GUIDE FOR MAJOR HAZARD FACILITIES

SAFETY ASSESSMENT

MARCH 2012

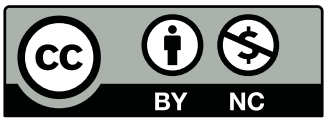
safe work australia

safe work australia

Safe Work Australia is an Australian Government statutory agency established in 2009. Safe Work Australia consists of representatives of the Commonwealth, state and territory governments, the Australian Council of Trade Unions, the Australian Chamber of Commerce and Industry and the Australian Industry Group.

Safe Work Australia works with the Commonwealth, state and territory governments to improve work health and safety and workers' compensation arrangements. Safe Work Australia is a national policy body, not a regulator of work health and safety. The Commonwealth, states and territories have responsibility for regulating and enforcing work health and safety laws in their jurisdiction.

ISBN 978-0-642-33374-2 [PDF]
ISBN 978-0-642-33375-9 [RTF]



Contact information
Safe Work Australia
Phone: +61 2 6121 5317
Email: info@safeworkaustralia.gov.au
Website: www.safeworkaustralia.gov.au

safe work australia
Australian Government
Comcare
ACT Government
Justice and Community Safety
WORKSAFE ACT
WorkCover
NEW SOUTH WALES
Workplace Standards
Tasmanian Government
NTWorkSafe
Government of South Australia
SafeWork SA
WORKSAFE
Western Australia
Queensland Government

TABLE OF CONTENTS

1. INTRODUCTION

The Work Health and Safety Regulations (the WHS Regulations) require operators of determined major hazard facilities (MHFs) to conduct a safety assessment in order to provide a detailed understanding of all health and safety risks associated with major incidents.

The purpose of this Guide is to assist operators of MHFs to prepare and conduct a safety assessment in accordance with the WHS Regulations.

The guidance has been prepared for operators of MHFs from all sectors—processing, storage and warehousing—notwithstanding the significant differences in complexity. Examples have been given where possible to illustrate possible application to each sector. Applicability will depend on the specific circumstances of the MHF. Operators are advised to refer to reputable texts or engage suitable specialists when choosing to apply a specific technique.

The guidance will provide:

- assurance to the operator that the potential risk of major incidents will be eliminated or controlled
- a detailed understanding of all aspects of risks to health and safety associated with major incidents
- the production of a documented safety assessment that meets the requirements of the Regulations and which can be used to form part of the safety case submitted for licensing.

This Guide forms part of a set of guidance material for MHFs that includes information on:

- Notification and Determination
- Safety Management Systems
- Developing a Safety Case Outline
- Preparation of a Safety Case
- Safety Case: Demonstrating the Adequacy of Safety Management and Control Measures
- Information, Training and Instruction for Workers and Others at the Facility
- Providing Information to the Community
- Emergency Plans.

WHAT IS A SAFETY ASSESSMENT?

A safety assessment is a comprehensive and systematic investigation and analysis of all aspects of risks to health and safety associated with major incidents that may potentially occur in the course of operation of the major hazard facility, including:

- the nature of each major incident and major incident hazard
- the likelihood of each major incident hazard causing a major incident
- in the event of a major incident occurring, its potential magnitude and the severity of its potential health and safety consequences
- the range of control measures considered
- the control measures the operator decides to implement.

The following are expected outcomes from a safety assessment for a major hazard facility.

- for each major incident:
  - the identification of all major incident hazards and the path by which the major incident hazards could lead or have led to a major incident
  - the identification of consequences for each major incident without controls
  - an analysis of risk (likelihood and consequence) for each major incident (with current controls and then with future control measures)
  - the identification of all reasonably practicable control measures with a documented justification of any potential control measure determined to not be reasonably practicable
  - a description of how the identified risk control measures prevent or mitigate the major incidents and major incident hazards
  - demonstration of adequacy of risk control measures for each major incident, so far as is reasonably practicable (see also demonstration of adequacy guidance)
- for the facility:
  - the provision of a list of all potential major incidents
  - the provision of an assessment of the cumulative effects of the major incidents (knock on effects, sum of all risks, common cause incidents, etc.)
  - a summary of the likelihood and consequences of the major incidents
  - the identification of the local community potentially affected by the consequences of any major incident.
  - the identification of the maintenance and monitoring requirements and the critical operating parameters identified for the selected control measures
  - a demonstration of the adequacy of control measures (so far as is reasonably practicable)
  - the preparation of an implementation plan for required risk control measures not yet in place.
- a description of how the risk assessment will be reviewed and updated to continuously maintain its currency.

WHAT DO THE REGULATIONS REQUIRE?

Operators of determined MHFs must conduct a safety assessment in relation to the operation of the MHF. The operator of a licensed major hazard facility must keep a copy of the safety assessment at the facility and review and revise it as necessary. Further details of the regulations are set out in Appendix A.

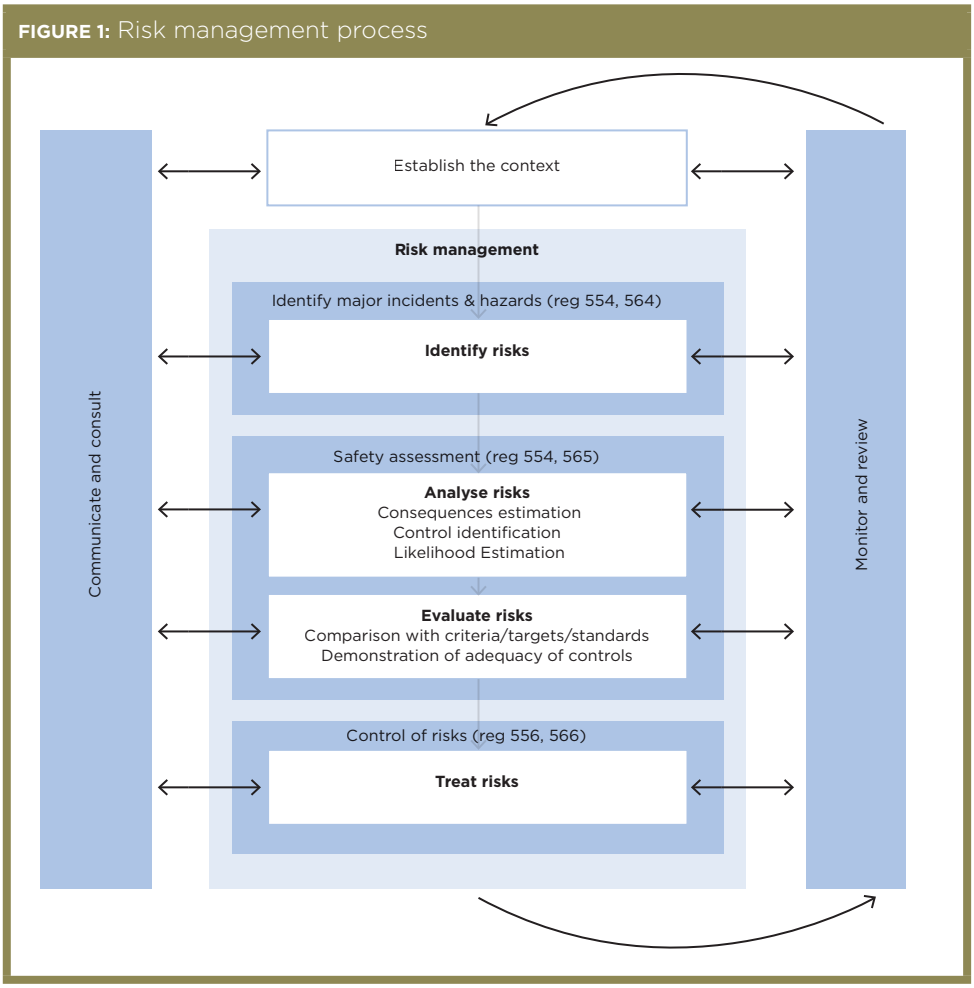
Relevant definitions are set out in Appendix B.

2. RISK MANAGEMENT

There are many authoritative texts on risk management that may be of use to an operator or intending operator of a MHF. This Guide is not intended to be a risk management text. It is designed to explain and describe how an operator may comply with the WHS legislation.

The hazard identification and safety assessment are components of the overall risk management process (see Figure 1).

FIGURE 1: Risk management process



This Guide outlines the main components of risk management as follows:

Establish the context:

- Major incident and major incident hazard identification
- Safety assessment:
  - control identification
  - consequence estimation
  - likelihood estimation
  - risk evaluation
- Control of risk
- Monitoring and review.

3. ESTABLISHING THE CONTEXT

3.1 Establishing the Scope and Objectives

The scope should cover the whole of the facility, all activities on site, routine or abnormal operations, and any off-site hazard that could impact on the site, leading to a major incident.

The objectives should include providing assurance that the risks have been eliminated, so far as is reasonably practicable, and if it is not reasonably practicable to eliminate a risk, ensure it is minimised so far as is reasonably practicable (see Example 1).

An operator may declare the achievement of a risk target or risk tolerance criteria as an objective of the safety assessment (see Example 2). This is particularly appropriate for operators of complex facilities, multiple facilities or where a quantitative risk assessment is proposed. Operators of simple facilities with the ability to personally supervise the safety assessment process may find it more appropriate to focus on eliminating and systematically controlling the risks rather than calculating a risk number or rating.

It should be noted that a risk that meets an operator's risk tolerance criteria must still satisfy the regulatory obligation to eliminate or minimise risk so far as is reasonably practicable (see Regulation 556). Consultation with the regulator is advised if quantitative tolerance criteria are to be used.

EXAMPLE 1 – SCOPE AND OBJECTIVES

ABC Chemical Company is a new MHF. They established the objectives of the safety assessment as follows:

- to eliminate or, where that is not reasonably practical, reduce risk of each major incident so far as is reasonably practical
- to systematically identify and assess all major incidents and major incident hazards in accordance with the Regulations
- to identify and demonstrate the adequacy of controls for major incidents.

EXAMPLE 2 – RISK TOLERANCE CRITERIA: COMPLEX PROCESSING PLANT

ABC Multinational Company has an internal safety policy which requires that new facilities are built and operated such that the HIPAP 4[1] risk criteria are met. Additionally, they have adopted target IRPA values. Existing facilities that do not meet the criteria must submit a risk reduction program and continue to manage risk as low as is reasonably practical.

- Incident heat flux radiation at residential or sensitive use areas should not exceed 4.7 kW/m^2 at a frequency of more than $50x10^{-6}$ pa.
- Incident explosion overpressure at residential and sensitive use areas should not exceed 7kPa at frequencies of more than $50x10^{-6}$ pa.
- Toxic concentrations in residential and sensitive use areas which could cause acute physiological consequences should not exceed $50x10^{-6}$ pa (ERPG, SLOD or SLOT values chosen as appropriate).
- IRPA must not exceed 10^{-4} at any occupied area e.g. control rooms, safe havens, maintenance workshops and administrative areas.

1. NSW Department of Planning, Hazardous Industry Planning Advisory Paper (HIPAP) No. 4 – Risk Criteria for Land Use Safety Planning

3.2 Key items for preparation

PREPARATION

The following items need to be considered in preparing for a safety assessment:

- information required
- resources: people and time
- resources: tools/techniques
- systematic approach
- communication and consultation
- documentation of process and results.

INFORMATION REQUIRED

The following information may be required during the safety assessment process. The operator should gather this information both before and during the process, and commit to ensuring this information is up-to-date to facilitate future reviews and revisions of the safety assessment.

- data on the safety properties of the materials e.g. MSDS, explosivity data, reactivity, degradation, any conditions under which materials become dangerous, etc.
- incident history from the facility, corporation, national, industry or global sources
- existing studies e.g. HAZID, HAZOP, PHA, fire safety studies, likelihood analysis, QRA, hazardous substance risk assessment, SIL/SIF and hazardous area zoning studies. These studies may need to be reviewed and re-validated to ensure that they are still current
- previous studies e.g. fire safety studies and mechanical integrity studies

- design envelopes/criteria for plant and equipment, engineering safety margins, designed operating conditions and design safety philosophy
- any design standards (Australian, international or corporate) relevant to the operations at the facility
- critical operating parameters that have already been identified.
- assessment of current plant condition e.g. integrity, reliability, equipment maintenance history, etc.
- description of operations or tasks undertaken at the facility, such as handling, storage and processing
- existing operational issues and problems
- existing control performance
- maps or diagrams showing layout (e.g. storage or processing areas), process flows (P&IDs etc), control strategies, etc.
- surrounding population demographics and density
- personnel experience
- maintenance records, including breakdown data
- equipment reliability/failure rate data.

Sources of generic data and justification of its use, as well as any assumptions made, need to be documented for the safety case. Weight should be given to data sources most relevant to the facility, taking into account local conditions and equipment configurations.

EXAMPLE 3 – AVAILABLE INFORMATION

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

- hazard identification records
- vessel inspection records for the storage vessel
- test records for the pressure relief valve 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 Safety Data Sheets (SDSs)
- exposure levels (e.g. Immediately Dangerous to Life and Health (IDLH), Short Term Exposure Limit (STEL), Emergency Response Planning Guidelines (ERPG))
- any consequence information available (e.g. modelling).

RESOURCES: PEOPLE AND TIME

The process should involve personnel with a range of knowledge, skills and work experiences. This should include personnel ranging from those experienced in the chosen techniques, those who carry out the tasks, supervisors, those with expertise in the design intent who can explain why the plant design choices were made, and those with expertise in the hardware, systems and materials. In some cases this may involve third parties such as consultants or contractors (see Example 4).

Successful engagement of workers in the hazard identification and safety assessment tasks improves outcome quality and complies with the worker consultation provisions of the WHS Act (Sections 47–49) and the WHS Regulations (574 and 575).

Even for a simple major hazard facility, the hazard identification and safety assessment may be lengthy, involving many workshops over an extended time period.

Decisions on adequacy of controls and further risk reduction will have to be made. Improvements will need to be included in the relevant business and capital plans. Progress will need to be monitored. Management should plan sufficient time and resources for the process to be done effectively.

EXAMPLE 4 – RESOURCES

The workshop team for ABC Chemical Company ammonia hazard identification is:

- facilitator
- electrical maintenance worker
- mechanical maintenance worker
- two shift workers
- area supervisor
- ammonia truck driver (contractor).

Even though the ammonia truck driver is not an ABC Chemical Company employee, the driver has been invited specifically for hazard identification associated with ammonia unloading. As the driver is the one doing this work, he/she may have an insight into hazards and controls which the employees will not have.

RESOURCES: TOOLS/TECHNIQUES

The operator of the major hazard facility should apply hazard identification and safety assessment tools and techniques that are suited to its objectives and capabilities, and to major incidents and major incident hazards considered. Justification of the reasons for technique selection should be included in the safety case and/or safety case outline.

A variety of hazard identification and assessment techniques exist that can be used successfully. Multiple techniques may be required to adequately identify and assess the major incident scenarios.

- The facility should ensure the techniques:
- are fit for the complexity and scale of the facility
- involve worker participation to a suitable extent
- consider any external conditions or facility-specific attributes
- clearly document the relationships between the major incidents, hazards and controls
- reveal the rationale for the assessment, in particular the selection or rejection of control measures
- generate outputs that can be used in further risk assessments and integrated in the management systems of the facility.

Techniques may be qualitative or quantitative. The advantages of a qualitative process are that it is simple, easy to use and understand, and low cost. The disadvantages may include

a lack of differentiation between major incidents and difficulty establishing meaningful cumulative assessment. A quantitative technique has advantages in ability to compare major incidents and easy cumulative assessment, but disadvantages in being complex, harder to understand and use, and higher cost.

A qualitative process may be better suited to storage or simple process sites, while a quantitative process may be better suited to a site with a high level of complexity or high risks.

It is likely that a combination of techniques will need to be used to fully understand a complex major incident scenario.

SYSTEMATIC APPROACH

It is important to design the safety assessment approach so that all the possible major incidents at the facility are identified and assessed.

The following are examples only and are not an exhaustive list.

EXAMPLE 5 – THE LOCATION APPROACH

An operator of a warehouse and blending facility chose to divide the facility into sheds. A workshop examined the processes and tasks in each shed, and then checked for any cross-shed or system-wide interactions. The data was collated into a list of major incidents and major incident hazards for the site.
If this method is chosen, it is important to record the identified hazards and incidents in sufficient detail that there can be a check on consistency between workgroups. If similar major incidents are grouped together, the operator must be watchful that a specific incident initiator or escalating factor peculiar to a single shed is not dropped from the analysis.

EXAMPLE 7 – THE CHEMICAL APPROACH

An operator of a small facility with few Schedule 15 chemicals examined each chemical in turn, identifying the conditions under which it was kept and handled, and what could go wrong. They then examined system-wide challenges (for example, power failure, unauthorised access, etc.) and collated the results into a major incident list.

EXAMPLE 8 – THE REVIEW APPROACH

It is tempting, particularly if the facility has a history of risk assessments in place, to merely revisit the existing assessments using a modified version of the original techniques. If this approach is chosen, the operator needs to assure themselves and the regulator that the approach will uncover any new hazards rather than merely validating the status quo, and that the original assumptions remain valid. The operator must ensure they go “looking” for hazards.

EXAMPLE 9 – THE TOP DOWN APPROACH

An operator of several simple storage facilities (e.g. LPG or ammonia), with each facility built to similar standards and undertaking similar tasks, chose to define a representative set of major hazards and potential major incidents, to be validated by workshops at each site. While this allows significant technical input in constructing the representative set, the operator must ensure that the process allows incorporation of site-specific features and external conditions, such as the presence of threats from outside the facility boundary.

There is also the assumption that the tasks are performed the way envisaged by head office, which may not be the case on the ground. If the workshop attendees do not understand the assumptions behind the representative set, they may not detect how what they do on-site may cause or contribute to the major incident. Thus the composition of the workshop team is an important success factor for this approach.

EXAMPLE 10 – THE ENGINEERING APPROACH

Processing facilities usually commission a number of hazard studies through the various phases of design, construction, commissioning and operation. Some of these assessments are task-based (for example, lighting burners); others are hazard-based (e.g. hazardous area assessments); others are process-based (HAZOPs and SIL assessments); and yet others are based on an assessment of conditions and known failure mechanisms (e.g. as part of a RBI program). The operator's challenge is to assimilate all of these studies into a detailed understanding of all aspects of risks to health and safety.

A common approach is to divide the process into natural operating units (or management units) and conduct a process hazard analysis, utilising the results of all the abovementioned studies. The operator must have some method of checking for consistency and for ensuring that areas "at the interface" are covered. Areas of lesser apparent risk (for example, as dangerous goods management in the warehouse, or service systems) are included, as they can often potentially involve Schedule 15 chemicals and develop into major incidents.

COMMUNICATION AND CONSULTATION

This should occur at all stages of the safety assessment process and is covered in further detail in other guidance material. The Regulations require worker consultation and participation in hazard identification, safety assessment and many aspects of risk control (regulations 574 and 575).

Information acquired during consultation with the local emergency, security and local area authorities, required under different sections of the Regulations, should be utilised in the safety assessment process.

DOCUMENTATION OF THE PROCESS AND RESULTS

Under the WHS Regulations, the identification of major incidents and major incident hazards, and the safety assessment, must be documented.

Adequate documentation ensures that the risk management activities and decisions are traceable and reproducible. These records provide the basis for improvements to methods and tools, as well as to the overall process. Decisions concerning the level of detail, methods

used for documentation and applicable records management should take into account:

- the facility and organisation's needs for continuous learning
- benefits of reusing information for management purposes
- costs and efforts involved in creating and maintaining records
- legal, regulatory and operational needs for records
- method of access, ease of retrievability and storage media
- ability to revisit and update information (for example, licence renewal)
- retention period
- sensitivity of information.

4. HAZARD IDENTIFICATION

4.1 Understand the definitions

The hazard identification must identify all major incidents and all major incident hazards that could occur at the facility, including major incident hazards relating to the security of the major hazard facility.

- The meaning of a major incident is defined in regulation 531, and has the following qualities:
- they result from an uncontrolled event (i.e. unplanned and/or involving the failure of one or more controls)
- they involve or potentially involve Schedule 15 chemicals (which include events initiated by other circumstances that may knock-on to Schedule 15 chemical storage or handling facilities)
- they expose a person to serious risk to health and safety (at least one, and often more than one person, including those in the area surrounding the facility)
- the risk emanates from an immediate or imminent exposure to the incident (which excludes long-term cumulative impacts such as some types of cancer).

Occurrences that may be classified as a major incident include:

- fire (loss of containment which could lead to fire, jet fire, fireball, etc.)
- explosion (BLEVE, vapour cloud explosion, dust explosion, etc.)
- implosion (for example, vacuum from steam condensation, etc.)
- escape, spillage or leakage (damage, overfill, decay. etc.).

The uncontrolled event which may lead to a major incident has a spectrum of possible consequences. If any of the possible consequences of the event may lead to serious risk to health and safety of one or more people, then the event leading to the serious risk must be classed as a major incident. Serious risk includes risk leading to a single fatality.

The intent of the safety assessment is to focus on the high-consequence, low-probability events.

There are incidents that do not involve or potentially involve Schedule 15 chemicals, but that do potentially expose a person to serious risk to health or safety. These incidents do not have to be included in the safety assessment and safety case as they do not meet the definition of a major incident. Notwithstanding this, the operator still has the primary duty of care to ensure the health and safety of other persons is not put at risk from work carried out at the facility. These risks should be adequately managed by the safety management system and emergency plans prepared for the facility.

Major incident hazards are defined as those hazards that could cause or contribute to causing a major incident or uncontrolled event. The intent is for the facility to fully understand and control the chain of events (major incident pathways) that may lead to a major incident.

IDENTIFY ALL SCHEDULE 15 CHEMICALS

It is important that all Schedule 15 chemicals, including products, by-products, intermediates, raw materials and wastes—whether they are held in storage, or in process, or being transferred or otherwise handled—be considered in the safety assessment. This includes small quantities that may have been excluded from the initial facility notification requirement.

EXAMPLE 11 – INCLUSION OF SMALL QUANTITIES OF SCHEDULE 15 CHEMICALS

Examples of small quantities of Schedule 15 chemicals that have been considered in past safety assessments are as follows:

- A facility had a large gas-fired dryer inside a building where there were many employees. Because there was no gas stored on the site, only what was in the natural gas supply line, the natural gas did not have to be considered in the threshold calculations. The facility was determined as a MHF because of the total quantity of other Schedule 15 chemicals on site. Nevertheless there was clearly potential for a major incident such as an explosion and fire if a sizeable leak of natural gas (a Schedule 15 chemical) occurred inside the building followed by delayed ignition. The facility included this potential major incident in its safety case.
- A small hydrogen cylinder serving an online process gas chromatograph is another example of a small quantity that would have no influence on threshold calculations but, because of its location inside the plant, may need to be included in the safety assessment if it could initiate an incident that could in turn escalate to a major incident. Similar cylinders in an adequately ventilated laboratory area remote from the process areas of the facility may not need to be considered at all.

Suggested methods for identifying all Schedule 15 chemicals include a review of dangerous goods manifests, storages, safety data sheets for materials on the site, other information from chemical suppliers, etc. Refrigerants (for example, anhydrous ammonia), by-products and unintended products of reaction should also be considered and included.

4.2 Understand the chemical properties and how they could cause harm

The properties of the chemicals should be identified and understood. These properties may include:

- toxicity
- flammability
- explosivity
- degradation behaviour
- chemical reactivity and interactions
- incompatibilities
- physical state
- concentrations
- solubility
- properties at temperatures and pressures that may occur at the facility.

The properties need to be understood at the conditions encountered in the facility during both normal and abnormal operations. These properties will have a significant impact on what, if and how a major incident will occur.

EXAMPLE 12 – UNDERSTANDING OF PROPERTIES OF SCHEDULE 15 CHEMICALS

Personnel at MHFs should be aware of the properties of the Schedule 15 chemicals and how those properties may lead to a major incident if not properly managed. Some of the consequences are not obvious. For example:

- If chlorpyrifos is heated above 90°C it decomposes. Above 130°C there is an exothermic decomposition (runaway reaction).
- Sodium chlorate is stable as a solid and soluble in water. However, when mixed with other materials such as organics (for example, pesticides and herbicides) or acids, there is a risk of fire and explosion.
- Hydrogen peroxide is a strong oxidiser and can react violently with reducing agents. It also decomposes to oxygen and water naturally (or promoted by conditions), which can cause fire on contact with a flammable material.
- Storage of incompatible materials in proximity based on their Class and Division is recognised, but incompatibilities of materials based on subsidiary Class may not be recognised e.g. bromine chloride is Division 2.3 and subsidiary Classes 5.1 and 8 could react with other Division 2.3 goods.
- Material left in storage for prolonged periods or as intermediate products may result in unwanted product formation. Depending on the product, this could cause instability, increased toxicity or increased internal pressure (i.e. the IBC “bulges” and potentially ruptures).
- Ammonia is a toxic material and also soluble in water to form an alkaline solution. At high pressures and temperatures. ammonia is capable of forming an explosive mixture with air.

It is important to understand what needs to happen for a person to be exposed to a serious risk to their health and safety. This area of investigation also helps with exploring potential “knock-on” type events.

EXAMPLE 13 – UNDERSTANDING TOXICITY EXPOSURE MECHANISMS

The operator of a warehouse reviewed the toxicity of the chemicals stored and the mechanisms by which an employee may be exposed. They discovered that:

- paraquat, normally in liquid form, is very toxic by inhalation. Inhalation of a liquid in a warehouse setting is very difficult. It is not particularly uncommon, however, for paraquat to weep at the lid. If left in quarantine for a while, crystals form around the lid. An employee may conceivably receive a toxic dose if they are not cautious in opening an over-drum.
- aldicarb is very toxic by dermal and oral criteria. If a drum spills, an employee may receive a toxic dose either by skin contact or clothing to skin contact when cleaning up, or involuntarily ingesting the chemical if the leak is as a spray (for example, when a forklift spear is removed from the drum).

EXAMPLE 14 – UNDERSTANDING MINIMUM AMOUNT LIKELY TO CAUSE HARM

For an ammonia release to expose a person to serious risk to their health and safety, the ammonia must be in a sufficient concentration to cause harm. Lesser amounts cause nuisance and irritation. While all releases are undesirable, it is necessary to focus efforts on preventing leaks/releases of sufficient size to cause a major incident.

Consequence modelling of small releases found that 50 kg was needed for the immediate danger to life and health threshold (IDLH) to be reached at distances over 2 m.

4.3 Research previous major incidents and near misses

Incidents from industry and site are useful precedents, and graphically illustrate potential consequences and particular incident pathways. Sources of incidents and footage include:

- site and industry history
- site near miss incidents
- Chemical Safety Board (CSB) www.csb.gov
- Lees' Loss Prevention in the Process Industries
- Health and Safety Executive (HSE) www.hse.gov.uk.

IDENTIFY THE MAJOR INCIDENT AND MAJOR INCIDENT PATHWAYS

Identification of the major incident hazards and the potential major incidents they may lead to requires some creativity, technical expertise, and familiarity with the plant and equipment.

The major incident and major incident hazard identification is best performed in teams. It is important that the study teams:

- understand what constitutes a major incident
- are composed of an appropriate variety of people
- are aware of the properties of the Schedule 15 chemicals
- are aware of how the chemicals are used
- are aware of plant and industry incident history
- challenge assumptions and existing norms of design and operation
- think beyond the immediate experience of the facility
- look only at potential and ignore any consideration of likelihood or existing controls at this stage.

Hazard identification techniques need to be systematically applied to each plant area and each activity in order to generate a complete list for further exploration. The operator should be alert to common cause failures, possible knock-on scenarios and any external conditions which may affect the potential for a major incident to occur. The chosen technique needs to be suited to the hazard and the facility (see discussion in 5.2 Resources: tools/techniques).

EXAMPLE 15 – EXAMPLE MAJOR INCIDENTS: WAREHOUSE

Uncontrolled Event	Schedule 15 Chemical Involved	Potential Major Incident Description
■ 200 L drum falls and splits, spilling into a contained area	Flammable liquid, PG III	Pool fire of 200 L drum of flammable liquid
■ Forklift damages 1,000 L IBC of pesticide	Toxic solids and liquids	Toxic exposure from loss of containment of IBC of pesticide
■ Lightning strike ■ Electric arc from distribution box ■ Arson attack ■ Incompatibles stored in same bund leak and react	All/part of warehouse Schedule 15 chemicals inventory	Warehouse fire generating heat and toxic smoke

EXAMPLE 16 – EXAMPLE MAJOR INCIDENTS: STORAGE

Uncontrolled Event	Schedule 15 Chemical Involved	Potential Major Incident Description
■ Hose leaks under moderate pressure	Flammable liquid	Flash fire
■ Roof sinks due to failure to remove water ■ Lightning strike	Crude oil	Crude oil tank top fire
■ Feed valve fails, spillage to bund	Crude oil	Bund fire in crude oil storage
■ Hose failure ■ Valve failure	LPG	Vapour cloud explosion of LPG
■ Impact and guillotine failure of pipework	LPG	Jet fire from bullet
■ Sustained fire attack on bullet	LPG	BLEVE of bullet

EXAMPLE 17 – EXAMPLE MAJOR INCIDENTS: PROCESSING

Uncontrolled Event	Schedule 15 Chemical Involved	Potential Major Incident Description
■ Sabotage	Hydrogen	Terrorist attack on significant storage leads to explosion
■ Operator mistakes chemical identity and loads wrong chemical	Sodium hydrosulfide (class 4.2 PGII)	Accidental mixing of incompatible material releasing heat and toxic gas
■ Failure of cooling water	Methylcyclopentadienyl manganese tricarbonyl (MCMT) Class 6.1 PGI	Runaway exothermic reaction leading to loss of containment and explosion

REFINE THE MAJOR INCIDENT LIST

All identified major incident hazards with a scientifically credible mechanism linking to the major incident should be included. If the mechanism cannot be established then the incident can safely be removed from further consideration. It should not be deleted entirely, as inclusion demonstrates a comprehensive enquiry. This is not the same as establishing a very low likelihood.

EXAMPLE 18 – REJECTED POTENTIAL MAJOR INCIDENTS

- Hydrogen sulphide is present in a waste gas stream at a facility, and for environmental reasons the waste stream is sent to a thermal oxidiser. When conducting its Safety Assessment, the facility investigated if a leak from a hole in the duct to the thermal oxidiser could lead to a major incident. After carefully considering the maximum possible concentration of hydrogen sulphide, pressure in the duct and toxic exposure criteria, the facility concluded that people would not be put at serious risk unless they put their head in the hole in the duct (which was several metres above ground level). Hence this scenario was rejected as a potential major incident.
- Release of a very small quantity of a toxic material may only be sufficient to cause irritation rather than hospitalisation or fatality (inventory/toxicity combination insufficient).
- A tsunami impacting an aboveground tank located 100 km inland on a hill (diminishingly small likelihood).
- BLEVE of an underground LPG tank (burying the tank, however, introduces other loss of containment mechanisms which must be proven to be under control).
- A Schedule 15 chemical that is known to decompose exothermically at temperatures over 200°C is stored in full sunlight, away from fire risk material. The team could not establish a mechanism where the Schedule 15 chemical would approach 200°C.
- Opening a drain line on a vessel that could contain volatile components was considered a possible cause of low temperature and thus brittle fracture at one facility. However, flash calculations showed that the temperature would not fall low enough, even with the most volatile composition and highest pressure conditions.

EXAMPLE 19 – INCORRECTLY REJECTED MAJOR INCIDENTS

- Catastrophic failure of a storage tank was rejected because the tank was designed to Australian Standards and had pressure safety valves, pressure alarms and high level alarms and shutdowns. A mechanism to a major incident still exists.
- Electrical failure resulting in loss of control of reaction and hence potential runaway reaction, release and explosion was rejected because of a back-up power supply. A mechanism to a major incident still exists, even if it is a double-jeopardy situation.
- Mixing of incompatible materials in a storage warehouse was rejected because procedures state that they must not be stored together. Procedural controls do not remove the potential major incident.

These major incidents have been incorrectly rejected on the basis of the implemented controls. The major incidents can still occur.

VALIDATE THE MAJOR INCIDENT PATHWAYS

The objective is to gain a detailed understanding of what can go wrong in order to correctly assess what controls are necessary, and what performance standards are required. It is important to pursue understanding to sufficient depth that all avenues are uncovered to allow effective controls to be put in place. Work done at this stage is used later in consequence and likelihood analysis.

It is reasonable to focus effort in understanding the major incidents of highest concern (highest consequence and/or highest risk).

EXAMPLE 20 – UNDERSTANDING CORROSION AS AN INITIATOR

A HAZOP team identified the potential for corrosion to cause a loss of containment. It is necessary to further understand this hazard as there are a variety of approaches available to control it:

- Corrosion from erosion may be controlled by velocity.
- Internal corrosion from acid attack may be controlled by regulation of pH and monitoring of coupons.
- External “under insulation” corrosion occurs more often in dead legs and cannot occur above certain temperatures.
- Stress corrosion cracking prevention may require maintenance of water concentration within a certain range.

EXAMPLE 21 – UNDERSTANDING HOW THE EQUIPMENT IS DESIGNED TO FAIL

Engineers may design equipment with the intent that it shall "leak before break", giving the operators time to either isolate or remove the items before there is sufficient quantity to cause a major accident. The incident pathway is not eliminated, but the probability of the major incident is reduced. Examples include the following:

- LPG hoses are designed to leak before breaking. The hose can be safely taken out of service without a major incident even if it does leak.
- LPG hoses tend to creep as they deteriorate. Spraying the hose connection with paint allows detection of this creep and removal before any leak takes place.
- Piping carrying coolant to a nuclear reactor is designed so that a crack will grow through the wall, causing a leak that can be detected by leak detection systems before the crack would grow to a catastrophic guillotine failure.

5. SAFETY ASSESSMENT

5.1 Identification of controls

A control measure, in relation to a risk to health and safety, means a measure to eliminate or minimise the risk. Controls that eliminate or minimise the risk of a major incident occurring (i.e. impact on either likelihood or consequence) are sometimes referred to as preventative or preventive controls, while those which minimise the magnitude and severity of the consequences if a major incident occurs are referred to as mitigative. Controls may also be described by other terms, such as active or passive, engineering, organisational, administrative or physical, and hardware or software.

There are usually a range of controls available to an operator. In selecting controls, the hierarchy of controls must be considered in order as follows:

- substitution of a hazard by a hazard with a lesser risk
- isolating the hazard from the person at risk
- minimising the risk by engineering means
- minimising the risk by administrative means
- using personal protective equipment.

Selection of controls should be based on what is reasonably practical to reduce the risk. The safety assessment should identify existing controls and potential controls. This includes consideration of recognised and generally accepted good engineering practice (RAGAGEP), best practice, emerging technologies, published codes of practice and industry standards, as well as what is currently present.

When identifying controls it is important to understand what needs to happen for the control to be effective and manage that control in its entirety (this is discussed further in control of risk). For example, an alarm without an operator able to notice it and respond has no safety benefit. A procedure only has a safety benefit if it is technically adequate and personnel are trained, equipped and expected to use it. Engineering standards are only of benefit if they deal with the issue at hand and are applied.

The safety assessment must include the range of control measures the operator has decided to implement. The safety assessment should identify those controls that are absolutely necessary to avoid a major incident. They should be reliable and fail-safe. Some will already be defined; some will be identified in the course of the safety assessment.

5.2 Consequence estimation

CONSEQUENCE MODELLING (NO CONTROLS)

Any major incident has a range of potential consequences. The operator must identify the worst consequence of a major incident where no controls are in place. The basis of this calculation (inventory, external conditions, etc.) should be clearly documented and discussed.

The intent is to understand and be prepared for the worst major incident. Premature focus on the associated risk misses the opportunity to decide that the consequence is not to be tolerated on any account (as has been decided by many oil companies about locating temporary maintenance building near vents after the Texas City incident, and why society has deemed it inappropriate to have childcare centres adjacent to MHFs).

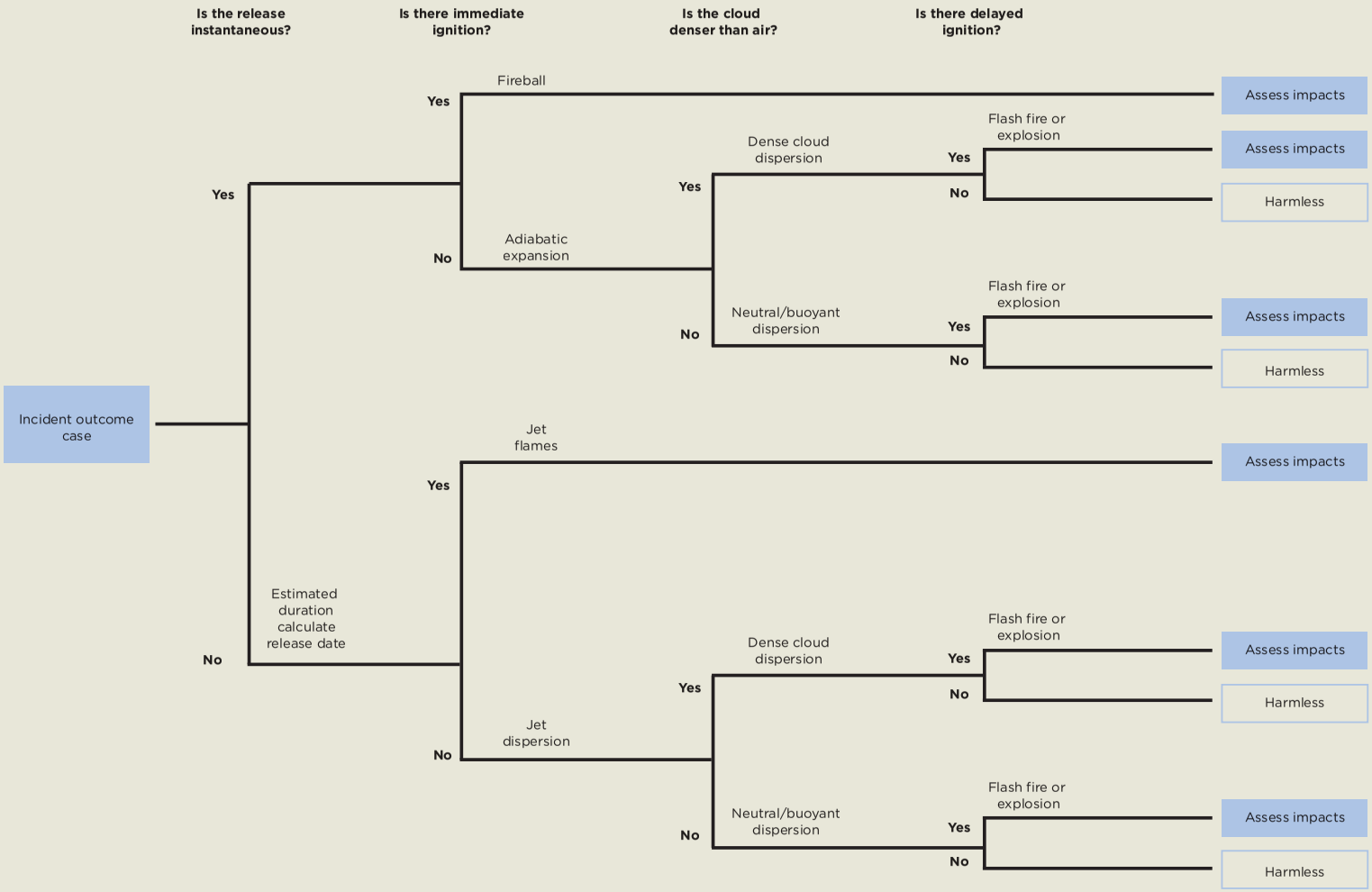
EXAMPLE 22 – CONSEQUENCE ANALYSIS OF A WAREHOUSE FIRE

ABC Warehousing was a MHF storing pesticides, flammable liquids, a small amount of flammable gases and general merchandise. They concluded that a fire at the warehouse would:

- generate a toxic plume, with possible rain-out of toxic material at the edges
- generate significant heat, potentially affecting neighbours
- generate projectiles and possibly fireballs
- generate significant quantities of contaminated fire-water run-off that would need to be contained.

They concluded that the near neighbours (up to 500 m) could be affected. The number of people affected would depend on the time of day. The nearest sensitive receptor was a residence 1 km away, unlikely to be affected by any event at the warehouse. A nearby office building, however, had significant amounts of glass facing the facility that could be particularly vulnerable to heat. The facility chose to commission modelling to establish the potential and recommend options to minimise potential impact in the event of a fire.

EXAMPLE 23 – CONSEQUENCE ANALYSIS FOR LOSS OF CONTAINMENT OF FLAMMABLE GAS



An operator of a MHF storing and handling significant quantities of LPG used the above event tree to identify the possibility of a BLEVE, a jet fire and vapour cloud explosion at their facilities. They modelled a BLEVE of the biggest tank caused by a sustained jet fire from the adjacent tank, a jet fire from the adjacent tank (to confirm if the second tank could be affected), a vapour cloud explosion and a BLEVE of a standard delivery tanker (the more likely event).

The selected modelling endpoints were heat flux and overpressure. The assumptions and methods used in the modelling were clearly stated in the relevant section of the safety assessment.

EXAMPLE 24 – POOL FIRE ASSESSMENT

ABC Chemical Company identified that a leak of flammable liquid may develop into a pool fire. They commissioned modelling to fully understand the potential consequence of such a fire.

The consultant delivered the following table:

Pool Fire in Plant Area	Pool Diameter (m)	Maximum distance from centre of the pool to heat flux of concern (kW/m²)		
		4.7	12.6	23
Pump A	20	45	32	25
Tank B	50	90	70	57
Met	10	35	24	16

The model gives estimates of distance to specified end-points of concern. In this example, the criteria and the predicted consequences are the same as in HIPAP 4.

A heat flux of 4.7kW/m² is considered high enough to trigger injury to people after 30 seconds exposure. This is particularly relevant to people who are unable to evacuate or seek shelter.

A heat flux of 12.6 kW/m² has a significant chance of fatality for extended exposure. At this level steel may reach a thermal stress level high enough to cause structural failure.

A heat flux of 23 kW/m² has a chance of fatality for instant exposure. Pressure vessels need to be relieved to avoid failure.

These results were used to validate the potential for knock-on events and incorporated into the quantitative risk assessment for the site.

SENSITIVITY ANALYSIS

The actual consequence of an event will be the result of a number of factors and is unlikely to be the worst case. It is important to understand which factors are important and how the consequence severity varies with variation in those factors (a sensitivity analysis). This allows the operator to understand the performance requirements for any emergency response system.

EXAMPLE 25 – WAREHOUSE FIRES

ABC Warehousing understood that the ferocity of the fire depends upon:

- the nature of the stored chemicals (for example, flammable liquids ignite easily)
- how the chemicals are stored (combustible materials add to fire load; high racking may inhibit sprinkler systems; packages of flammable liquids may burst with heat, ignite and spread fire throughout the bund compound)
- how long it takes to detect the fire (automatic vs manual detection)
- if the fire is caught early enough (small fires are easily extinguished).

The nature of the (toxic) smoke plume depends on:

- wind speed and direction
- fire temperature (there are different stages of a fire, with different temperature profiles)
- the nature of the burning chemicals.

The operator realised that weather conditions and inventory had the greatest impact on the consequence zone. The time of day also had a significant influence on how many people were likely to be affected. As the operator cannot control the weather, it was decided to focus on preventing the incident, and ensuring fast communications and response if an incident did occur.

CONSEQUENCE MODELLING WITH CONTROLS

The assessment of consequence with controls represents the most likely consequence.

All facilities benefit from being aware of the most likely consequence when determining priorities. Management should control the most likely events and simultaneously avoid the worst events. They can be different major incidents.

USING THE CONSEQUENCE MODELLING

A common mistake is to commission consequence and risk modelling from a consultant, fail to validate the results and fail to utilise the information in emergency response planning, in both the location of equipment and offices and in the identification of potential knock-on events.

When commissioning modelling, the facility operator should consider if it would be advantageous to complement fatality calculations with distances to injury or even distances to irritation/nuisance to fully understand the potential consequences. This may improve the understanding of the potential consequences, facilitate effective management of events and potentially justify additional protective measures.

KNOCK-ON EVENTS

An operator needs to ensure that they have addressed any potential events that may act as a knock-on event. Modelling effect ranges allows the operator to determine if it is reasonably foreseeable for one major incident to escalate and cause another.

Major incidents may also be triggered by significant process safety events associated with non-Schedule 15 chemicals that knock on or effect systems storing or handling Schedule 15 chemicals.

EXAMPLE 26 – KNOCK-ON EVENTS

- A small fire in a drum decanting operation could spread to an adjacent large drum store via a common drain system.
- A boiler ruptures when the drum level reduces below the fire line. Projectiles damage the adjacent control room, leading to a loss of control of a production unit processing Schedule 15 chemicals.
- A rupture of a large nitrogen storage vessel causes local evacuation and prevents operators from responding to a dangerous process excursion.

The escalation potential may warrant specific analysis and control of the initiating event, rather than using the generic initiator of "fire", "loss of control system" and "operator fails to intervene (operator error)".

CONSEQUENCE RANKING

The regulations do not strictly require the risks to be ranked or otherwise placed into a category. It is, however, very common to do so. Ranking allows the operator to prioritise resources in a coherent and traceable way. Many organisations have also set up governance structures around what the organisation determines to be acceptable or unacceptable, and specified required courses of action accordingly.

EXAMPLE 27 – CONSEQUENCE RATING

The following example is loosely based on Appendix C of the Code of Practice: Managing Risks of Hazardous Chemicals.

Consequence	Examples
Insignificant	■ Minor loss of containment ■ Potential chemical exposure ■ No adverse effect on workers' health and safety ■ No adverse effect on the workplace, other properties and premises.
Minor	■ Minor loss of containment ■ First aid treatment ■ Small fire.
Moderate	■ Major loss of containment ■ Medical treatment injury.
Major	■ Total loss of containment ■ Multiple MTI ■ Extensive damage to workplace.
Catastrophic	■ Death or multiple deaths ■ Extensive damage to the workplace ■ Adverse impact on surrounding environment.

5.3 Likelihood estimation

LIKELIHOOD ANALYSIS

The likelihood of each major incident hazard causing the major incident must be analysed.

The likelihood depends on the likelihood of the initiating event and the control effectiveness. Effectiveness is a measure of how well the control measure performs, or is likely to perform, if required. An assessment of effectiveness may include:

- functionality: ability of control to address a particular hazard
- reliability: whether control will be functional when/if required
- independence: control is not dependent on other controls functioning
- maintenance: whether control functionality can be maintained (e.g. availability of parts, access, training and knowledge)
- monitoring: whether it is possible to monitor that the control is fully functional or impaired, and how this could be done.

Other effectiveness criteria may include survivability; that is, that the control continues to function during a major incident, such as a fire or during abnormal process conditions, and cost.

Standard tools and techniques for the analysis include fault trees, event trees, LOPA and bow-tie analysis. All have been used successfully. Common mistakes are to misapply the techniques, claim benefit from controls that are not truly independent, failure to consider performance under all operating conditions and failing to validate the current performance of existing controls.

EXAMPLE 28 – BOW-TIE

ABC Warehouse Company elected to graphically represent each major incident that couldn't be eliminated using a bow-tie diagram. They then identified all existing controls in place, what other controls could be in place, the quality and effectiveness of those controls, and whether the controls were good enough. This was documented using a likelihood table.

Likelihood	What it means
Certain to occur	■ Expected to occur in most circumstances
Very likely	■ Will probably occur in most circumstances
Possible	■ Might occur occasionally
Unlikely	■ Could happen at some time.
Rare	■ May happen only in exceptional circumstances

EXAMPLE 29 – EVENT TREE ANALYSIS

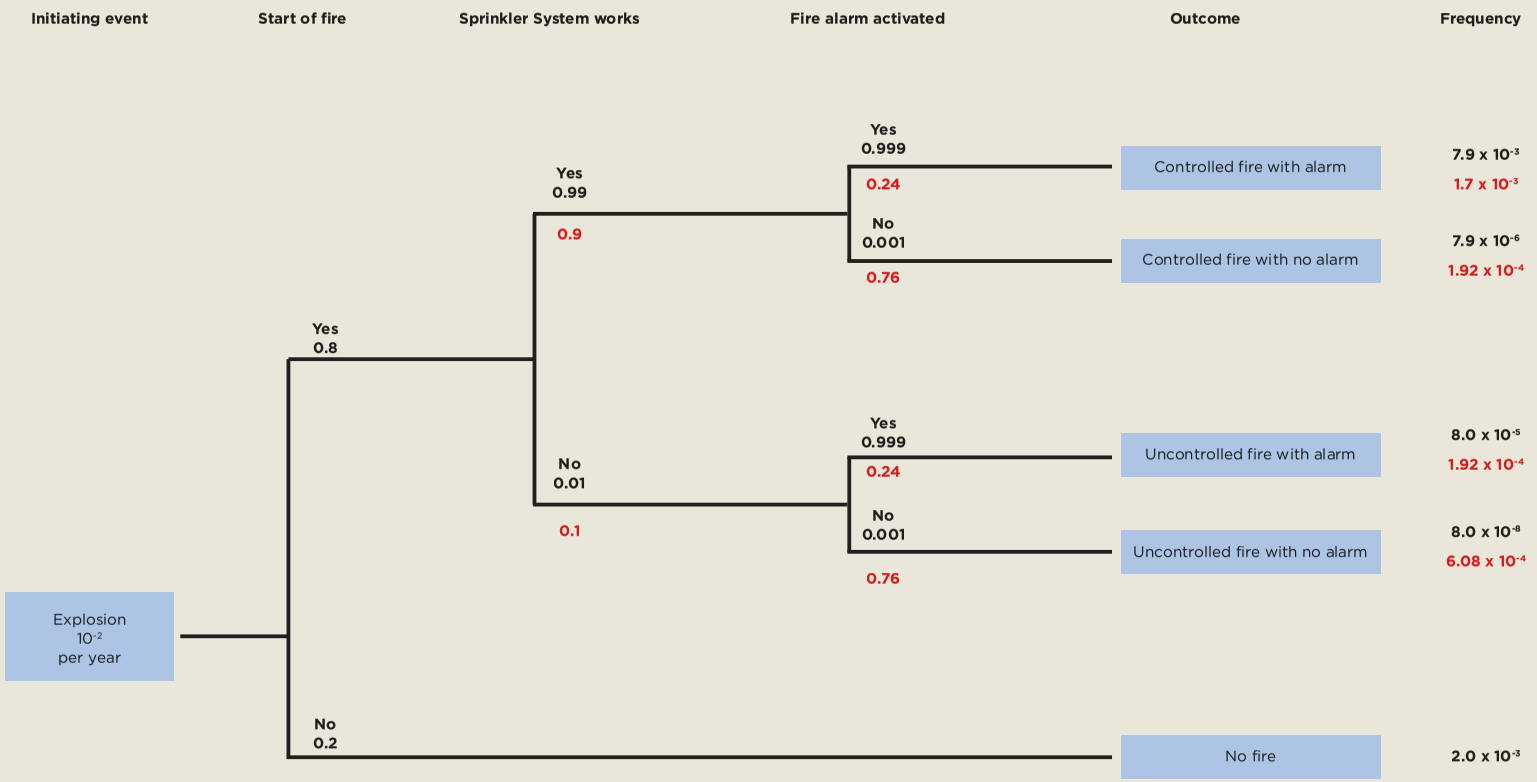
ABC Warehouse Company relied on a sprinkler system and fire alarm working to minimise the likelihood of a fire escalating. They initially thought these aspects combined gave the likelihood of a fire as unlikely.

Discussions with the operator of a neighbouring flammable gas storage facility highlighted the possibility of an explosion affecting the site. It was suggested that the sprinkler and alarm systems should be upgraded to cope with this eventuality. The company decided to quantitatively analyse the impact on likelihood of the sprinkler and alarm systems before deciding if it was reasonably practical to upgrade the systems.

The current sprinkler system was judged likely to work in controlling a fire 9 times out of 10 (probability 0.9). The new system, with enhanced reliability and functionality, would "work" in controlling the fire 99 times out of 100 (probability 0.99).

The current alarm system relied on operators informing the fire brigade. Operators were only present for 8 hours, 5 days a week, and so could at best be effective 40 hours/168hours (probability 0.24). It was assumed that the brigade would always respond. In contrast, the probability that an automated alarm system would call the brigade was 0.999. (There would also be a possible penalty of false alarms, say two per year, for which the fire brigade would charge).

The event tree is shown below. The current design figures are shown in red.



EXAMPLE 29 – EVENT TREE ANALYSIS (CONTINUED)

ABC warehouse wanted to avoid an uncontrolled fire with no alarm. This could result in serious harm to employees and customers, and the potential loss of all the stock, buildings, records, etc. and threaten the business. They took this as the worst possible extent of harm. They noticed that upgrading the systems reduced the likelihood of this worst case event by a factor of 7,600. The likelihood of better outcomes in all categories increased.

The introduction of numbers meant that they were able to meaningfully compare other options. For example, they examined the possibility of only implementing the improvement in the alarm system or implementing an improvement in the stand-alone sprinkler system. A stand-alone alarm improvement would be 50 per cent of the cost of a sprinkler plus alarm package. A stand-alone sprinkler system would be 90 per cent of the sprinkler plus alarm package cost. Armed with the estimates of likelihood, harm and (last of all) cost, they compared all of the options and decided that implementing the upgrade of the sprinkler and alarm system package was reasonably practical and the best option in their circumstances.

This methodology is consistent with the definition of reasonably practical in the WHS Act. Continued use of the qualitative assessment of "unlikely" would not have given the result required to make this decision.

EXAMPLE 30 – APPLICABLE FAILURE DATA AND USE IN A FAULT TREE

An operator of a chemical processing facility chose to use historical data on the likelihood of equipment failure using reputable sources such as Table A14.3 Appendix 14 of Lees' Loss Prevention in the Process Industries, 3rd Edition (2005). Data for some equipment is presented in forms such as:

Equipment	Failure rate (failures/106 h)
Pressure vessels (general) (high standard)	3 0.3
Pipes	0.2
Bellows	5
Relief valves - Leakage Blockage	2 0.5

The data was checked to confirm correct values and limitations and for relevance to the identified scenario. Where the conditions on site differed significantly from the source database, the data was adjusted. The adjustment and rationale was highlighted to management and the regulator.

The data was used in a fault tree analysis to estimate the frequency of a loss of containment.

It is also important to consider the influence of human factors on likelihood and including them in the safety assessment. This may be achieved by identifying the possible human factors at play and managing those factors within the safety management system. The influence of human factors is then subjectively included in the demonstration of adequacy. Quantitative human factor assessment tools are available (for example, HEART) and can be incorporated into the analysis of identified incident scenarios if appropriate or required.

EXAMPLE 31 – HUMAN FACTOR ANALYSIS

ABC Chemical Company recognised that the ability of the operators to respond to alarms was potentially affected by factors such as fatigue and workload. They implemented the following programs to promote performance:

- fatigue management program
- drug and alcohol policy
- leadership/supervision training for supervisors.

They also examined the workload during critical periods and introduced:

- additional resources for planned start-ups and shut-downs
- an alarm reduction program focused on removing alarm flooding.

LIKELIHOOD ASSESSMENT

Likelihood is either expressed qualitatively as a rating or given a numerical value as a frequency per annum. The operator must understand and document the basis of the assessment (the assumptions and incident pathway).

5.4 Risk assessment

Following the determination of likelihood and consequence, risk can be assessed.

Depending on whether a qualitative or quantitative technique was chosen, risk assessments may be expressed via a position on a risk matrix, a numerical value of individual risk per annum or similar. The risk assessment may be used to justify rankings and priorities for further work and the need for additional control measures.

EXAMPLE 32 – RISK ASSESSMENT

QUANTITATIVE

ABC Company conducted a quantitative risk assessment (QRA), which considered an ammonia release from one of three identical tanks at their premises as well as releases from transfer pumps, piping and other items of equipment. The analysis used industry data on failure rates for items of equipment to calculate likelihood and consequence modelling of expected releases to determine the extent of the consequences. The results were combined on a site map to show individual risk of fatality at specific points by a risk contour as in the following diagram.

ABC Company used these results to satisfy land use planning requirements and internal risk tolerability targets. It does not, of itself, establish that the risk has been reduced so far as is reasonably practical.

EXAMPLE 33 – RISK ASSESSMENT

Qualitative

ABC Company considered an ammonia release from one of three identical tanks at their premises (Incident 1). Based on incidents at similar facilities, they decided that the likelihood was "not likely to occur" while the consequence was that a number of fatalities were possible.

			Consequence				
			Insignificant circumstances	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 (MTI)	One or more Lost Time Injuries (LTIs)	One or more significant Lost Time Injuries (LTIs)	One or more fatalities	Significant number of fatalities
LIKELIHOOD	5	Possibility of repeated events (1×10^{-1} per year)	Significant risk				
	4	Possibility of isolated incidents (1×10^{-2} per year)	Moderate risk				
	3	Possibility of occurring sometimes (1×10^{-3} per year)	Low risk				
	2	Not likely to occur (1×10^{-4} per year)					Incident 1
	1	Rare occurrence (1×10^{-5} per year)					

The company used the relative placement on the matrix to prioritise risk reduction projects. Potential major incidents in the significant risk category had to be documented and their management explained to senior officers of the company.

High risk

Significant risk

Moderate risk

Low risk

CONSIDER CUMULATIVE RISK

Regulation 555(3) requires the operator to consider all potential major incidents and major incident hazards cumulatively, as well as individually, in the safety assessment.

Cumulative risk can be considered in a number of ways:

- **Consideration of risk in aggregate:** If there are a large number of different hazards and potential incidents at a facility, the total risk may be significant even if the risk arising from each individual hazard or incident is low.
- **Consideration of risk in concert:** the evaluation of the consequences of incidents occurring in quick succession (for example, an earthquake followed by tsunami).
- **Consideration of risk by location:** It may be useful for a facility to consider whether the major incident risk is concentrated in specific locations or roles, and therefore whether any additional controls may be prudent to reduce the likelihood or consequence, and thus reduce the risk.

There is no specified quantitative risk level that is considered acceptable, so the above should not be interpreted as a requirement to conduct a quantitative risk assessment (QRA). It should also be recognised that meeting any of the quantitative risk criteria suggested or recommended by different jurisdictions does not necessarily prove that a facility has reduced risk to a level so far as is reasonably practicable.

EXAMPLE 34 – ANALYSIS OF CUMULATIVE RISK

Hazard identification had identified that there were six possible mechanisms that could lead to a major incident from a batch polymerisation reactor at a facility:

- reactor overfill
- high pressure
- runaway reaction - excess reactant added
- runaway reaction - excess catalyst
- runaway reaction - agitator failure
- agitator seal failure.

The safety assessment determined that each hazard individually was in the Medium Risk zone on a risk matrix. However, the one operator responsible for this area is exposed to the risk presented by all of them since he spends the shift close to the reactor. Therefore, cumulatively, the likelihood of the operator being exposed to a major incident is sufficient to increase the risk faced by that operator into the High Risk zone.

CONSEQUENCE

After reviewing this situation, the company decided to relocate the operator's control console, etc. to a central control room.

High risk

Significant risk

Moderate risk

RISK EVALUATION

Risk evaluation is the decision that the risks have been reduced so far as is reasonably practical and is acceptable to all stakeholders. Comparison of the level of risk found during the analysis process with risk criteria or with the standards declared in the safety policy is often a good predictor of whether risk could practicably be reduced further.

The risk evaluation has three possible outcomes:

- well below criteria: further risk reduction is probably impracticable
- sufficiently close to or above criteria for further risk reduction controls to be investigated seriously
- well above criteria: further controls need to be found or continued operation questioned.

It is very unusual for an operator to complete a safety assessment without a risk reduction program and without a list of items that are "on watch" for changes in technology or other means that may move risk reduction from impractical to reasonably practical.

EXAMPLE 35 – RISK EVALUATION

QUANTITATIVE

The results of the quantitative risk assessment (QRA) conducted by ABC Company were compared with the NSW planning criteria. This states that individual risk should not exceed 1×10^{-6} per year in residential areas[2]. This may eliminate some areas as possible locations for the operation.

2. NSW Department of Planning, Hazardous Industry Planning Advisory Paper (HIPAP) No. 4 – Risk Criteria for Land Use Planning.

EXAMPLE 36 – RISK EVALUATION

QUALITATIVE

The ranking on the risk matrix determined by ABC Company can be compared with their internal risk criteria, which state that any risk classified as a high risk must be reviewed to ensure that all potential control measures have been identified and implemented where practicable. In addition, any high risk items must be approved by management for the risk to remain without alteration.

EXAMPLE 37 – RISK EVALUATION: IMPLEMENTATION OF ADDITIONAL CONTROLS

ABC Chemical Company identified during the control measure assessment that an additional control measure (high level trip) should be considered to protect against overfilling of 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 was judged to have 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 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.

5.5 Demonstration of adequacy

The operator must demonstrate that the identified controls are adequate i.e. that the controls eliminate or reduce the risk so far as is reasonably practicable.

The following factors should be considered:

- The assessment includes both preventative and mitigative controls.
- The full range of operating and start-up/shutdown conditions has been considered.
- All identified hazards that could lead to a major incident should have at least one reliable control which acts to limit or prevent their occurrence. Defence in depth (multiple and a variety of controls) has been implemented where necessary.
- The hierarchy of controls has been applied in understanding effectiveness (the wearing of personal protective equipment and application of administrative controls are less effective than engineering solutions).
- Control independence has been considered and correctly accounted for (particularly important in quantitative assessments e.g. SIL studies).
- Critical operating parameters have been identified for all controls, compliance with which is necessary to avoid a major incident.
- Existing performance indicators for selected controls have been considered (or devised if absent), and validated against required performance standards.
- The operator should be able to show that the adopted controls are capable of maintaining operation within the identified critical operating parameters.
- Controls that have been identified but rejected during the safety assessment are recorded, together with the reason why they have not been adopted (i.e. the justification of why they are not reasonably practicable).

This is discussed further in the Major Hazards Facility Guide: Safety Case: *Demonstrating the Adequacy of Safety Management and Control Measures.*

6. CONTROL OF RISK

Regulations 556 and 566 require the operator of determined or licensed MHFs to implement risk control measures that eliminate or, if that is not reasonably practical, minimise the risk of a major incident from occurring, and to implement control measures that reduce the magnitude and severity of the consequences. The safety assessment has identified what could and should be done to minimise and control the risk; the onus is now to adopt and implement those measures.

The means of implementing and maintaining the effectiveness of the selected control measures is via the safety management system. Separate guidance is available on the requirements of a safety management system at a MHF. The following discussion emphasises the elements of the safety management system that interact directly with the safety assessment.

6.1 Performance standards and indicators

Performance standards and performance indicators are required for each adopted control to ensure the effectiveness of that control is tested and that a control failure is detected and remedied.

A performance standard is the acceptable level of response, or the required performance, for a control to be considered effective in managing the risk. Standards may include both the current required level of performance and also a target level to be achieved within a specified timeframe.

A performance indicator is an objective measure that shows current and/or past performance. The overall effectiveness of the control measure can then be judged by comparing its performance against the performance standard.

EXAMPLE 38 – PERFORMANCE INDICATORS AND STANDARDS FOR CONTROL MEASURES

General standards may be set up for completion of testing, calibration or maintenance within a fixed timeframe.

Control Measure	Performance Indicator	Performance Standards
PSV	Pop test pressure	Within + or - 2% of set pressure 98% function at set pressure
Operating Procedure	Compliance check	0 major deviations ≤ 1 minor deviation

For the pressure safety valve in the table above, the corrective action in the event of failure (i.e. not relieving at the set pressure) may be replacement, re-calibration or a reduction in the test interval, depending on the valve and service. The second performance standard may be reported to management, while the first is used primarily as a guide for maintenance personnel to determine what their action should be in response to failure.

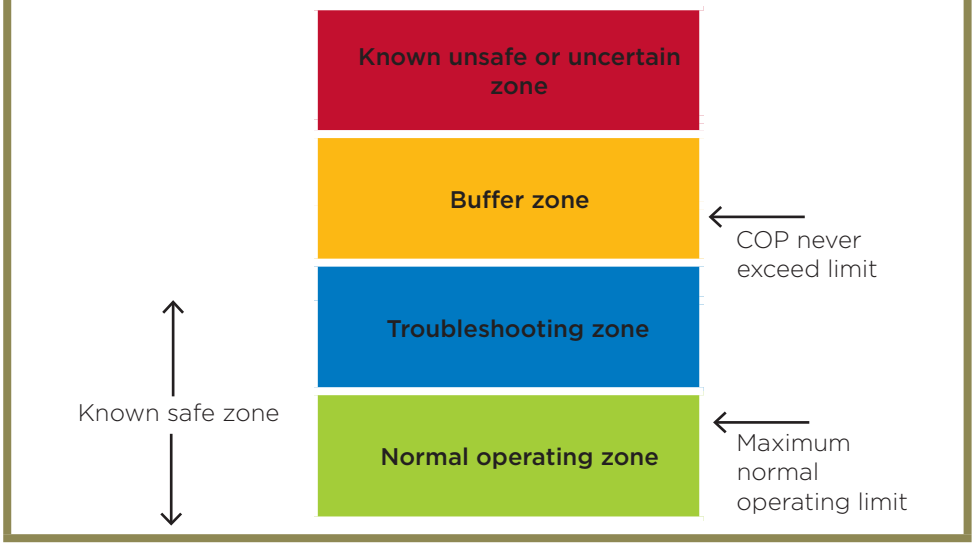
6.2 Critical operating parameters

Critical Operating Parameters (COPs) are the upper or lower performance limits of any equipment, process or procedure that, if not complied with, could result in a major incident. COPs define the safe operating envelope for a facility, where any exceedence could undermine the safe operation of the facility.

Generally, the main difference between a COP and a performance standard is that COPs are continuously monitored and managed, while performance against a performance standard is generally periodically assessed (and included in the audit component of the safety management system).

The operator should ensure that the critical operating parameters are monitored and excursions outside the safe operating zone are minimised.

FIGURE 2: Safe operating zone and identification of critical operating parameters



EXAMPLE 39 – CRITICAL OPERATING PARAMETERS

Typical COPs in use at some MHFs include:

- facility minimum manning level
- the number of fire pumps available
- maximum operating pressure of a pressure vessel
- minimum operating temperature
- maximum reactant addition rate for a reactor
- minimum cooling water flow rate for a reactor
- maximum running hours before service of a forklift truck
- maximum rpm of a high speed turbine
- maximum number of pallets to be stored in a specific area
- maximum height or number of vertically stacked pallets in a storage area.

7. REVIEW OF RISK MANAGEMENT

Determined and licensed MHFs must review and, as necessary, revise the safety assessment:

- if there is a modification
- if a control measure does not minimise the risk so far as is reasonably practicable (e.g. in the event of an incident or near miss, or the performance standard is not being met)
- if new hazards are identified
- if there is a reasonable belief that it needs review
- at least every five years.

The monitoring and review of control measure performance is a core component of the safety management system.

EXAMPLE 40 – MONITORING AND REVIEW

ABC Company reviews the control measure performance results at a monthly safety meeting, which includes maintenance and operations personnel, a health and safety representative and the site manager. Control measure performance results are grouped for presentation. The safety management system performance is also reported at this meeting.

ABC Company has also established linkages in its systems that require review of the safety assessment if an incident occurs at the facility or at a similar operating facility. Incident investigation triggers a review of the safety assessment, as does the reporting of a near-miss event and activation of the site emergency plan. Change management is another system that may also trigger a review of the safety assessment.

APPENDIX A - REVIEW OF RISK MANAGEMENT

OPERATORS OF DETERMINED MAJOR HAZARD FACILITIES

Regulation	Requirement
554	**Identification of major incidents and major incident hazards** (1) The operator of a determined major hazard facility must identify: (a) all major incidents that could occur in the course of the operation of the major hazard facility; and (b) all major incident hazards for the major hazard facility, including major incident hazards relating to the security of the major hazard facility. (2) In complying with subregulation (1), the operator must have regard to any advice and recommendations given by: (a) the emergency service organisations with responsibility for the area in which the major hazard facility is located; and (b) any government department or agency with a regulatory role in relation to major hazard facilities. (3) The operator must document: (a) all identified major incidents and major incident hazards; and (b) the criteria and methods used in identifying the major incidents and major incident hazards; and (c) any external conditions under which the major incident hazards, including those relating to the security of the major hazard facility, might give rise to the major incidents.
555	**Safety assessment** (1) The operator of a determined major hazard facility must conduct a safety assessment in relation to the operation of the major hazard facility. (2) In order to provide the operator with a detailed understanding of all aspects of risks to health and safety associated with major incidents, a safety assessment must involve a comprehensive and systematic investigation and analysis of all aspects of risks to health and safety associated with all major incidents that could occur in the course of the operation of the major hazard facility, including the following: (a) the nature of each major incident and major incident hazard; (b) the likelihood of each major incident hazard causing a major incident; (c) in the event of a major incident occurring, its potential magnitude and the severity of its potential health and safety consequences; (d) the range of control measures considered; (e) the control measures the operator decides to implement.

Regulation	Requirement
555	(3) In conducting a safety assessment, the operator must: (a) consider major incidents and major incident hazards cumulatively as well as individually; and (b) use assessment methods (whether quantitative or qualitative, or both), that are suitable for the major incidents and major incident hazards being considered. (4) The operator must document all aspects of the safety assessment, including: (a) the methods used in the investigation and analysis; and (b) the reasons for deciding which control measures to implement. (5) The operator must keep a copy of the safety assessment at the major hazard facility.
559	**Review of risk management** (1) The operator of a determined major hazard facility must review and as necessary revise each of the following, in accordance with this regulation: (a) the safety assessment conducted under regulation 555 in order to ensure the adequacy of the control measures to be implemented by the operator; (b) the major hazard facility's emergency plan; (c) the major hazard facility's safety management system. (2) Without limiting subregulation (1), the operator must conduct a review and revision in each of the following circumstances: (a) a modification to the major hazard facility is proposed; (b) a control measure implemented under regulation 556 does not minimise the relevant risk so far as is reasonably practicable; **Example** An effectiveness test indicates a deficiency in the control measure. (c) a new major hazard risk is identified; (d) the results of consultation by the operator under Part 9.5 indicate that a review is necessary; (e) a health and safety representative requests the review; (f) the regulator requires the review.

Regulation	Requirement
559	(3) In reviewing and revising the emergency plan, the operator must consult with the emergency service organisations referred to in Regulation 557(2). (4) For the purposes of subregulation (2)(e), a health and safety representative at a workplace may request a review if the representative reasonably believes that: (a) a circumstance referred to in subregulation (2)(a), (b), (c) or (d) affects or may affect the health and safety of a member of the work group represented by the health and safety representative; and (b) the operator has not adequately conducted a review in response to the circumstance.
564	**Identification of major incidents and major incident hazards** (1) The operator of a licensed major hazard facility must identify: (a) all major incidents that could occur in the course of the operation of the major hazard facility; and (b) all major incident hazards for the major hazard facility, including major incident hazards relating to the security of the major hazard facility. (2) In complying with subregulation (1), the operator must have regard to any advice and recommendations given by: (a) the emergency service organisations with responsibility for the area in which the major hazard facility is located; and (b) any government department or agency with a regulatory role in relation to major hazard facilities. (3) The operator must document: (a) all identified major incidents and major incident hazards; and (b) the criteria and methods used in identifying the major incidents and major incident hazards; and (c) any external conditions under which the major incident hazards, including those relating to the security of the major hazard facility, might give rise to the major incidents. (4) All major incidents and major incident hazards identified and documented under Regulation 554 in relation to the major hazard facility are taken to have been identified and documented under this regulation.
565	**Safety assessment** The operator of a licensed major hazard facility must keep a copy of the safety assessment documented under Regulation 555 as revised under Part 9.3 and this Part at the facility.

Regulation	Requirement
569	**Review of risk management** (1) The operator of a licensed major hazard facility must review and as necessary revise the following, in accordance with this regulation: (a) the safety assessment for the facility in order to ensure the adequacy of the control measures to be implemented by the operator; (b) the major hazard facility's emergency plan; (c) the major hazard facility's safety management system. (2) Without limiting subregulation (1), the operator must conduct a review and revision in each of the following circumstances: (a) a modification to the major hazard facility is proposed; (b) a control measure implemented under regulation 566 does not minimise the relevant risk so far as is reasonably practicable; **Example** An effectiveness test indicates a deficiency in the control measure. (c) a new major hazard risk is identified; (d) the results of consultation by the operator under Part 9.5 indicate that a review is necessary; (e) a health and safety representative requests the review; (f) the regulator requires the review; (g) at least once every 5 years. (3) In reviewing and revising the safety assessment, the operator must comply with the requirements set out in Regulation 555(2), (3) and (4). (4) In reviewing and revising the emergency plan, the operator must consult with the emergency service organisations referred to in Regulation 557(2). (5) For the purposes of subregulation (2)(e), a health and safety representative at a workplace may request a review if the representative reasonably believes that: (a) a circumstance referred to in subregulation (2)(a), (b), (c) or (d) affects or may affect the health and safety of a member of the work group represented by the health and safety representative; and (b) the operator has not adequately conducted a review in response to the circumstance.

APPENDIX B - DEFINITIONS

BLEVE is an acronym for Boiling Liquid Expanding Vapour Explosion, which arises from the sudden rupture (due to fire impingement) of a vessel/system containing liquefied flammable gas under pressure. The immediate ignition of the expanding fuel-air mixture leads to intense combustion creating a fireball, a blast wave and potential missile damage.

Comprehensive process means a process that is complete, broad, extensive and thorough.

Consequence means the degree of harm that might result from a major incident

Change at a facility includes:

a change to any plant, structure, process or chemical or other substance used in a process, including the introduction of new plant, a new structure, a new process or a new chemical

- a change to the quantity of Schedule 15 chemicals present or likely to be present at the facility
- a change to the operation, or the nature of the operation, of the facility
- a change in the safety role of workers
- a change to the safety management system
- an organisational change at the facility, including a change in senior management of the facility.

Control measure, in relation to risk to health and safety, means a measure to eliminate or minimise the risk.

Critical operating parameters - the upper or lower performance limits of any equipment, process or procedure, compliance with which is necessary to avoid a major incident.

Hazard means a situation or an intrinsic property with the potential to cause harm to people, property, or the built or natural environment

Hazard identification is the systematic and comprehensive process of identifying hazards.

IRPA is the calculated individual risk of fatality per annum at a specified location

Local community, in relation to a major hazard facility, means the community in the surrounding area

Magnitude, in relation to a major incident, refers to the scale, size, range or extent of the major incident consequence.

Major hazard facility (MHF) means a facility:

- at which Schedule 15 chemicals are present or likely to be present in a quantity that exceeds their threshold quantity
- that is determined by the regulator under Part 9.2 to be a major hazard facility.

Major incident at a major hazard facility is an occurrence that:

- results from an uncontrolled event at the major hazard facility involving, or potentially involving, Schedule 15 chemicals
- exposes a person to a serious risk to health or safety emanating from an immediate or imminent exposure to the occurrence.

An **occurrence** includes any of the following:

- escape, spillage or leakage.
- implosion, explosion or fire.

Major incident hazard means a hazard that could cause, or contribute to causing, a major incident.

Major incident pathway is the process or sequence by which the major incident hazards develop into a major incident. Depending on the incident process model adopted, this includes how the initiators, contributing factors, enabling conditions, system failures and mechanisms come together into the incident.

Major incident scenario – see major incident pathway.

Modification is a reference to a change at the facility that has or would have the effect of:

- creating a major incident hazard that has not previously been identified
- significantly increasing the likelihood of a major incident occurring
- in relation to a major incident that may occur, significantly increasing:
  - its magnitude
  - the severity of its health and safety consequences.

Near miss means an uncontrolled or unintended event or condition involving Schedule 15 chemicals that is of low consequence, but has the potential to escalate to a major incident. They may include abnormal occurrences that are controlled or detected failures in major incident controls.

Operator

- in relation to a facility, means the person conducting the business or undertaking of operating the facility, who has:
  - management or control of the facility
  - the power to direct that the whole facility be shut down
- in relation to a proposed facility, means
- the operator of a proposed facility that is an existing workplace
- the person who is to be the operator of a proposed facility that is being designed or constructed.

Performance indicator is an objective measure which shows current and/or past performance.

Performance standard is the acceptable level of response, or the required performance, for a control to be considered effective in managing the risk.

Recognised and Generally Accepted Good Engineering Practice (RAGAGEP) is a term referred to by OSHA and the EPA in the USA and are “engineering, operation, or maintenance activities based on established codes, standards, published technical reports or recommended practices (RP) or a similar document. RAGAGEPs detail generally approved ways to perform specific engineering, inspection or mechanical integrity activities, such as fabricating a vessel, inspecting a storage tank, or servicing a relief valve.”

Risk is the likelihood of a specific level of harm occurring from a hazard.

Risk assessment involves considering what could happen if someone is exposed to a hazard and the likelihood of it happening.

Risk control means taking action to eliminate health and safety risks so far as is reasonably practicable, and if that is not possible, minimising the risks so far as is reasonably practicable.

Safety assessment is the process by which the operator of a major hazard facility systematically and comprehensively investigates and analyses all aspects of risks to health and safety associated with all major incidents that could occur in the course of the operation of the major hazard facility.

Safety case is a written presentation of the technical, management and operational information covering the hazards and risks that may lead to a major incident at a major hazard facility and their control, and which provides justification for the measures taken to ensure the safe operation of the facility.

Schedule 15 chemical means a hazardous chemical that:

- is specified in Schedule 15, table 15.1 of the WHS Regulations
- belongs to a class, type or category of hazardous chemicals specified in Schedule 15, table 15.2 of the Regulations.

SLOD is a description of the exposure conditions, in terms of airborne concentration and duration of exposure, which would produce Significant Likelihood of Death in the general population, used in land use planning by the Health and Safety Executive, UK.

SLOT is a description of the exposure conditions, in terms of airborne concentration and duration of exposure, which would produce a Specified Level of Toxicity in the general population, used in land use planning by the Health and Safety Executive, UK.

Severity, in relation to a major incident, means the effect of the major incident on the health and safety of nearby people.

Surrounding area, in relation to a facility, means the area surrounding the facility in which the health and safety of persons could potentially be adversely affected by a major incident occurring.

Threshold quantity, in relation to a Schedule 15 chemical, means:

- the threshold quantity of a specific hazardous chemical as determined under clause 3 of Schedule 15
- the aggregate threshold quantity of 2 or more hazardous chemicals as determined under clause 4 of Schedule 15 (regulation 5).

Threshold quantities are used in the notification and determination of a major hazard facility.

Worst case means the worst consequence arising from each identified incident scenario. This normally involves the total failure of risk control measures and the maximum inventory available in the incident. This is used as a guide for understanding the possible consequences and may not necessarily be a realistic scenario.

APPENDIX C - REFERENCES

REFERENCE TEXTS
Lees' Loss Prevention in the Process Industries

Guidelines for Developing Quantitative Safety Risk Criteria CCPS

Guidelines for Chemical Process Quantitative Risk Analysis CCPS

Guidelines for Safe Warehousing of Chemicals CCPS

RISK CRITERIA
NSW Department of Planning, Hazardous Industry Planning Advisory Paper (HIPAP) No. 4 – Risk Criteria for Land Use Planning.

STANDARDS
AS/NZS ISO 31000:2009 Risk management – Principles and guidelines

AS IEC 60300 Dependability Management

AS IEC 61511 Functional safety – Safety instrumented systems for the process industry sector

TOOLS/TECHNIQUES
IEC/ISO 31010:2009 Risk management – Risk assessment techniques

AS IEC 60812 – 2008 Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)

AS IEC 61511 Functional safety – Safety instrumented systems for the process industry sector

Lees' Loss Prevention in the Process Industries

THIS GUIDE PROVIDES INFORMATION FOR THE OPERATOR OF A MAJOR HAZARD FACILITY ON HOW TO CONDUCT A SAFETY ASSESSMENT FOR THE FACILITY.