1 Introduction

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

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

This guidance note will assist operators through the process of identifying, selecting and assessing control measures which are significant components of the Safety Case.

Control measures are the features of a facility that eliminate, prevent, reduce or mitigate the risk to health, safety and property from potential major incidents at an MHF. Control measures take many forms including physical equipment, process control systems, management processes, operating or maintenance procedures, the emergency plan and key personnel and their actions. One purpose of control measure identification and assessment is to help the operator understand how the risks to health and safety associated with potential major incidents are managed.

The MHF regulations require the operator to consider a range of existing and potential control measures for each hazard and consequence of a major incident, and to provide reasons why certain control measures were selected and other control measures were rejected. The process should allow the operator to:

- gain sufficient knowledge, awareness and understanding of the control measures for major incidents to be able to prevent and deal with dangerous occurrences
- identify all existing and potential control measures
- provide a basis for identifying, evaluating, defining and justifying the selection (or rejection) of control measures for eliminating or reducing risk
Guidance Note Control measures for a major hazard facility

• lay the foundations for demonstrating the adequacy of the controls necessary to assure the safety of the facility
• show clear links between control measures and the potential major incidents
• assist in demonstrating that risk is reduced so far as is reasonably practicable in the Safety Assessment process (see WorkSafe guidance note – Safety Assessment for a major hazard facility)
• understand the effectiveness of the control measures and the impact of this on risk
• provide a monitoring regime to ensure the ongoing effectiveness of the control measures.

1.1. Features of control measure identification and assessment

The following factors lead to successful control measure identification and assessment:

- Control measure identification and assessment should be workable and relevant to the facility. It should reflect the Safety Case philosophy.
- Existing knowledge should be reviewed and it should not automatically be assumed that no new knowledge is required.
- The information is provided to persons who require it in order to work safely.
- An appropriate group of workers is actively involved and consultation occurs.
- Uncertainties are identified and reduced to an acceptable level.
- All methods, results, assumptions and data are documented.
- Control measures and their affects on risk are explicitly addressed.
- The assessment is regularly maintained and used as a live document.

Figure 1.1 shows the important steps in the control measure identification and assessment process.

Figure 1.1 – The key steps required to identify, select and assess control measures to minimise the risks from potential major incidents

<table>
<thead>
<tr>
<th>Control measures</th>
<th>Identify, select and assess control measures to minimise the risks from potential major incidents</th>
<th>Establish effectiveness criteria for each individual control, to enable ongoing assurance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify/ select control measures</td>
<td>Identify additional control measures</td>
<td>Adequacy of assessment of controls for each major incident</td>
</tr>
<tr>
<td>What are the existing control measures? For example: • pressure relief valve • equipment specification &amp; design to standard • refer to Figure 3.3 for more controls</td>
<td>What additional measures could we consider to improve the level of safety? For example: • build a barrier around storage tank 3.3</td>
<td>Are the overall control measures adequate to reduce the risk of a major incident? Assess control measures based on (refer to section 3 for more details): • Are there controls from the top end of the risk hierarchy? • Are there different types of controls? • Are there enough layers of protection in place? • Are the controls adequate for the operating circumstances?</td>
</tr>
</tbody>
</table>
1.2. Key definitions

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

**Critical control measures:** Control measures that significantly reduce or eliminate the likelihood of hazards or reduce the severity of consequences. Identification of critical control measures is not required by the MHF regulations.

**Critical Operating Parameter (COP):** The upper or lower performance limit of any equipment, process or procedure, compliance with which is necessary to avoid a major incident.

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

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

**Major incident (related to an MHF):** An uncontrolled incident, including an emission, loss of containment, escape, fire, explosion or release of energy that involves Schedule 9 materials and poses a serious and immediate risk to health and safety.

**Performance indicator:** Any quantitative or qualitative information used to measure the performance of any functional aspect of a control measure. Schedule 10, clause 7 of the OHS Regulations specifies that performance indicators for the effectiveness of adopted control measures, must include –
(a) tests of the effectiveness of the control measures
(b) indicators of the failure of any control measure
(c) actions to be taken in reporting any such failure
(d) other corrective actions to be taken in the event of any such failure.

**Performance standard:** A benchmark, target or reference level of performance set for a control measure as measured by the performance indicator, or for an aspect of the Safety Management System (SMS), against which performance may be tracked. For example, a limit set for the number of false alarms for a process. Performance standards include the methodologies, frequency and results of the audit process.

**Safety Assessment:** A Safety Assessment process consistent with international risk assessment standards, including AS/NZS ISO 31000 – Risk Management.

A Safety Assessment involves an investigation and analysis of the major incident hazards and major incidents to provide the operator with a detailed understanding of all aspects of risk to health and safety associated with major incidents, including –
(a) the nature of each hazard and major incident
(b) the likelihood of each hazard causing a major incident
(c) in the event of a major incident occurring –
(i) its magnitude, and
(ii) the severity of its consequences to persons both on-site and off-site
(d) the range of risk control measures considered.

**So far as is reasonably practicable:** To reduce risk to a level so far as is reasonably practicable involves balancing reduction in risk against the time, trouble, difficulty and cost of achieving it. This requires consideration of:
(a) the likelihood of the hazard or risk concerned eventuating
(b) the degree of harm that would result if the hazard or risk eventuated
(c) what the person concerned knows, or ought reasonably to know, about the hazard or risk and any ways of eliminating or reducing the hazard or risk
(d) the availability and suitability of ways to eliminate or reduce the hazard or risk and
(e) the cost of eliminating or reducing the hazard or risk.

More information on key terms is found in other MHF guidance material available from the WorkSafe website and in the definitions of the OHS Regulations (reg 1.1.5).

2. PLANNING AND PREPARATION

2.1. Coordinating the Safety Case approach

The MHF regulations require the operator to produce and submit a ‘Safety Case outline’ (see the guidance note – Safety Case outline for a major hazard facility) before developing the Safety Case. WorkSafe recommends that this process is used as an opportunity to look at the overall requirements of the Safety Case and to identify areas in which the operator can save time and resources in developing the Safety Case. How each step is planned will need to be structured to suit the facility. This process will also be useful for any review and revision of the Safety Case.
2.2. Scope

Each component of the Safety Case needs to be considered during its compilation. When identifying and assessing control measures, it’s important to consider the following if available:

- the size of the facility
- pilot studies/Safety Cases from similar facilities
- the properties of the Schedule 9 materials and other dangerous goods on-site
- all potential major incidents that have been identified
- the hazards and consequences associated with those major incidents.

Step 1 in Figure 2.1 illustrates the combination used in this example.

**Figure 2.1 – Steps for minimising overlaps**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Step 2</th>
<th>Step 3</th>
<th>Step 4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Hazard identification</strong></td>
<td>Identify major incidents. Identify hazards and outcomes.</td>
<td>Assess likely frequency of each hazard without controls in place. Conduct the initial Safety Assessment to assess the level of risk posed by each major incident, taking existing controls into account. Ensure all practicable steps to reduce risk for each major incident have been considered.</td>
<td>Conduct the final Safety Assessment – assess the level of risk posed by each potential major incident assuming improvement actions are in place.</td>
</tr>
<tr>
<td><strong>Safety Assessment</strong></td>
<td></td>
<td>Ensure all practicable steps to reduce risk associated with each major incident have been considered.</td>
<td></td>
</tr>
<tr>
<td><strong>Control measures</strong></td>
<td>Identify/select control measures. Identify potential additional controls.</td>
<td>Initial ranking of controls for effectiveness (optional).</td>
<td>Adequacy assessments of controls for each major incident.</td>
</tr>
</tbody>
</table>
2.3. Workforce requirements

Because ownership of the Safety Case process is the responsibility of the whole organisation from management to shop floor, and because of the amount of work required to demonstrate a case for safety, the Safety Case requires a large commitment from site personnel.

When carrying out control measure identification, selection and assessment, it is recommended that the operator involves representatives from management, supervisors, operators, maintenance and relevant technical personnel. The operator may also need to employ a third party to provide guidance on the assessment (ie a workshop facilitator) or bring in technical expertise in a specific area.

Table 2.1 – Workforce commitment

Table 2.1 shows the estimated site commitment for a medium-sized site which identified 20 major incident scenarios. The time specified is based on information gathered using a workshop format.

<table>
<thead>
<tr>
<th>Process</th>
<th>Personnel</th>
<th>Time commitment</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Planning and preparation</td>
<td>Safety Case coordinator. HSR.</td>
<td>Two weeks.</td>
<td>Note: this would be carried out at the same time as planning for other steps in the Safety Case.</td>
</tr>
<tr>
<td>Identification/selection of control measures</td>
<td>Workshop participants (six-eight people). Facilitator and scribe.</td>
<td>Two-day workshop.</td>
<td>Note: this would often be carried out as part of hazard identification (see the guidance note – Hazard identification). Additional control measures may be further identified during control measure assessment or Safety Assessment.</td>
</tr>
<tr>
<td>Adequacy assessment of control measures.</td>
<td>Workshop participants (six-eight people). Facilitator and scribe.</td>
<td>Four-day workshop. One day each person gathering information. Follow up – one to two weeks by appropriate personnel if information is readily available on site.</td>
<td>If information is not readily available, as is typical for an older facility, then this follow up work can be significant. Sufficient contingency needs to be allowed.</td>
</tr>
<tr>
<td>Final identification/selection of potential controls for action plan.</td>
<td>Workshop participants (six-eight people). Facilitator and scribe.</td>
<td></td>
<td>This would normally be part of final Safety Assessment (see the guidance note – Safety Assessment for a major hazard site) or SFARP workshop (to confirm that risks have been reduced so far as is reasonably practicable).</td>
</tr>
<tr>
<td>Prepare performance standards and ensure procedures/audit processes in place.</td>
<td>Team or defined individuals.</td>
<td>The time required will depend on what is currently in place.</td>
<td>This may be a significant task. Plan early and estimate the time and resources required.</td>
</tr>
</tbody>
</table>
2.4. Role of workers and health and safety representatives

The operator should develop a role for all workers in the Safety Case process that allows them to contribute and gain knowledge in relation to identification/selection of control measures, assessment of control adequacy, selection of ongoing management criteria and selection of improvement actions. The operator needs to ensure that information is considered on the basis of technical/working knowledge and not on the seniority of the contributor. Decision-making should be transparent and reproducible.

If the workers are represented by any health and safety representatives (HSR), the HSR should be involved in:

- development of the process
- choice of personnel and scheduling
- some workshops (particularly those where decision-making processes are involved)
- reviewing the workshop results
- implementation of any changes arising.

2.5. Scheduling

If it is decided that workshops are the most appropriate method for collecting information, and the scope and personnel involved have been finalised, then the workshops need to be scheduled. They should be conducted as soon as possible to enable Safety Case development/revision to occur within the specified time frame.

When scheduling the workshops, the following should be considered:

- availability of key personnel
- need to maintain production
- need to maintain mental alertness
- need for continuity and consistency
- duration (e.g., keep to a maximum of four to six hours per day to avoid fatigue).

Due to the large number of concurrent tasks, and the pressure on people’s time, it is important to ensure that workshop participants understand the steps involved, the time required and the objectives of each stage of the Safety Case. It is also important in terms of commitment and buy-in that people understand the process upfront. See Figure 2.2 for an example of a workshop timeline.

If a workshop format is not chosen, an appropriate schedule for control selection and assessment work should still need to be drawn up in accordance with the Safety Case outline. Alternative formats may include meetings or informal consultation and information gathering.

---

**Figure 2.2 – Example of timeline for workshops**

<table>
<thead>
<tr>
<th>ID</th>
<th>Task name</th>
<th>Start</th>
<th>Finish</th>
<th>Duration</th>
<th>Aug 2011</th>
<th>Sep 2011</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>24.8.11</td>
<td>27.8.11</td>
<td>4d</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Hazard and control selection</td>
<td>30.8.11</td>
<td>7.9.11</td>
<td>7d</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Initial Safety Assessment</td>
<td>8.9.11</td>
<td>9.9.11</td>
<td>2d</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Control adequacy assessment workshop</td>
<td>10.9.11</td>
<td>20.9.11</td>
<td>7d</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Final safety assessment and implementation plan</td>
<td>21.9.11</td>
<td>23.9.11</td>
<td>3d</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Preparation of Safety Case report</td>
<td>13.9.11</td>
<td>30.9.11</td>
<td>13d</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Notes: This timeline may also need to include time for review and comment. This example is appropriate for small sites or single units of a complex site. Large sites may require a number of similar schedules with some overlap of the tasks or with the tasks occurring at the same time for different areas of the site.
3. Identifying and selecting control measures

3.1. Identifying control measures

Control measures can be identified in a range of ways but this often works best in a workshop format using brainstorming techniques to ensure that the full range of people's experience is captured. An experienced facilitator will help get maximum value from the workshop by drawing out people's knowledge and experience and guiding people through the process. The facilitator's experience and tools such as a prompt list will assist the process (see The Appendix for a list of typical control measures that may be useful as prompts and for a list of considerations for control measures). It may also be useful to draw on outside information as shown in Table 3.1.

<table>
<thead>
<tr>
<th>Stage of process</th>
<th>Information required</th>
<th>Supporting documents/information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control measure identification/selection.</td>
<td>Major incident scenarios, hazards and outcomes of major incident scenarios.</td>
<td>• Handout/poster/presentation on control measure hierarchy and types of control measures.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Examples of specific control measures should be given as prompts.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Protective system lists (eg cause and effect sheets).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Previous risk studies such as hazard and operability study (HAZOP), FMECA (Failure mode, effects and criticality analysis), human reliability studies.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Guidance notes/presentation/poster on layers of protection.</td>
</tr>
<tr>
<td>Selection of potential additional control measures.</td>
<td>Control measures in place. Potential additional control measures.</td>
<td>• As above.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Hazard identification process (major incidents, hazards and consequences for each major incident ie hazard registers, bow ties, fault trees).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Corporate design standards for similar installations.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Australian Standards and design codes for storing or handling the chemicals under review.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• MSDS.</td>
</tr>
</tbody>
</table>

See Figure 3.1 for an example of a hazard register format for recording information from the workshop process.
Understanding the link between control measures and major incident hazards

An understanding of the links between a control measure, the major incident and the hazards giving rise to the major incident will be critical in assessing the ability of the control measure to protect against each hazard. The operator needs to understand the mechanism by which the control works to prevent or manage the potential major incident (i.e. the nature, scale and range of hazards and consequences that each control measure is designed to address and the relationship of the control measure to the hazard, major incident, consequences and other control measures). An understanding is needed of these mechanisms for the range of operating conditions that might exist at the facility (i.e. normal, abnormal and emergency conditions). It is also necessary to determine whether there are sufficient control measures for all possible hazards and consequences and that the control measures in place are robust enough to reduce the risk associated with the potential major incident to an acceptable level.

One way the relationships between hazards, outcomes, control measures and the potential major incident can be represented is a ‘bow tie’ diagram (also called a cause-consequence diagram). The relationship between the proactive control measures, the major incident, reactive control measures and consequences (or outcomes) for each hazard is shown in Figure 3.2. Proactive controls can also be referred to as ‘preventative controls’ and reactive controls referred to as ‘mitigative controls’. The hazard side of the diagram is often referred to as the left hand side and the outcome side as the right hand side for ease of reference during discussions.
Guidance Note Control measures for a major hazard facility

The benefit of using a bow tie diagram is that it is an easily accessible method of documenting information for subsequent readers. However, this information or parts of this information can be recorded in formats such as hazard registers, fault trees and event trees, FMECA reports or any other format which clearly shows linkages.

Figure 3.3 (over the page) shows a bow tie for a major incident. It should not be considered complete as more detail would be expected in a Safety Case submission.
Figure 3.3 – Bow tie of an ammonia release from storage major incident

**Hazard**
- Ammonia release at storage tank

**Consequence**
- Exposure to ammonia

**Key Bow Tie**
- External heat source (e.g., sun)
- NDT inspection program
- Equipment specification and design to ABC standards
- Storage area is protected (chained off/vehicle barriers) – restricted access
- ABC operating procedures for filling tank
- Tank designed for 50°C service (as per design standards)
- Valve and flange fitting training
- Speed limits on-site
- Lifting gear inspection maintenance and testing
- Pressure relief valves
- Component failure
- Storage tank punctured
- Overpressure
- Ammonia release
- At storage tank
- Ignition
- Hot work
- Furnace
- Emergency response plan
- Emergency isolation valve
- Gas detection
- Hot work permit
- Separation distance
- Gas detection in storage area
- Natural ventilation of storage area
- PPE (breathing apparatus available)
- Medical assistance available on-site
- PPE (breathing apparatus available)
- Medical assistance available on-site
- Foam generation capabilities

**Exposure**
- Exposure to ammonia
- Inhalation of ammonia fumes
- Generation of chlorine
- Ammonia mixing with nearby store of hypochlorite
- Escalation to other vessels

**Contingency**

**Control Measures**
- Natural ventilation of storage area
- Gas detection
- Hot work permit
- Emergency response plan
- Medical assistance available on-site
- Gas detection
- Lifting gear inspection maintenance and testing
- Pressure relief valves
- Storage tank design for 50°C service
- Equipment specification and design to ABC standards
- ABC operating procedures for filling tank
- Tank designed for 50°C service (as per design standards)
- Valve and flange fitting training
- Speed limits on-site
- Lifting gear inspection maintenance and testing
- Pressure relief valves
- Component failure
- Storage tank punctured
- Overpressure
- Ammonia release
- Ignition
3.3. Adequacy assessment

3.3.1. Assessing control measures

As part of the Safety Assessment process (described in the guidance note – Safety Assessment for a major hazard facility), the operator needs to demonstrate that the full suite of control measures in place for each potential major incident is adequate to reduce the risk so far as is reasonably practicable.

The assessment of control measures therefore needs to keep in mind that the operator will need to demonstrate that control measures:

- are sufficient to reduce risk so far as is reasonably practicable for all hazards leading to the major incident
- comply with the control hierarchy (see Figure 3.5) which dictates hazards should be eliminated, prevented, reduced or mitigated in that order of preference
- are distributed appropriately with representation of different types of control measures (physical, engineering and administrative/procedural) and of hierarchical categories of control measures (elimination, prevention, reduction and mitigation)
- show layers of protection commensurate with the inherent level of risk posed by the major incident
- consider the full range of operating circumstances
- are effective and viable.

When conducting an adequacy assessment it is important to involve people who have a thorough knowledge of the use and possible failure modes of the control measures. The operator needs to demonstrate that it has considered a reasonable number of existing and alternative control measures, which will vary depending on the scale and complexity of the facility, the nature of the risk profile and changes to technology over time. The MHF regulations require an assessment of all controls.

To ensure time and resources are used where they provide the most benefit, critical control measures may be identified for more in-depth adequacy assessment. The identification of critical controls may be most useful for new operators or new MHFs as this gives a way of prioritising further work on controls. If critical controls are identified, a clear definition of what makes a control 'critical' is required. Also, WorkSafe expects all identified control measures to be implemented and functional irrespective of whether they are described as critical or not.

Figure 3.4 shows the stages of control measure adequacy assessment sequentially. During this process the operator may find that there is a need to select additional control measures or identify improvement actions for current control measures. Figure 3.4 also shows that the process ends when the operator is able to conclude that, with the adopted control measures in place, the risk of a particular major incident has been reduced so far as is reasonably practicable (refer to the guidance note – Safety Assessment for major hazard facility). Table 3.2 shows the information needed for control measure adequacy assessment.
Figure 3.4 – Process of control measure adequacy assessment

<table>
<thead>
<tr>
<th>All selected controls.</th>
<th>Related to major incident.</th>
<th>Are the control measures linked to the major incident?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control measure hierarchy.</td>
<td>Is there a control measure further up the hierarchy which would more effectively manage the hazard?</td>
<td></td>
</tr>
<tr>
<td>Type of control measure.</td>
<td>Is there a spread of physical, engineering and administrative control measures?</td>
<td></td>
</tr>
<tr>
<td>Layers of protection.</td>
<td>Are there enough control measures to ensure coverage is maintained in the event of failure of a control?</td>
<td></td>
</tr>
<tr>
<td>Range of operating circumstances.</td>
<td>Have the full range of operating circumstances been considered?</td>
<td></td>
</tr>
<tr>
<td>Identifying critical control measures (optional).</td>
<td>Have the control measures that are really relied upon been chosen as critical?</td>
<td></td>
</tr>
<tr>
<td>In depth effectiveness and viability.</td>
<td>Will the control measures be effective and viable in a wide range of circumstances?</td>
<td></td>
</tr>
</tbody>
</table>

Table 3.2 – Information required for control measure adequacy assessment

<table>
<thead>
<tr>
<th>Stage of process.</th>
<th>Information required.</th>
<th>Examples of information source</th>
</tr>
</thead>
</table>

Information above is used to show that risk is reduced so far as is reasonably practicable (guidance note – Safety Assessment for a major hazard facility).
3.3.2. Applying the control measure hierarchy

Figure 3.5 represents the generally accepted control hierarchy, which shows the preferential order for the selection of controls. When assessing the effectiveness of control measures, the operator needs to ensure that, where possible, the control has been chosen from the top of the control hierarchy. Where hazards cannot be eliminated, reducing the frequency and/or the magnitude of the major incident are the next most effective routes of control. If a potential major incident cannot be eliminated, robust prevention and mitigation control measures must be in place. It is also important that an appropriate spread of control measures is in place. It would be rare that all hazards or potential major incidents could be eliminated, so in most cases reduction, prevention and mitigation control measures will be required.

See the following examples of application of the hierarchy of control, based on the ammonia release incident at ABC Chemical Company, shown in Figure 3.3.

Figure 3.5 – Control measure hierarchy.

Preference for treatment options

The hierarchy of controls should be applied in the following order:

- **Elimination controls** form the ‘first line of defence’. They eliminate the underlying hazard and are therefore the most effective category of control measure. If practicable they should be selected in preference to any other type, as their existence removes the need for other controls eg a corrosion - resistant metal could replace the original material of construction.

- **Prevention controls** are intended to remove certain causes of incidents or reduce their likelihood. The corresponding hazard remains, but the frequency of incidents involving the hazard is lowered eg introduction of regular maintenance programs can prevent the development of hazards.

- **Reduction controls** are intended to limit the scale and consequence of incidents. They include systems that detect incidents and take some action (eg to reduce the rate of leakage of a toxic gas) and also aspects such as inter-unit separation that prevent escalation of fire and explosion incidents.

- **Mitigation controls** take effect in response to an incident. They may include firefighting systems and, in particular, emergency response plans. Whilst they are on the lowest rung of this hierarchy they remain necessary if risk cannot be eliminated by other means.

A number of these options may be considered and applied individually or in combination.

Example 1

This example shows the benefit of the use of the control hierarchy. Different controls can provide a higher level of protection than others and will better ensure that the risk is reduced so far as reasonably practicable.

For the ammonia storage tank example (Figure 3.3), one hazard is an object being dropped while lifting a piece of equipment over the tank, resulting in a loss of containment. The equipment has to be lifted over the tank because of a lack of access.

One control currently in place (not shown on Figure 3.3) is the use of procedures for conducting all lifts on site. This is a prevention control but it relies on people.

A higher level of control would be to eliminate the need for lifting over the storage tank by relocating the piece of equipment.
3.3.3. Demonstrating adequacy using different types of control measures

Hazard prevention is generally more effective when a range of controls is available. A range of controls may help with demonstrating several layers of protection and independence of controls.

The types of control measures can be categorised into three broad areas – physical, engineering and administrative:

- Physical controls include separation distances, bunding etc but can often be grouped with engineering controls rather than being classed in a separate category.
- Engineering control measures usually involve hardware such as pressure relief valves, automatic shutdowns/trips or deluge systems.
- Administrative control measures can be procedures for site-wide usage such as inductions or Job Safety Analysis (JSA) as well as procedures for specific tasks or providing instruction for a defined activity (in the form of work instructions, inspection checklists or duties to be performed by a particular role).

Example 2

There is more than one control measure that can be used for most hazards. Using the previous example of the dropped object, other control measures which could be considered and/or implemented are administrative:

- vehicle access control
- qualifications for driving mobile equipment
- work instruction covering vehicle access to the ammonia storage area.

While the engineering solution described earlier is the preferred approach, these controls provide protection on a broader range of possible needs, do not cost much to implement and consideration should be given to their implementation.

3.3.4. Common mode failures

Common mode failures are those where two or more controls may fail as the result of a common cause. Without consideration of common mode failures an overly optimistic assessment of the degree of protection provided by the controls in place can be made. Common mode failures can affect all control types – procedural, administrative and engineering controls.

Example 3

Examples of common mode failures for the ammonia storage tank are:

1. The level indicator and high level trip on the ammonia storage vessel could be on the same level transmitter.

Therefore a failure of this single transmitter would fail both controls.

2. All temperature measurement devices are calibrated incorrectly during testing.

3. The power (or utility) supply for a control system fails, impacting multiple controls.

4. Two independent alarms should rely on the same operator to take the same corrective action to be effective.

The common mode failures shown in failure 1 above are best assessed when considering a specific hazard and major incident. Other common mode failures (failures 2 and 3 above) impacting on multiple major incidents need only be assessed once. For these common mode failures, it is helpful to describe how this common mode failure mechanism is managed, which may be via components of the SMS. Some failure modes may need to be covered by both approaches. It is important that any consideration of the adequacy of controls in preventing a specific hazard considers whether the identified controls are independent eg that a common failure cannot render them all non-functional.

3.3.5. Applying ‘layers of protection’

For many potential major incidents, there are numerous layers acting as barriers to prevent, reduce or mitigate incidents. A robust control measure regime will feature a range of independent layers, the number and integrity of which should reflect the inherent level of hazard or risk within the facility. Generally, layers considered for inclusion are: design standards; operating standards; control systems; safety devices; and emergency systems as described in Figure 3.6.

Sometimes all of these layers are not present. Additional layers of protection may be required where:

- the residual risk is high for the hazard
- too much reliance is placed on a single control measure or
- controls are not fully independent and a common cause could result in the ‘loss of control’ and a failure of more than one control measure.

The operator needs to look at the layers of protection provided for each hazard related to each major incident and, taking associated risk into account, to determine whether an appropriate level of protection is provided.
Example 4

The hazard ‘overfilling of a storage tank’ has controls covering a range of layers of protection as follows:

- design standards – dictate that the pump cannot deliver enough pressure to overpressure the storage tank
- operating procedures – procedure for filling the storage tank
- control systems – process monitoring
- safety devices – pressure relief valves
- emergency systems – emergency response plan, emergency isolation valve, gas detection.

If these controls were shown in full on Figure 3.3 the hazard of overfilling the storage tank would be shown as follows:

And the following mitigation controls would appear on the right hand side of the bow tie:

In assessing these layers of protection, the following points would appear:

- while the pump can’t overpressure the storage tank, it can still be overfilled.
  The contents may then expand on a hot day and still overpressure the storage tank
- the pressure relief valves have been designed for fire relief and not sized for the two phase release that will occur with ammonia.

Hence, the important controls are process monitoring and the filling procedures. These rely on a single level indicator and the attention of an operator who may get distracted eg with other tasks requiring attention.
An alternative is to add a high level trip on the pump to the storage tank. The decision was then made to add the high level trip based on the suite of control measures, their effectiveness and viability, and the potentially significant consequences.
3.3.6. Range of operating circumstances
Control measures may vary for different stages of the facility’s lifecycle eg design and construction standards are important for new facilities, but as the facility ages more importance may need to be given to asset integrity management. Similarly, control measures may themselves have lifecycles that may need to be considered. Operating circumstances caused by other factors also need to be considered eg environmental conditions such as heavy rain or drought or low staffing levels caused by emergency callouts.

To determine control measure adequacy, the operator should consider whether the type of control measures in place are appropriate to the lifecycle phase of the facility.

Example 5
When undertaking maintenance on the ammonia storage tank, the operator needs to consider the various operating circumstances.

The potential for a maintenance error leading to a ‘loss of containment’ may normally be managed effectively by the maintenance contractor. However, the storage tank may be inspected during a major site shutdown when a large number of contractors unfamiliar with the site and its standards do the work. These contractors may not be familiar with the facility’s engineering standard or with the procedures associated with different components of the work.

To assess the adequacy of control measures, the operator must consider whether the contractor management system adequately controls maintenance during a major shutdown as well as routine maintenance.

3.3.7. Identifying critical control measures
Some MHFs put effort into classifying some of their control measures as critical and then subject them to more scrutiny appropriate to the level of protection they need to provide. Neither the MHF regulations or WorkSafe require this step in the adequacy assessment process. However, it may be useful for prioritising effort and resources for new operators, new MHFs or where there are a large number of control measures across the facility. Critical control measures may represent between 10 to 25% of control measures identified for a large facility. The following specific factors are a guide in determining whether a control measure is critical:
• a control measure is relied upon to reduce or mitigate incidents having very severe potential consequences
• a single control measure can reduce or prevent a major incident hazard and therefore prevent a major incident.

The following may also be taken into account:
• other control measures that provide ‘back-up’, are known to be weak (eg of poor reliability or effectiveness)
• a control measure is relied on to control a number of different major hazards
• a control measure is relied on to prevent the most likely hazards that cause a major incident.

Example 6
For the ammonia storage facility, one of the critical controls selected is the relief valve as it protects against a number of hazards (eg overpressure and overfilling) and mitigates against events with very severe consequences (eg large release of toxic ammonia).

3.3.8. Effectiveness and viability
The adequacy of control measures for the major incidents they control depends upon various factors such as the effectiveness and viability of the control measures. Effectiveness is a measure of how well the control measure performs, or is likely to perform, and can be defined in terms of: functionality and reliability including reliance on people, independence from other controls, diversity and maintainability.

Viability assesses the ongoing practicality of the control. It can be defined as compatibility, availability, survivability in the given scenario, cost and whether it is a proven approach or technology. A control measure may have been viable when first implemented but may no longer be viable due to obsolescence.

3.3.9. Effectiveness and viability criteria
Whether each control measure is effective and viable needs to be determined. Following is a series of questions which might help to determine whether or not this is the case:
• What is the functionality of a control measure against the relevant hazards? Is it sufficient to control the hazard in the intended manner ie is it fit for purpose, will it suppress the hazard completely, prevent escalation or simply mitigate effects? Functionality can include a wide range of performance characteristics eg the quantity of firefighting water, the delivery rate per square metre and the response time from onset of the fire to applying water/other media.
• What is the survivability of the control measure in an incident? Is the control measure able to function as intended during the types of incidents it is expected to reduce or mitigate? Survivability can include the ability to survive fire or blast damage, and the other possible
consequences of major incidents, and also the ability to continue to function as intended under abnormal process conditions, e.g., extreme temperature.

- **Reliability** dictates whether the control measure will function at all if required in an incident. Is the reliability of individual control measures, and of all control measures in combination, appropriate to the level of risk presented by the associated hazards? Is function testing sufficiently frequent to detect failures and will failures, once detected, be rectified promptly?

- **Reliance on individuals including outside parties.** Many control measures are expected to be within direct control of the operator. There may also be control measures that require cooperation with other parties. An example is fire protection systems which will require cooperation with the fire brigade or contractors. The operator needs to ensure the quality, standard and frequency of work by those individuals meets the facility’s requirements.

- **Independence** and **diversity** are related factors in assessing control measures, and in selecting or rejecting them. If a set of control measures can all be disabled by one failure mechanism, or the failure of one control measure is likely to cause the failure of others, then the control measures are not independent and it may not be appropriate to count such measures as separate. Adopting a diverse range of control measures (such as inherent safety features, hardware and procedural controls and other preventative and mitigative measures) will assist in achieving independence. Is there a balance of different types of control measures for each hazard, i.e., is there a diversity of control measures?

- Can the control be **maintained**? This will rely on factors such as availability of parts, physical access, availability of specialist knowledge, etc. Consistency across the plant for the type of control can simplify the process of maintenance, e.g., consistent gasket specifications for similar service.

- **Compatibility** takes into consideration how alternative control measures may interact with the rest of the facility, if introduced. Are new control measures compatible with the facility and any other control measures already in use? For example, does the valve on a manual shutoff turn in the same direction as other shutoff valves in the plant?

- The **availability** of a control measure relates to how easy it is to obtain the control measure initially and to maintain supply of spare parts or replacements. Can the control measures be implemented at the facility considering their availability and cost?

- A control measure may be considered appropriate based on compliance with an **applicable standard**. However, if this approach is used, the operator needs to demonstrate that the standard is applicable. In addition, the control measure should be kept up-to-date with any changes to the standard. A **proven** control measure can be demonstrated by the period of time that it has been used successfully.

- Does this control measure provide sufficient benefit for the **cost**? Is there something which would be more effective for the same or lower cost?

### Example 7
The effectiveness and viability of the relief valve on the ammonia storage tank was assessed against the following criteria:

- **Functionality** – The scenarios considered included overfilling and thermal expansion of contents. Calculations are available that demonstrate that the pressure relief valve capacity is adequate for the service.

- **Survivability** – During release the temperature will drop, however, the design specification shows that this was allowed for in the design and the vendor/supplier information shows that the material selected will handle this low temperature.

- **Reliability** – The pressure relief valve is listed on the site relief valve register and is on the planned inspection program. The inspection program is up to date.

- **Reliance on individuals** – The operator only uses qualified personnel for relief valve inspection and maintenance. There are detailed procedures in place to control the work.

- **Independence** – The pressure relief valve is independent of any initiating cause and other control measures. No common causes have been identified.

- **Maintainability** – There is an installed spare that allows the pressure relief valve to be maintained whilst retaining the protection required.

- **Compatibility** – There are many pressure relief valves on-site and skills are available for their management. The site has standardised to one manufacturer (note that this may introduce a common mode failure).

- **Availability** – Equipment installed and spares are still available or can be manufactured.

- **Cost** – Relief valve already installed. Cost not an issue.

- **Applicable standards** – Relief valve managed as per AS/NZS 3788.

- **Proven** – Pressure relief valves in ammonia service have been used reliably for many years.
When selecting performance indicators, the SMART principle (Specific, Measurable, Appropriate, Realistic and Timely) should be considered. Indicators should relate to the specific function performed by the control measure, and there may be more than one performance indicator necessary for a single control measure.

### Example 9

One of the control measures on the ammonia storage vessel is a pressure relief valve, also referred to as a pressure safety valve (PSV). The pressure relief valve is a control measure for two hazards 'overfilling of storage tank' and 'external heat source'. Performance indicators and related performance standards have been established for this control measure, as follows.

#### Performance indicators and standards – pressure relief valve

<table>
<thead>
<tr>
<th>Performance indicator</th>
<th>Performance standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relief capacity</td>
<td>x' kg/sec</td>
</tr>
<tr>
<td>Pop pressure of relief valve</td>
<td>Standard is +/- 3% of set pressure as for a new valve supplied to AS 1271. If pop pressure exceeds +/- 3% from set pressure then overhaul as per AS 1271. If pop pressure exceeds 110% of set pressure then reduce test interval.</td>
</tr>
<tr>
<td>Test interval</td>
<td>Five years (max. interval as per AS 3788).</td>
</tr>
<tr>
<td>Reliability</td>
<td>98%</td>
</tr>
</tbody>
</table>

Notes:
The relief capacity is only required for the specification and purchase of the equipment. Once installed the relief capacity is assumed to be correct providing the relief valve and piping is clear, no changes to the process have occurred and the relief valve is maintained.

Performance indicators should measure not only how well the control measures perform, but also how well the management system is monitoring and maintaining them. This requires performance indicators and standards for each control measure, as well as having them for the SMS (see the guidance note – Safety Management System for a major hazard facility).
Example 10
Performance indicators for the relief valve management system

These indicators assess how well relief valves are being managed for the whole facility including the relief valve on the ammonia storage vessel. Due to the large number of relief valves, it may be possible to measure reliability for relief valves as a group.

Performance indicators that can be applied to the overall management of relief valves are:

<table>
<thead>
<tr>
<th>Performance indicator</th>
<th>Performance standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Percentage of relief valves tested within scheduled time</td>
<td>95%</td>
</tr>
<tr>
<td>% reliability</td>
<td>98%</td>
</tr>
<tr>
<td>Number of PSV exceeding inspection interval by three months</td>
<td>‘y’ valves</td>
</tr>
</tbody>
</table>

Note:
Reliability is assessed as the percentage of failed valves (‘failed in dangerous state’) when tested.

Performance indicators take many forms and can be quantitatively or qualitatively expressed.

3.4.2 Critical Operating Parameters

COPs represent the upper or lower limit of any process or operational parameter beyond which the risk of a major incident substantially increases. The sum total of COPs may define the safe operating envelope of the facility. COPs are singled out due to their fundamental importance to the safe operation of the facility.

A COPs is usually a process or other variable (e.g. temperature, pressure, composition) that can be measured quantitatively. If this parameter is exceeded it is liable to undermine the safe operation of the facility. This is illustrated in Figure 3.7.

While a COP is typically defined as a continuous variable (such as pressure) that is constantly displayed on a control system, it may also be appropriate to define a discrete value as a COP. For example, the staffing level of the facility or the number of firewater pumps on-line.

The critical difference between a COP and a performance standard is that COPs need to be monitored and managed on a continuous basis, whereas performance standards are generally something against which performance is periodically assessed. Both are necessary in determining whether operations are safe.

The purpose of identifying a COP is to ensure that more robust monitoring and management of that parameter occurs. COPs are best defined for those parameters where there is a high reliance on the operator to respond to a process or manage an activity appropriately.

COP documentation needs to be continuously available to operating personnel and provide clear guidance as to how people should respond if a breach occurs.
Guidance Note Control measures for a major hazard facility

4. Output of control measure assessment

4.1. Control measure outputs

At the end of the process of control measure identification, selection and assessment, the operator will have the following information for input into the Safety Case:

- a list of the existing and potential control measures and an understanding of their relationship to major incidents
- adequacy assessment information for existing controls and any new controls which are to be implemented
- a list of improvement actions recommended for current and potential control measures
- a list of hazards where additional control measures may be desirable
- a list of performance indicators, standards and COPs.

These outputs should be documented with clear linkages between the hazard identification and Safety Assessment processes, the SMS and the outcomes from the control measure assessment. Good documentation at this stage will significantly help the demonstration of the adequacy of control measures that is required in the Safety Case under reg 5.2.15(2). This is covered in more detail in the guidance note – Requirements for demonstration.

4.2. Uses of control measure outputs

The control measure outputs can be used:

- as an input to a demonstration that risk is reduced so far as is reasonably practicable
- to improve control measures by implementing improvements where deficiencies have been identified eg by modifying procedures, implementing training or using a specified supplier
- to identify new control measures to be implemented
- to monitor ongoing effectiveness of individual control measures and the systems that manage them
- as an input to the action plan arising from the Safety Assessment.

3.5. Greenfield sites

When assessing control measures for greenfield sites the requirements do not change. However there are some differences in approach and expectation. As control measures have only been specified in the design phase, the following should be considered:

- a wider consideration of alternative control measures. In particular newer and more effective control measures may be available. Simply applying technology from older plants may not demonstrate that risk has been reduced so far as is reasonably practicable
- controls that are higher in the hierarchy of controls.

With many greenfield sites the operating personnel are often not available early in the design process when control measures are selected, as they may not have been employed. There is significant benefit in seeking operator input (eg from another site) in the control selection to ensure practical, hands-on experience is incorporated into the selection process.

Design personnel are largely responsible for ensuring that the control measures are adequate for all operational modes. The operator needs to ensure that there is a robust and transparent assurance process that operational personnel can verify before, during and after commissioning.

All personnel need to be consulted and informed. Therefore, even though personnel may not be able to be fully involved during the design, the operator must provide adequate training on control measures prior to commencing operation of the plant.

Example 11

In the incident scenario previously described where there is overpressure of the storage vessel due to overfill of the tank, sufficient space is required to allow for thermal expansion. There is no high level protection and the relief valve is not designed for liquid release which has resulted in a high reliance placed on operator action. The level is therefore defined as a COP with a never-to-exceed level of 85%.
Table 4.1 gives an indication of the type of information usually included in an implementation plan. The plan is designed to be an evolving document and there should be many actions in it and actions should be continually added to it as well as being closed out.

**Table 4.1 – Example implementation plan**

<table>
<thead>
<tr>
<th>No.</th>
<th>Action</th>
<th>Time frame</th>
<th>Responsibility</th>
<th>Status/comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Feedback from workshops to plant operator representatives</td>
<td>Due mid September 2011</td>
<td>Plant Manager – A. Brown</td>
<td>Complete (meeting held 15/9/11).</td>
</tr>
<tr>
<td>2</td>
<td>Control measure training for Plant A operators</td>
<td>Due start October 2011</td>
<td>Plant Manager – A. Brown</td>
<td>Training materials prepared. Training schedule issued and first session scheduled for 20/10/11.</td>
</tr>
<tr>
<td>3</td>
<td>Audit of maintenance of control measures</td>
<td>Due end November 2011</td>
<td>Safety Manager – P. Jones</td>
<td>25% of control measures audited. On schedule.</td>
</tr>
<tr>
<td>4</td>
<td>Review of critical control measure list</td>
<td>Due end August 2012</td>
<td>Safety Manager – P. Jones</td>
<td>Not started.</td>
</tr>
<tr>
<td>5</td>
<td>Relocate equipment requiring lifting</td>
<td>Due mid September 2011</td>
<td>Plant Manager – A. Brown</td>
<td>Completed (equipment relocated 10/9/11).</td>
</tr>
</tbody>
</table>

5. **Review and revision**

At a minimum, a facility is expected to review and revise its Safety Case every five years. During the review and revision of a Safety Case, it is expected that facilities will review information which was prepared for the existing Safety Case, to revalidate assumptions and ensure accuracy. This means that control measures will be reassessed and additional controls may be identified to ensure that risk has been reduced so far as is reasonably practicable. New knowledge and/or information based on experience during the existing Safety Case should be included. This may include changes to effectiveness of control measures or identification of new, required control measures.

6. **Quality assurance**

At the completion of the control measure assessment phase it is important that the operator conducts quality assurance or a check of the results. The following table (Table 6.1 over page) outlines the key activities and checks that should be undertaken to ensure quality in the control measure selection and assessment process. These checks will also assist in ensuring that all control measures have been identified, selected and assessed for major incidents.
<table>
<thead>
<tr>
<th>Activity</th>
<th>Check</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify all control measures have been identified</td>
<td>Use a checklist to confirm that all types of control measures have been identified.</td>
</tr>
<tr>
<td></td>
<td>Have personnel, who were not present when control measures were identified, reviewed the hazard register (or bow tie diagrams)?</td>
</tr>
<tr>
<td></td>
<td>Review previous risk assessments to identify incidents and controls not identified during the hazard identification.</td>
</tr>
<tr>
<td></td>
<td>Review other documents that may indicate additional control measures eg cause and effect diagrams for protective systems, manufacturer (of equipment) manuals.</td>
</tr>
<tr>
<td>Verify accuracy of information</td>
<td>There is a need to confirm that the control measures are in place. Experience shows that this is not always the case. An individual should be appointed to verify the control measure is in place and meets the description provided in the hazard register.</td>
</tr>
<tr>
<td></td>
<td>A field check will identify whether a control measure has been changed over the life of the facility. Frequently it is found that the control measure has been modified and the documentation not updated to reflect the change.</td>
</tr>
<tr>
<td></td>
<td>A review process is included to verify the output of control monitoring eg adequacy assessments, criticality assessment.</td>
</tr>
<tr>
<td></td>
<td>Where the adequacy assessment includes verifying the functionality for the control measure, is there documentary evidence? Is it linked with the Safety Case?</td>
</tr>
<tr>
<td>Verify outcomes have been communicated (adequacy assessment, performance indicators, critical operating parameters)</td>
<td>Is there a communication/training plan in place?</td>
</tr>
<tr>
<td></td>
<td>Is there a requirement for this training to be signed off after completion?</td>
</tr>
<tr>
<td></td>
<td>Is this training list available and does it confirm that all relevant personnel have been trained?</td>
</tr>
<tr>
<td></td>
<td>Are written procedures in place where required eg COPs?</td>
</tr>
</tbody>
</table>
## 7. Compliance checklist

Table 7.1 contains information on the MHF regulations as they relate to control measures.

### Table 7.1 – MHF regulations relating to control measures

<table>
<thead>
<tr>
<th>Section</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reg 5.2.5</td>
<td>The operator must establish and implement an SMS that provides a comprehensive and integrated management system for all aspects of adopted control measures. The SMS must include performance indicators for the effectiveness of those control measures.</td>
</tr>
<tr>
<td>Reg 5.2.7</td>
<td>The operator must conduct a Safety Assessment that provides a detailed understanding of the risk associated with major incidents and which considers a range of control measures. The Safety Assessment must document the viability and effectiveness of the range of control measures considered, and the reasons for their selection or rejection.</td>
</tr>
<tr>
<td>Reg 5.2.8</td>
<td>The operator must adopt control measures which eliminate or, if it is not practicable to eliminate, reduce so far as is reasonably practicable, risk to health and safety. Control measures must include measures to reduce the magnitude and severity of incidents in the event that they occur.</td>
</tr>
<tr>
<td>Reg 5.2.9</td>
<td>The emergency plan must be included among the control measures adopted under reg 5.2.8.</td>
</tr>
<tr>
<td>Reg 5.2.12</td>
<td>The operator must review and revise the hazard identification, Safety Assessment and adoption of control measures, to ensure continuing compliance with the requirement to eliminate or reduce risk so far as is reasonably practicable. Such reviews are necessary before a modification of the MHF, after a major incident occurs, when a deficiency is indicated in a control measure, at WorkSafe’s direction and at least every five years.</td>
</tr>
<tr>
<td>Reg 5.2.13</td>
<td>The operator must develop a role for workers in relation to adopting/reviewing control measures.</td>
</tr>
<tr>
<td>Reg 5.2.15</td>
<td>The Safety Case must contain a summary of the contents of the SMS, a summary of the documentation from the hazard identification and Safety Assessment activities and the information specified in Schedule 12. The Safety Case must demonstrate that the adopted control measures are adequate and that the SMS is comprehensive and integrated for all aspects of them. The Safety Case must contain a statement signed by the chief executive certifying certain prescribed matters.</td>
</tr>
<tr>
<td>Division 5</td>
<td>The operator must consult, if reasonably practicable, with HSR on the adoption and review of control measures, and must inform, instruct and train employees and other relevant persons in the implementation of control measures and the associated hazards.</td>
</tr>
<tr>
<td>Reg 5.2.35</td>
<td>The operator must adopt control measures to eliminate or reduce so far as is practicable the extent of damage to property caused by any major incident.</td>
</tr>
<tr>
<td>Schedule 10</td>
<td>The SMS must include a description of the procedures and instructions for the safe operation of the plant, the mechanical integrity of the plant, plant processes and control of abnormal operations. It must also include performance standards for the SMS and performance indicators for control measures and provision for auditing performance against these measures.</td>
</tr>
<tr>
<td>Schedule 12</td>
<td>The Safety Case must include a detailed description of the control measures, their critical operating parameters, performance indicators and standards, and the key personnel and resources available to intervene in the event of their failure.</td>
</tr>
</tbody>
</table>
8. **Further reading**

The following are recommended sources of general information which may be useful in addition to the information provided in this guidance note.


**Human error**


9. **Appendix**

**Examples of control measures**

<table>
<thead>
<tr>
<th>Active/passive fire protection</th>
<th>Lifting procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarms/trips/interlocks</td>
<td>Maintenance procedures</td>
</tr>
<tr>
<td>Contractor management</td>
<td>Material Safety Data Sheets (MSDS)</td>
</tr>
<tr>
<td>Control room design</td>
<td>Operating procedures</td>
</tr>
<tr>
<td>Control systems</td>
<td>Permit to Work systems</td>
</tr>
<tr>
<td>Corrosion/selection of materials</td>
<td>Plant layout</td>
</tr>
<tr>
<td>Design codes – buildings/structures</td>
<td>Plant modification/change procedures</td>
</tr>
<tr>
<td>Design codes – jetties</td>
<td>Quench systems</td>
</tr>
<tr>
<td>Design codes – pipework</td>
<td>Raw materials control/sampling</td>
</tr>
<tr>
<td>Design codes – plant</td>
<td>Reaction/product testing</td>
</tr>
<tr>
<td>Drum/cylinder handling</td>
<td>Reliability of utilities</td>
</tr>
<tr>
<td>Earthing</td>
<td>Relief systems/vent systems</td>
</tr>
<tr>
<td>Emergency isolation</td>
<td>Roadways/site traffic control/immobilisation of vehicles</td>
</tr>
<tr>
<td>Emergency response/spill control</td>
<td>Secondary containment (eg bunds)</td>
</tr>
<tr>
<td>Explosion relief</td>
<td>Segregation of hazardous materials</td>
</tr>
<tr>
<td>Hazardous area classification/flame/flameproofing/roofing</td>
<td>Site security</td>
</tr>
<tr>
<td>Inerting</td>
<td>Training</td>
</tr>
<tr>
<td>Inspection/non-destructive testing (NDT)</td>
<td>Warning signs</td>
</tr>
<tr>
<td>Leak/gas detection</td>
<td></td>
</tr>
</tbody>
</table>
Guidance Note Control measures for a major hazard facility

Control measure considerations

<table>
<thead>
<tr>
<th>Control measure hierarchy</th>
<th>Type of control measure</th>
<th>Layers of protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elimination</td>
<td>Engineering</td>
<td>Design standards</td>
</tr>
<tr>
<td>Substitution</td>
<td>Administrative</td>
<td>Control systems</td>
</tr>
<tr>
<td>Prevention</td>
<td>Physical</td>
<td>Operating procedures</td>
</tr>
<tr>
<td>Reduction</td>
<td></td>
<td>Safety devices</td>
</tr>
<tr>
<td>Mitigation</td>
<td></td>
<td>Emergency systems</td>
</tr>
<tr>
<td>PPE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Is there a control higher up the hierarchy that would more effectively manage the hazard?
Where appropriate, is there a spread of controls across the hierarchy?
Are the layers of protection adequate for the level of risk posed by the hazard?

Further Information
Contact the WorkSafe Victoria Advisory Service on 1800136089 or go to worksafe.vic.gov.au

Related WorkSafe publications
Guidance note – Safety Assessment for a major hazard facility
Guidance note – Safety Case outline for a major hazard facility
Guidance note – Safety Management System for a major hazard facility

Other publications
Australian Standard AS127:2003 Safety valves, other values, liquid level gauges and other fittings for boilers and unfired pressure vessels.

Note: This guidance material has been prepared using the best information available to the Victorian WorkCover Authority and should be used for general use only. Any information about legislative obligations or responsibilities included in this material is only applicable to the circumstances described in the material. You should always check the legislation referred to in this material and make your own judgement about what action you may need to take to ensure you have complied with the law. Accordingly, the Victorian WorkCover Authority cannot be held responsible and extends no warranties as to the suitability of the information for your specific circumstances; or actions taken by third parties as a result of information contained in the guidance material.

On 18 June 2017, the Occupational Health and Safety Regulations 2017 (OHS Regulations 2017) replaced the Occupational Health and Safety Regulations 2007 (OHS Regulations 2007), which expired on this date. This publication has not yet been updated to reflect the changes introduced by the OHS Regulations 2017 and should not be relied upon as a substitute for legal advice.

Information on the key changes introduced by the OHS 2017 Regulations can be found in the guidance titled Occupational Health and Safety Regulations 2017: Summary of changes - available at https://www.worksafe.vic.gov.au/__data/assets/pdf_file/0011/207659/ISBN-OHS-regulations-summary-of-changes-2017-04.pdf. However, this guidance document contains material of a general nature only and is not to be used as a substitute for obtaining legal advice.