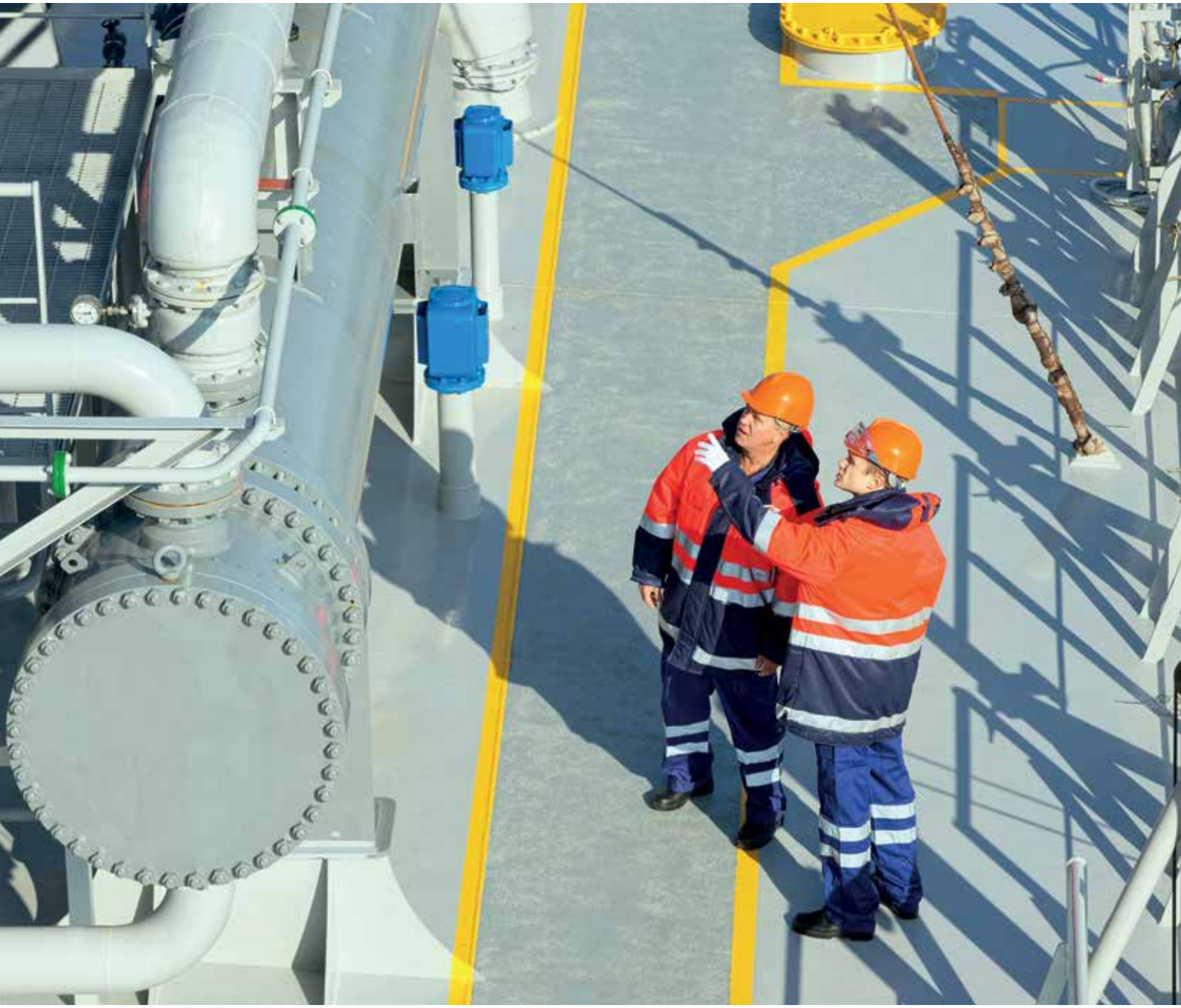
Exhibit M

GOOD PRACTICE GUIDELINES

MAJOR HAZARD FACILITIES: Safety Assessment

JULY 2016



New Zealand Government

WORKSAFE NEW ZEALAND | MAHI HAUMARU AOTEAROA

This guideline offers advice on how to conduct a safety assessment that meets the requirements of the Health and Safety at Work (Major Hazard Facilities) Regulations 2016.

ACKNOWLEDGEMENTS

In recognition of the valuable contribution made towards the development of this guideline, WorkSafe New Zealand (WorkSafe) would like to thank the members of the guidance group and those who provided input and feedback during reviews and consultation.

WorkSafe would also like to acknowledge the following organisations for providing information used to develop this guideline:

> Health and Safety Executive (UK)

> National Offshore Petroleum Safety and Environmental Management Authority (Australia)

> Safe Work Australia

> WorkSafe Victoria (Australia).

SAFETY ASSESSMENT KEY POINTS:

Operators of designated upper tier major hazard facilities must conduct a safety assessment.

Operators of designated lower tier major hazard facilities must conduct a safety assessment for the purposes of preparing and implementing the major accident prevention policy.

A safety assessment is a documented, comprehensive, and systematic investigation and analysis of all health and safety risks associated with major incident hazards.

Operators must engage with workers, and consult with the emergency services organisations and certain government agencies and consider their advice and recommendations.

TABLE OF CONTENTS

TABLES

FIGURES

01/

INTRODUCTION

IN THIS SECTION:

This guideline will help an operator conduct a safety assessment to understand all the risks to health and safety associated with potential major incidents and explain how those risks are reduced so far as is reasonably practicable.

1.1 PURPOSE AND SCOPE OF THIS GUIDELINE

The Health and Safety at Work (Major Hazard Facilities) Regulations 2016 (the MHF Regulations) identify the facilities to which the MHF Regulations apply. The status of a facility depends on the types and quantities of specified hazardous substances present or likely to be present, among other factors.

Table 1 presents an overview of the different types of facility and the corresponding obligations imposed by the MHF Regulations. The focus of this guideline is on the safety assessment.

DUTIES	EXISTING FACILITY	PROPOSED FACILITY	DESIGNATED LOWER TIER MAJOR HAZARD FACILITY	DESIGNATED UPPER TIER MAJOR HAZARD FACILITY
Notification	✓	✓		
Design notice (For a proposed facility that may exceed the upper threshold only)		✓		
Major accident prevention policy (MAPP)			✓	
Safety management system (SMS)			✓	✓
Emergency plan			✓	✓
Safety assessment			✓	✓
Safety case				✓

Table 1: Overview of duties under the MHF Regulations

1.2 WHAT IS A SAFETY ASSESSMENT?

A safety assessment is a comprehensive and systematic investigation and analysis of all health and safety risks associated with major incident hazards and major incidents. It demonstrates 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 that controls are adequate and that risk has been reduced so far as is reasonably practicable.

A safety assessment generally follows the hazard identification process although some duplication between the two processes may be necessary. Hazard identification determines the hazards and causes of major incidents and starts to identify the range of controls that provide protection against a major incident occurring. Knowledge of hazards and their

consequences is necessary for the safety assessment but only worthwhile if it informs and improves decision making and seeks to reduce risk so far as is reasonably practicable.

A systematic safety assessment employs a logical, transparent and repeatable process. This enables you as the operator to compare the range of incidents and identify which are the key contributors to the overall risk profile of the MHF.

1.3 HOW YOU CAN USE THIS GUIDELINE

This guideline is for you as an MHF operator, process safety engineer, manager, and worker of MHFs. It is for all facilities designated as MHFs and is non-industry specific.

For operators of lower tier major hazard facilities (LTMHF) this guideline will help you carry out a safety assessment proportionate to your major incident hazards. This will inform the major accident prevention policy (MAPP) and safety management system (SMS). While you are not required to carry out a safety assessment to the standard of Regulation 38, use this guideline to help you complete a proportionate safety assessment.

For operators of upper tier major hazard facilities (UTMHF) this guideline will help you with conducting the safety assessment required by the MHF Regulations.

Some industries have guidelines that deal with specific problems faced in their working environments, such as the petroleum or electricity sectors. When carrying out a safety assessment or how to do a job safely, make sure you check any industry specific guidance.

Coloured boxes summarise sections of the MHF Regulations or the Health and Safety at Work Act 2015 (HSWA).

Grey boxes contain examples. These expand on the content of the section and help in providing further clarification.

1.4 HOW THIS GUIDELINE FITS INTO THE SUITE OF GUIDELINES

Figure 1 describes how the suite of major hazard facilities good practice guidelines (GPG) interacts. The expanded detail is a simplification of the content described in this guideline.

This guideline contains advice on:

> what a safety assessment should cover
> selecting the right technique
> major incident and major incident hazard identification
> risk assessment
> identifying controls
> performance standards.

This guideline forms part of a set of guidance that includes information on:

> Emergency planning
> Major accident prevention policies
> Notifications and designation
> Safety cases
> Safety management systems.

HOW THE SAFETY ASSESSMENT LINKS TO THE SMS

The SMS is the system by which the MHF's hazards and risks can be effectively managed. The safety assessment needs to be integrated into the SMS with review and improvement processes to enable you to understand the impact on the system and any changes to the safety of the facility.

Regulation 39 requires the SMS to manage all aspects of risk control in relation to major incidents at the facility.

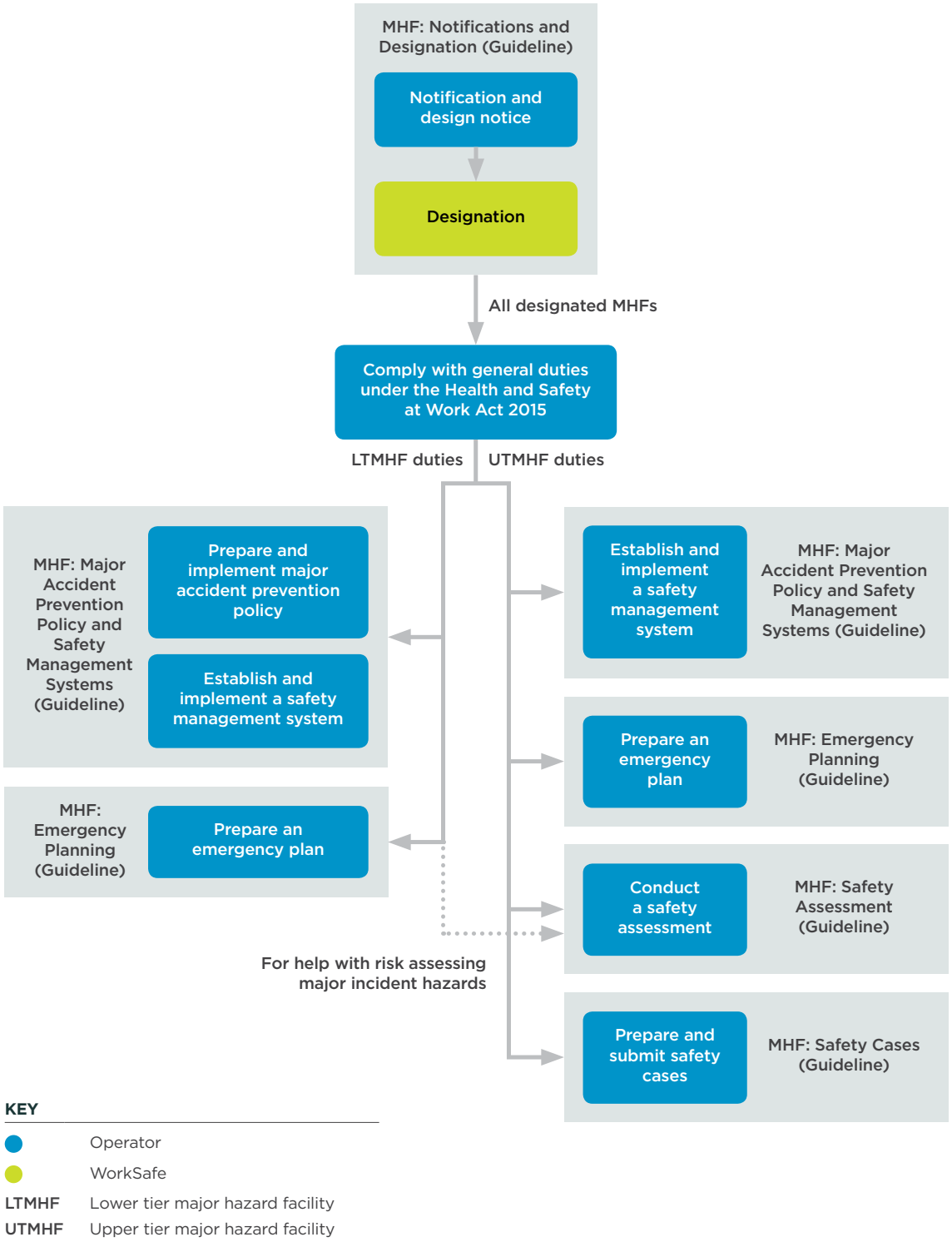


Figure 1: Overview of major hazard facilities guidelines

HOW THE SAFETY ASSESSMENT LINKS TO THE EMERGENCY PLAN

The MHF must have an emergency plan that effectively addresses all health and safety consequences of a major incident occurring. The plan must be specific to the facility's major incident hazards identified in the safety assessment.

The safety assessment will feed directly into emergency planning. So it is vital to make sure the safety assessment covers all possible areas of impact, and all possible hazards, to make sure the emergency plan covers all identified major incidents.

Regulation 31 requires the emergency plan to be specific to the facility and the major incident hazards identified in the safety assessment.

HOW THE SAFETY ASSESSMENT LINKS TO THE SAFETY CASE

The safety assessment is a key part of any safety case. It is a comprehensive and systematic investigation and analysis of all health and safety risks associated with major incident hazards and major incidents. The safety assessment should identify:

> the nature of each major incident and hazard
> hazards and conditions that could lead to a major incident
> the risk (likelihood and consequence) of each hazard causing a major incident
> its potential magnitude, and the severity of health and safety consequences in the event of a major incident
> the range of controls considered
> the implemented controls
> the rejected controls (and the reasons).

Schedule 7 requires the safety case include a summary of the safety assessment.

1.5 WORKER ENGAGEMENT, PARTICIPATION AND REPRESENTATION PRACTICES

Both you, as the operator, and workers have general health and safety duties of care. Figure 2 shows your twin duties to engage with workers and to have effective worker participation practices.

For certain duties under the MHF Regulations you must engage with, and make sure there is participation of, workers and any worker representatives who are:

> identifiable at the time
> working, or likely to be working, at the MHF.

These are stronger requirements than the twin duties placed on a person conducting a business or undertaking (PCBU) under HSWA. The set of workers the duties apply to also differ. The twin duties under HSWA only apply to workers who carry out work for the business or undertaking. In comparison, the duties under the MHF Regulations apply to any identifiable worker 'working, or likely to be working,' at the MHF.

For more information, see WorkSafe's GPG *Major Hazard Facilities: Major Accident Prevention Policy and Safety Management Systems* and WorkSafe's GPG *Worker Engagement, Participation and Representation*, which:

> describes a PCBU's two duties:
  - to engage with workers
  - to have effective worker participation practices
> provides practical advice on how to engage on health and safety matters
> describes effective worker participation practices, including representation, with examples.

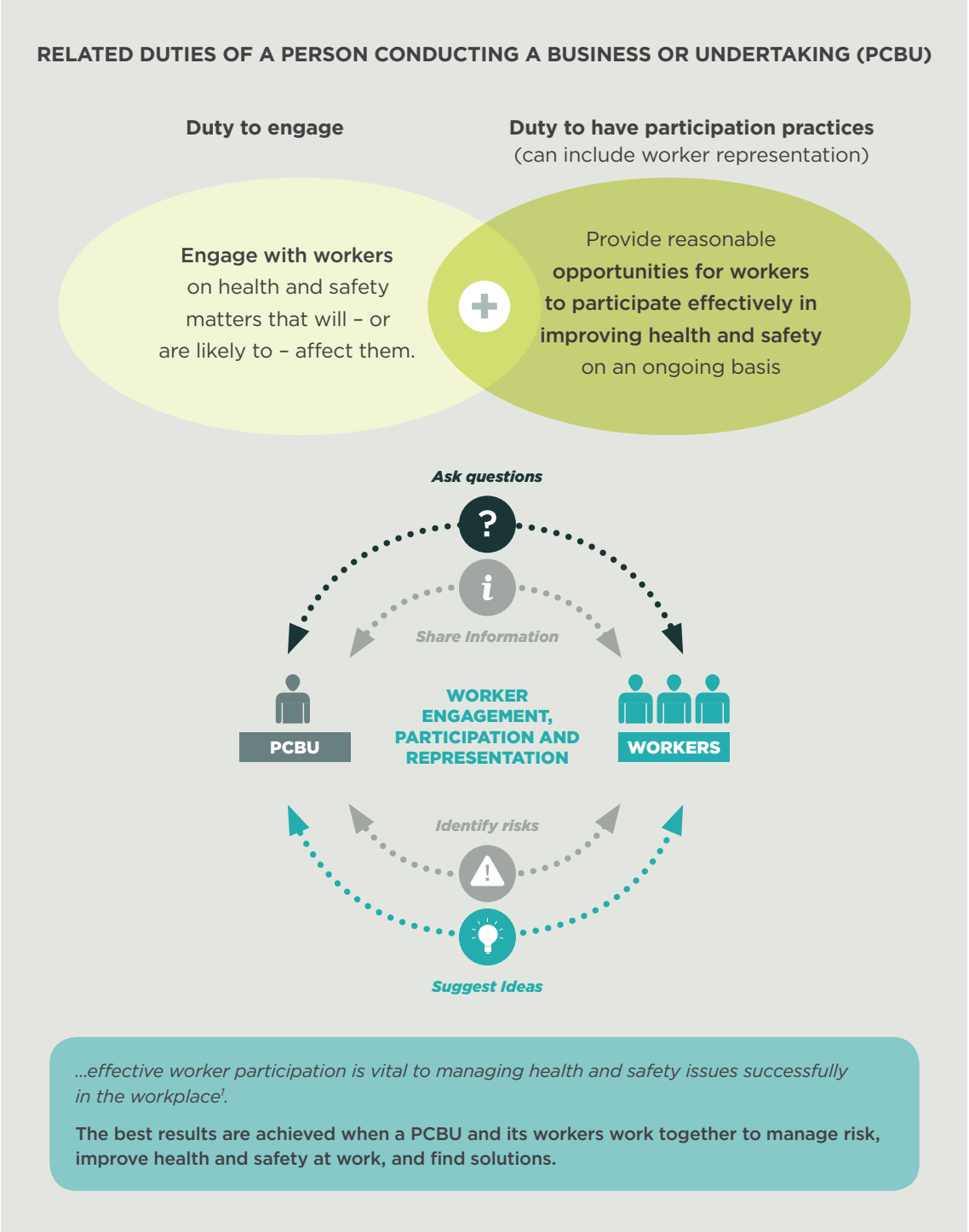


Figure 2: Worker engagement, participation and representation at a glance

[1] The Report of the Independent Taskforce on Workplace Health & Safety: He Korowai Whakaruruhau (2013) http://hstaskforce.govt.nz

02/

SAFETY ASSESSMENT OVERVIEW

IN THIS SECTION:

Go through the safety assessment process in a systematic way to identify all major incident hazards and controls.

The safety assessment should cover:

> the whole MHF and all activities on-site

> routine or abnormal operations

> any off-site hazard that could reasonably impact on the site, leading to a major incident.

2.1 EXPECTED OUTCOMES

The safety assessment should demonstrate you are reducing risks of major incidents so far as is reasonably practicable and there is ongoing review.

The outcomes of a robust safety assessment process should be:

> a list of all identified major incidents/ scenarios

> the criteria and methods used to identify the major incident hazards and major incidents

> an assessment of the cumulative effects of the major incidents:
  - incidents that could reasonably lead to initiating further incidents
  - multiple incidents from one common hazard
  - the exposure of one person or group of people to several hazards.

> identification of consequences for each major incident without controls

> analysis of risk (likelihood and consequence) for each major incident (with current controls and then with planned controls)

> identification of the local community potentially affected by the consequences of any major incident

> identification of maintenance and monitoring requirements

> the critical operating parameters identified for the selected controls

> the reasons for deciding which controls to implement with a documented justification of any potential control considered not be reasonably practicable

> a description of how the identified controls prevent or minimise the major incidents and major incident hazards

> demonstration of the adequacy of controls for each major incident, so far as is reasonably practicable

> an implementation plan for controls not yet in place

> a description of how you will review and continually update the safety assessment

> the path by which the major incident hazards could lead or have led to a major incident.

Use safety assessment tools and techniques appropriate to your facility. Make sure you can explain and justify your choice.

2.2 THE SAFETY ASSESSMENT PROCESS

Table 2 summarises the steps to take when conducting one type of safety assessment and describes some matters to consider when undertaking each step. Note that this list is an example of an approach. It is not exhaustive, and there may be other matters to consider at each step.

STEP	CONSIDER
Prepare facility description to establish context	> Establish scope: whole or part of facility, include routine and non-routine activities, on and off-site hazards. > Linkages between the facility description and hazard identification.
Gather input data/ documentation	> Facility design limits/standards. > Incident reports from facility or similar facilities. > Up-to-date facility drawings, plans and maps. > Existing studies (eg fire studies, hazard studies, mechanical integrity studies and consequence modelling). > Data on specified hazardous substances/hazardous substances, safety properties, quantities, locations, safety data sheets (SDS). > Current plant condition, maintenance history.
Select hazard identification technique	> Appropriateness of hazard identification techniques (eg quantitative or qualitative).
Establish required hazard identification team and competency	> Composition of the hazard identification team, worker engagement and participation. > Competence and expertise of the hazard identification team. > Competency and independence of the facilitator.
Determine hazard identification timing	> Appropriateness of hazard identification timing. > Sufficient time allocation for hazard identification. > Availability of team members.
Conduct assessment (see Figure 3)	> Presentation tools, format of meetings, worker involvement. > Method of documenting the safety assessment.
Documentation	> Capturing all hazard identification actions. > Justification and documentation of discarded hazard identification scenarios. > Activities and decisions are traceable and reproducible. > Documentation and recording process of the sessions (for audit purposes).
Track remedial actions	> Method for tracking and closure of remedial actions and committed further actions.
Update hazard register	> Compiling findings into a register.
Monitor and review	> Revise safety assessment as necessary, for example, if there are changes to the facility, process or new controls identified.

Table 2: Steps of the safety assessment process

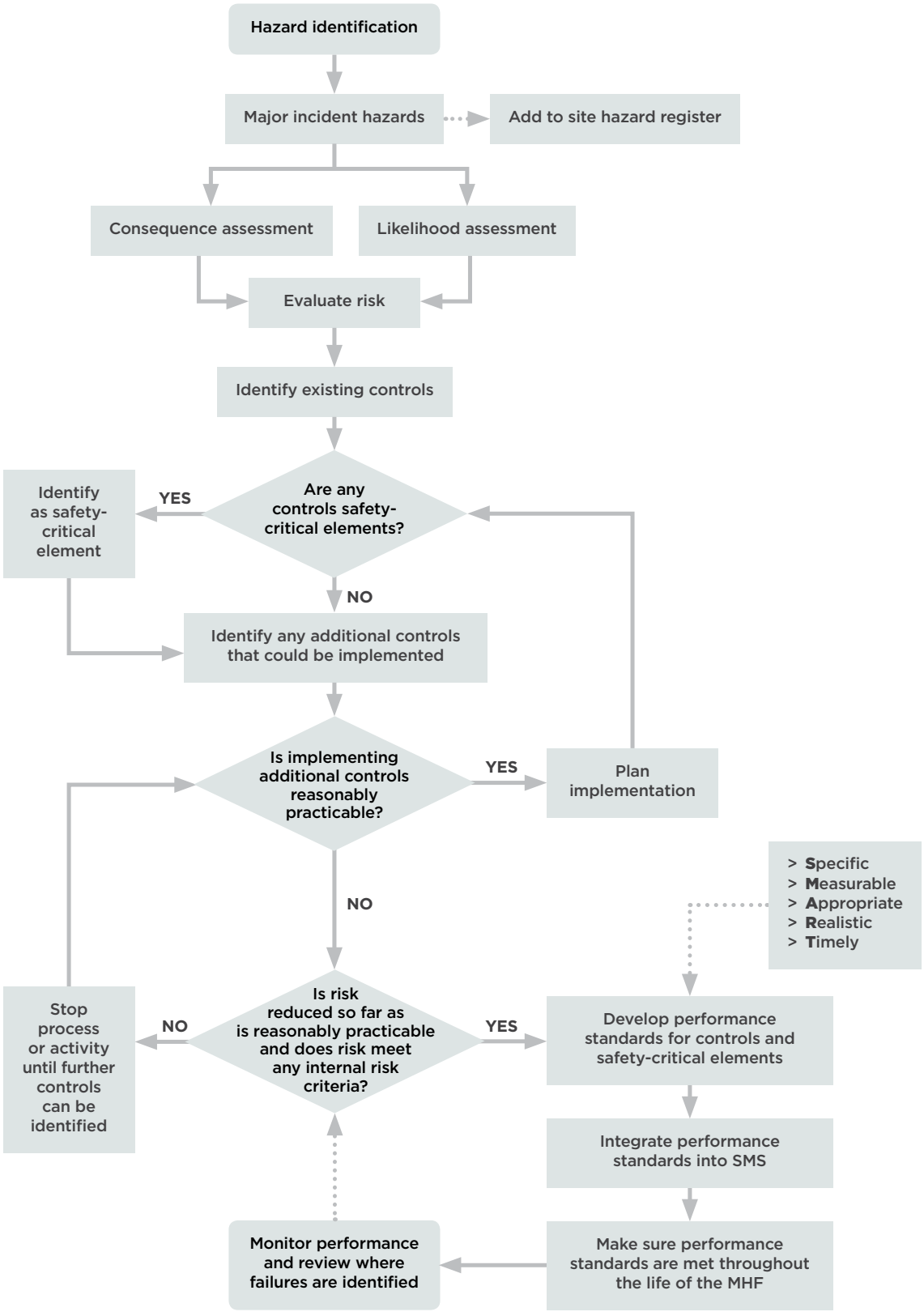


Figure 3: Safety assessment process

2.3 ENGAGEMENT AND CONSULTATION

As well as your general duties under HSWA, you have specific engagement duties under the MHF Regulations. You must engage with, and make sure there is participation of, workers and any worker representatives identifiable, and consider their advice and recommendations. You should involve workers working or likely to be working at the time, at all stages of the safety assessment process. There should be a team approach, accountability and roles assigned, and a clear plan established regarding who does what. An elected and trained health and safety representative (HSR) could be assigned to the project.

The assessment process will benefit if a cross-section of workers attends workshops, with sufficient resources allocated to them. Consider using workers who have insight into the risks, and could directly influence and advise on controls. You may choose to use workers to lead hazard identification workshops. Consider appointing external facilitators for the hazard identification and risk analysis processes.

CONSULT WITH EMERGENCY SERVICES, WORKSAFE, AND LOCAL AUTHORITIES

You must consult with the Police, Ambulance, and New Zealand Fire Service emergency services and WorkSafe. Use the information and recommendations they provide to inform the safety assessment process.

For more information on consulting with the emergency services see WorkSafe's GPG *Major Hazard Facilities: Emergency Planning*.

Regulation 38 requires the operator to engage with, and have regard to any advice and recommendations given by workers, and consult with emergency services, WorkSafe, or any government department or agency with a regulatory role in relation to MHFs.

2.4 REVIEW OF SAFETY ASSESSMENT

You must review the safety assessment on an ongoing basis. Whether this review is continuous or periodic depends on your SMS.

Continually review residual risks and determine if the risk should be re-evaluated.

Review and, as necessary, revise the safety assessment when:

- ongoing review indicates a change or proposed change to the MHF could:
  - create a major incident hazard that had not been previously identified
  - increase the likelihood of a major incident
  - increase the magnitude or severity of the consequences from a major incident.
- a control no longer minimises the risk so far as is reasonably practicable
- a new major incident hazard, or risk associated with that hazard, is identified
- the results of engagement with workers indicate that a review is necessary
- a HSR requests a review because the HSR reasonably believes that grounds for review exist (which may affect the health and safety of workers) and you have not adequately conducted a review
- there is a change of operator.

For UTMHFs, where reviews result in a significant change to the level of risk identified, you may also need to revise the safety case. For more information see WorkSafe's GPG *Major Hazard Facilities: Safety Cases*.

Example 1: Monitoring and review

Company X reviews control performance results at a monthly safety meeting, which includes maintenance and operations workers, a HSR and the site manager. Control performance results are grouped for presentation. The SMS performance is also reported at this meeting. If issues are identified with a control's performance, then the safety assessment is reviewed.

Company X has also established linkages in its systems that require review of the safety assessment if an incident occurs at the facility or one like it. Incident investigation triggers a review of the safety assessment, as does reporting a near miss event and activation of the emergency plan. Management of change (MoC) also triggers a review of the safety assessment.

Regulation 35 requires the operator to review and, as necessary, revise the safety assessment in particular circumstances.

03/

MAJOR INCIDENT AND MAJOR INCIDENT HAZARD IDENTIFICATION

IN THIS SECTION:

The safety assessment must identify all potential major incidents and the major incident hazards which can cause or contribute to them.

3.1 SELECT THE RIGHT TECHNIQUE

Apply hazard identification and safety assessment methodology suited to your operation and the major incident hazards considered. For a UTMHF, justify your reasons for technique selection in the safety case as well.

Hazards vary depending on the industry and operation. Hazards in complex chemical operations will be different from those for storage operations. Various hazard identification and assessment techniques exist that can be used successfully. Multiple techniques are usually required to adequately identify and assess all the major incident scenarios. Make sure techniques:

> are fit for the complexity and scale of the MHF
> are chosen with meaningful engagement and participation by appropriately skilled and knowledgeable workers
> consider any external conditions or facility-specific attributes
> clearly document the relationships between the major incidents, hazards, and controls
> show the reason for the safety assessment, in particular your choice of controls
> generate outputs you can use in further safety assessments and integrate in the SMS.

Identify hazards systematically using current information. Listed below are some of the commonly used techniques for hazard identification and risk assessment at different stages of an MHF's life cycle. Expect to apply multiple methods – but only use those most relevant and best suited to the MHF:

> Audit findings and pending issues
> Bow ties
> Chemical reactivity hazard matrix
> Concept hazard analysis
> Event tree analysis (ETA)
> Failure modes and effects analysis (FMEA)
> Failure modes, effects and criticality analysis (FMECA)
> Fault tree analysis (FTA)
> Fire and explosion study
> Hazard and operability study (HAZOP)
> Hazard Identification (HAZID)
> Historic records of incidents both at the facility and within industry, including near misses
> Human reliability analysis (HRA)
> Job safety analysis (JSA)
> Layers of protection analysis (LOPA)
> Process hazard analysis
> Repair history
> Risk-based inspection (RBI) outputs
> Scenario based hazard identification
> Task analysis
> 'What if' analysis

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.

Regulation 38 requires the operator to document all aspects of the safety assessment.

Example 2: Chemical warehouse

An operator of a warehouse decided to map stock movement within the warehouse and analyse what could go wrong at each step. They checked the systemic hazards (eg power failure, lightning strike, major incident from another facility) and assessed the non-routine tasks.

The operator must ensure the task/condition interaction has been thoroughly explored when using this approach. For example, when opening in the morning, is there a risk that toxic vapours from a leak have accumulated overnight?

Example 3: With similar multiple facilities

An operator has several simple storage facilities (eg LPG or ammonia), with each facility built to similar standards and undertaking similar tasks. They choose to define a representative set of major hazards and potential major incidents. These will be validated by workshops at each site. This allows significant technical input in constructing the representative set. However, the operator must ensure the process incorporates site-specific features and external conditions, such as the presence of threats from outside the facility boundary.

There is also the assumption the tasks are performed the way envisaged by head office, which may not be the case. 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. The composition of the workshop team is an important success factor for this approach.

Example 4: Using multiple techniques

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 (eg lighting burners)
> hazard-based (eg hazardous area assessments)
> process-based (eg HAZOPs and safety integrity level (SIL) assessments)
> based on an assessment of conditions and known failure mechanisms (eg as part of an RBI system).

The operator's challenge is to include all of these studies in 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, using the results of all the above mentioned studies. The operator needs some method of checking for consistency and for ensuring that areas 'at the interface' are covered. Areas of lesser apparent risk (eg as dangerous goods management in the warehouse, or service systems) are also included, as they can often potentially involve specified hazardous substances and develop into major incidents.

3.2 MAJOR INCIDENT IDENTIFICATION

The intent of the safety assessment is to focus on the high-consequence, low-probability events. The hazard identification must identify all major incidents and all major incident hazards that could occur at the facility, including those relating to the security of the MHF.

Major incident is defined in Regulation 9, and has the following qualities:

> they result from an uncontrolled event (ie unplanned or involving the failure of one or more controls)

> they involve or potentially involve specified hazardous substances. This includes events initiated by other circumstances that may knock-on to specified hazardous substance storage or handling facilities

> they expose multiple people to a serious risk to health and safety (at least two, and often more than two people, including those in the area surrounding the facility)

> the risk emanates from an immediate or imminent exposure (which excludes long-term cumulative impacts such as some types of cancer) to:

  – one or more of those substances as a result of the event

  – the direct or indirect effects of the event.

Occurrences that may be classified as a major incident include:

> escape, spillage or leakage of a substance (eg damage, overfill, decay)

> implosion (eg vacuum from steam condensation)

> explosion (eg boiling liquid expanding vapour explosion (BLEVE), vapour cloud explosion)

> fire (eg loss of containment which could lead to fire, pool fire, jet fire, flash fires, fireball).

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 multiple people, then the event leading to the serious risk must be classed as a major incident. Serious risk includes risk leading to death.

The definition of major incident is not limited to uncontrolled events which only cause or have the potential to cause multiple fatalities. This is because the MHF Regulations cover substances with a variety of hazardous properties, some of which cannot cause fatalities.

There are incidents that do not involve or potentially involve specified hazardous substances, but that do potentially expose multiple people to a serious risk to their 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. However, you still have the primary duty of care to make sure workers and others are not at risk from work carried out at the facility. Adequately manage these risks via the SMS 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.

Identifying the potential major incidents requires some creativity, technical expertise, and familiarity with the plant and equipment. Major incident hazard identification should be performed in teams. It is important teams:

> understand what constitutes a major incident

> are composed of an appropriate variety of people

> are aware of the properties of the specified hazardous substances

> are aware of how the hazardous substances are used

> are familiar with the activities that occur within the processes, operation and maintenance of the facility

> 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.

3.3 IDENTIFY THE MAJOR INCIDENT AND MAJOR INCIDENT PATHWAYS

Include all identified major incident hazards with a credible pathway linking to a major incident. If the mechanism cannot be established, the incident can be safely removed from further consideration. Do not delete it entirely, as including it demonstrates a comprehensive inquiry. This is not the same as establishing a very low likelihood of the incident occurring.

Example 5: Appropriately rejected potential major incident scenarios

- 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 the safety assessment, the facility investigated whether a leak from a hole in the duct to the thermal oxidiser could lead to a major incident. The facility carefully considered the maximum possible concentration of hydrogen sulphide, pressure in the duct and toxic exposure criteria. They concluded 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).
- Release of a very small quantity of a toxic material may only cause irritation rather than hospitalisation or fatality (inventory/toxicity combination insufficient).
- A tsunami impacting an above-ground tank located 100km inland on a hill (diminishingly small likelihood).
- A 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 specified hazardous substance, 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 specified hazardous substance 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 the temperature would not fall low enough, even with the most volatile composition and highest pressure conditions.

Example 6: Inappropriately rejected potential major incident scenarios

- Catastrophic failure of a storage tank was rejected because the tank was designed to New Zealand Standards. It had pressure safety valves, pressure alarms and high-level alarms and shutdowns. However, the potential for a major incident still existed, so the hazard should not have been rejected.
- Electrical failure, resulting in loss of control of reaction and potential runaway reaction, release and explosion, was rejected because of a back-up power supply. The major incident hazard still exists, even with that back-up.

> The hazard of incompatible materials mixing in a storage warehouse was rejected because procedures state they must not be stored together. Procedural controls do not remove the potential major incident.

These potential major incidents have been inappropriately rejected based on the selected controls. These major incidents can still occur.

Regulation 38 requires the safety assessment identify hazards and conditions that could lead to a major incident.

VALIDATE THE MAJOR INCIDENT PATHWAYS

The objective is to gain a detailed understanding of what can go wrong. This helps you assess which controls are necessary, and what performance indicators and standards are required. Use work done at this stage later in the likelihood analysis and consequence estimation. It is reasonable to focus effort in understanding the major incidents of highest concern.

Example 7: 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 various approaches available to control it:

> Regular pre-emptive maintenance to prevent corrosion.

> 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 8: 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 incident. The incident pathway is not eliminated, but the probability of major incident is reduced. Examples include:

> 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.

3.4 IDENTIFY ALL SPECIFIED HAZARDOUS SUBSTANCES

Consider all specified hazardous substances in the safety assessment, including:

> products

> by-products

> intermediates

> raw materials

> waste.

It does not matter whether they are held in storage, in process, or being transferred or otherwise handled.

This includes small isolated quantities that may be excluded from the notification requirement. For more information, see WorkSafe's GPG *Major Hazard Facilities: Notifications and Designation*.

Example 9: Inclusion of small quantities of specified hazardous substances

A small hydrogen cylinder serving an online process gas chromatograph is an example of a small quantity that would have no influence on the threshold calculations. However, because of its location inside the plant, it 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.

3.5 UNDERSTAND THE HAZARDOUS SUBSTANCES PROPERTIES AND HOW THEY COULD CAUSE HARM

Identify and understand the properties of the hazardous substances. 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 10: Understanding the properties of specified hazardous substances

Workers at facilities should be aware of the properties of the hazardous substances and how those properties may lead to a major incident if not properly managed. Some of the consequences are not obvious. For example:

- Sodium chlorate is stable as a solid and soluble in water. However, when mixed with other materials such as organics (eg 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.
- 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 (ie the intermediate bulk containers (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.
- If chlorpyrifos is heated above 90°C it decomposes. Above 130°C there is an exothermic decomposition (runaway reaction).

Example 11: Understanding toxicity exposure mechanisms – the Bhopal incident

In December 1984, toxic gas was released from a vent stack from Union Carbide's facility in Madhya Pradesh, India. This happened after a runaway reaction likely occurred in a tank after methyl isocyanate (MIC) came into contact with water. MIC is a highly toxic irritant to mucous membranes.

> MIC reacts readily with many substances, including water, and itself.
> It has a low boiling point.
> It has a high vapour pressure.

This combination of properties resulted in emergency venting of a huge amount of MIC, and the gas affected hundreds of thousands of people, as well as having lasting environmental damage.

Example 12: 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 metres.

3.6 IDENTIFY MAJOR INCIDENT HAZARDS OVER THE FACILITY LIFE CYCLE

The major incident hazards that must be identified by the safety assessment are those which involve specified hazardous substances. As such, they will only exist from some point during the commissioning of the plant onwards. However, major incident hazards need to be identified as early in the project life cycle as possible, as there is a greater ability to implement some controls early in the project.

Consider how the nature of the major incident hazards change during different stages of the operational life of the facility. Table 3 sets out some considerations when identifying major incident hazards.

ENGINEERING / DESIGN	COMMISSIONING	OPERATING	MAINTENANCE	DECOMMISSIONING
> Choice of process technology > Choice of equipment > Quality of materials > Infrastructure considerations (eg transport, communications, occupied buildings) > Construction standards > Compliance with legislation > Process hazards (eg temperature, pressure and flow changes) > Electrical (eg equipment, rating, static electricity, grounding, surges) > Firefighting equipment > Certifications > Factor of safety used in the design	> Start-up procedures > Plant change process > Loss of containment issues (because of pumping, equipment testing and other process start-up activities) > Emergency preparedness > Initial fill prior to start-up > Checking fail safes and monitoring > Hauling, mobilization & positioning of equipment and facilities > Pressure testing and maintenance coordination > Simultaneous operations involved in pre-commissioning	> Chemical hazards (eg flammable, poisonous, corrosive) > Process hazards (eg temperature, pressure and flow changes) > Fire and explosion (eg heat radiation, overpressures, thermal flux) > Procedures related (eg normal operations, operating outside design envelopes > Plant and process changes > Human factors > Required controls and their critical operating parameters	> Physical hazards (eg dropped objects, vehicle collisions) > Chemical hazards (eg welding, acid cleaning) > Site security > Electrical (eg equipment, rating, static electricity, grounding, surges) > Permit-to-work system (eg for high pressure lines, mechanical and electrical systems) > Coordination/ notification with operations re maintenance activities > Depressurising and cooling of hydraulics, pneumatics, and thermal equipment before repair	> Draining and emptying of dangerous goods > Hazardous waste disposal > Disassembling of equipment > Transportation and disposal etc > Loss of expertise and plant knowledge if in receivership etc > Shut-down requirements > Hauling and demobilisation > Lock off of facilities

Table 3: Some considerations for identifying major incident hazards during the facility life cycle

Note: Some stages may overlap, with considerations starting in one and continuing into another, or being relevant through multiple stages.

04/

SAFETY ASSESSMENT

IN THIS SECTION:

A safety assessment must involve a comprehensive and systematic investigation and analysis of all risks to health and safety associated with all major incidents.

Likelihood analysis and consequence estimations are generally considered at the same time as the hazard identification for developing controls against the hazard leading to a major incident. After finding out likelihood and consequence, risk can be assessed.

Regulation 38 requires the safety assessment to 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 facility.

4.1 LIKELIHOOD ANALYSIS

To determine the likelihood of each potential major incident, assess:

> the likelihood of the initiating event

> how well the control performs, or is likely to perform (ie its effectiveness).

An assessment of effectiveness may include:

> **Functionality**: The ability of the control to address a particular hazard.

> **Availability**: Assessing the control for the proportion of time it is actually capable of performing (operating time plus standby time).

> **Reliability**: Whether the control will be functional when required.

> **Survivability**: How likely the control is to continue to be effective, if required, after a major incident has been initiated.

> **Independence**: The control is not dependent on other controls functioning.

> **Maintenance**: Whether the controls functionality can be maintained (eg availability of parts, access, training and knowledge).

> **Monitoring**: Whether it is possible to monitor the control is fully functional or impaired, and how this could be done.

Table 4 lists typical data sources and matters to consider while carrying out likelihood analysis.

LIKELIHOOD ANALYSIS – DATA SOURCES	CONSIDER
Historic incidents, incidents, near misses	> Reliability and relevance of data > References for the data > Statistical significance based on population sample size
Manufacturer's or technology provider's database	> Failure frequencies based on manufacturer or provider's experience, adjusted for local environmental conditions
Fault tree, event tree, cause consequence diagrams	> Estimation of failure frequencies

LIKELIHOOD ANALYSIS – DATA SOURCES	CONSIDER
Standard databases and literature	> Suitability of data for the given conditions > Referencing the source of data (eg generally used sources for obtaining information on standard failure frequency rates, Health and Safety Executive (HSE), DNV GL, OREDA, Chlorine Institute literature) > Statistical relevance of the data source in the literature
Safety alerts/bulletins	> Alerts from WorkSafe and various regulatory agencies and institutes (eg HSE, Chemical Safety Board, Chlorine Institute, American Petroleum Institute, Centre for Chemical Process Safety)
Experiences and other sources	> Based on the experience and expertise of the workers involved in the likelihood analysis process > Failure frequency database or incident database maintained by the industry

Table 4: Typical considerations during likelihood analysis

Standard tools and techniques for the analysis include fault trees, event trees, LOPA and bow-tie analysis. These have all been used successfully. Common mistakes are to:

> claim benefit from controls that are not truly independent

> misapply the techniques

> fail to:

  - involve workers to gain realistic views/assumptions of the situation
  - validate analysis with audit findings, previous incidents, repair history, modifications and worker changes
  - define likelihood criteria clearly
  - consider performance under all operating conditions
  - validate the current performance of existing controls.

It is also important to consider the influence of human factors on likelihood and include them in the safety assessment. This may be achieved by identifying the possible human factors at play and managing those factors within the SMS. Quantitative human factor assessment tools are available, for example human error assessment and reduction technique (HEART), and can be incorporated into the analysis of identified incident scenarios if appropriate or required.

Example 13: Human factor analysis

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

> fatigue management plan

> 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 shutdowns

> an alarm reduction system focused on removing alarm flooding.

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

4.2 CONSEQUENCE ESTIMATION

CONSEQUENCE MODELLING (NO CONTROLS)

Any major incident has a range of potential consequences. You must identify the worst credible 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 the consequence is not to be tolerated (as has been decided by many oil companies about locating temporary maintenance building near vents after the Texas City incident).

CONSEQUENCE ESTIMATION PROCESS	CONSIDER
Modelling software selection and validation	> Industry recognised model > Appropriateness of modelling software > Limitations of modelling software > Validity of software > Independent validation of consequence modelling > Selection of appropriate 'probit' equations
Modelling assumptions and considerations	> Isolatable sections – documentation of omissions or exclusion of parts (referenced to up-to-date piping and instrumentation diagrams) > Storage, pipelines and process inventory > Modelling scenarios > Weather data > Topography > Exposure times
Alternative assessment process	> Use of appropriate qualitative or semi-quantitative measures relevant to situation

Table 5: Typical considerations during consequence estimation

Example 14: Consequence analysis of a warehouse fire

ABC Warehousing is a MHF storing pesticides, flammable liquids, a small amount of flammable gases and general merchandise in separate stores. They concluded a fire at the warehouse could:

> 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 nearby 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 and 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.

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 you to understand the performance requirements when planning for an emergency, and identifies additional risk minimisation methods.

For more information on emergency planning, see WorkSafe's GPG *Major Hazard Facilities: Emergency Planning*.

Example 15: Warehouse fires

ABC Warehousing understood the ferocity of the fire depends upon:

- the nature of the stored chemicals (eg flammable liquids ignite easily)
- how the chemicals are stored (combustible materials add to fire load, high racking may inhibit sprinkler systems, and 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 versus 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 significantly influenced 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

Assessing consequences with controls represents the most likely consequence. All facilities benefit from being aware of the most likely consequence when deciding priorities. You should control the **most likely** events and 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 use the information in emergency planning, in both locating equipment and offices and in identifying potential knock-on events. When commissioning modelling, consider if it would be worthwhile to complement fatality calculations with distances to injury or even distances to irritation/nuisance to understand fully the potential consequences. This may

improve understanding of the potential consequences and aid implementing effective controls.

Assess the level of consequence arising from a major incident for all populations exposed to that incident (both near and far field populations). Make sure to assess and categorise the exposure as chronic or acute (rather than the potential effects).

Regulation 38 requires the safety assessment determine the risk associated with each hazard, including the likelihood and consequences of each major incident.

KNOCK-ON EVENTS

Make sure you have addressed any potential credible events that may act as a knock-on event. Assessing effect ranges allows you to find out 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-specified hazardous substances that knock-on or affect systems storing or handling specified hazardous substances.

Example 16: Knock-on events

> A small fire in a drum decanting operation could spread to an adjacent large drum store by 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 specified hazardous substances.

> 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 'fails to intervene (error)'.

4.3 RISK ASSESSMENT

Depending on whether you choose qualitative, quantitative or both techniques, risk assessments may be expressed by 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 controls.

Types of risk assessments include:

> quantitative risk assessments – all risks are quantified by using recognised data and are numerically expressed

> semi-quantitative risk assessments – risks associated with a major incident are generally quantified by using industry specific or site data

> qualitative risk assessments – assessment of risk from subjective, considered opinion based on operating experience.

There is no specified quantitative risk level that is acceptable, so do not interpret ranking as a requirement to conduct a quantitative risk assessment. Also, meeting any of the quantitative risk criteria does not necessarily prove that you have reduced risk so far as is reasonably practicable.

Risk matrices can be useful tools, but need to be simple, relevant, and used by skilled assessors. They should not be the only risk analysis technique employed. The best results are when a risk matrix is used where controls are in place, to test whether the remaining risk is acceptable. Appendix A: Risk criteria offers further detail on risk matrices.

Example 17: Quantitative risk assessment

ABC Company conducted a quantitative risk assessment, 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 equipment failure rates 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.

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

Example 18: Qualitative risk assessment

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 the likelihood was 'not likely to occur', while the consequence was that a number of fatalities were possible.

LIKELIHOOD		CONSEQUENCE				
		Insignificant	Minor	Moderate	Major	Catastrophic
		1	2	3	4	5
		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 LTIs	One or more fatalities	Significant number of fatalities
5	Possibility of repeated events (1×10^{-1} per year)					
4	Possibility of isolated incidents (1×10^{-2} per year)					
3	Possibility of occurring sometimes (1×10^{-3} per year)					
2	Not likely to occur (1×10^{-4} per year)					Incident 1
1	Rare occurrence (1×10^{-5} per year)					

KEY

Low risk | Moderate risk | Significant risk | High risk

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

The risk to individuals and workgroups from both individual and collective events (total risk) needs to be considered for all populations exposed to or affected by those events (near and far field).

You can use risk matrix to represent the relative consequence and likelihood of an incident. Determine the level of risk acceptable to the organisation collaboratively, engaging with workers and consulting other key stakeholders.

Regulation 38 requires the safety assessment be conducted using assessment methods (including quantitative or qualitative, or both) that are suitable for the hazards and major incidents being considered.

RISK RANKING

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

CONSIDER CUMULATIVE RISK

Consider all potential major incidents and hazards cumulatively, as well as individually, in the safety assessment. You can consider cumulative risk in a number of ways:

> **Consider risk in aggregate:** If there are a large number of different hazards and potential major incidents at a facility, the total risk may be significant even if the risk arising from each individual hazard or major incident is low.

> **Consider risk in concert:** the evaluation of the consequences of major incidents occurring in quick succession (eg an earthquake followed by tsunami).

> **Consider risk by location:** It may be useful to consider whether the major incident risk is concentrated in specific locations or roles. In these cases, additional controls may be prudent to reduce the likelihood or consequence, and reduce risk.

Where the determination of cumulative risk from multiple scenario is necessary, a quantitative risk assessment tool (eg Quantitative Risk Assessment) other than, or as well as a risk matrix, may be appropriate. The risk matrix method may underestimate the likelihood of an event by taking credit of a barrier that could be a causal factor for a failure event in another scenario.

4.5 RISK EVALUATION

Risk evaluation is the decision the risks have been reduced so far as is reasonably practicable. Compare the level of risk found during the risk assessment with any chosen risk criteria for the facility or with the standards declared in the objective. This is often a good predictor of whether risk could practicably be reduced further (but does not prove the risk has been reduced so far as is reasonably practicable). The risk evaluation has three possible outcomes:

> **well below criteria:** further risk reduction is probably impracticable, but still carry out an assessment to make sure risk is reduced so far as reasonable practicable.

> **sufficiently close to or above criteria:** seriously investigate further controls to reduce risk.

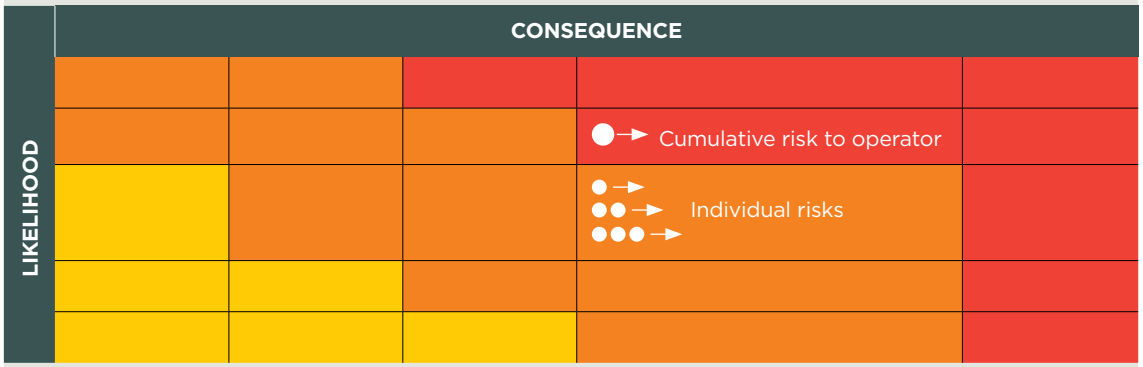
> **well above criteria:** further controls need to be found or continued operation questioned.

Example 19: Analysis of cumulative risk

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

> 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 significant 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.



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

You will need to complete risk evaluation several times during the safety assessment process:

> Before the controls are considered to determine the level of risk of the major incident hazard without controls in place.
> After the existing controls are considered to determine the current level of risk of the major incident hazard and whether the risk is acceptable and has been reduced so far as is practicable.
> After additional controls are identified to determine whether the additional controls reduce the risk so far as is practicable.

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

Example 20: Qualitative risk evaluation

The ranking on the risk matrix determined by ABC Company in Example 18 can be compared with their internal risk criteria. These state that any risk classified as a high risk must be reviewed to ensure that all potential controls 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 21: Risk evaluation: Implementation of additional controls

ABC Chemical Company identified during the risk assessment that an additional control (high-level trip) should be considered to protect against overfilling of the storage vessel. The risk of overfilling was considered high during the 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 was higher on the hierarchy of controls than alternative controls.

An alternative control was 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 was 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.

05/

CONTROLS

IN THIS SECTION:

The safety assessment process must identify existing controls that prevent or limit the effects of a major incident hazard. The safety assessment must also consider whether there are further controls that could be implemented to reduce the risk so far as is reasonably practicable.

5.1 IDENTIFY CONTROLS

The safety assessment must include the range of controls you decide 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 and some will be identified in the course of the safety assessment.

A control, 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 (ie impact on either likelihood or consequence) are sometimes referred to as preventative controls. 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
> hardware or software.

There are usually a range of controls available. In selecting controls, consider the hierarchy of controls.

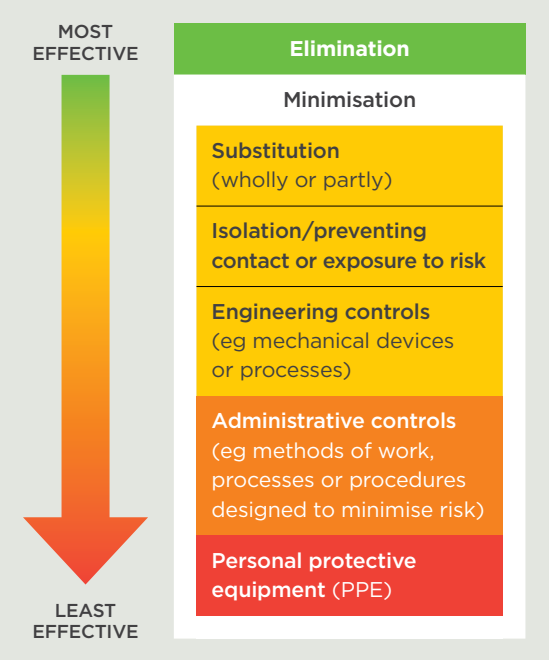


Figure 4: Hierarchy of controls

Base the selection of controls on what is reasonably practicable to reduce the risk. The safety assessment must identify existing controls and potential controls. Consider recognised and generally accepted good engineering practice, good practice, emerging technologies, published codes of practice and industry standards, as well as what is currently present.

To identify controls, you need to understand what needs to happen for the control to be effective, and manage that control in its entirety. For example, an alarm without an operator to notice its activation and respond, has no safety benefit. A procedure only has a safety benefit if it is technically adequate and workers are competent in its use. Engineering standards are only of benefit if they deal with the issue at hand and are applied.

5.2 DEMONSTRATION OF ADEQUACY

The MHF Regulations are an example of a proactive, performance-based regime, where a general expectation for performance is set in HSWA but you select the best way to achieve it.

HSWA requires a performance standard of 'so far as is reasonably practicable'. You must demonstrate the identified controls eliminate or, if it is not reasonably practicable to eliminate, minimise risks so far as is reasonably practicable.

Consider the following factors:

- The assessment includes both controls that eliminate and minimise risks.
- The full range of operating and start-up/shut-down conditions.
- 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. Where necessary, multiple controls are implemented.
- The hierarchy of controls has been applied in understanding effectiveness (eg wearing PPE and applying administrative controls are less effective than engineering solutions).
- Control independence has been considered and correctly accounted for (particularly important in quantitative assessments).
- Critical operating parameters have been identified for safety-critical elements, compliance with which is necessary to avoid a major incident.
- Existing performance standards for adopted controls have been considered (or devised if absent).
- You can show the adopted controls are capable of maintaining operation within the identified safe operating window.
- Record identified controls rejected during the safety assessment, and the reason why they were rejected (ie the justification of why they are not reasonably practicable).

The safety assessment will have identified what could and should be done to minimise and control risks. The onus is now to adopt and implement those controls. The means of implementing and maintaining the effectiveness of the adopted controls is via the SMS.

An assessment of whether doing something is reasonably practicable must be carried out in accordance with Section 22 of HSWA. Regulation 30 requires the controls in the event of a major incident occurring, minimise the magnitude and severity of its health and safety consequences to people on-site and off-site, so far as is reasonably practicable.

5.3 WHAT IS REASONABLY PRACTICABLE?

In determining what is 'reasonably practicable' you are expected to exercise judgement, considering the five factors specified in Section 22 of HSWA, namely:

- the likelihood of the hazard or risk concerned occurring

- the degree of harm that might result from the hazard or risk (eg fatality, multiple injuries, medical or first aid treatment, long-or short-term health effects)
- what the person concerned knows, or ought reasonably to know, about:
  - the hazard or risk
  - ways of eliminating or minimising the risk
- the availability and suitability of ways to eliminate or minimise the risk
- the cost associated with available ways of eliminating or minimising the risk. This includes whether the cost is grossly disproportionate to the risk. In other words, controls should be implemented unless the risk is insignificant compared with the cost of implementing the controls.

Example 22: Identifying what is reasonably practicable and recording this information

Using an ammonia plant (UTMHF) as an example, the identification and assessment steps may have identified the area with the highest likelihood of a loss of containment is the tanker loading area. It is reasonable to expect the operator has thought about the controls needed for this area. The safety case should be able to explain this.

The operator and MHF designers may also have concluded the worst case scenario (ie major incident with the highest consequence) is catastrophic failure of the large ammonia storage tank. Therefore it is reasonable to expect that more effort is put into the design and controls for this part of the MHF because of the high-consequence should this failure occur. The information in the safety case should demonstrate that this worst case scenario has been addressed.

The massive explosion that occurred at the Buncefield Fuels Terminal in the UK in 2005 significantly changed what that sector 'knows, or ought reasonably to know' about the hazards or risks at this type of facility. As a result, it is now reasonable to expect that controls to prevent similar tank overflows would be more robust than before.

The final consideration is to weigh up the cost of additional controls against the extent of risk reduction that could actually be obtained. This is similar to the process many operators go through each year when deciding which improvement projects to add to next year's investment plan and which to defer. For many possible projects/improvements, qualitative comparisons are sufficient. However, more detailed quantitative comparisons are often undertaken for more important or high-cost projects.

Although the cost of eliminating or minimising risk is relevant in determining what is reasonably practicable, there is a clear presumption in favour of safety ahead of cost. Only consider cost after identifying the extent of the risk and the available ways of eliminating or minimising the risk.

The costs of implementing a particular control may include costs of purchase, installation, maintenance, and operation of the control and any impact on productivity as a result of the introduction of the control.

A calculation of the costs of implementing a control should consider any savings from fewer incidents, injuries and illnesses, potentially improved productivity and reduced staff turnover.

Where the cost of implementing controls is grossly disproportionate to the risk, it may be that implementing them is not reasonably practicable and therefore not required. This does not excuse you from doing anything to minimise the risk so far as is reasonably practicable. Instead use a less expensive way of minimising the likelihood or consequence.

Safety cases submitted by UTMHFs may contain examples where you've made similar comparisons of alternative controls before deciding which to adopt for specific risk scenarios.

The safety assessment should provide the information needed to make these judgements. Therefore much of the reasoning behind your selection of controls may already be presented in the safety case (ie in the summary of the safety assessment). The extra information required to make a convincing demonstration will depend on the amount of detail included in the summary.

For more information on safety cases, including the safety assessment summary, see WorkSafe's GPG *Major Hazard Facilities: Safety Cases.*

DO CONTROLS MINIMISE RISK SO FAR AS IS REASONABLY PRACTICABLE?

The first component of a demonstration showing you've eliminated or minimised a risk so far as is reasonably practicable is to show you've addressed each hazard and potential major incident with specific controls. The use of bow-tie diagrams is one clear graphic means of doing this (see Figure 5 for an example). This shows there are controls in place for each hazard that could lead to a major incident. It is also possible to show this in tabular form (eg database printout or spreadsheet).

Table 6 is a mock-up derived from Figure 5 that shows specific controls listed for specific hazards. However, tables showing a list of hazards in one column and a list of controls in another column (such as the mock-up in Table 7) do **not** help demonstrate that controls reduce the risk of all identified hazards. They do not clearly show which controls act for which hazards and whether all hazards have an identified control.

The second aspect is the level of risk that remains after you have decided it is not reasonably practicable to do any more. One means of gauging the validity of these decisions is by comparing the final risk with a suitable published benchmark.

Numerical evaluation of risk is only as good as the data you use in the evaluation of likelihood and consequences, both of which are subject to much uncertainty.

Appendix A: Risk criteria provides examples of criteria that can be used in relation to major incidents. These are not exhaustive and you may choose to use criteria different from these examples. Whatever criteria are used, you will have to justify the criteria as suitable and appropriate to the specific facility.

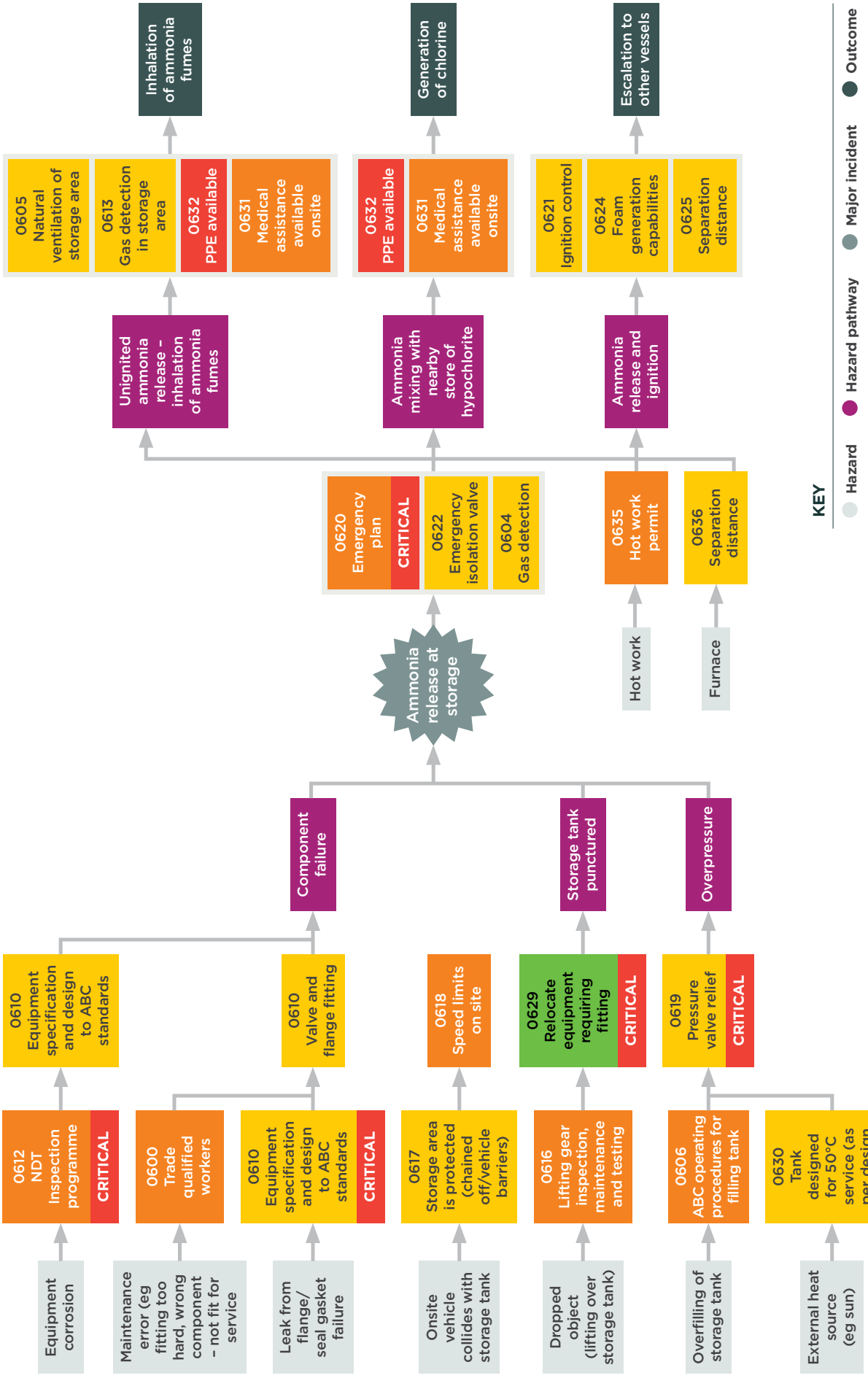


Figure 5: Example bow-tie showing an ammonia release at storage (control colour as per the hierarchy of controls)

MAJOR INCIDENT: AMMONIA RELEASE AT STORAGE (ABC CHEMICAL COMPANY)		
CAUSE: Component failure		
HAZARD	**CONTROLS**	**EFFECTIVENESS**
Equipment corrosion	> Non-Destructive Testing (NDT) inspection program > Equipment specification and design to ABC standards	> High > Medium
Maintenance error (eg fitting tightened too far, wrong component – not fit for service)	> Trade qualified workers > Valve and flange fitting training	> Low > Medium
Leak from flange/seal – gasket failure	> Equipment specification and design to ABC standards > Valve and flange fitting training	> Medium > Medium
CAUSE: Storage tank puncture		
HAZARD	**CONTROLS**	**EFFECTIVENESS**
On-site vehicle collides with storage tank	> Storage area is protected (chained off/vehicle barriers) – restricted access > Speed limits on-site	> High > Low
Dropped object (lifting over storage tank)	> Lifting gear inspection, maintenance and testing > Relocate equipment requiring lifting	> Medium > High

Table 6: Hazard/control register

MAJOR INCIDENT: AMMONIA RELEASE AT STORAGE (ABC CHEMICAL COMPANY)	
HAZARD	**CONTROLS**
> Dropped object (lifting over storage tank) > Equipment corrosion > External heat source (eg sun) > Leak from flange/seal – gasket failure > Maintenance error (eg fitting tightened too far, > wrong component – not fit for service) > On-site vehicle collides with storage tank > Overfilling of storage tank	> ABC operating procedures for filling tank > Equipment specification and design to ABC standards > Lifting gear inspection, maintenance and testing > NDT inspection program > Pressure relief valves > Relocate equipment requiring lifting > Speed limits on-site > Storage area is protected (chained off/vehicle barriers) – restricted access > Tank designed for 50°C service (as per design specification) > Trade qualified workers > Valve and flange fitting training

Table 7: Hazard/control register that does **NOT** help demonstration

COULD MORE OR BETTER CONTROLS BE USED?

An alternative way to demonstrate the controls in place at the facility will minimise risk so far as is reasonably practicable is to show that additional or alternative controls are not justified.

You can use systems like LOPA or SIL reviews to determine acceptable risk levels and whether they will be met. To ensure these types of systems remain useful, it's important to include a testing schedule into the system. Testing and recalibrating allows for continual improvement.

Additional or alternative controls can be included in these analyses and their effect on the final risk estimated. There are also techniques for estimating the probability of failure on demand (PFD) of procedural controls, such as HRA. There is published data available for the PFD of procedural tasks, depending on their complexity, frequency of use and environmental factors[2].

5.4 SAFETY-CRITICAL ELEMENTS

A safety-critical element is defined in the MHF Regulations as any part of a facility or its plant (including a computer program) that:

> has the purpose of preventing, or limiting the effect of, a major incident and

> the failure of which could cause or contribute substantially to a major incident.

The 'and' that links the two parts of the definition means that something is a safety-critical element on the basis of its 'purpose' and its contribution to causing a major incident.

Some safety-critical elements could be plant or systems that:

> could cause a major incident if it failed, including:
  - particular safety features of primary containment, vessels, and pipe work
  - uninterruptable power supplies
  - a process logic controller or other electronic control system where its malfunction could contribute substantially to a major incident)

> detect smoke, fire, accumulations of flammable (and other hazardous) gases, leakages of flammable liquids, and other events that may require an emergency response

> give warning of an emergency by audible and, where necessary, visual alarm systems. Alarms which are for process control purposes and do not alert of an emergency may not necessarily be safety-critical elements

> limit the extent of an emergency, including:
  - measures to combat fire and explosions. For example:
    - inert-blanketing in tanks
    - integrity of equipment located in hazardous area zones
    - auto and manually operated deluge systems
    - foam-systems
    - fire-water supply and distribution systems
    - natural and forced ventilation systems
    - explosion hatches/doors
    - emergency shut-down systems
    - facilities to monitor and control the emergency and for organising evacuation

> protect workers from explosion, fire, heat, smoke, hazardous gas, or fumes during any period while they may need to remain at the facility during an emergency

> ensure safe evacuation of all workers to a place of safety

> provide safe means of escape in the event that arrangements for evacuation fail.

[2] See *Layers of Protection Analysis, Simplified Process Risk Assessment*, Center for Chemical Process Safety, American Institute of Chemical Engineers, 2001.

Information on safety-critical elements can also be found in the GPG *Major Hazard Facilities: Safety Cases*.

5.5 DEVELOP PERFORMANCE STANDARDS FOR CONTROLS

The MHF Regulations require that the SMS specifies the performance standards that apply. In relation to a control, a performance standard is the acceptable level of response against a target, or the required level of performance, for the control to be considered effective in managing the risk. Performance standards may include both the current required level of performance and also a target level to be achieved within a specified timeframe.

The performance standards are the parameters against which controls are assessed to make sure they reduce risk so far as is reasonably practicable.

In developing these standards you should consider what level of performance is reasonable to achieve from each control. It is important the parameters set in the performance standard are specific (well defined and not open to wide interpretation), measurable, appropriate, realistic and timely (SMART).

Performance standards are required for each control to make sure the effectiveness of that control is tested and that a control failure is detected and remedied. The overall effectiveness of the control can be judged by measuring its performance against the standard.

For more information on performance monitoring of controls and SMS elements see WorkSafe's GPG *Major Hazard Facilities: Major Accident Prevention Policy and Safety Management Systems*.

Example 23: Performance standards for controls

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

CONTROL	PERFORMANCE STANDARD	EFFECTIVENESS MEASURE
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

Table 8: Performance standards for controls

For the pressure safety valve in the table above, the corrective action in the event of failure (ie not relieving at the set pressure) may be:

> replacement

> recalibration

> reset.

This depends on the valve and service. The root cause of a trend of failures should also be investigated. The second effectiveness measure may be reported to management, while the first is used primarily as a guide for maintenance workers to determine what action to take in response to failure.

5.6 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 window, where any operation outside the safe operating window could undermine the safe operation of the facility.

The purpose of identifying a COP is to make sure more robust monitoring of that parameter occurs. Define COPs for those parameters where there is a high reliance on a worker to respond to a process or manage an activity appropriately. Make sure that COP documentation is continuously available to workers and that it provides clear guidance as to how people should respond if a deviation occurs. In the event that a COP is exceeded, an investigation, including risk assessment, should be conducted and outcome documented.

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 SMS).

Monitor COPs to minimise any excursions outside the safe operating window.

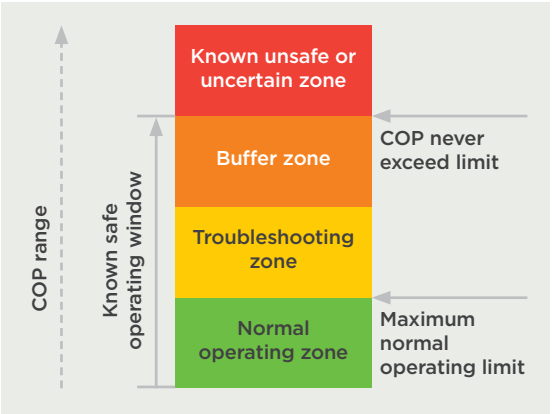


Figure 6: Safe operating window and critical operating parameters

Example 24: Critical operating parameters

Typical COPs might include:

- maximum operating pressure of a pressure vessel
- maximum and minimum operating temperature
- minimum metal temperature (cold brittle facture)
- facility minimum manning level
- voltage requirements
- the number of fire pumps available
- maximum reactant addition rate for a reactor
- minimum cooling water flow rate for a reactor
- 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.

06/

APPENDICES

IN THIS SECTION:

6.1 APPENDIX A: RISK CRITERIA

Comparison of estimated risk levels against set criteria may be useful as part of demonstrating the overall adequacy of controls, although it is unlikely that adequacy can be demonstrated solely by this means. This appendix provides a brief discussion of the types of risk criteria that have been adopted internationally. These approaches may be useful for applying to individual MHFs, to specific aspects of major incident risk at MHFs (eg the off-site risk), or to particular sections of individual MHFs (eg if a purely qualitative approach proves insufficient in particular areas).

GENERAL BASIS

Risk criteria can provide a basis for judging the tolerability of risks that have been assessed, and for deciding the urgency or priority with which any identified hazard or risk should be addressed.

However, all risk assessment is subject to uncertainty, and hence use of rigid risk criteria may be inappropriate. A possible alternate approach is provided by the UK HSE framework for the tolerability of risk and it's 'as low as reasonably practicable' (ALARP) concept. This is based on broad ranges of risk, rather than on specific criteria. The HSE's policy document *Reducing Risks, Protecting People – HSE's decision-making process* (2001) presents the risk tolerability framework. This represents risk on an inverted triangle as increasing from a broadly acceptable region, through a tolerable region, to an unacceptable region (see Figure 7). This broad framework is used in HSE's permissioning guidance, *Guidance on 'as low as reasonably practicable' (ALARP) decisions in control of major accident hazards (COMAH)* and provides for the following broad risk ranges:

- an upper region where ALARP has not been demonstrated and risk is unacceptable
- a middle region where risk is tolerable if ALARP is demonstrated through arguments based on relevant good practice, additional risk reduction methods and grossly disproportionate costs for further risk reduction
- a lower region where risk is broadly acceptable and does not need further reduction because relevant good practice is applied.

Although the broad risk ranges appear compatible with HSWA's performance standard of 'so far as is reasonably practicable', the interpretation does not incorporate the continuous improvement aspects contained within the MHF Regulations. This means that at the lowest risk band, some risks may remain not reduced, even where it may be reasonably practicable to further reduce the risk.

An interpretation of the broad risk ranges, which manages or reduces all risks and includes consideration of continual improvement, is shown in Table 9 and described in more detail below.

The overall demonstrations you make need to consider hazards and risks in all regions, and may need to specifically show that:

- there are no hazards or risks currently in the upper region, and any hazards or risks that may arise in the upper region in the future will be immediately and effectively dealt with
- all hazards and risks in the middle and lower regions have had all reasonably practicable risk reduction measures applied
- there are suitable and reliable processes for continuing to manage hazards and risks at all levels and for achieving continual improvement.

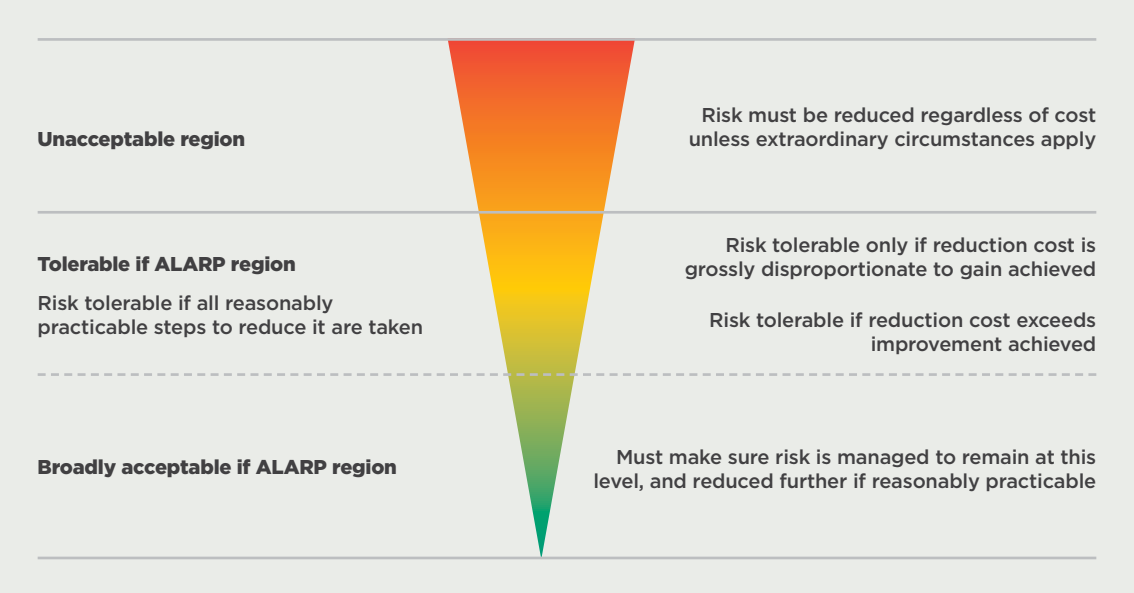


Figure 7: The broad risk regions

Upper region	Unacceptable risk	Take prompt action to reduce risk regardless of cost, unless extraordinary circumstances apply.
Middle region	Tolerable risk	Implement controls so far as is reasonably practicable, considering the available measures, relevant good practice, cost etc.
Lower region	Broadly acceptable risk	Manage risks at this level so far as is reasonably practicable and continuously try and reduce risk further.

Table 9: An interpretation of the risk ranges (refer to Figure 7)

RISK MATRICES

A risk matrix categorises the risk of individual major incidents, based upon the judgement of an assessment team about the order of magnitude of the likelihood and consequence of the incident occurring. Typical risk matrices for hazardous industrial facilities range in size from 3 x 3 to 5 x 5. Typically, this has likelihood on the Y axis and consequence on the X axis of the matrix. The frequency or likelihood scale should be one order of magnitude per row or column.

Risk increases diagonally across the matrix and bands of broad risk levels can be established on the matrix, perpendicular to the direction of risk increase. These bands broadly relate to the risk bands in Figure 7, and can be used to show areas where risk is intolerable/unacceptable and where risk is tolerable, subject to all practicable measures being taken and subject to continuous improvement. The broad risk bands can also be related to the urgency of action required.

In general, preventative controls (left hand side of a bow-tie diagram) lead to a decrease in the likelihood of an incident occurring, which usually means a decrease in the Y coordinate on the matrix. Mitigative controls (right hand side of a bow-tie diagram) lead to a decrease in the consequence of an incident if it occurs, which usually means a decrease in the X coordinate on the matrix.

However, note the risk matrix approach—while it may be useful in ranking risks and to support a demonstration of adequacy—is unlikely to be sufficient on its own for many facilities. For example, separate and additional analysis of the effects of alternate controls is likely to be needed, as a risk matrix is often too coarse a tool to distinguish between options. It may also be difficult to fully address cumulative risk using matrices alone.

If using risk matrices, give clear definitions for the matrix and any categorisation used within it, and show what action or significance is attributed to each position on the matrix, and whether the matrix is applicable to an incident, or to an individual scenario which leads to the incident. You should check the risk matrices, and any risk criteria implied through their use, are consistent with commonly adopted risk criteria, such as any quantitative risk criteria.

QUANTITATIVE RISK ASSESSMENT AND QUANTITATIVE CRITERIA

Quantitative approaches to risk assessment have different strengths and weaknesses. They allow a more precise and consistent approach to defining the likelihood, consequence and severity of a major incident but the results can vary significantly depending on assumptions made for the calculations. They can also be resource-intensive, may lack transparency, may be difficult for a non-specialist to understand and may give a misleading sense of accuracy of risk estimates.

If you choose to conduct a Quantitative Risk Assessment (QRA), then the results may be used by comparison with predetermined criteria or for comparing different options as part of the overall demonstration of adequacy. There are two main types of quantitative risk measure that may be used to define risk criteria:

- **Individual risk** is the frequency at which an individual may be expected to sustain a given level of harm from the realisation of specified hazards. The purpose of criteria based on this risk measure is to ensure that no single person is overexposed to risk. Risk assessment results using this measure are often based on risk 'contour' plots.
- **Societal risk** is the relationship between the frequency of occurrence of major incidents and the number of people suffering from a specified level of harm in a given population from those incidents. The purpose of criteria based on this risk measure is to control risk to society as a whole. Risk assessment results using this measure are often based on frequency-consequence graphs.

These criteria may in principle be applied to any exposed population, on-site or off-site, although for a variety of reasons the actual levels of risk tolerability may vary between the different exposed groups. Risk tolerability values for individuals exposed to major incident hazards should relate in a sensible manner to levels of risk from other industrial and non-industrial activities.

In the case of off-site risk to the general population, a set of 'interim' criteria have been used in a number of cases in Victoria, for example, in relation to land use planning (Interim Victorian Risk Criteria – Risk Assessment Guidelines, prepared for the Altona Chemical Complex and the Victorian Government, by DNV Technical, October 1988). The criteria do not have legal status but can provide guidance on values.

Comparison with a benchmark such as the Victorian risk criteria are a straightforward exercise if you use QRA in the formal safety assessment. QRA is not mandatory and you can use alternative qualitative assessment

techniques such as risk matrices. Since most matrices show a consequence band of one fatality on one axis, and some form of numerical frequency (or likelihood) estimate on the other axis, it is usually possible to determine what sort of fatality rate you consider to be 'High', 'Medium' or 'Low' on-site risk.

POTENTIAL LOSS OF LIFE AND COST BENEFIT OF CONTROLS

Societal risk can also be expressed as a 'Potential Loss of Life' (PLL), which is the number of fatalities that may be expected to occur each year, averaged over a long period.

Such calculations are often controversial as they appear to require a value to be placed on life, but these calculations are commonly used internationally and may aid decision making in regard to adopting controls for major incident hazards.

OTHER ISSUES

Other issues to consider in relation to risk criteria include the following:

> Quantitative criteria for risk to persons on-site have not been established and would need to be set and justified by any operator proposing to use QRA methods.

> Hazards (and therefore possibly risks) must be assessed both individually and cumulatively, and hence the adopted criteria will need to be applicable to hazards both individually and cumulatively. The risk matrix approach considers hazards and risks individually, while the interim risk criteria apply to all hazards cumulatively. Therefore, a combination of criteria may be needed.

> Most established criteria relate specifically to fatality rates but the MHF Regulations do not require any specific form of criteria. It may be appropriate to consider measures of risk related to lower levels of harm, for example, serious injury.

6.2 APPENDIX B: MORE INFORMATION

NEW ZEALAND

ENVIRONMENTAL PROTECTION AUTHORITY

For information about how to manage hazardous substances visit the Environmental Protection Authority's website www.epa.govt.nz or call 0800 376 234.

NEW ZEALAND LEGISLATION

To access all legislation including Acts and regulations visit the New Zealand Legislation website www.legislation.govt.nz

INTERNATIONAL

EUROPEAN COMMISSION (EUROPE)

For information and guidance about the European Seveso-Directives industrial accident policy visit the commission's website www.ec.europa.eu/environment/seveso/

HEALTH AND SAFETY EXECUTIVE (UK)

For information and guidance about the UK's Control of Major Accident Hazards (COMAH) Regulations and what HSE expect from ALARP demonstrations visit the HSE's website www.hse.gov.uk/comah/ and www.hse.gov.uk/risk/expert

NATIONAL OFFSHORE PETROLEUM SAFETY AND ENVIRONMENTAL MANAGEMENT AUTHORITY (AUSTRALIA)

For guidance to assist with a risk assessment of major accidents visit the National Offshore Petroleum Safety and Environmental Management Authority's (NOPSEMA) website www.nopsema.gov.au

SAFE WORK AUSTRALIA (AUSTRALIA)

For guidance to assist with preparing an effective safety case that meets Australia's Work Health and Safety Regulations visit Safe Work Australia's website www.safeworkaustralia.gov.au

WORKSAFE VICTORIA (AUSTRALIA)

For guidance to assist with a safety assessment of a MHF visit WorkSafe Victoria's website www.worksafe.vic.gov.au

FURTHER READING

For information and guidance about health and safety or to contact the High Hazard Unit visit WorkSafe's website www.worksafe.govt.nz or call 0800 030 040.

Related WorkSafe publications:

- *Hazardous Substances in Transit Depots*
- *Introduction to the Health and Safety at Work Act 2015*
- *Major Hazard Facilities: Emergency Planning*
- *Major Hazard Facilities: Major Accident Prevention Policy and Safety Management Systems*
- *Major Hazard Facilities: Notifications and Designation*
- *Major Hazard Facilities: Safety Cases*
- *Worker Engagement, Participation and Representation*

A Guide to the Control of Major Incident Hazards Regulations 1999
Health and Safety Executive www.hse.gov.uk/comah/

Good Practice and Pitfalls in Risk Assessment
Health and Safety Executive – Health & Safety Laboratory

Guidelines for Integrated Risk Assessment and Management in Large Industrial Areas
International Atomic Energy Agency www.iaea.org/index.html

Guidelines for Quantitative Risk Assessment 'Purple Book' TNO
Committee for the prevention of disasters http://content.publicatiereeksgevaarlijkestoffen.nl/documents/PGS3/PGS3-1999-v0.1-quantitative-risk-assessment.pdf

Guidance Note: Control Measures for a Major Hazard Facility
WorkSafe Victoria www.worksafe.vic.gov.au

Guidance Note: Hazard Identification at a Major Hazard Facility
WorkSafe Victoria www.worksafe.vic.gov.au

Guidance Note: Risk Assessment
National Offshore Petroleum Safety and Environmental Management Authority (NOPSEMA) www.nopsema.gov.au

Guidance Note: Safety Assessment for a Major Hazard Facility
WorkSafe Victoria www.worksafe.vic.gov.au

Guide for Major Hazard Facilities – Safety Assessment
Safe Work Australia www.safeworkaustralia.gov.au

Guide for Major Hazard Facilities – Safety Case: Demonstrating the Adequacy of Safety Management and Control Measures
Safe Work Australia www.safeworkaustralia.gov.au

Hazardous Industry Planning Advisory Paper No.4 – Risk Criteria for Land Use Safety Planning (HIPAP 4)
Former NSW Department of Planning www.planning.nsw.gov.au

How to Determine What is Reasonably Practicable to Meet a Health and Safety Duty
Safe Work Australia www.safeworkaustralia.gov.au

HSE's Land Use Planning Methodology
Health and Safety Executive www.hse.gov.uk

Layers of Protection Analysis, Simplified Process Risk Assessment
Centre for Chemical Process Safety, American Institute of Chemical Engineers

Beer, T. & Ziolkowski, F. (1995). Environmental Risk Assessment: An Australian Perspective, Supervising Scientist. (Report 102). Canberra, Australia.

Hutchison R.B., Perera J., Witt H.H. (1996) *Preliminary Environmental Risk Ranking* ANSTO Safety and Reliability. Risk Engineering Seminar Munro Centre for Civil and Environmental Engineering, University of NSW.

Suarez, A. & Kirchsteiger, C. A. (1998) *Qualitative Model to Evaluate the Risk Potential of Major Hazardous Industrial Plants*. EUR 18128 EN

6.3 APPENDIX C: GLOSSARY

TERM	BRIEF EXPLANATION
Accepted safety case	A safety case which WorkSafe has accepted under Regulation 48.
Amended safety case	If WorkSafe has initially rejected a safety case or revised safety case under Regulation 48, an operator may amend the safety case and resubmit it for acceptance. This is an amended safety case.
Change or proposed change at a MHF	Defined in the MHF Regulations. It means a change or proposed change of any kind, including: > a change to any plant, structure, process, hazardous substance or other substance used in a process, (including the introduction of new plant, new structure, new process or new hazardous substance) > a change to the quantity of specified hazardous substances that are 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 to the facility's SMS > an organisational change at the facility (including a change in its senior management).
Control	A measure to eliminate or minimise, so far as is reasonably practicable, the risk of a major incident occurring; or to minimise so far as is reasonably practicable, the magnitude or severity of a major incident, as described in Regulation 30.
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.
Designated transfer zones	Defined in Regulation 11 of the Hazardous Substances (Classes 1 to 5 Controls) Regulations 2001.
Designation	A formal decision made by WorkSafe that a facility is or will be either an LTMHF or an UTMHF for the purposes of the MHF Regulations.
Emergency	An incident at a MHF requiring activation of the emergency plan.
Environmental Protection Authority (EPA)	A government agency responsible for certain regulatory functions concerning New Zealand's environmental management.
Facility	Defined in the MHF Regulations, means the whole area under the control of the same person where specified hazardous substances are present in 1 or more places. Two or more areas under the control of the same person and separated only by a road, railway, inland waterway, pipeline, or other structure are treated as 1 whole area for the purposes of this definition.
Facility emergency control centre (FECC)	An area where designated personnel co-ordinate information, develop strategies for addressing the media and government agencies, handle logistical support for the response team, and perform management functions. A centralised support facility allows emergency managers and staff to contend with incident issues more effectively.
Facility emergency controller (FEC)	The person in charge of managing an emergency for the facility and has overall responsibility for all functions performed by facility personnel during an emergency.
Failure of a control	This means if the control: > is a positive action or event: the non-occurrence or the defective occurrence of that action or event > consists of a limitation on an operational activity, process or procedure: the breach of that limitation.

TERM	BRIEF EXPLANATION
GHS	The Globally Harmonized System of Classification and Labelling of Chemicals, Fifth revised edition, published by the United Nations.
Greenfield	An area of land, or some other undeveloped site earmarked for commercial development.
Hazard	A situation or thing that could harm someone, and includes a person's behaviour. For example, an unguarded machine, hazardous substances etc.
Hazard identification	The systematic and comprehensive process of identifying hazards.
Isolated quantity	Defined in the MHF Regulations, means a quantity of a hazardous substance where its location at the facility is such that it cannot on its own initiate a major incident elsewhere at the facility.
Knock-on effects	Secondary events (such as toxic releases) triggered by a primary event (such as an explosion), resulting in an increase in consequences or in the area of an impact zone over the initial event.
Local authority	A territorial authority within the meaning of section 5(1) of the Local Government Act 2002.
Local community	This is defined in the MHF Regulations as: (a) meaning, at a minimum, all persons within a 1 km radius of any point on the perimeter of a MHF, and (b) including all persons in an area which might be affected by a major incident occurring at a MHF. The words 'at a minimum' mean the 1 km radius does not mark the extent of the definition. Paragraph (b) may extend the scope of the definition well beyond 1 km in some circumstances.
Lower threshold quantity	Defined in the MHF Regulations, the quantity specified in column 4 of table 1 or column 3 of table 2 of Schedule 2, and calculated in accordance with Part 3 of the MHF Regulations.
Lower tier major hazard facility (LTMHF)	Defined in the MHF Regulations, a facility that WorkSafe has designated as an LTMHF.
Major hazard facility (MHF)	Defined in the MHF Regulations, a facility that WorkSafe has designated as an LTMHF or a UTMHF.
Major incident	Defined in the MHF Regulations as an uncontrolled event at a MHF that involves, or potentially involves, specified hazardous substances, and exposes multiple persons to a serious risk to their health and safety (including a risk of death) arising from an immediate or imminent exposure to: > 1 or more of those substances as a result of the event > the direct or indirect effects of the event.
Major incident hazard	Defined in the MHF Regulations, a hazard that has the potential to cause a major incident.
Major incident pathway	The process or sequence by which the major incident hazard develops 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.

TERM	BRIEF EXPLANATION
Near miss	A situation where a worker or any other person is exposed to a serious risk to their health and safety, even if no harm was incurred.
Notifiable event	This is defined in HSWA as: > the death of a person > a notifiable injury or illness > a notifiable incident.
Notifiable incident	Defined in HSWA, generally an incident that exposes workers or other people to a serious risk to health or safety. It must be reported to WorkSafe, or the relevant designated agency.
Notification	The notification to WorkSafe required by MHF Regulations 12, 13, and 17. Notification is required if specified hazardous substances are present or likely to be present at a facility in a quantity equal to or exceeding the lower threshold quantity or if there is a proposed new operator.
Off site	Defined in the MHF Regulations, this means not on site.
Officer	Defined in HSWA, in summary it means a person that exercises significant influence over the PCBU's management. For example, the CEO, a director, or a partner in a partnership.
On site	Defined in the MHF Regulations, this means at or in a facility.
Operator	Defined in the MHF Regulations, the PCBU who manages or controls a facility or a proposed facility, and has the power to direct the whole facility be shut down.
Person conducting a business or undertaking (PCBU)	Defined in HSWA, generally any legal person running a business or undertaking. For example, includes a limited liability company, partnership, trust, incorporated society, etc.
Pipeline	Defined in Regulation 2 of the Health and Safety in Employment (Pipelines) Regulations 1999.
Proposed facility	Defined in the MHF Regulations. It is an existing workplace that is to become a facility or a facility that is to be built in the future.
Qualitative risk assessment	A relative measure of risk based on ranking or separation into descriptive categories such as low, medium, high.
Quantitative risk assessment	The use of data to determine risk. Requires calculations of two components of risk; the consequence of the hazard, and the likelihood that the hazard will occur.
Risk	The likelihood of a specific level of harm occurring from a hazard.
Risk assessment	This involves considering what could happen if someone is exposed to a hazard and the likelihood of it happening.
Safety assessment	Defined in the MHF Regulations, the general process by which the operator of a MHF systematically and comprehensively investigates and analyses all aspects of risks (including decisions around which controls to implement) to health and safety associated with all major incidents that could occur in the course of the operation of the MHF.
Safety case	Defined in the MHF Regulations, generally a written presentation of the technical, management and operational information covering the hazards and risks that may lead to a major incident at a UTMHF, and their control. It provides justification for the measures taken to ensure the safe operation of the facility.

TERM	BRIEF EXPLANATION
Safety management system (SMS)	Defined in the MHF Regulations, generally a comprehensive integrated system for managing all aspects of risk control at a MHF and used by the operator as the primary means of ensuring safe operation of the MHF.
Safety-critical element	Defined in the MHF Regulations, means any part of a facility or its plant (including a computer program): > that has the purpose of preventing, or limiting the effect of, a major incident; and > the failure of which could cause or contribute substantially to a major incident.
Specified hazardous substances	Defined in the MHF Regulations, these are table 1 or 2 hazardous substances.
Structure	Defined in HSWA, means anything that is constructed, whether fixed, moveable, temporary, or permanent; including: > buildings, masts, towers, frameworks, pipelines, quarries, bridges, and underground works (including shafts or tunnels) > any component of a structure > part of a structure.
Table 1	The table of categories of hazardous substances in Schedule 2 of the MHF Regulations.
Table 1 or 2 hazardous substance	Defined in the MHF Regulations, this means: > hazardous substances specified in column 1 of table 2 of Schedule 2 > categories of hazardous substances referred to in column 1 of table 1 of Schedule 2.
Table 2	The table of named hazardous substances in Schedule 2 of the MHF Regulations.
Threshold quantity	Defined in the MHF Regulations, means the lower threshold quantity or the upper threshold quantity.
Transit depot	Defined in Regulation 3 of the Hazardous Substances (Classes 1 to 5 Controls) Regulations 2001.
Union	Is an organisation that supports its membership by advocating on their behalf. The Employment Relations Act 2000 gives employees the freedom to join unions and bargain collectively without discrimination. Workers can choose whether or not to join a union. A union is entitled to represent members' employment interests, including health and safety matters.
Upper threshold quantity	Defined in the MHF Regulations, means the quantity specified in column 5 of table 1 or column 4 of table 2 of Schedule 2, and calculated in accordance with Part 3 of the MHF Regulations.
Upper tier major hazard facility (UTMHF)	Defined in the MHF Regulations, means a facility that WorkSafe has designated as a UTMHF.
Worker	Defined in HSWA, generally a person who carries out work in any capacity for a PCBU. It covers almost all working relationships, including employees, contractors, sub-contractors, and volunteer workers.

TERM	BRIEF EXPLANATION
Worker representative	In relation to a worker, means: > the health and safety representative for the worker > a union representing the worker > any other person the worker authorises to represent them (eg community or church leaders, lawyers, occupational physicians, nurses, respected members of ethnic communities). Workers can ask a worker representative to raise health and safety issues with a PCBU on their behalf.
Workplace	Defined in HSWA, generally a place where work is carried out for a PCBU, including any place where a worker goes, or is likely to be, while at work.

DISCLAIMER

WorkSafe New Zealand has made every effort to ensure the information contained in this publication is reliable, but makes no guarantee of its completeness. WorkSafe may change the contents of this guideline at any time without notice.

This document is a guideline only. It should not be used as a substitute for legislation or legal advice. WorkSafe is not responsible for the results of any action taken on the basis of information in this document, or for any errors or omissions.

ISBN: 978-0-908336-36-4 (online)

Published: July 2016 Current until: 2018

PO Box 165, Wellington 6140, New Zealand

www.worksafe.govt.nz

WSNZ_2253_JULY 2016

WorkSafe New Zealand
Level 6
86 Customhouse Quay
PO Box 165
Wellington 6140

Phone: +64 4 897 7699
Fax: +64 4 415 4015
0800 030 040
www.worksafe.govt.nz
@WorkSafeNZ

ISBN: 978-0-908336-36-4 (online)

New Zealand Government

WORKSAFE NEW ZEALAND | MAHI HAUMARU AOTEAROA