

# Major Hazard Facilities Regulations Guidance Note

## The Requirements for “Demonstration” Under the Occupational Health and Safety (Major Hazard Facilities) Regulations

MHD GN-16

Rev 1

January 2006

### Core Concepts

- The Safety Case that the operator prepares for a major hazard facility must include information sufficient for the purpose of demonstrating that the control measures adopted at the facility are adequate and that the safety management system is comprehensive and integrated for all aspects of the adopted control measures.
- This information needs to be sufficiently transparent and detailed for it to be understood by others, and for WorkSafe to decide whether it is satisfied with the adequacy of the control measures and the effectiveness of the SMS. WorkSafe’s experience in assessing Safety Cases has shown that the operator, as well as describing the approach taken, and the overall results, should also provide some detailed worked examples.
- In order to demonstrate that the adopted control measures are adequate, they must be shown to eliminate, or reduce so far as is reasonably practicable, the risk to health and safety. Under Victorian legislation, the factors that dictate what is practicable are the severity of each hazard or risk, the state of knowledge about each hazard/risk and possible control measures, the availability and suitability of control measures, and the cost of control measures. The adopted control measures should also be shown to provide suitable breadth, depth and reliability of control.
- In order to demonstrate that the SMS is comprehensive and integrated for all aspects of the control measures, it needs to be shown to fully support and maintain the performance of the control measures within an integrated management framework.
- The effort expended to make the demonstrations should be proportionate to risk, with the majority of the analysis and assessment focussed on the higher risk hazards and potential major incidents.
- Before deciding to issue an MHF licence, WorkSafe must be satisfied that:
  - The Safety Case has been prepared in accordance with Reg 402;
  - The operator has complied with Part 3 of the Regulations;
  - The operator has the ability to operate the facility safely; and
  - The operator has complied with Part 5 of the Regulations.

Only Regulation 402 requires information for the purpose of making a demonstration, but the operator should ensure that evidence is available to enable WorkSafe to make an assessment in relation to the other three factors.

- In assessing a Safety Case and the other matters relevant to licensing, WorkSafe will carry out a range of general and specific tests, addressing whether the operator:
  - has complied with all of the duties under the Regulations;
  - is conducting the necessary activities under the Regulations in a manner that links coherently and functions effectively;
  - is doing all that is necessary and sufficient to provide for safe operation.
- The approach that each operator employs in making the required demonstrations should reflect the nature of the facility, its culture and its risks. Depending on the circumstances, it may include:
  - comparison with standards, codes and industry practices;
  - analysis of the risks, and of the benefits and costs of alternative control measures;
  - assessment of the appropriateness of control measures and their performance indicators;
  - comparison with benchmarks for risk and for management performance;
  - comparison with best practice management system frameworks;
  - judgement by different affected groups; and
  - demonstration of past and planned improvements.

In practice a combination of approaches is likely to be necessary.

## 1 Introduction and Purpose of This Guidance Note

This document provides guidance on the areas where the operator of a major hazard facility is required (as part of the Safety Case) to make a 'demonstration' to WorkSafe, and on areas where WorkSafe must be 'satisfied' in relation to the operator's regulatory compliance and safety management.

The purpose of the guidance is to amplify the meaning and intent of the Regulations. General issues that need to be considered are identified, and high-level examples of approaches that could be taken are provided. The guidance does not provide a detailed approach to meeting the requirements of the Regulations. In keeping with the overall goal-setting philosophy of the Regulations, the operator should decide on an approach appropriate to the facility, the nature of its hazards and risks, and the operator's own methods of safety management, but should ensure the method is transparent to VWA.

Guidance Notes indicate what is explicitly required by the Regulations, discuss good practice and suggest possible approaches. An explicit regulatory requirement is indicated by the word **must**, other cases are indicated by the words should, may, etc. WorkSafe acknowledges that what is good practice, and what approaches are valid and viable, will vary according to the nature of different MHFs and their inherent hazards.

**This Guidance Note does not purport to be a comprehensive statement on all or any provision of the Regulations. The document necessarily contains matters of interpretation and policy and is not exhaustive. The document is not a substitute for detailed advice on the Regulations or the Acts under which the Regulations have been made.**

This guidance will be of use to those with responsibility for development of the Safety Case (GN-3) and for compliance with the overall MHF Regulations.

The objective of making 'demonstrations' via a Safety Case is to provide all stakeholders with assurance that the operator is achieving safe operation of the facility, by use of adequate control measures and satisfactory management systems. In particular, effective demonstration within the Safety Case provides WorkSafe with some of the evidence necessary to support the issuing of a licence to operate the MHF. Subsequently, WorkSafe will conduct inspections and other verifications against the Safety Case and its demonstrations. Periodically, and following major changes to the facility or its operations, the demonstrations will need to be reviewed to ensure safe operation is being maintained. Hence, the required demonstrations are of critical importance in first obtaining and then maintaining an MHF licence.

Demonstration is a challenging area, where there is limited local experience, as there has been no formal requirement to demonstrate adequacy of safe operation in previous WorkSafe legislation in Victoria.

### Definitions

In the context of this Guidance Note, demonstration means the provision (in a transparent manner) of information, data and evidence, analysis and reasoned argument, such as to form a logically constructed and convincing case. The overall process of demonstration will include an argument, backed-up by documentation from technical analyses, observation of the behaviour of equipment, management systems and control measures, records of tests and drills, real-time information, electronic media and other data.

Adequacy has the same general meaning as "fit for purpose" or "fully sufficient". Adequacy is achieved if everything necessary to meet the overarching regulatory objective of providing for safe operation has been (or will be) implemented, and if all specific requirements of the Regulations are met.

In fact it is an aspect that operators of major hazard facilities within the European Community continue to find challenging, even after many years with a Safety Case regime in place.

## 2 Legislative Basis

Reg 402	The contents of the Safety Case must be sufficient for the purposes of demonstrating: <ul style="list-style-type: none"><li>• that the Safety Management System provides a comprehensive and integrated system for all aspects of control measures adopted for major hazards and major incidents; and</li><li>• the adequacy of the control measures adopted or reviewed under Regulations 304 and 306.</li></ul>
---------	---

Reg 803	<p>Before deciding to grant a licence to the operator of an MHF, WorkSafe must be satisfied that:</p> <ul style="list-style-type: none"> <li>the safety case has been prepared in accordance with Regulation 402;</li> <li>the operator has complied with the provisions of Part 3;</li> <li>the operator has the ability to operate the MHF safely; and</li> <li>the operator has complied with the provisions of Part 5.</li> </ul>
---------	---

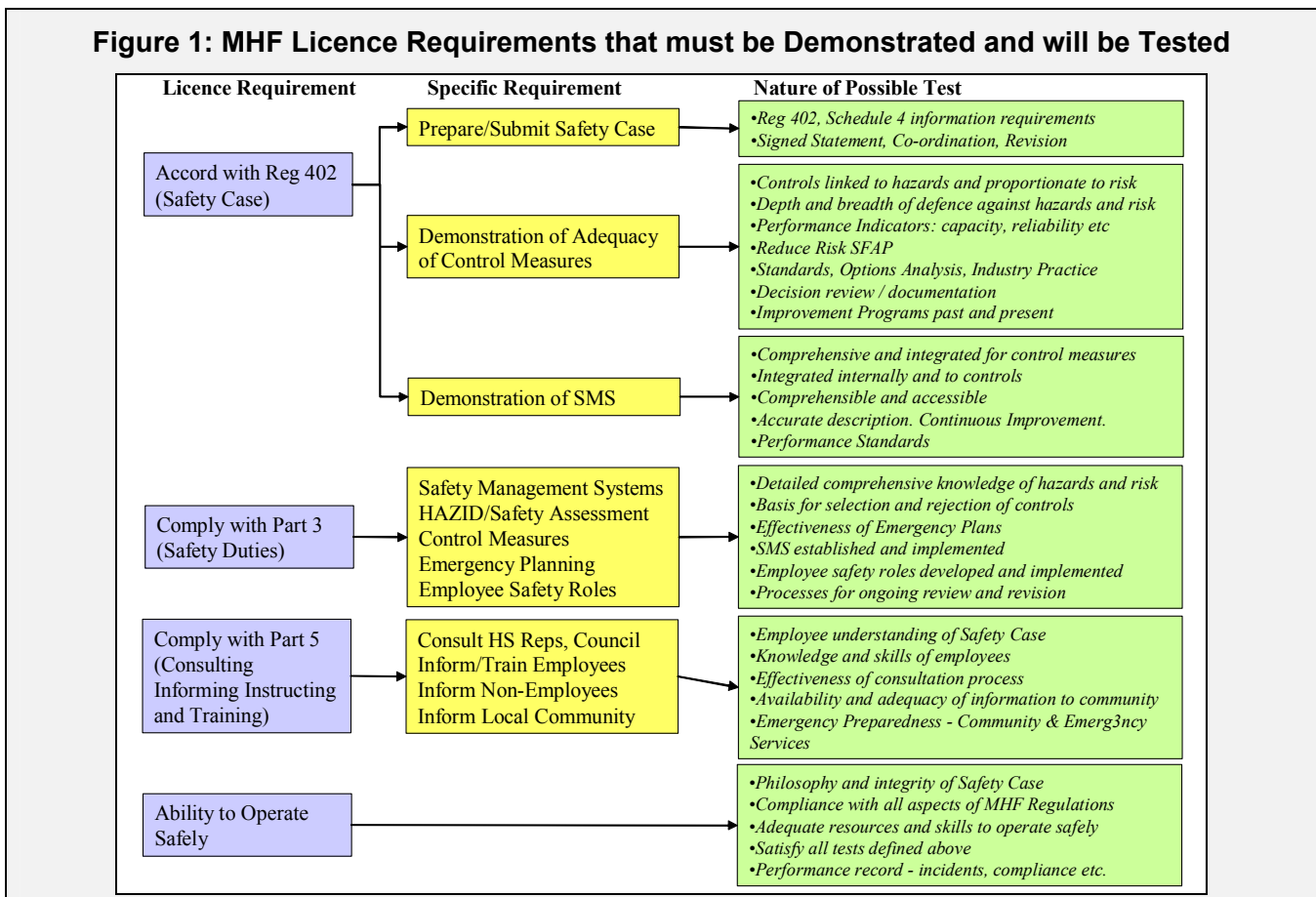
### 3 What Demonstrations are Required?

As noted above, there are four aspects about which WorkSafe must be satisfied before deciding to grant a licence to operate an MHF. However, there is a requirement for the operator to make a 'demonstration' to WorkSafe only in relation to one of these items, Regulation 402, which states that the content of the Safety Case must be "sufficient for the purposes of demonstrating" that:

- The control measures adopted or reviewed under Regulations 304 and 306 are adequate; and
- The SMS is comprehensive and integrated for all aspects of those control measures.

These demonstrations are required because of the importance of control measures and the SMS. Specifically, control measures are the means by which risk to health and safety is eliminated or reduced so far as reasonably practicable (Regulation 304(1)), whilst the SMS is the primary means of ensuring safe operation (Regulation 301(2)). Furthermore, it is activities that are carried out under the SMS that ensure the necessary performance of the control measures.

However, whilst 'demonstration' is required only in relation to these specific aspects, the full content of Regulation 803(1) indicates that granting of an MHF licence will depend on WorkSafe being satisfied in relation to other matters. The operator should therefore consider all of the matters relevant to Regulation 803(1), evaluate what evidence is required to satisfy WorkSafe, and provide this information in the Safety Case or make it available to WorkSafe by other means. The various licence requirements, and the general nature of the tests against these requirements, are summarised in Figure 1.



Operators should develop approaches to these demonstrations that are appropriate and meaningful to the facility and to the operator's safety culture. In addition the demonstrations need to be conveyed in a way that WorkSafe can understand from an external perspective, and be satisfied with. Operators should bear in mind the nature of the tests that WorkSafe will carry out, which will include:

- **Assessment of the operator's compliance with individual requirements of the Regulations.** For example, the operator must have carried out a hazard identification and safety assessment, using appropriate techniques, which considered a range of control measures. This must have resulted in identification of all potential major incidents and related hazards, and a detailed understanding of all aspects of the risk. WorkSafe would therefore assess the operator's processes for hazard identification and safety assessment, and may test the understanding of the hazards, potential major incidents and control measures of a range of the operator's personnel.
- **Evaluation of whether the operator's main duties under the Regulations link together coherently.** As well as conducting individual activities in accordance with the Regulations, the operator needs to ensure that these activities interface correctly. For example the control measures adopted under Part 3 should relate directly to the identified hazards, and have overall reliability proportionate to the risk as determined by safety assessment. Training should be based on the understanding of hazards and risks that has been derived. Therefore WorkSafe will assess whether the operator has satisfactorily used the outcomes of selected activities under the Regulations as input to other relevant activities.
- **Assessment of whether the operator has done, and will continue to do, all that is necessary and sufficient to meet the overarching regulatory objective of providing for safe operation.** As well as testing the operator's current and past compliance with the Regulations, WorkSafe may assess whether the operator has established suitable processes and has the resource and knowledge necessary to ensure continued compliance.

#### 4 What are the Fundamental Approaches to Demonstration?

There is no prescribed methodology for demonstrating the adequacy of control measures for safe operation or the comprehensiveness of an SMS. However there are several basic approaches which may be used to support an operator's demonstration. Operators should consider using one or more of these approaches, but should also be prepared to consider developing specific approaches appropriate to their facilities. **In practice, it is likely that most facilities will require a combination of approaches.**

- **Hazard / Risk Criteria Approach** - define criteria that relate to 'risk reduced so far as is reasonably practicable', assess performance quantitatively or qualitatively and compare against the criteria.
- **Comparative Assessment of Risks, Costs and Benefits** - evaluate risk, hazard or consequence levels and associated costs for a range of options for the facility and compare the relative merits of the different options, selecting the option which gives the best balance of costs and benefits.
- **Comparison with Codes and Standards** – compare design, the management system framework and operational procedures against national or industry standards, codes of practice, guides etc.
- **Audit against good practice** – audit the basis and implementation of the management system against good practice for major hazard facilities in the same or similar industries.
- **Technical Analysis** - evaluate control measures in technical terms, assess strengths and weaknesses, e.g. effectiveness, reliability, technical feasibility, compatibility, correspondence of control measures to hazards and risks, appropriateness of performance standards, etc.
- **Performance Data** – evaluate major incident safety-related performance data as evidence of adequacy or satisfactory levels of performance, e.g. data on the operational effectiveness or reliability of a control measure may support the demonstration of its appropriateness for that service.
- **Improvement Approach** - demonstrate the extent of relative improvements in performance for the facility based on past, present and planned modifications and enhancements.
- **Judgement Approach** – present considered judgements as to the adequacy of control measures and the management systems, or the perceptions of a cross-section of various stakeholders, e.g. employees, senior management, plus independent observers.
- **Practical Tests** - demonstrate that the management system and/or control measures function effectively, using major incident simulations, management system tests, equipment breakdown and recovery tests, etc.

Whatever approach or approaches are used, this needs to be meaningful for the facility and consistent with the operator's culture. The approach as presented in the Safety Case should be transparent to WorkSafe.

For licensing purposes, WorkSafe will evaluate the approach to demonstration in terms of its robustness, transparency and appropriateness to the facility. The operator should therefore define the underlying rationale, criteria and decision-making basis for the demonstration, as well as present the results of supporting studies that have been performed. The degree of analysis in support of the demonstration should be proportionate to the risk and to the complexity of the facility, hazards and the control measures. WorkSafe suggests that operators provide full details of the studies for a small number of cases (ie. some worked examples). WorkSafe will assess that the operator's criteria for demonstration are appropriate for the facility. An overall satisfaction with the demonstrations can be achieved if WorkSafe's assessment shows that the criteria have been met, how the results of the worked examples have been derived, and if WorkSafe can replicate the results for additional cases.

## 5 Demonstrating Adequacy of Control Measures

The Occupational Health and Safety Act 2004 introduces the performance standard of 'so far as is reasonably practicable' (SFARP). Transitional provisions in the Act mean that the SFARP standard applies in regulations made originally under the OHS Act 1985, as if they had been made under the current Act. Thus, under Regulation 304, the basic requirement for control measures is that they must eliminate or, if it is not practicable to eliminate, reduce so far as is reasonably practicable, risk to health and safety. It is the Safety Assessment that provides the information necessary to test this requirement, and this information must be included in the Safety Case. The Safety Assessment must address hazards and risk both individually and cumulatively; consequently the demonstration that risks are eliminated or reduced so far as is reasonably practicable may need to be made for control measures individually, in groups and as a whole.

Section 20(2) of the Act describes the matters that must be taken into consideration by employers in determining what is reasonably practicable in a given situation:

- **The likelihood of the hazard or risk actually occurring.** That is, the probability that someone could be injured or harmed through the work being done;
- **The degree of harm that would result if the hazard or risk occurred.** For example fatality, multiple injuries, medical or first aid treatment, long or short term health effects;
- **The availability and suitability of ways to eliminate or reduce the hazard or risk;**
- **What you know, or ought reasonably to know, about the hazard or risk and any ways of eliminating or reducing it;** and
- **The cost of eliminating or reducing the hazard or risk.** That is, control measures should be implemented unless the risk is insignificant compared with the cost of implementing the measures.

Some advice can also be provided on the factors that further inform a judgement of SFARP, through expanding on the concepts of 'degree of harm' and 'availability and suitability of ways to eliminate the risk':

- **The severity of the hazard or risk in question.** The total extent of control applied to each hazard needs to be proportionate to the scale, or severity, of that hazard. The balance of controls applied between those that eliminate, prevent, reduce or mitigate should also be considered. The minimum expectation is that operators can demonstrate there are control measures in place for each hazard or major incident that has been identified.;
- **The state of knowledge about that hazard or risk and the feasible control measures.** The adequacy of control measures should be judged against contemporary knowledge of the hazards and their means of control. This doesn't mean that control measures must be kept fully up to date with latest technology and knowledge. It does mean, however, that operators need to periodically review existing controls against the changing state of knowledge and form a judgement of when the gap between existing controls and the current approaches is such that it is practicable to implement improved controls. Part of the judgement of practicability (or feasibility) will include the **availability and suitability** of control measures. New or

improved controls should ideally be relatively easily obtainable, capable of implementation at the operator's site, compatible with other existing controls and equipment, and (ideally, though this is not essential) proven to work in the service they are required for.

Performance indicators must be set for control measures, and hence the "demonstration of adequacy" will most likely need to include a convincing argument that these indicators are appropriate and sufficient. These factors are discussed in greater detail in Guidance Note GN10 – Control Measures and Performance Indicators. To summarise, the tests of adequacy of individual control measures are as follows:

#### Factors in Selecting or Rejecting Control Measures

- Are there **controls clearly linked to each hazard**, or are there some hazards having no (or insufficient) control measures? Does the number of controls reflect the **severity** of the hazards?
- What is the **functionality** of a control measure against the relevant hazards. Is it sufficient to control the hazard in the intended manner?
- 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 intended to reduce or mitigate?
- 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 sufficiently promptly?
- Has the **hierarchy** of control measures been considered, with measures to eliminate the hazard adopted first if practicable, followed by measures to prevent, reduce and mitigate?
- Is there a balance of different types of control measure for each hazard, i.e. is there a **diversity** of control measures? Are the control measures associated with individual hazards **independent** of each other, or can they all be disabled by the same mechanism?
- Are new control measures **suitable** for the facility, and compatible with any other control measures already in use?
- Can the control measures be implemented at the facility considering their **availability** and **cost**?

The operator should also consider additional or alternative control measures and show that all reasonable steps have been taken to reduce risk SFARP.

Clearly, the balance between benefits in terms of reduced risk and the costs of further control measures will play a part in achieving and demonstrating SFARP. For example, if an option has a benefit that greatly outweighs the cost, this option would almost always have to be implemented, or very good reasons provided for not doing so. In contrast, if the cost greatly outweighs the benefit, demonstrating that the option is not appropriate is straightforward, as other options will almost certainly exist that are able to achieve at least as great risk reduction at lower cost. If benefits and costs are both high, or are both low, more careful consideration may be required before selecting or rejecting control measures.

The operator may be able to rank available options according to their benefits and costs in qualitative or quantitative terms. This will enable the operator to show that the appropriate balance point has been achieved, where further steps to reduce risk would incur unreasonably high cost at little gain.

The operator may refer to past and planned risk reduction programs, in support of the demonstration that all reasonable steps have been and are being taken to meet the SFAP criterion; implementation plans should be included for any improvements not yet made.

The historical track record of performance of a control measure may also be useful in showing adequacy. For example, industry, manufacturer or site-specific data may indicate that a particular control measure is "fit for purpose" on the basis that it has performed to acceptable standards, and at least as well as is typical in the application. Also, the reliability and effectiveness of a control measure may be illustrated by data from routine function tests, and by records of its behaviour in simulated or real emergency conditions. Results from experiments (e.g. fire tests) may also be used within the demonstration of suitability of control measures.

Where an operator decides that additional control measures should be adopted to those already existing, the safety assessment and demonstration of adequacy should show the additional risk reduction and hazard elimination / reduction, by comparison to the previous situation. The demonstration of adequacy will also need to show that no further reduction, beyond that produced by the adopted additional controls, is reasonably practicable at this time. In undertaking the safety assessment and demonstration, operators should also consider if the newly adopted control measures could add hazards or incident scenarios, e.g. during installation or commissioning of new control equipment, or arising from 'spurious' operation of control measures.

Given all of the issues that may need considering in demonstrating adequacy of control measures, it is in the operator's interests to develop an approach that is logical, structured and efficient. For example, it would be pointless to assess the effect of a control measure in detail if its cost prohibited its implementation. Equally, if there may be control measures that can eliminate hazards, or prevent them with a high degree of reliability, there may be little purpose in devoting significant effort to the assessment of measures for reduction or mitigation.

In addition, on many facilities a large proportion of the risk may arise from a small set of hazards or a specific area of the facility. In such a case, the majority of the control measures and the majority of effort expended in demonstrating adequacy should be directed towards those critical hazards and areas. Proportionally less effort would be needed to address the remaining aspects, although it is important not to neglect any area.

## 6 Risk Criteria, Reduced 'SFARP' and 'ALARP'

Many operators of MHFs may elect to assess and evaluate risks in a quantitative or semi-quantitative manner, and to develop criteria against which to compare the estimated risk levels. Appendix I provides a discussion of different types of quantitative and semi-quantitative risk criteria, including the Victorian Interim Off-Site Risk Criteria.

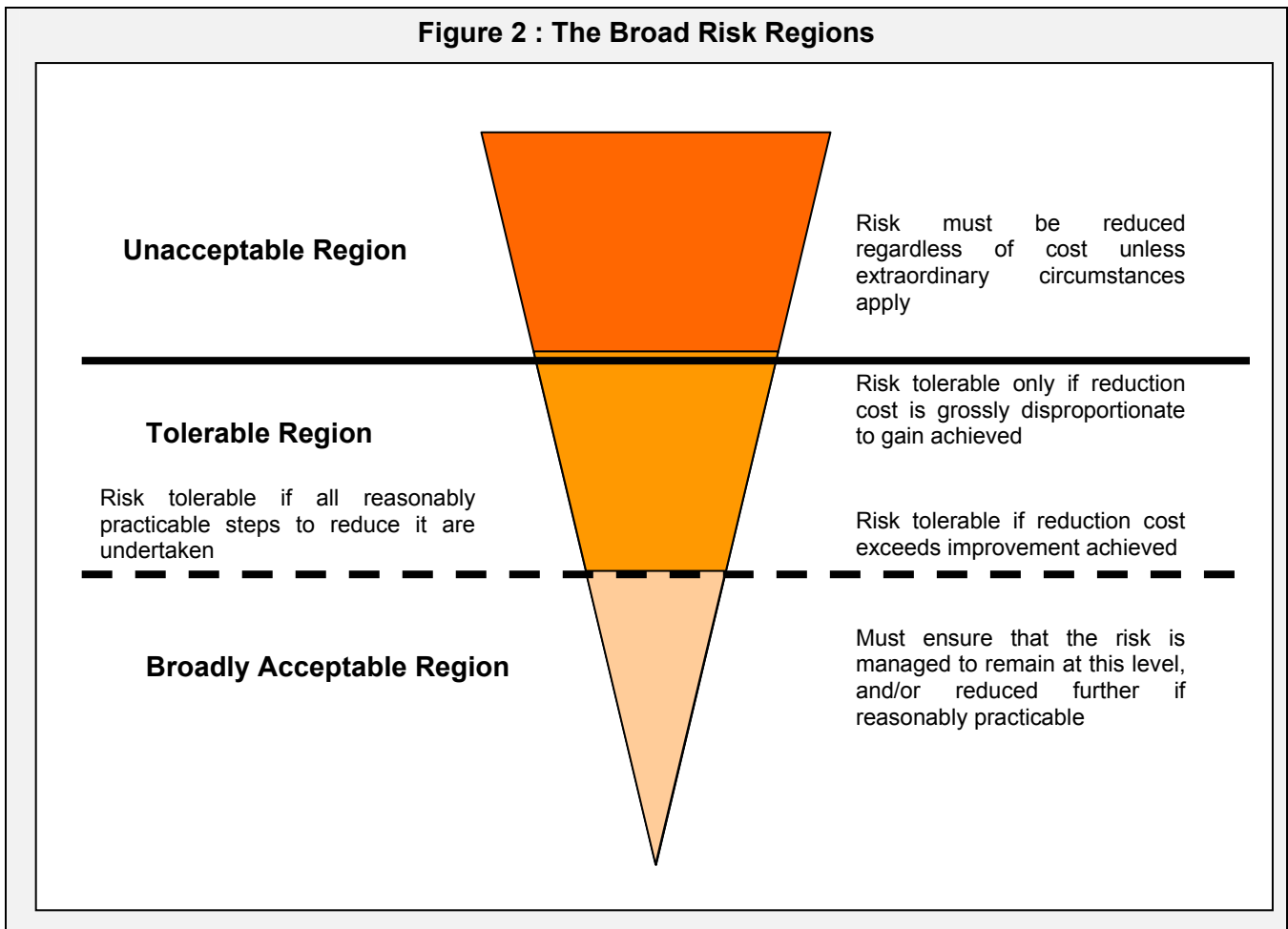
However, all risk assessment is subject to uncertainty, and hence use of rigid risk criteria may be inappropriate. A possible alternate approach is provided by the UK HSE's framework for the tolerability of risk, and 'As low as reasonably practicable' (ALARP) concept. This is based on broad ranges of risk, rather than on specific criteria. The UK 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 (Figure 1: HSE framework for the tolerability of risk). This broad framework is used in HSE's permissioning guidance SPC/Permissioning/12 "Guidance on 'as low as reasonably practicable' (ALARP) decisions in control of major accident hazards (COMAH)" and provides for the following three 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 described above may appear broadly compatible with the OHS Act 2004 performance standard of 'so far as is reasonably practicable', the interpretation above 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 treated, even where it may be reasonably practicable to further reduce the risk.

WorkSafe's preferred interpretation of the broad risk ranges, which manages or treats all risks and includes consideration of continuous improvement, is shown in Figure 2 and described in more detail below.

**Figure 2 : The Broad Risk Regions**



Upper region	Unacceptable risk	Prompt action must be taken to reduce risk regardless of cost, unless extraordinary circumstances apply
Middle region	Tolerable risk	Risk reduction measures must be implemented so far as is reasonably practicable, taking into account the available measures, relevant good practice, cost etc
Lower region	Broadly acceptable risk	Risks must be managed and, so far as reasonably practicable, continuously reduced

The overall demonstrations the operator has to make through the Safety Case need to consider hazards and risks in all regions, and may need specifically to 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; and
- there are suitable and reliable processes for continuing to manage hazards and risks at all levels, and for achieving continual improvement.

However, it is appropriate to apply the concepts of 'proportionality' in the demonstrations. The control measures themselves should be proportionate to the inherent risk, and in addition the degree of demonstration may be proportionate, with a greater degree of justification made in some areas compared to others. For example, if it is found that 95% of the risk arises from hazards and potential major incidents in the upper and middle regions of the ALARP diagram, then only around 5% of the effort of making the demonstration can be applied to cases in the lower region.

## 7 Use of Industry Codes and Standards

For some MHFs, compliance with industry standards, codes or practices may play an important role in demonstrating adequacy of control measures. In principle, such standards may be Australian Standards, equivalents from overseas organisations, international industry practices such as those from the American Petroleum Institute, or company-specific standards. However, whichever standards are being used, these standards, and the control measures that they require, should all be shown to be suitable and appropriate to the specific MHF, taking account of its type, scale, activities, location, etc. In addition, the facility should be clearly demonstrated to be in compliance with the adopted standards, or to have achieved equivalent levels of safety by other means.

In some industries there may be a single over-arching standard that appears to apply. Examples include AS1940 for storage and handling of flammable liquids, and AS1596 for liquefied petroleum gas. For simple facilities within such industries, it may be possible to base a demonstration of adequacy largely on such standards. However, for particularly large or complex facilities of these types, or facilities in sensitive locations, it may be necessary to go beyond the established standards in order to demonstrate adequacy. For example:-

- The standards may not address the types of incident that are of prime concern to the facility;
- A standard may not consider issues of cumulative risk, escalation to/from adjacent facilities, and similar;
- The standard may only address quantities of materials up to some limit, or certain configurations of storage, which may be exceeded at the MHF;
- There may be gaps in the standards, such that standard do not govern all aspects of hazards and risks at a facility;
- The standard has fallen behind current good practice, or the facility has fallen behind the standard as that has been further developed.

Conversely, in the petroleum and chemical processing and other industries, there are no single over-arching standards for all aspects of facility design and operation. Rather, there are detailed standards in specific areas of design such as pressure vessels, area classification, fire-protection, and so on, plus general standards related to safety management. In these industries it is common for an operator to adopt a suite of standards, perhaps taken from a number of different organisations. In such cases, significant effort may be necessary to demonstrate that this overall suite of standards is suitable and appropriate, as well as the individual parts. Particular issues that will need additional consideration, which may not be covered by the individual standards, include plant layout, routing of escape-ways and protection of manned areas. In such cases there will be particular benefit in the operator developing a particular “basis for safety” for the specific facility.

### Example of Failure of the Overall Set of Standards

In 1988, the Piper Alpha oil platform suffered an explosion and massive fire that resulted in 167 fatalities. The platform would have been designed to comply with the generally-accepted industry standards for offshore structures, pressure vessels, process piping, relief/blowdown systems, process fire-protection, accommodation, evacuation, helicopter landing, etc, at the time it was developed in the early 1970s, but this failed to protect the persons on board. The reasons for this were complex and varied, but included:

- At the time the facility was designed, little information was available on the severity of explosions within confined and congested spaces, or the effects of fire and explosion on process systems and steel structures. As a consequence, the standards, and hence the design, did not allow for events of the severity that occurred; the initial explosion damaged process pipework, the ensuing fire caused failures of large diameter pipeline “risers” which further fuelled the fire, and ultimately the structure collapsed.
- There were in effect no standards for fire protection and isolation of the area where the pipeline risers reached the platform topsides, where they could be exposed to fires and explosions associated with the processing plant. As a result, there was little fire protection in this area and there were no isolation valves located such as to have any beneficial effect in the circumstances. This contrasted with standards for fire protection of the wellhead area, and for isolation of the platform from the sub-sea reservoir. These

standards were relatively stringent, with the result that the (unmanned) wellhead area was the only part of the platform to survive.

- Some of the individual standards were developed for circumstances that were substantially different to those on an offshore oil platform. For example, the standards for evacuation systems were based largely on those for shipping, whilst the standards for fire-protection of the living quarters were based to a large extent on fires of cellulose materials rather than hydrocarbons. The standards for helideck location and layout were based on those applying on land, and focussed on the ability of helicopters to land and take off unobstructed in a range of weather conditions; conditions that might arise from process fires and explosions were not considered.
- There were in effect no standards to govern the overall layout of the facility. The layout that was adopted may have been convenient for the purpose of construction and operation but, in the circumstances of the explosion and fire that occurred, the layout led to rapid escalation of the event, and to impairment of escape and evacuation routes. Many of the persons on board were trapped in the accommodation areas, which subsequently filled with smoke.

Whatever standard or set of standards is used, the operator should take care to justify applicability and recognise limitations of those standards. Where standards are being used as part of a demonstration of adequacy, such issues need to be considered, and more extensive arguments will be required in cases where the particular MHF does not fall within the range of facilities for which the standard was specifically developed.

As noted, it is necessary not only to demonstrate that the standards are suitable and appropriate, but also that the facility is in compliance with the standards. Compliance may be demonstrated by reference to certification, independent verification, and/or detailed statements against each clause within the adopted standards.

There may be cases where the current most relevant standard cannot be complied with in certain respects. An example may be a complex or novel facility where there are no applicable standards; another may be an ageing facility designed and constructed to standards now superseded. In such cases, the operator should show that additional measures have been introduced to compensate (ie. to show that equivalent safety has been achieved), or that additional measures are not reasonably practicable. Examples of measures that may achieve equivalent safety are re-rating of equipment, introduction of more frequent testing or inspection, or staff rostering changes to enable better operator intervention. Where weaknesses are known or suspected to exist, for example if there is a gap in overall control measures, or a measure has been compromised by age, this should be explicitly identified. Solutions for addressing these weaknesses should be explored, and the chosen solution incorporated into the demonstration of adequacy.

## 8 Risk Assessment and Demonstrating Adequacy

Operators of MHFs must adopt a comprehensive and systematic method for assessing the risks of major incidents at their facilities. Some operators may choose to adopt quantitative methods, in particular if this is common practice in their company, whereas others may choose to adopt qualitative methods. The results of such assessments should be used to support the overall demonstration of adequacy of control measures, and to show that risks are eliminated or reduced SFARP.

Approaches to safety assessment are discussed in numerous publications, and in Guidance Notes GN14 – Safety Assessment and GN15 – Protection of Property, so no details of safety assessment methods are given here. Rather, this section discusses how safety and risk assessment may be used to support the requirement for ‘demonstration of adequacy’.

The requirement is for the operator to select an approach to making a demonstration of adequacy that is appropriate to the facility, and which supports decision-making on control measures. Risk assessment will be an important part of this process, by showing that risks are reduced so far as is practicable, and by showing that decision-making relates to the level of risk.

Criteria cannot always be set in stone prior to an assessment, but it is desirable to have an initial view of what criteria should apply before commencing any assessment; the criteria can then be refined as the operator develops an understanding of the risks. Ideally, the initial criteria should have been presented in the Safety Case Outline, for discussion with WorkSafe. The nature of the criteria

particularly depend on the nature of the assessment methods. If these methods are not completely defined then it will be difficult to precisely specify corresponding criteria.

WorkSafe will review risk assessment approaches and the criteria that are used, to test their applicability, and to examine how they have been applied in decision making. This is as important as assessing the outcome of the comparison of risks against criteria. Further, WorkSafe needs to view all criteria of any format used in the demonstration of adequacy, in order to evaluate the residual risk the operator considers tolerable. WorkSafe will evaluate how the criteria used in the Safety Case compare with those used by others: are they as stringent as general industry practice, how do they compare with other states and countries, and in similar industry sectors, are they equivalent to risks reduced 'SFARP'?

Appendix I provides examples of risk criteria that have been used in relation to major incidents. However, it should be stressed that these are not exhaustive, and the operator may choose to formulate criteria that differ from the examples. WorkSafe expects the operator to justify the adopted criteria as suitable and appropriate to the specific facility.

## 9 Demonstrating the SMS is Comprehensive and Integrated

The demonstration operators must make regarding the SMS is that it "provides a comprehensive and integrated management system for all aspects of control measures adopted in relation to hazards and major incidents". This demonstration should relate specifically to the effectiveness of the SMS in supporting and maintaining the control measures that are adopted for major hazards. To be comprehensive and integrated, the SMS will need to fully support **all** aspects of **all** adopted control measures, and would need to operate in a coherent fashion which monitors the performance of the control measures and ensures they are not compromised. In order to achieve continuous improvement, it should also contain elements equivalent to the plan-do-check-act quality management cycle.

Thus the demonstration in relation to the SMS may need to show the following:

- The necessary performance of each adopted control measure is clearly defined;
- Adopted control measures are inspected, tested and maintained under the SMS;
- Performance of the control measures is monitored and reviewed against the defined indicators;
- The SMS manages corrective actions to address individual deficiencies or failures in the control measures and to address long-term performance.
- Employees are informed, educated and trained as necessary to ensure control measures are operated, tested, maintained and repaired correctly;
- The SMS provides a reliable process for prompting review and revision of control measures if there are changes to the facility or to the state of knowledge of hazards or of associated control measures;
- Any control measures adopted are able to function effectively, do not conflict with or compromise other control measures, and this is not adversely affected by facility or control measures changes; and
- The SMS clearly and unambiguously defines what activities are needed to ensure safe operations, when these activities should take place, and who should carry them out.

It will need to be clear that sufficient resources, priorities, responsibilities, accountabilities, plans, implementation and monitoring processes, etc. are allocated to control measures not only individually, but also as a whole. Issues that need to be considered in relation to the SMS are dealt with in more detail in Guidance Note GN12 – Safety Management Systems.

## 10 Other Aspects where WorkSafe must be 'Satisfied' for Licensing

**The Safety Case is prepared in accordance with Regulation 402.**

- The Safety Case must contain a summary of the SMS, a copy of documentation from hazard identification and safety assessment, and the information specified in Schedule 4. The information must apply to the

whole of the MHF and its operations, and to all major hazard control measures and all aspects of the SMS. The information must be accurate, and of sufficient quality to make the necessary demonstrations.

- The Safety Case must contain a signed statement certifying that the SMS summary is accurate, that the operator has a detailed understanding of risk, that the adopted control measures reduce risk SFARP, and that the employees have the necessary knowledge and skills to carry out their safety roles.

**The operator has complied with the provisions of Part 3.** This will require evidence that an SMS has been established and implemented, hazards and major incidents identified, a safety assessment carried out, appropriate control measures adopted, an emergency plan prepared, and necessary safety roles established for employees. In relation to these requirements:

- The operator must properly implement the SMS established under Part 3, i.e. the SMS as written must accurately represent the actual management processes used to ensure safe operation.
- Safety roles for employees must be developed (and reviewed as required) in relation to the Part 3 operator duties. Where practicable this must be conducted in consultation with HSRs (or Deputy HSRs).
- The hazard identification and safety assessment need to be carried out using appropriate tools, to a satisfactory level of detail and completion. These activities must be documented comprehensively, and must lead to a correct understanding of the potential major incidents, hazards and risks.
- A range of control measures must be considered, and the basis for rejection and selection provided. The adopted control measures must eliminate risk or reduce it so far as is reasonably practicable.

The Part 4 duty on some operators to coordinate Safety Cases would be tested here, as the hazard identification, safety assessment, control measures and emergency planning all need coordination.

**The operator has the ability to operate the facility safely.** The operator may wish to provide a range of information to show that this is the case, as this is a general clause that enables WorkSafe to consider any information in relation to the operator's processes for achieving safe operation. Examples of information that may be considered include the following:

- Details of the resources available to the operator, including the number of personnel in safety-critical roles, the competency of these personnel, the processes by which competency is assured, and the knowledge that these personnel have of the potential major incidents, hazards, risks and control measures.
- The quality of the processes for ensuring continued regulatory compliance, for example the management of change processes and procedures, and the mechanisms for audit, monitoring and review of performance.
- The history of operations at the facility, as evidence that the operator has a record of preventing major incidents, identifying and rectifying circumstances that could lead to major incidents, and appropriately acting upon any incidents that may occur.

The need for ongoing review and maintenance of the Safety Case, whilst a Part 4 duty, would be included within this test, for example under the management of change processes.

**The operator has complied with the provisions of Part 5.** The operator will need to show that:

- There has been adequate consultation with HSRs during the operator's Part 3 activities.
- There has been adequate consultation with local municipal councils regarding the off-site health and safety impacts that may arise from major incidents.
- There has been (or will be) proper provision of information, instruction and training to all relevant parties.

Processes for on-going Part 5 compliance may also be tested.

## 11 Bibliography

The following documents are suggested as sources of general information, which may be useful in addition to the information provided in this guidance note. However, it is important to note that the

references have not been written specifically as guidance on how to comply with the duties under the Regulations.

COMAH Safety Report Assessment Manual. UK HSE – Hazardous Installations Directorate, January 2003

Reducing Risks, Protecting People – HSE’s decision-making process. UK HSE, HSEBooks, 2001, ISBN 0 7176 2151 0

HID’s approach to ‘As low as reasonably practicable’ (ALARP) decisions. UK HSE – Hazardous Installations Directorate, SPC/Permissioning/09

Guidance on ‘As low as reasonably practicable’ (ALARP) decisions in control of major accident hazards (COMAH). UK HSE – Hazardous Installations Directorate, SPC/Permissioning/12

For more information regarding this Guidance Note, contact the Major Hazards Unit at the Victorian WorkCover Authority (telephone 03 9641 1528, e-mail [mhunit@workcover.vic.gov.au](mailto:mhunit@workcover.vic.gov.au)).

## Appendix I Risk Criteria

As noted in the main text of this Guidance Note, comparison of estimated risk levels against set criteria may be useful as part of an overall demonstration of adequacy of control measures, 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 nationally and internationally. These approaches may be useful for application to individual MHFs, to specific aspects of major incident risk at MHFs (e.g. the off-site risk), or to particular sections of individual MHFs (e.g. 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, assessment of risks is subject to uncertainty. Hence use of rigid criteria may be inappropriate. In line with this, a common approach has been to define three broad risk levels rather than fixed and rigid criteria, as discussed in the main text and shown in Figure 2 of this Guidance Note.

### Risk Matrices

A risk matrix categorises the risk of individual major incidents, based upon judgement by an assessment team of the order of magnitude of the likelihood and consequence of occurrence of the incident. Typical risk matrices for hazardous industrial facilities range in size from 3 x 3 to 5 x 5. An example of a risk matrix is provided in GN-14.

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 can be seen to broadly relate to the risk bands in Figure 2, and therefore can be used to show areas where risk is intolerable, and where risk is tolerable subject to all practicable measures being taken and subject to continuous improvement. Again, the broad risk bands can also be related to the urgency of action required.

However, operators should note that the risk matrix approach, whilst 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 control measures 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 the requirement for cumulative consideration of hazards using risk matrices alone.

Operators who use risk matrices should give clear definitions for the matrix and any categorisation used within it, and should show transparently what action or significance is attributed to each position on the matrix. Operators should check that their risk matrices, and any risk criteria implied through their use, are broadly consistent with commonly adopted risk criteria, such as the (quantitative) interim Victorian risk criteria (see the next section).

### QRA 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. However they can be resource-intensive, may lack transparency and be difficult for a non-specialist to understand, and may give a misleading sense of accuracy of risk estimates.

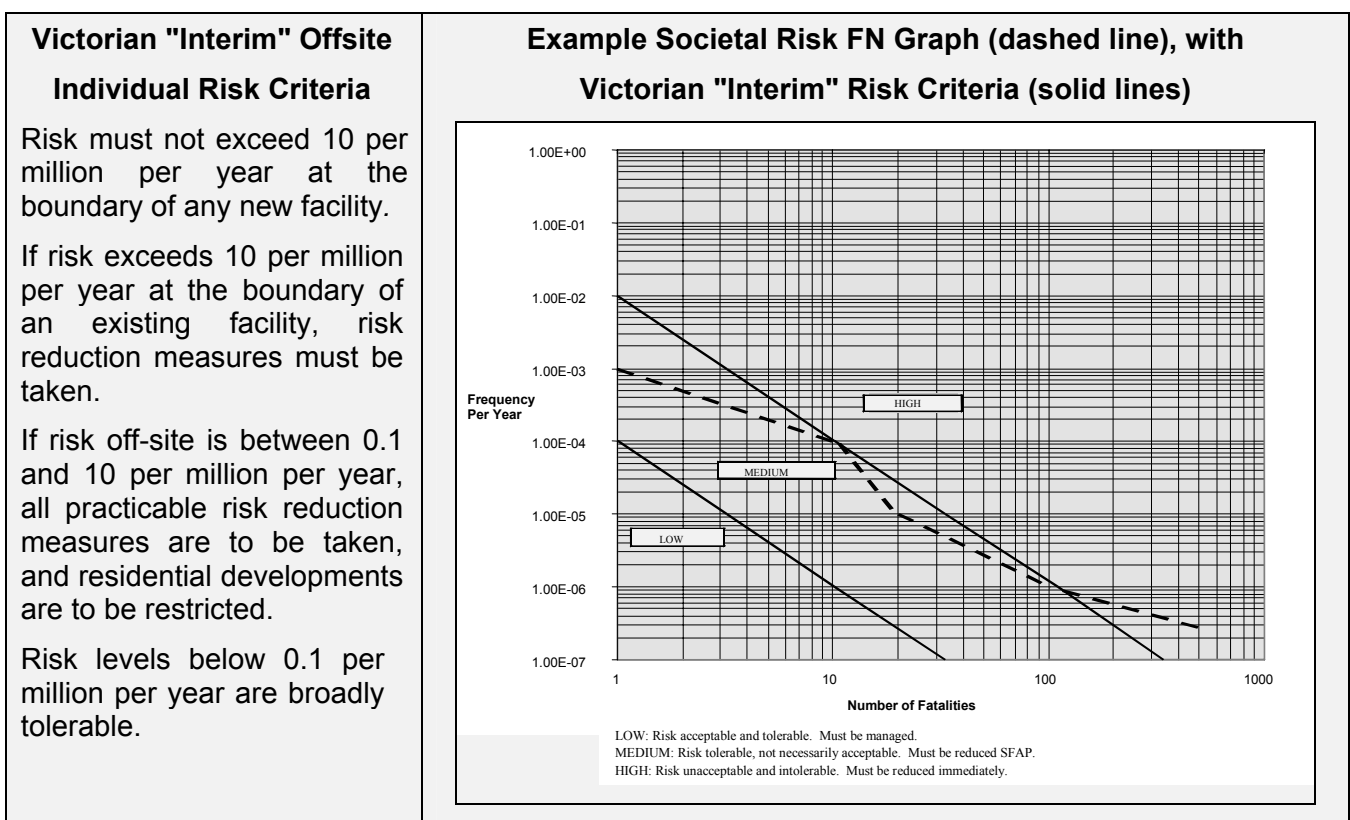
If an operator chooses to conduct a quantitative risk assessment, then the results of the QRA may be used by comparison with pre-determined criteria or for comparing different options, as part of the overall demonstration of adequacy. There are two main types of quantitative risk measure, which may be used to define risk criteria:

- Individual Risk, which 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, which 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 (FN) 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 has 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 ACC & Victorian Government, by DNV Technica, October 1995). Whilst these criteria do not have legal status, they are offered here for consideration as reference values. These values are:



Operators should note that the issue of risk criteria is being further discussed at a national level, and this guidance may be modified in future to reflect the outcomes of that exercise. Therefore whatever criteria are adopted need to be justified as appropriate.

**Potential loss of life & ICAF**

Societal risk can also be expressed as the "Potential Loss of Life" (PLL), which is the number of fatalities that may be expected to occur each year, averaged over a long period. The number should be small: if 100 people are each exposed to a risk level of 10 in a million per year, the PLL is 0.001.

The PLL is a useful basis for cost-benefit analyses of risk reduction measures, via the "Implied Cost of Averting Fatality" (ICAF):

$$ICAF = \text{cost of measure} / (\text{initial PLL} - \text{reduced PLL})$$

Such calculations are often controversial as they appear to require a value to be placed on human life, but these calculation are commonly used internationally, and may be suitable to aid decision-making in regard to adopting control measures for major hazards. For example, a low ICAF for a proposed risk reduction measure implies that the measure is highly effective, because the cost is low compared to

the risk reduction achieved. Conversely, a high ICAF implies a relatively ineffective risk reduction measure, indicating that the money should be diverted to an alternate.

### 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 for on-shore Victorian industry and would need to be set and justified by any operator proposing to use quantitative risk assessment 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, for example, considers hazards and risks individually, whilst the Victoria interim quantitative criteria apply to all hazards in cumulation. Therefore a combination of criteria may be needed.
- Criteria may need to address risks to both individual persons and to society as a whole. This may include consideration of the concept of "risk aversion", which is the greater relative significance society attributes to hazards and risks which could impact on large groups of people.
- Criteria should relate sensibly to the general level of risk present in industry and other day-to-day activities.
- Most established criteria relate specifically to fatality rates, but the MHF Regulations do not require any specific form of criteria, and it may be appropriate to consider measures of risk related to lower levels of harm, e.g. serious injury.
- At any facility there will be fluctuations in the risk level, due to changes in operations, short-term higher risk activities, changes in throughput or process conditions, etc. These variations should be allowed for in the overall setting of criteria.

### Bibliography

The following documents are suggested as sources of general information, which may be useful in addition to the information provided in this guidance note. However, it is important to note that the references have not been written specifically as guidance on how to comply with the duties under the Regulations.

Risk criteria for land use planning in the vicinity of major industrial hazards. UK HSE, 1989

Reducing Risks, Protecting People – HSE's decision-making process. UK HSE, HSEBooks, 2001, ISBN 0 7176 2151 0

Fire, Explosion and Risk Assessment Topic Guidance. UK HSE – Hazardous Installations Directorate – Offshore Division. February 2003

Good practice and pitfalls in risk assessment. UK HSE – Health & Safety Laboratory, Research Report 151, 2003

HIPAP Number 4. Risk Criteria for Land Use Safety Planning. Former NSW Department of Urban Affairs & Planning, 1992

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