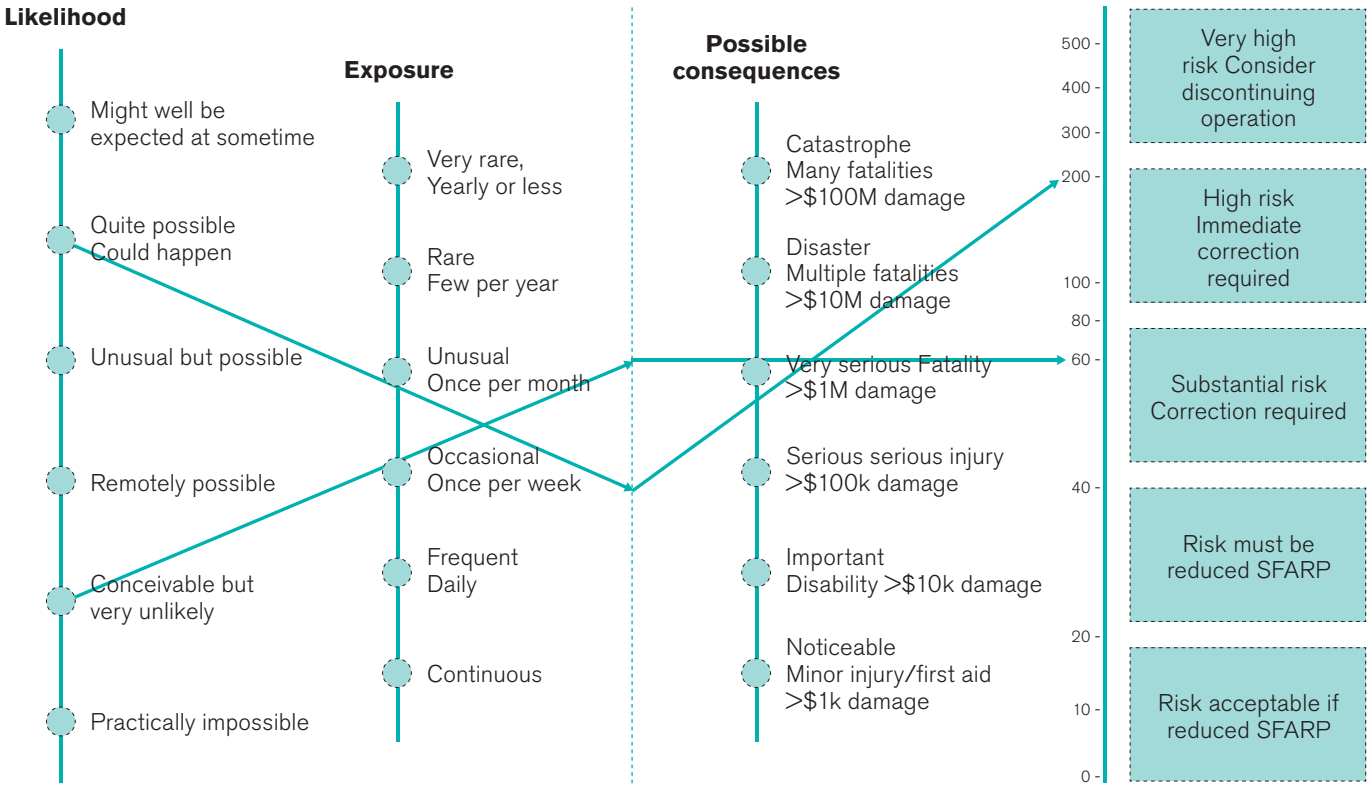
More, rather than fewer, categories should be considered to avoid grouping of hazards. This decision will also have an impact on risk. However, given that people are involved in decisions that have a level of associated uncertainty; guidance needs to be provided to ensure consistency. For example, the categories for different chemicals may be different (such as petroleum versus chlorine). It is also possible to rank either each hazard with potential to cause a major incident (and therefore have several rankings for each incident) or each major incident.

9.2. Risk nomograms or risk graphs

Risk nomograms provide an alternative approach to the use of matrices. An example of a risk nomogram is shown in Figure 9.2. One advantage of the risk nomogram technique over risk matrices is that risk reduction delivered by additional risk control measures can be more accurately measured, since risk is presented on a continuous scale, rather than in discrete cells as is the case on a matrix. However, the development of risk nomograms is not a straightforward matter, and users should ensure they clearly understand the principles involved before considering such an approach.

Such methods can provide a relatively rapid understanding of the risk profile of the facility, and can be based on judgement alone or be refined using more detailed (possibly numerical) information.

Figure 9.2 – Example risk nomogram



When using nomograms it is important to define individual incidents or scenarios on a consistent basis, so that comparable events are assessed. Failure to do this will produce results that cannot be directly compared against one another, therefore limiting their usefulness.

9.3. Layers of Protection Analysis

LOPA is one of a number of techniques developed in response to a requirement within the process industry to be able to assess the adequacy of the layers of protection provided for an activity. The Center for Chemical Process Safety (CCPS) has published a comprehensive book (CCPS, LOPA, 2001) on the application of LOPA, and only a brief summary of the technique is provided here. The technique uses simplifying rules to evaluate initiating event frequency, independent layers of protection, and the impact of consequences to provide order of magnitude estimates of risk.

The LOPA process normally follows these steps:

(a) identify hazardous event – this includes both the hazard and outcome (consequence)

(b) identify the frequency of initiation

(c) estimate the inherent likelihood of a fatality – this includes the level of exposure for an individual, the likelihood of ignition etc

(d) identify the independent preventative layers of protection and the risk reduction factors that apply to each layer

(e) identify the independent consequence mitigation layers of protection and the risk reduction factors that apply to each layer

(f) calculate the estimated likelihood of the consequence.

The results may be plotted on a risk matrix if required. This may assist the workforce to understand the calculated risk, especially if they are used to using risk matrices, eg for Job Safety Analysis. A further step that can be applied is to compare the estimated likelihood against a target likelihood which has been defined for each consequence category. Any difference must therefore be altered by the identification or implementation of additional risk control measures.

This process may be conducted using a quantitative approach that references initiation frequencies and control measure failure rate data. Alternatively it may be conducted using an index approach where the protection layer credits

(described in CCPS, LOPA, 2001) are applied to the risk reduction measure. These figures are indicative of the level of protection provided by a control.

Benefits of this approach are:

- a rigorous assessment of likelihood
- the effectiveness of risk control measures is explicitly shown
- cumulative risk can easily be shown
- where unacceptable residual risk is found, the technique helps define the level of performance required from additional or alternative risk control measures to meet all relevant criteria. These requirements can then be used as performance specifications when designing or purchasing new risk control measures.

Issues that need to be considered include:

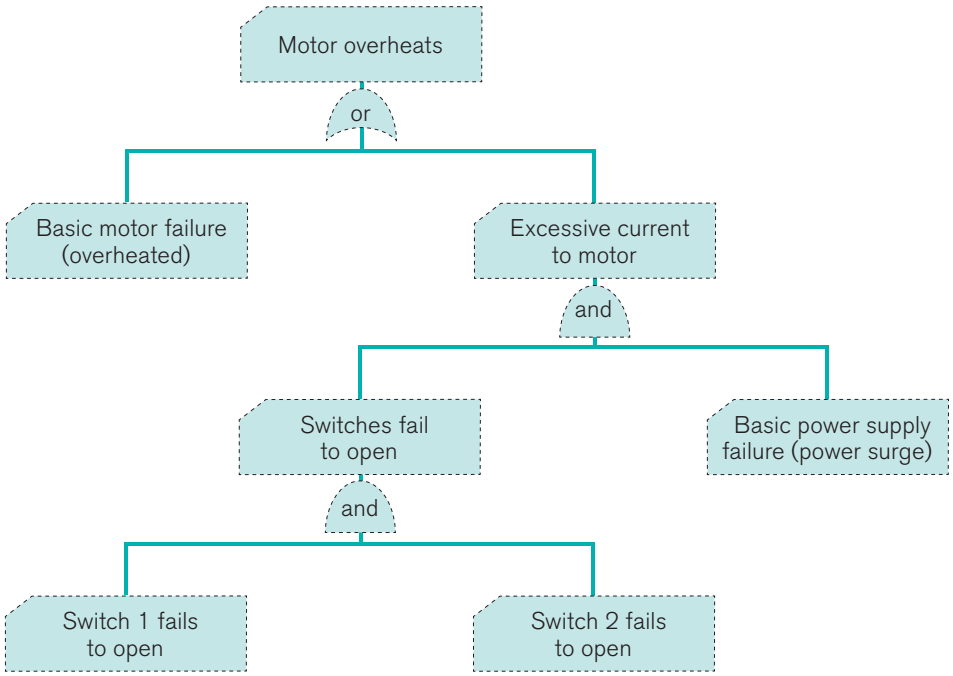
- it is more time-consuming than other qualitative and semi-quantitative approaches
- independence
- as each hazard may result in several outcomes there can be a need to conduct the assessment for a single hazard several times for each of the consequence outcomes.

9.4. Fault and event trees

A fault tree may be used to provide an estimate of the likelihood of failure occurring. The starting point is the main event of interest (referred to as the top event). The analyst works down in order to identify the sequences of events required to produce that event. The technique is useful both for the quantification of likelihood and as a method for identifying which event sequences and hazards could lead to a major incident. It is also useful for identifying the major contributors to the likelihood of the top event.

For example, it may be used to show how low level failures, combined with external aspects such as a loss of power supplies, operator errors etc may combine to cause overall system failure. An example fault tree is shown in Figure 9.3.

Figure 9.3 – Example – Fault tree



Similarly, an event tree can be used in the process of estimating likelihood. Event trees start with a single incident (eg release of product from a process vessel) and then fan out to the possible outcomes (eg pool fire, jet fire). An example of an event tree is provided in Figure 3.2. Any point in the event tree can be characterised by a particular consequence and an associated likelihood.

The benefits of applying these techniques are that they provide:

- an in-depth analysis of the potential causal chains that result in the final outcomes
- a demonstration of the value of each control measure with respect to preventing or mitigating the incident
- a reproducible and justifiable estimate of likelihood.

The use of these techniques is very time-consuming and should only be applied to those scenarios where a more formal method is required to analyse risk eg incidents with high risk or where there is significant uncertainty as to the likelihood or the hazards which could lead to the incident.

9.5. Quantitative or Quantified Risk Assessment

The application of quantitative methods is considered desirable when:

- several risk reduction options have been identified whose relevant effectiveness is not obvious
- the exposure to the workforce, public, or the strategic value of the asset is high, and reduction measures are to be evaluated
- equipment spacing allows significant risk of escalation
- novel technology is involved resulting in a perceived high level of risk for which no historical data is available
- demonstration of relative risk levels and their causes to the workforce is needed to make workers more conscious of the risks.

A QRA is one form of quantitative risk assessment. A QRA seeks to:

- provide numerical estimates (for all hazards) of both consequences and their likelihood of occurrence based on historical data and computer simulations
- develop a quantified analysis of risk for the entire site (generated using the cumulative effects of the individual hazards).

The analysis of the risk incorporates the various effects from the range of applicable meteorological conditions, as well as from various release conditions, types and sizes and the population distribution on the site and surrounding areas. The output is typically in the form of fatality or individual risk contours or societal risk figures.

A number of software tools are available to assist with some or all of the calculations that may be required in a QRA. The 'Purple Book' (1999) has been published by Dutch regulatory authorities as a guide to performing QRA. It contains an extensive list of such tools. The accuracy and usefulness of such tools depends heavily on the knowledge and skill of the user and the accuracy of the input data.

The results of a QRA can offer greater consistency, however there are a number of potential shortcomings:

- the output may be misleading if the selection of failure statistics is not well considered
- there is a lower involvement of the workforce in the risk analysis
- the industry data may not reflect how well, or poorly, the facility is managed
- on its own it does not provide sufficient understanding of the full range of controls present at a facility.

A QRA is best suited to differentiating design, layout, location and engineering options. However, the application of QRA should not be limited to large, complex, expensive studies. It is a technique that can be used quickly and cheaply to help structure the solution to problems for which the solution is not immediately obvious.

A sensitivity analysis may be necessary to cover any assumptions made or data utilised during the analysis of the risk. This should illustrate the sensitivity of the results to changes in the data and assumptions, and identify any inputs that significantly affect the results. This analysis is an essential part of a QRA as it ensures that the user fully understands the results of QRA and how they were developed.

Further Information

Contact the WorkSafe Victoria Advisory Service on 1800 136 089 or go to worksafe.vic.gov.au

Related WorkSafe publications

Guidance note – *Control measures*

Guidance note – *Hazard identification*

Guidance note – *Emergency planning*

Guidance note – *Renewal of a major hazard facility licence*

Guidance note – *Requirements for demonstration*