Guidelines for major hazard facilities

C - Systematic risk assessment

Queensland the Smart State

Queensland Government
Department of Employment and Industrial Relations

Disclaimer

Any representation, statement, opinion or advice, expressed or implied in this guideline is made in good faith but on the basis that the State of Queensland, its agent and employees are not liable (whether by reason of negligence, lack of care or otherwise) to any person for any damage or loss whatsoever which has occurred or may occur in relation to that person taking or not taking (as the case may be) action in respect of any representation, statement or advice referred to above.

1 Introduction 1

2 Systematic risk assessment (SRA) intent and process 2

2.1 Intent 2

2.2 Process 3

2.3 Timeframe for completion or revision 6

3 Define SRA objectives 7

4 Agree on techniques and collect input data 9

4.1 SRA techniques 9

4.2 Data requirements regarding facility assets 10

5 Hazard identification 17

5.1 Objectives and methodology 18

5.2 Hazard identification outputs 21

6 Worst case consequences of major accident scenarios 22

7 Define accident pathways 24

8 Likelihood and consequence analysis with existing safeguards 27

8.1 Objectives and methodology 27

8.2 Likelihood and consequence analysis with existing safeguards outputs for the SRA report 31

8.3 Acceptable risk criteria 33

9 Possible risk reduction measures and reasonableness assessment 35

9.1 Objectives and methodology 36

9.2 Risk reduction outputs 37

10 Likelihood and consequence analysis with all reasonable risk reduction measures 40

11 Implementation and demonstration that risk is reduced to a level that is as low as reasonably practicable 41

11.1 Objectives and methodology 41

11.2 Outputs of implementation and demonstration that risk is reduced to a level that is as low as reasonably practicable 41

12 SRA report 43

12.1 Summary of occupier's requirements 47

13 Further reading 50

14 (i) Sections of the Act relevant to this guideline 53

15 (ii) Sections of the Regulation relevant to this guideline 55

List of guide notes and figures

Guide note 1	Employee involvement	7
Guide note 2	Sample SRA objectives	8
Guide note 3	SRA techniques	9
Guide note 4	Plant layout	11
Guide note 5	Current plant condition, design and construction	12
Guide note 6	Acceptance of construction	15
Guide note 7	Example major accidents	17
Guide note 8	Example major accident initiators	18
Guide note 9	Hazard identification study team	19
Guide note 10	Study information	20
Guide note 11	Hazard identification tools	20
Guide note 12	Typical hazards list	21
Guide note 13	Example worst case consequences	22
Guide note 14	Defining pathways for major accidents	24
Guide note 15	Safety critical equipment	25
Guide note 16	Consultants	28
Guide note 17	Modelling tools	28
Guide note 18	Example SRA techniques	28
Guide note 19	Example individual risk contours	29
Guide note 20	Sources of likelihood data	30
Guide note 21	Scenario modelling logic	30
Guide note 22	Model data inputs and assumptions	31
Guide note 23	Sensitivity analysis	32
Guide note 24	Communication of results	32
Guide note 25	Acceptable risk criteria	33
Guide note 26	What is an acceptable level of risk?	35
Guide note 27	Hierarchy of control	36
Guide note 28	Risk reduction measures	37
Guide note 29	Effectiveness, reliability and survivability	38
Guide note 30	Operating parameters	39
Guide note 31	Implementation plan	42
Guide note 32	Impact of risk reduction measures	43
Guide note 33	Example summary format	47
Figure 1	SRA process	5
Figure 2	Fault / event tree example	26

1 Introduction

The objective of the *Dangerous Goods Safety Management Act 2001* (the Act) and the *Dangerous Goods Safety Management Regulation 2001* (the Regulation) is to protect people and prevent damage to property and the environment from hazardous materials. To achieve this objective, the Act and Regulation have a number of obligations with which the occupier of a major hazard facility (MHF) must comply. These are detailed in sections at the end of this guideline. One of these obligations is to complete a systematic risk assessment (SRA).

The SRA is the vehicle by which the occupier documents all the major accidents and demonstrates that they have been identified, assessed and managed and in this way contribute to the safety report discussion at the higher level to give the philosophy. The SRA is a standalone document which comprehensively and systematically addresses hazards associated with the operation of the facility. A review of the SRA will form a major component of the facility's final safety report. The SRA will be reviewed by the regulator as part of assessing if facility risk is acceptable.

This guideline is intended to aid the occupier of a major hazard facility in the preparation of a SRA as required by section 41(1) of the Act and sections 17 – 20 of the Regulation.

The regulator does not intend to prescribe the content of an SRA but instead to provide examples of the content and the approach that may be used. In keeping with the performance based nature of the legislation, occupiers should use approaches and content appropriate to their operations to meet the intent of the legislation. MHFs should feel free to contact the regulator to clarify any issues arising during preparation of the SRA.

2 Systematic risk assessment (SRA) intent and process

2.1 Intent

Through the completion of the SRA, it is intended that the occupier will have:

- enhanced the understanding and awareness of site personnel regarding the hazards at the facility and the associated risks
- identified and documented all the major accident scenarios on-site and their pathways
- reviewed all possible risk reduction measures and made decisions concerning the selection of risk reduction measures through the application of acceptable criteria and due justification
- identified the areas of particular importance for community consultation
- identified critical safeguards such as equipment, infrastructure, safety management system controls and the emergency plans
- achieved a level of risk both on and off-site that is acceptable, i.e. as low as reasonably practicable, and
- demonstrated that the occupier has a good understanding of the risks associated with the operation of the facility, and has addressed the management of these hazards in a structured and technically rigorous manner. This would include identifying appropriate monitoring points, safeguard performance criteria and measurement techniques to provide timely warnings of inadequacies in facility safeguards.

The SRA must be clearly and concisely documented, having been completed in consultation with employees at the facility along with suitably qualified personnel with experience in the risk assessment process.

The SRA report should be documented in a fashion that can be readily understood by all personnel needing to understand the facility risks including the regulator.

When reviewing the SRA, consideration should be given to the following:

- new technology for reducing or eliminating risk
- new lessons from incidents on-site and elsewhere
- new or revised standards that are directly applicable the facility (e.g. Australian Standards)
- new or revised standards that indicate development of best practice (e.g. overseas standards, accepted good industry practices)
- changes in the safety management system (SMS)
- changes in data such as:
  - toxicity values
  - failure rate data
  - performance history of existing safeguards
  - probit equations
  - changes in other relevant data
- updated computer software, and
- changes in neighbouring land-use.

2.2 Process

The SRA process (see Figure 1) requires the occupier to follow several key steps that should form the basis for addressing risk to people, property and the environment. These steps are:

- define the objectives of the SRA study
- agree SRA techniques and data requirements including current plant integrity
- complete a comprehensive and up-to-date hazard identification study that identifies all major accident scenarios
- assess the consequences of each worst case accident
- define the pathways for each major accident scenario
- complete a likelihood and consequence analysis with existing safeguards in place
- identify all possible risk reduction measures and then the subset of reasonable risk reduction measures necessary to ensure that the overall level of risk at the facility is as low as reasonably practicable,

- complete a likelihood and consequence analysis with all reasonable safeguards in place
- identify appropriate monitoring points, performance standards for each safeguard and measurement techniques to provide timely warnings of inadequacies in facility safeguards
- implement the reasonable risk reduction measures to attain an overall level of risk that is as low as reasonably practicable, and
- prepare the SRA report.

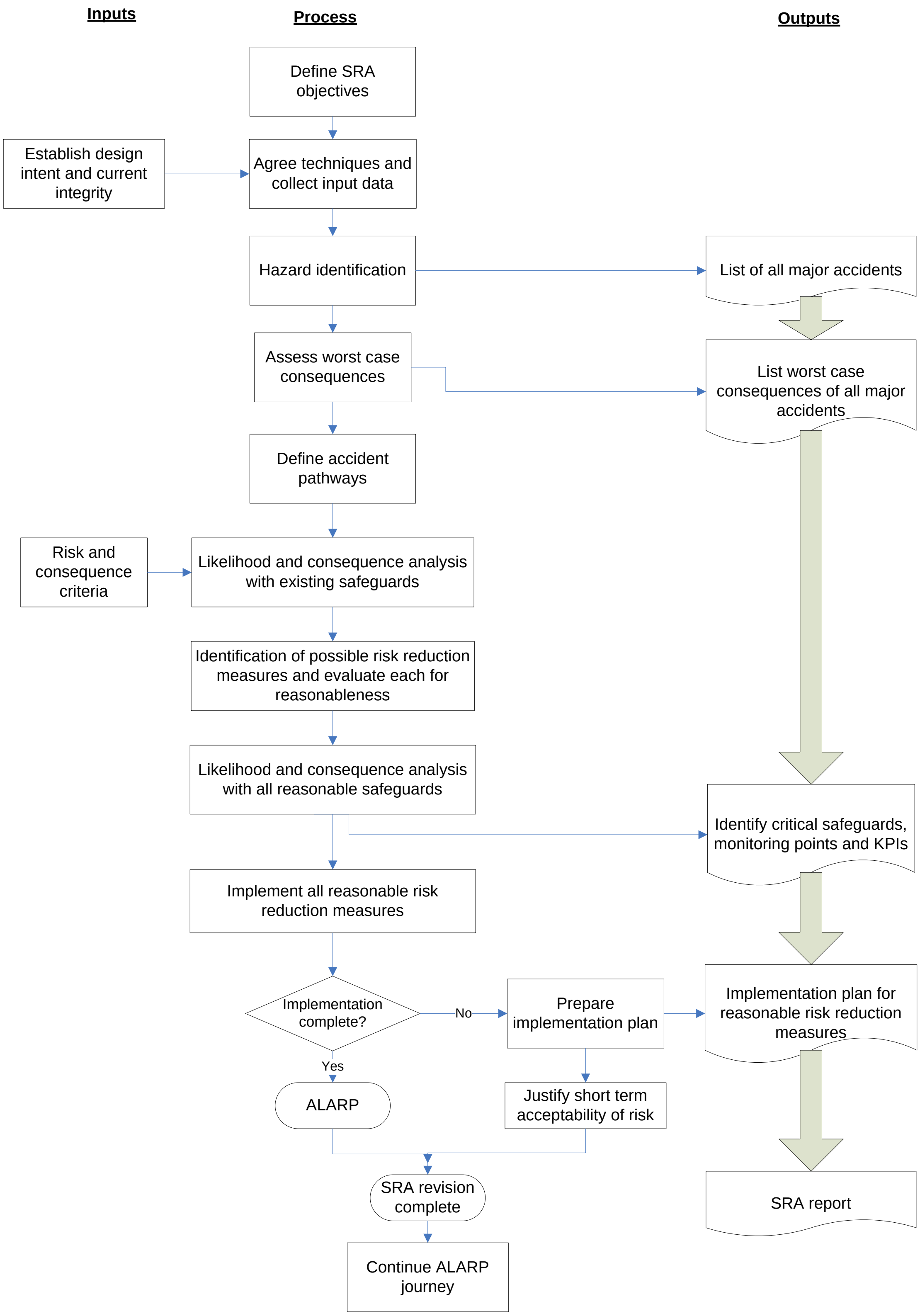


Figure 1 : SRA process

Each of the above steps is addressed separately in subsequent sections of this guideline with the flowchart numbers matching the guideline sections.

Under each heading, there is an explanation of what the regulatory authority expects to see given consideration in an occupier's SRA. These explanations are supported with guide notes which expand and give ideas and examples of how to address particular aspects of the SRA.

2.3 Timeframe for completion or revision

As required by section 41(2) of the Act, the occupier is required to carry out and document the SRA within 3 months after classification.

As required by the legislation (refer Act section 41(3) and (Regulation 19 (2)), the SRA must be reviewed by the occupier and updated at least every five years. If a modification occurs at the facility that significantly alters the risk associated with the facility, or when conducting the five yearly update of the safety report (as required under section 47 (5) of the Act).

3 Define SRA objectives

The occupier should clearly identify the goals of the SRA that will define both the process to be used and the outcomes that should be delivered. The goals for the process may include the techniques to be used, the degree of employee involvement (see Guide note 1 below) and elements from this guideline. The goals should be commensurate with the nature and scale of the facility, the type of operations carried out and its location.

Guide note 1 – Employee involvement

Senior management must be involved in the development of objectives to demonstrate commitment to the process. Plant managers should also be involved to provide the necessary plant-specific knowledge. It may be appropriate to include professionals experienced in the production of hazard and risk assessments to aid the selection of techniques. This includes contractors / consultants where appropriate.

For an SRA resubmission, this is an opportunity to critically assess the weaknesses in previous submissions or the processes used. Feedback from the regulator, other external bodies as well as internal review may be considered. Guide note 2 provides some examples of SRA objectives.

<u>Guide note 2 – Sample SRA objectives</u>

Typical objectives of the systematic risk assessment may include:

- identification of all possible major accident scenarios
- identification of potential knock-on effects to and from adjoining plants on-site and off-site
- gaining a thorough understanding of the nature, causes, likelihood and consequences of these scenarios and to communicate these to the facility employees
- assessing the risks from potential major accidents against acceptable risk criteria
- identification and reliability assessment of existing safety critical equipment (refer to Guide note 15) and procedures
- identification of possible risk reduction measures
- evaluating, selecting and implementing all reasonable risk reduction measures to reduce the risk to a level that is as low as reasonably practicable
- identifying employee training needs
- identifying the geographic area of the community to be consulted
- identifying critical safety management system components
- identifying critical emergency planning elements, and
- identifying monitoring points, performance criteria and suitable measurement techniques to provide timely warning of safeguard inadequacies.

4 Agree on techniques and collect input data

The occupier should clearly and comprehensively identify how the SRA study shall be conducted and the information required for the study.

4.1 SRA techniques

The techniques used for the SRA should also be identified at this stage with justification for their selection. This will highlight data (e.g. population, land uses, incident frequency, reliability) which has to be collected. Early resolution of the SRA techniques and data requirements should preclude the need to revisit previous work when further into the assessment (see Guide note 3).

Guide note 3 – SRA techniques

The following techniques may be used separately or in combination for the SRA:

- quantitative
- qualitative
- semi-quantitative (e.g. quantitative consequence analysis accompanied by a qualitative likelihood analysis), and
- mechanism of failure techniques e.g. bowtie diagrams, layer of protection Analysis, fault and event trees.

The quantitative risk assessment technique is useful for generating risk contours for land use planning purposes and can provide major input, because of its rigour, into the SRA process.

It may be prudent to discuss the appropriateness of the proposed techniques with the regulatory authority to ensure that is considered adequate.

The occupier should be able to demonstrate:

- the process followed to ensure employee participation
- the degree of employee involvement in setting the systematic risk assessment objectives (see Guide note 1), and

- the appropriateness of the technique selected for the SRA (see Guide note 3) with particular attention paid to how off-site consequences will be handled.

4.2 Data requirements regarding facility assets

The SRA report must contain details concerning the plant design, material selection, plant construction and the current plant integrity. Without a thorough understanding of the original design intent, the current operating limits of the plant and its general integrity, it will be impossible to determine whether the facility is operating with the originally intended safety margins. These details are critical if an accurate estimation of the overall facility risk is to be made.

4.2.1 Design

There must be a demonstration of an adequate provision for safety in the design of the facility included in the SRA report and should directly address the following aspects for the original design **and** subsequent modifications that have occurred.

The standards used for the design of safety critical equipment should be provided with evidence that they are appropriate. In fulfilling the obligation to minimise risk and demonstrate that risk is reduced to a level that is as low as reasonably practicable, the occupier should review best practice, good industry practice as well as relevant overseas and national codes and standards to decide which standards are appropriate to the facility.

For an existing facility or an SRA revision, the occupier should also indicate whether the original design standards are still applicable. Where they have been superseded, the occupier should provide an explanation of how this has been accounted for. Any deviation from best practice, good industry practice and accepted codes and standards should be justified.

These considerations should be applied to each of the following design sections.

4.2.2 Safe layout of the plant

The SRA report should demonstrate how the plant layout prevents or reduces the development of major accidents (see Guide note 4) and include plans for future improvements if the plant layout is sub-optimum.

Guide note 4 – Plant layout

The following examples would prevent or reduce the development of major accidents:

- open-walled LPG compressor house to aid rapid dilution of flammable atmospheres in the event of a leak
- large separation distances between ignition sources and flammable inventories
- absence of horizontal surfaces in a plant processing potentially explosive dusts to avoid possible dust build-up and subsequent explosion, and
- separation of hazardous plant from the site boundary to reduce off-site risk and risk to the plant from off-site hazards.

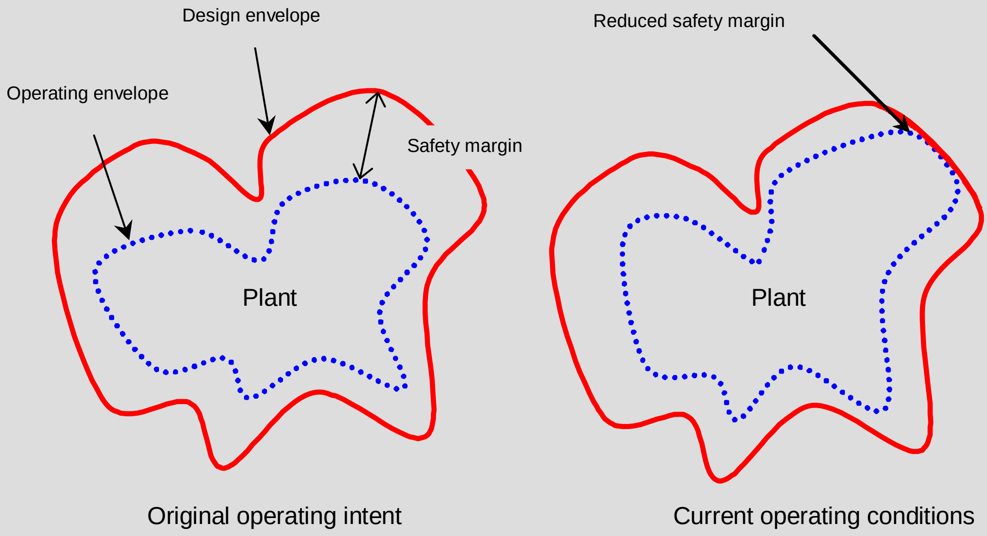
There should be evidence in the SRA report that utilities that are integral in preventing or reducing the development of major accidents are always available in sufficient quantities when required, e.g. firewater, foam, compressed air, electricity, etc.

Where material selection is critical to safety, the SRA report should include a description of the material selection philosophy. There should be evidence in the SRA report that the materials of construction selected for safety critical equipment are suitable for their environment. Consideration should be given to both the internal and external conditions of the equipment.

Where fabrication is critical to safety, the SRA report should show that equipment has been fabricated to appropriate standards. Where established standards are not followed the basis for the fabrication should be described and justification given for not using them. The procedure for confirming that fabrication has met the standards should also be referenced.

The SRA report should describe the originally intended operating conditions and the margin of safety, the current operating conditions and any foreseen operational extremes of safety critical equipment (see Guide note 5). Evidence that the plant can withstand such conditions should be provided, e.g. reference to applicable codes or standards. How the effects of degradation (i.e. daily wear and tear, corrosion, erosion, etc.) of the plant have been accounted for should also be provided.

Guide note 5 – Current plant condition, design and construction



It is expected that operating conditions will always be maintained within the well defined, safe operating envelope for the facility even during abnormal operation. It may be, however, that the current operating conditions of the plant have pushed the originally intended operating envelope to a point close to the design envelope significantly increasing the possibility of a dangerous excursion beyond the safe operating envelope. Therefore, it is important that the current operating conditions are considered in the hazard identification study along with the original design intention.

This will require data on all the current operating parameters of the plant, maintenance procedures, etc to be compared against the plant's original operating parameters. A review will also be required of the plant operating parameters during startup and shutdown compared to the design operating parameters. This will help identify whether the plant is presently running as originally intended or if further risk reduction measures are required to enable it to continue to run with an appropriate safety margin between the operating envelope and design envelope. **It is essential that the plant integrity is established to support the operating philosophy.**

Guide note 5 – Current plant condition, design and construction (Cont.)

Examples of relevant plant condition changes:

1) In the past, the requirement to increase the throughput of a process led to an increase in the operating pressure of a pressure vessel. The regulator would require the occupier to show that the design of the pressure vessel and associated safety systems (e.g. pressure relief valves, etc.) was still adequate through the application of the current relevant standards.

2) Fluctuations in warehouse inventory may lead to coming close to or exceeding bunding capacity.

3) If the pump rate is increased to deliver greater production rates, there may be unplanned effects such as increased failure rates of other equipment that may take the actual operating conditions beyond the designed safe operating envelope.

The condition of the safety management system is also important as it supports the ongoing integrity of the safeguards and should also be assessed. Consideration should be given to the adequacy of management systems such as management of change, design review, commissioning, validation, maintenance management systems and auditing processes in this assessment.

Details of the philosophy applied to the setting of design envelopes over maximum expected operating envelopes should be included in the SRA report.

For safety critical equipment susceptible to a particular failure mechanism, the SRA report should describe the measures taken to eliminate, mitigate or allow for the mechanism of failure. Example failure mechanisms could include but is not limited to:

- deterioration of equipment integrity, for example:.
  - corrosion – internal and external corrosion should be considered
  - erosion – from e.g. excessive fluid velocity, particulates
  - fatigue
  - inappropriate inspection schedules
  - cumulative abuse

- External impacts, for example:
  - external loading – from e.g. cyclonic winds, seismic events; tsunami; fire in adjacent structure or offsite
  - impact – from e.g. vehicle impact, missile impact, blast overpressure
  - forced abandonment of facility due to natural disaster or sustained emergency
- Inadvertent release caused by:
  - pressure – from e.g. failure of pressure relief devices, external fire, excessive reaction rate, unplanned vacuum conditions
  - temperature – from e.g. external fire, extreme process conditions
  - vibration – from e.g. changes in phase, cavitation, closely located plant equipment, and
  - human error – resulting in overfilling, overloading or other manually initiated maloperation.
- Equipment abuse, for example:
  - Operating equipment outside expected range
  - Failed protective systems.

4.2.3 Construction

There must be a demonstration in the SRA report that safety critical equipment was constructed to appropriate standards and that the construction was assessed and verified against the appropriate standards.

Evidence should be provided to show that construction work of safety critical equipment was carried out by suitable personnel in accordance with appropriate procedures. Relevant construction codes and standards should be referenced. Where codes or standards were not used for whatever reason, the SRA report should provide evidence that the procedures adopted were adequate.

Evidence should show that the construction of the plant, including deviations from the original design, was documented to give an assurance of conformity.

The SRA report should provide an explanation of the methods used to assess and verify that safety critical plant and equipment was constructed as intended. The acceptance criteria for testing and inspection should be identified (see Guide note 6).

Guide note 6 – Acceptance of construction

Evidence that the construction is acceptable may include:

- leak testing to confirm the capability of containment to prevent liquid or gaseous leakage
- certification for non destructive testing of equipment
- the mechanisms used to confirm the safety of all elements of control systems including valves, instruments, software, trips and alarms, and
- the role and competency of any inspection authority employed to verify compliance with code requirements.

There must be evidence that commissioning procedures have been prepared for all safety critical equipment. There must be an assurance that during commissioning there is appropriate expertise on-site in, for example:

- process engineering
- process control
- equipment design
- chemistry.

Safety critical equipment should be recommissioned and verified as being effective on a periodic basis, when an associated change is made or if maintenance is conducted that may impair functioning.

4.2.4 Unavailable information

Some older facilities may not have all the information above available to include in the SRA report. In this case the occupier will be required to fill the knowledge gaps concerning the current status of safety critical equipment justifying its continued operation. This may be achieved through an integrity inspection or captured from existing information. Irrespective of the method used, the information must be gathered and its quality justified.

Without information regarding the current integrity of equipment, the plant operating envelopes cannot be set, estimates of incident likelihood will not be accurate and the hazard identification study will be deficient. This information must therefore be gathered prior to the hazard identification stage of the SRA. The occupier must then demonstrate how this information was utilised in the hazard identification study.

4.2.5 Linkages

All elements of the design, construction and the operating envelope should be transparent. For example, where SMS procedures for the validation of plant construction are used, appropriate references should be provided.

5 Hazard identification

This step of SRA should demonstrate that the occupier has completed an up-to-date hazard identification study that systematically and comprehensively identifies **all** potential major accidents associated with the facility. Guide note 7 defines a major accident as described in the Act.

Guide note 7 – Example major accidents as defined in the Act

A major accident means a sudden occurrence (**including, in particular, a major emission, loss of containment, fire, explosion or release of energy**) leading to serious danger or serious harm to people, property or the environment, whether immediate or delayed and is defined in the legislation.

Examples could include:

- a significant release of a corrosive material into the environment requiring clean-up costs greater than $50,000
- a significant release of a flammable material at the facility resulting in a pool fire that injures a number of facility employees requiring overnight hospitalisation
- a runaway reaction between a number of chemicals in a batch process resulting in the over-pressurisation of the reaction vessel and its subsequent failure where the overpressure and associated missiles cause significant property damage on-site and off-site
- a storage vessel fails due to the impact of a crane, releasing significant quantities of a toxic material where the cloud drifts off-site and results in serious health impacts on the neighbouring community, or
- a power distribution board catches fire causing a warehouse containing toxic material to be engulfed with a toxic plume that travels offsite causing serious health effects in the neighbouring community.

It is important that **all** major accidents are identified at this stage, and are not dismissed because of their likelihood or the risk reduction measures in place. Guide note 8 includes relevant examples of initiating events that could be considered.

For example, the catastrophic rupture of a well designed vessel should not be discounted even if the event is considered incredible. It is important to identify such critical risk reduction measures for later consideration in the analysis.

Guide note 8 – Example major accident initiators

Some examples of initiating events for major accidents are:

- failure of the management system
- failure of hardware
- human error
- poor human factors design
- loss of utilities
- unusual chemical reactions
- failure of risk reduction measures
- abnormal operating conditions such as startup, shutdown, commissioning and maintenance
- breach of security/terrorist attack
- flawed software logic
- forced facility abandonment, or
- external conditions which may include:
  - floods/cyclones/earthquakes/ lightning strikes/tsunami,
  - impact on a support structure or containment vessel (e.g. by road/rail/air/sea/cranes/etc), or
  - hazardous events on neighbouring sites.

5.1 Objectives and methodology

The occupier should be able to demonstrate:

- the degree of employee involvement in the process of hazard identification
- that suitably qualified personnel with experience in the risk assessment process are used to facilitate this element of the SRA in conjunction with plant designers and company personnel with relevant operating and maintenance experience (see Guide note 9)
- that accident databases have been consulted and the lessons learnt from past incidents and near-misses have been incorporated into the study (see Guide note 10)

- that assessment teams have used up-to-date design information
- the tools used in hazard identification and the appropriate reasons for their selection (see Guide note 11)
- that the hazard identification study addresses the current plant condition compared to the original design and construction (see Guide note 5)
- that the type and extent of hazard identification studies undertaken is commensurate with the nature and scale of the facility, the type of operations carried out and its location
- that **all** hazards that could lead to a major accident have been initially included in the hazard identification study and have not been not been discounted due to low likelihood or because of existing risk reduction measures – **all** major accident hazards must be identified, and
- comprehensive hazard identification documentation (see Guide note 12).

Guide note 9 – Hazard identification study team

In conjunction with suitably qualified personnel experienced in the risk assessment process, the following people may be involved in the hazard identification process:

- chemical engineers
- mechanical engineers
- civil engineers
- control engineers
- relevant technical experts
- plant supervisors
- chemists
- plant operators
- maintenance personnel
- safety professionals
- other suitably experienced personnel.

The number of people in the study team will usually depend on the technique employed. The most appropriate personnel available should be utilised, which may include employees from sister plants within the company.

Guide note 10 – Study information

Prior to running the selected hazard identification study, it is appropriate to research past incidents and near-misses involving similar equipment, plant, processes, chemistry and systems. Challenges to plant safeguards should be included (e.g. excursions beyond safe operating envelope) even if not classified as an incident in facility terminology. It will also be necessary to gather other relevant information, such as chemical and physical property data relevant to the hazardous materials on-site. Sources of information could include:

- published literature
- past incidents and near misses at:
  - other facilities owned by the occupier
  - comparable plants in Australia and overseas.
- material safety data sheets
- previous hazard studies on-site
- incident databases
- past incidents and near misses on-site including process safety incidents such as challenges to systems or safe operating envelope, and
- other relevant sources.

Guide note 11 – Hazard identification tools

Many tools are available for hazard identification, some examples are:

- Hazard identification (HAZID);
- hazard and operability studies (HAZOP)
- checklists
- failure modes and effects analysis (FMEA or FMECA)
- what-if analysis
- fault tree analysis
- event tree analysis
- fire and explosion analysis (FEA)
- job safety analysis
- methodical leak/rupture approach
- safety reviews
- near-miss reports
- task-based reviews
- past incident reports
- human error identification methods.

Other appropriate equivalent methodologies may also be used accompanied with a detailed description of the technique.

5.2 Hazard identification outputs

In the SRA report, the major accidents for the entire facility operating under both normal and abnormal conditions during start-up, shut-down, commissioning, maintenance and routine operations should be documented. Consideration should also be given to the "knock on" potential of adjacent activities. An example of a major accident list is provided in Guide note 12

Guide note 12 – Typical major accident list

A major accident list would typically include the following information:

- the identified major accident
- a reference to the associated hazard study where it was identified
- some form of identifier to enable that particular major accident to be tracked throughout the SRA process
- the physical and chemical properties of materials involved that could be of a hazardous nature and possible worst case consequence
- the major accident scenario including, for example equipment involved location, initiators and possible sequence of events
- assumptions made, and
- the risk reduction measures currently in place such as hardware and systems.

Where identified hazards have consequences that when unmitigated are still deemed to be low and would not directly or indirectly contribute to a major accident, they may be dismissed from further consideration. However, they should not be dismissed because of their likelihood or risk reduction measures in place.

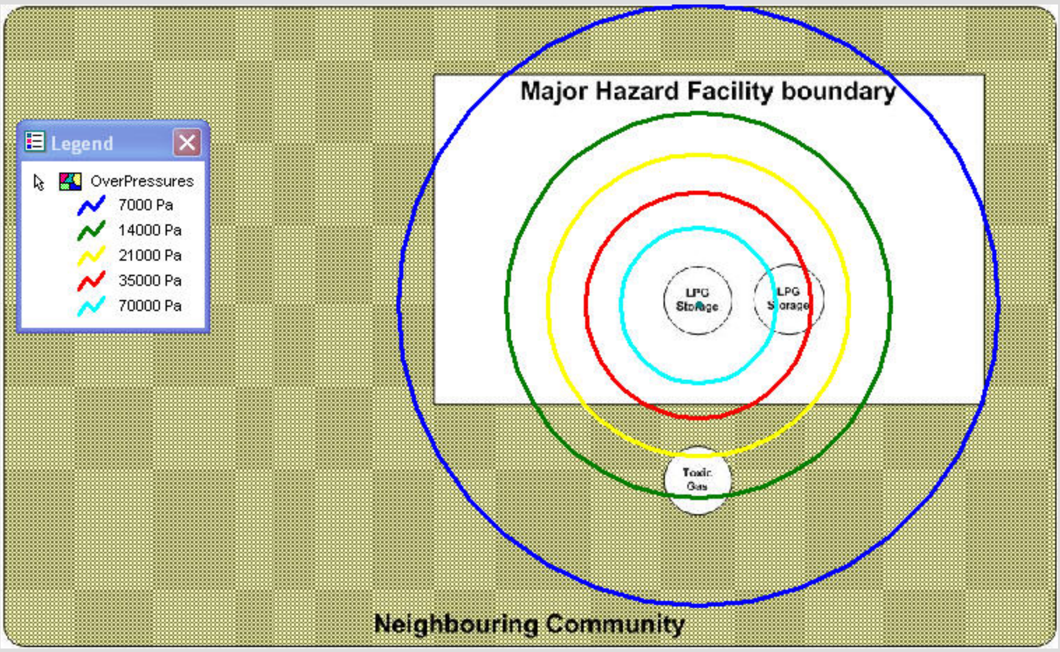
6 Worst case consequences of major accident scenarios

The occupier should determine the maximum consequences that could occur for each major accident scenario. This should be in terms of the heat radiation, explosion overpressure or toxic exposure relevant to the event identified. This analysis should be carried out on the assumption that all safeguards are removed even though it may well be argued that failure of all safeguards is an incredible situation. The purpose is to clearly understand the reason for the safeguards that already exist or are proposed. Guide note 13 provides an example of such modelling.

Guide note 13 – Example worst case consequences

For an LPG storage tank, the worst case scenario could be determined to be a BLEVE of the maximum inventory and the distances to the relevant injury risk levels such as explosion overpressure and heat radiation could then be provided. The following example shows simplistic modelling of the explosion overpressure from a BLEVE blast at an LPG storage vessel.

Importantly, the 70kPa overpressure in the example can impact on a neighbouring LPG storage vessel with expected “knock-on”, the 35kPa overpressure contour extends beyond the site boundary and the 21 kPa overpressure contour effects an offsite inventory of toxic gas. These issues need to be addressed in later sections of the SRA to provide adequate safeguards and achieve an acceptable level of risk.



When determining the major accident consequences, appropriate injury and fatality criteria should be applied. The regulator utilises the consequence criteria identified in HIPAP No.4 (see Guide note 23 for further information) which are nationally and internationally accepted.

Accurate determination of worst case, major accident consequences requires considerable experience, professional judgement and typically the use of specialised computer programs. The modelling needs to be carried out and documented in such a way as to be able to be verified by the regulator if required.

The occupier should be able to demonstrate:

- that assessments have been performed by competent analysts with experience in the risk assessment process (see Guide note 16)
- where software is used for modelling, experienced personnel are employed to operate it (see Guide note 17)
- the systematic approach used for the consequence analysis including the techniques employed (see Guide note 18) and justification for their selection
- the worst case consequences of all major accidents are modelled
- where a quantitative technique is used, that the methods behind it are explained along with key data
- where a qualitative technique is used, that its basis and the logic behind it is clearly explained
- the consequence analysis is commensurate with the nature and scale of the facility, the type of operations carried out and its location, and
- the methods used for verifying results from the consequence analysis (including verification of results from software modelling).

7 Define accident pathways

The pathways for each major accident to occur should be identified along with the safeguards (hardware and systems) that prevent or mitigate the major accident. Accidents will occur when a pathway exists through the facility safeguards ("Swiss cheese model" of accidents). The effects of several hazards occurring in combination (chain events) must be considered, as well as any potential for escalation of incidents (see Guide note 14).

Guide Note 14 – Defining pathways for major accidents

It is important that the mechanism by which a major accident can occur and escalate is understood and clearly defined. Techniques such as fault and event trees (bow tie diagrams, layer of protect analysis) can be applied to link the initiating event to the major accident and to the end consequences. The safeguards can be also included. Defining the mechanism for major accidents in this way enables:

- understanding of the likelihood of a major accident occurring with and without the safeguards
- defining whether major accident mechanisms are credible or incredible
- understanding the susceptibility to specific failure mechanisms such as human error
- understanding the adequacy of safeguards and demonstrating the application of the control hierarchy, particularly where human error can lead to a major accident
- understanding the criticality of safeguards, and
- defining appropriate monitoring points for safeguards.

It is therefore not only important to understand the route by which an accident can occur but to critically assess the adequacy of facility safeguards for each scenario (Guide note 15). Assessing safeguard adequacy should include:

- considering if safeguards are sufficiently robust (big enough, strong enough, fast enough, obvious enough)
- adequately located (will the safeguard be operational for each specific scenario at full capability)
- independent (avoiding the potential for common cause failure, and

- assessing and ensuring that human interfaces are designed so that errors that can lead to a major accident are clearly identified and minimised.

Guide note 15 – Safety critical equipment or system

Equipment or system that could directly or indirectly lead to a major accident if it fails can be considered safety critical. Examples could include:

- a storage vessel containing a significant inventory of liquefied ammonia
- a flow-controller that regulates the addition of chemicals to a batch reactor where there is the potential for a runaway reaction
- a flammable or toxic gas detector;
- a high inventory LPG pipeline on-site
- relief valves on a LNG storage vessel
- temperature control on the heater for material susceptible to exothermic degradation
- overfill protection on flammable liquid storage vessel
- isolation process, or
- management of change process.

Figure 2 shows a sample fault / event tree to indicate the accident mechanism along with the safeguards that are in place to prevent or mitigate the accident.

The occupier should make a judgement as to the extent of accident pathway analysis for each scenario and the analysis tools utilised or provide justification that such analysis is not required. Analysis should be commensurate with the scale and complexity of the facility. For example a LPG facility with a number of bullets that are of similar design and environment could be covered by one accident pathway. Consideration must then be given to any differences in order to cover all pathways for the facility. As a minimum, the occupier should demonstrate that a comprehensive understanding of the major accident pathways and safe guards has been achieved.

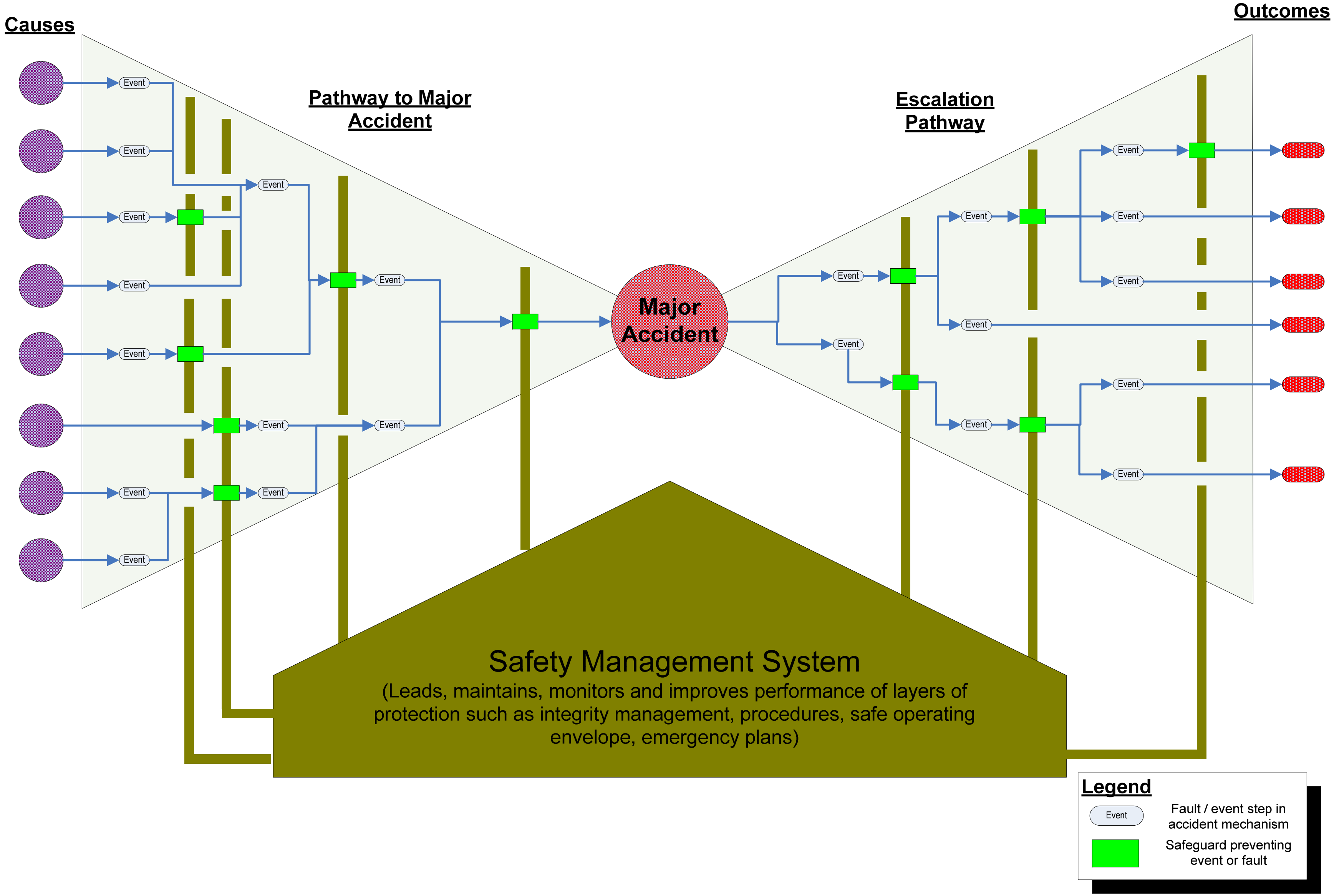


Figure 2 : Fault / event tree example

8 Likelihood and consequence analysis with existing safeguards

The occupier should determine the likelihood and consequences of all major accident scenarios identified in the hazard identification study assuming that all existing safeguards are in place. The results from this step will feed into the risk evaluation where they can be ranked and priorities determined for further study.

8.1 Objectives and methodology

The occupier should be able to demonstrate:

- that assessments have been performed by competent analysts with experience in the risk assessment process (see Guide note 16)
- where software is used for modelling, experienced personnel are employed to operate it (see Guide note 17)
- the systematic approach used for the likelihood and consequence analysis including the techniques employed (see Guide notes 18 and 19) and justification for their selection
- the approach is comprehensive and takes appropriate account of the all identified pathways leading to the major accident. This should include various pathways identified during normal operation as well as during abnormal operation such as shutdown, start-up and maintenance
- where a quantitative technique is used, that the methods behind it are explained along with key data
- where a qualitative technique is used, that its basis and the logic behind it is clearly explained
- the likelihood and consequence analysis is commensurate with the nature and scale of the facility, the type of operations carried out and its location, and
- the methods used for verifying results from the likelihood and consequence analysis (including verification of results from software modelling).

Guide note 16 – Consultants

If consultants are employed to complete some or all of the elements in the SRA it is critical that corporate knowledge be retained. To enable this, there must be some form of 'knowledge hand-over' between the consultants and the facility employees. It would be expected that the consultant would not be working in isolation, and that there would be strong interaction between the consultant and occupier during the generation of the SRA.

Guide note 17 – Modelling tools

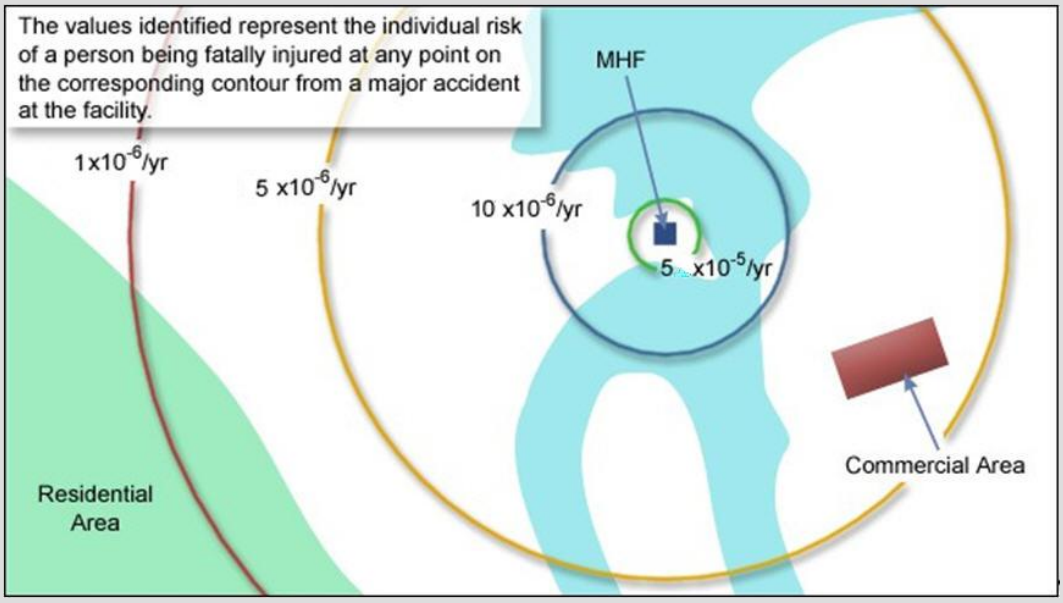
Proprietary software and spreadsheet-based software are tools that may be used for likelihood and consequence analysis. The results obtained from new and/or untested software or unprotected spreadsheets/models should be verified by other means, for example, an audit of the results using a known and accepted software package. All assumptions made during the data input process of modelling should be checked and recorded so that outcomes can be verified by the regulator if required. Full details of any proprietary software used (package, vendor, version) should be detailed in the SRA.

Guide note 18 – Example SRA techniques

SRA techniques may be qualitative, quantitative or semi-quantitative. Techniques include matrix, diagrammatic, table lookup and quantitative risk assessment.

Examples of risk analysis tools are provided in AS/NZS 4360:2004 Risk management and its companion document *HB 436:2004 Risk management guidelines*.

Guide note 19 – Example individual risk contours



Individual risk contours may represent the risk of injury/fatality/etc of a person at a particular point as an output. A facility using a quantitative risk assessment may be able to compare the facility risk contours against acceptable criteria to determine whether the risk is acceptable or not at particular locations, see example above. Guide note 25 discusses acceptable risk criteria.

As an output of the risk assessment, the occupier should document and discuss information which has been used to validate assumptions in order to fully assess the risk. Information to be included could be:

- the sources of generic data used and justification for its comparison and application in site specific circumstances (see Guide notes 5 and 20)
- the logic behind the event sequences that lead to major accident scenarios (see Guide notes 14 and 21)
- justification for the relevance, validity and significance of assumptions made to enable accident scenarios to be modelled (see Guide note 22) that each scenario can be traced back to the hazard identification study using the hazard identifier mentioned in Guide note 12, and
- assumptions made to enable hazards to be screened out.

Guide note 20 – Sources of likelihood data

The likelihood of major accidents arising out of hazards previously identified may be determined from a variety of sources including:

- site-specific failure rate data (provided that the sample size and time period of data collection are sufficiently large) including from site incidents
- generic historical failure rate data, and
- techniques such as fault tree analysis and event tree analysis.

Sources of likelihood data need to be stated and be credible. Examples of credible data sources include *Loss prevention in the process industries* by F.P. Lees and *Guideline for quantitative risk assessment* – CPR 18E known as the Dutch "Purple book". For uncertain data, sensitivity analysis can be used to determine the impact of assumptions on the analysis.

Guide note 21 – Scenario modelling logic

For each major accident scenario, the logic behind event sequences should be considered and made transparent. Consideration of cumulative effects is also essential so that 'knock-on' effects on-site and to neighbouring sites are not overlooked.

The following models should be considered in sequence to accurately model the outcomes of a loss of containment:

Discharge model ➨ **Dispersion model** ➨ **Consequence model**

- Fire
- Explosion
- Toxic release

Guide note 22 – Model data inputs and assumptions

In running the models mentioned in Guide note 21, inputs of conditions relevant to the release will be required such as:

- physical and chemical properties of the released material
- storage or operating conditions prior to the release
- size of release orifice and equipment involved
- release rate and duration
- assumptions regarding factors such as meteorological conditions, surface roughness, ignition sources, etc
- assumptions regarding the scenario, e.g. why management factors were applied to the likelihood analysis
- other relevant or special information, and
- consideration of abnormal situations such as start up and shut down.

8.2 Likelihood and consequence analysis with existing safeguards outputs for the SRA report

In the SRA report, the occupier should document the following:

- the sequence of events leading to all possible major accidents starting with the initiating events
- evidence to show that the event sequences triggering the scenarios are correctly identified and clearly justified
- sensitivity analyses for critical variables (see Guide note 23)
- the likelihood and consequences of all major accidents, such that all impacts are fully understood by the occupier so they can be communicated to the local community and employees
- demonstration that the results have been verified adequately;
- demonstration that identified hazards and major accidents are consistent with referenced studies from similar facilities
- how the results from the likelihood and consequence analysis have been used to identify the major accident scenarios

- a transparent ranking and screening process for the selection of the major accident scenarios
- how the risk from the identified major accident scenarios has been compared against acceptable risk criteria;
- how critical safeguards have been selected and appropriate monitoring established, and
- the mechanism for communicating the major accident scenarios to employees (see Guide note 24).

Guide note 23 – Sensitivity analysis

A sensitivity analysis should be carried out when there is a degree of variation in the operating conditions, failure rate data or modelling assumptions which may significantly effect the outcome of the assessment and perceived level of risk.

When carrying out a sensitivity analysis, if varying an input assumption by an order of magnitude, has little or no effect on the results, then the input assumption should need no further validation. However, if the results appear to be highly dependent on the validity of the input assumption, its quality should be scrutinised. If there is low confidence in the value, there should be a demonstration as to how this is accounted for in the analysis.

Guide note 24 – Communication of results

The mechanism for communicating the results from the various studies, the identification of major risk contributors and the risk reduction measures to employees may entail:

- the involvement of employees during the hazard identification process
- risk awareness training particular to critical jobs and plant
- bow-tie diagrams / fault and event trees etc
- safety awareness workshops; and
- other relevant methods.

8.3 Acceptable risk criteria

The occupier should record the risk criteria used for assessing risk to people, property and the environment (see Guide note 25); and any assumptions made in evaluating the analysis results, particularly in the selection of the major accident scenarios.

Guide note 25 – Acceptable risk criteria

The New South Wales Department of Urban Affairs and Planning individual risk criteria described in the *Hazardous industry planning advisory paper No. 4* (HIPAP No. 4), 1997 will be used by the regulatory authority as a guide in assessing quantitative risk assessments.

HIPAP No. 4 provides key qualitative principles that are applied to land use safety planning and can also be applied to risk assessments, irrespective of the numerical value of any risk criteria level.

- "All avoidable risk should be avoided. This necessitates the investigation of alternative locations and alternative technologies, wherever applicable, to ensure that risks are not introduced in an area where feasible alternatives are possible and justified.
- The risk from a major hazard should be reduced wherever practicable, irrespective of the numerical value of the cumulative risk level from the whole installation. In all cases, if the consequences (effects) of an identified hazardous incident are significant to people and the environment, then all feasible measures (including alternative locations) should be adopted so that likelihood of such an incident occurring is made very low. This necessitates the identification of all contributors to the resultant risk and the consequences of each potentially hazardous incident. The assessment process should address the adequacy and relevancy of safeguards (both technical and locational) as they relate to each risk contributor.
- The consequences (effects) of the more likely hazardous events (i.e. those of high probability of occurrence) should, wherever possible, be contained within the boundaries of the installation.
- Where there is an existing high risk from a hazardous installation, additional hazardous developments should not be allowed if they add significantly to that existing risk."

<u>Guide note 25 – Acceptable risk criteria (cont.)</u>

HIPAP No. 4 also provides quantitative individual fatality risk levels that may be used by the regulator for land use planning advice as follows:

(a) Hospitals, schools, child-care facilities and old age housing development should not be exposed to individual fatality risk levels in excess of half in one million per year (0.5×10^{-6} per year).

(b) Residential developments and places of continuous occupancy, such as hotels and tourist resorts, should not be exposed to individual fatality risk levels in excess of one in a million per year (1×10^{-6} per year).

(c) Commercial developments, including offices, retail centres, warehouses and showrooms, restaurants and entertainment centres, should not be exposed to individual fatality risk levels in excess of five in a million per year (5×10^{-6} per year).

(d) Sporting complexes and active open space areas should not be exposed to individual fatality risk levels in excess of 10 in a million per year (10×10^{-6} per year).

(e) Individual fatality risk levels for industrial sites at levels of 50 in a million per year (50×10^{-6} per year) should, as a target, be contained within the boundaries of the site where applicable.

The application of risk criteria less stringent than those commonly recognised in Australia will not be accepted.

Where qualitative studies are employed, the regulatory authority will consider the criteria on a case-by-case basis. It is envisaged that if the facility poses an off-site risk, some form of quantification will be necessary.

The occupier, in the SRA report, should demonstrate:

- a comparison of the risks against acceptable risk criteria with justification for the application of the criteria
- the degree of uncertainty in the results (particularly where the likelihood of occurrence is low whilst the consequences are high);
- the methods of communicating the results to the relevant employees, and
- on a map, the area around the facility requiring community consultation derived from the SRA.

9 Possible risk reduction measures and reasonableness assessment

The occupier should demonstrate that appropriate risk reduction measures exist or have been identified for implementation to reduce the risk to people, property and the environment to an acceptable level (see Guide note 26).

Guide note 26 – What is an acceptable level of risk?

Each facility is required to demonstrate that risk is at an acceptable level, through the process of reducing risk to 'as low as reasonably practicable' (refer to Act section 17). This requires an ongoing process of assessment and challenge that includes the following

- Analysis of all major accident scenarios and evaluation of their overall risk (as detailed in previous sections of this guideline).
- Identification of all possible risk reduction measures for each pathway of each major accident scenario. This should include consideration of best practice, emerging technologies, relevant standards and industry practices. Control hierarchies should be considered to avoid all avoidable risks and to move to higher integrity controls where possible.
- Authoritative, good engineering practice is expected as a minimum. Identified, additional risk reduction measures should be assessed for practicability where the benefit that will be delivered from the measure is balanced against the impacts of putting it in place.
- Any measures that are rejected should be justified (normally by comparing the costs of introducing the measure to the risk reduction benefits).
- All practicable risk reduction measures should be implemented expeditiously.
- Once all practicable risk reduction measures are implemented then risk reduction to a level that is as low as reasonably practicable is achieved at that point in time.
- A periodic review of current facility standards, new best practices, industry standards, emerging technologies and previous assessments of rejected measures should be conducted to ensure that risk is maintained at a level that is as low as reasonably practicable . In this way, reducing risk to a level as low as reasonably practicable is an ongoing journey of improvement that takes into account facility changes as well as new solutions, improved economics of existing solutions and changes in expectations for operating standards.

Guide note 26 – What is an acceptable level of risk? (cont.)

Striving to reduce risk to a level that is as low as reasonably practicable requires recognition that existing risk reduction measures may not be operating optimally and that the occupier actively seeks out deterioration in performance. In this way the occupier can better understand true performance of the safeguards and address their deterioration.

9.1 Objectives and methodology

The occupier should demonstrate the following in the SRA report:

- that each pathway of all major accident scenarios have been assessed to determine what risk reduction methods can be applied;
- that all possible risk reduction measures have been considered and their link to the relevant hazards
- the methods used for the selection or rejection of risk reduction measures with appropriate justification
- the hierarchy of risk reduction methods has been applied (see Guide notes 27 and 28), and
- an appropriate degree of employee consultation in choosing risk reduction measures.

Guide note 27 – Hierarchy of control

The following hierarchy of risk reduction measures should be applied:

Elimination - removal of the hazard

↓

Substitution - use of a less hazardous substance

↓

Intensification - use of smaller inventories of hazardous materials

↓

Engineering controls – use of engineering methods

↓

Isolation – separation of hazards

↓

Administrative controls – systems of work or safe work practices

↓

Personal protective equipment should be provided where necessary.

<u>Guide note 28 – Risk reduction requirements</u>

All risk reduction methods considered should be recorded including details for their inclusion or rejection. Risk reduction measures should do at least one of the following:

- remove the hazard
- decrease the event frequency
- decrease the consequences of the event, and/or
- decrease the potential for escalation.

9.2 Risk reduction outputs

In the SRA report, the occupier should document the following for each major accident scenario:

- the potential risk reduction measures considered
- assumptions made in the methods used to select the risk reduction measures
- justification for the selection and rejection of risk reduction measures
- details concerning the effectiveness, reliability, survivability and performance criteria of the critical risk reduction measures (see Guide note 29)
- the degree of diversity and level of independence in the risk reduction measures;
- operating parameters compared against the design parameters of the critical risk reduction measures adopted including those already in place (see Guide note 30)
- the effects of those risk reduction methods on the consequence and likelihood for the major accident scenario
- identification of the criticality of the risk reduction measures
- that the extent of control is commensurate with the nature and scale of the hazards
- that there are clear links between the risk reduction measures identified through the SRA and the associated SMS, emergency plans and community consultation
- identification of appropriate performance criteria, and measurements that indicate the effectiveness of the risk reduction measures, and

- justification for level of risk for the major accident scenario being as low as reasonably practicable.

Guide note 29 – Effectiveness, reliability and survivability

The occupier must demonstrate that critical risk reduction measures implemented are sufficient to manage the hazard as intended and the number of measures is proportional to the severity of the hazard.

The reliability of the critical risk reduction measures must be proportional to the severity of the hazard. A high degree of reliability would be expected of risk reduction measures associated with severe hazards and hazards that occur frequently. The occupier must address the reliability of all critical risk reduction measures including hardware and human factors. If a human operation is critical to the prevention of a major accident and an unrealistically high level of reliability is assumed to make the level of risk as low as reasonably practicable there must be a thorough justification provided for the degree of reliability. Instead automatic risk reduction measures can be used to reduce the reliance on the operator.

The occupier must demonstrate the critical risk reduction measures will continue to function as intended during the types of incidents they are employed to reduce or mitigate, for example its ability to survive fire or blast damage.

For each critical risk reduction measure appropriate performance criteria and measures should be established and discussed in both the SRA report and the safety report.

Guide note 30 – Operating parameters

The occupier must should revisit the safe operating envelope for all risk reduction measures and provide details of the operating parameters with clear linkages to the control of major accidents as previously discussed in Guide note 5. For example:

- A high temperature trip system will automatically trip the steam heating to a vessel if the temperature level exceeds 350°C. Above 380°C the hazard identification study identified that the vessel contents would proceed to a runaway reaction which in turn could lead to failure of the vessel.
- A procedural risk reduction measure ensures that dangerous goods of class 8 (corrosive substances) are separated from dangerous goods of class 5.1 (oxidising substances) in a warehouse. The hazard identification study identified that an initiator of one of the major risk contributors was a violent chemical reaction between incompatible materials within the warehouse.

10 Likelihood and consequence analysis with all reasonable risk reduction measures

The aim of this section of the process is characterise the likelihood and consequence of each major accident scenario with all practicable risk reduction measures in place. This is to differentiate from the previous analysis of likelihood and consequence with all existing risk reduction measures in place that provided a starting point for the SRA.

It is possible that at the time of completion of the SRA, some identified, practicable risk reduction measures may not have been fully implemented. This section should analyse the overall risk profile when all proposed risk reduction measures are complete.

The process for conducting this analysis and the outputs expected are otherwise identical to that described in previous sections.

11 Implementation and demonstration that risk is reduced to a level that is as low as reasonably practicable

The occupier should effectively and expeditiously implement all reasonable risk reduction measures identified in the previous steps and in doing so demonstrate that overall facility risk is acceptable (as low as reasonably practicable) (refer to Guide note 26). Until this has been achieved, the facility cannot claim to have a level of risk that is as low as reasonably practicable and should justify its ongoing interim operation.

11.1 Objectives and methodology

The occupier should be able to demonstrate:

- the overall risk of each major accident scenario is as low as reasonably practicable
- the overall risk of the facility is as low as reasonably practicable
- If risk reduction to a level that is as low as reasonably practicable is not achieved for the scenario or the facility:
  - the level of risk posed by the facility in the short, interim period is appropriate and addresses the likelihood and consequences of accidents occurring. Consideration should be given to temporary controls in this period
  - an implementation plan is devised and the appropriate personnel are included
  - how the implementation of risk reduction measures is prioritised including any assumptions, and
  - the time period for implementation and reducing risk to a level that is as low as reasonably practicable is minimised and justified.

11.2 Outputs of implementation and demonstration that risk is reduced to a level that is as low as reasonably practicable

For each major accident scenario, the occupier should detail:

- the implementation status of the reasonable risk reduction measures

- implementation plan for any measures incomplete (see Guide note 31)
- justification that the implementation timeframe is as short as possible
- justification that the risk of operating the relevant parts of the facility is tolerable for the interim period.

The occupier should provide a reasoned argument that each scenario and the facility has in this review reduced risk to a level that is as low as reasonably practicable or will shortly achieve this level of acceptable risk through the completion of the justified implementation plan.

The occupier should demonstrate for the facility:

- the extent of safeguards are commensurate with the nature and scale of the hazards;
- there are clear links between the risk reduction measures identified through the SRA and associated SMS, community consultation and emergency plans;
- evidence that risk reduction measures have been adequately reviewed prior to implementation (see Guide note 32), and
- the final date by which an acceptable level of risk will be achieved.

Guide note 32 – Impact of risk reduction measures

Where the proposed implementation of risk reduction measures affects the process flow of the plant or operating procedures, a formal review of the measure must be carried out to ensure hazards are not introduced by its implementation. For example the addition of an emergency shut-off valve to the inlet of a tank may, when actuated, lead to over-pressurisation of upstream vessels and the subsequent failure of equipment.

12 SRA report

The purpose of the SRA report is to demonstrate to the regulator that the facility achieves and acceptable level of risk to people property and the environment. The SRA report shall provide inputs to the safety report, safety management system emergency plans and procedures and community consultation. The SRA report should argue the case that the hazards and major accidents are comprehensively understood and the safeguards are well selected, appropriately placed and adequate to achieve acceptable levels of risk. The SRA report must provide sufficient detail for the regulator to understand if the facility has or will achieve a level of risk that is as low as reasonably practicable.

The SRA report is also a commitment by the occupier to the safeguards that prevent and mitigate major accidents and the standards to which they will be operated. As such the SRA report will be a significant input to regulator audits.

The SRA report is required to demonstrate the occupier has:

- a comprehensive and detailed understanding of the facility hazards and particularly the major accident scenarios and corresponding risks to people, property and environment
- considered all possible risk reduction measures to prevent or mitigate the major accident scenarios
- implemented all reasonable measures to achieve a level of risk that is as low as reasonably practicable or committed to prompt implementation
- involved and consulted with employees throughout the process
- identified appropriate monitoring points for risk reduction measures to be included in the SMS.

The occupier should document each major accident scenario as detailed in the previous sections and also summarise the analyses for the facility (Guide note 33 provides examples of the content) in the SRA report.

Additionally an assessment should be made of facility risk prioritizing and summarizing the learnings from the individual assessments and demonstrate the following:

- understanding of the most significant risks for the facility
- list and location of each major accident scenario on a scaled map of the facility
- an understanding of the potential "knock-ons" for each major accident scenario
- a summary that shows, for each major accident, the worst case consequences, as well as the consequences and likelihood for the facility with existing safeguards and then with all proposed safeguards. The severity of these consequences should also be addressed in terms of the effects on people, property and the environment
- the facility consequences, expressed as injury risk levels for the major accident scenarios
- the overall facility risk showing the frequency of occurrence (may be qualitative or quantitative)
- the risk reduction measures that are in place or proposed to achieve a level of risk that is as low as reasonably practicable
- an implementation plan for proposed risk reduction measures that will achieve a level of risk that is as low as reasonably practicable if not already attained
- justification for the short term acceptability of risk while the implementation plan to attain a level of risk that is as low as reasonably practicable is progressed
- a list of critical risk reduction measures for the facility including both hardware and systems
- detail of the monitoring points, performance measures and operating standards for critical safeguards
- identify supporting SMS components that ensure that the risk reduction measures are monitored, maintained and remain effective
- identify emergency mitigation measures addressing the consequences of the various major accident scenarios, and
- justification that facility risk is at an acceptable level.

In addition to the information gathered in previous sections of the SRA process, the occupier should provide the following information to assist the regulator to understand the context of the facility:

- a scaled diagram showing the facility and surrounding land-use
- the population densities on-site and off-site for all foreseeable situations
- a concise process description and process flow diagrams for all parts of the facility storing or handling hazardous materials
- a detailed list of the materials on-site that could contribute to a major accident and their hazardous properties (flammability, reactivity and toxicity) under normal and abnormal conditions during start-up, shut-down and routine operations
- a plan with an appropriate scale showing the detailed location and quantities of materials listed in Tables 1 and 2 of Schedule 2 of the Regulation and other materials present which could contribute to the risk of fire, explosion or dispersion of hazardous materials
- details of significant past incidents, their root causes and remedial action;
- other information relevant to hazardous materials on-site through the consideration of the site as a whole, including on-site transport of hazardous materials, pipelines including associated pipe-bridges, etc, and
- all sources of information used in identifying hazards including their relevance, validity and significance.

Guide note 33 – Example summary format

<table>
<tr><td colspan="2">Hazard identifier:</td><td colspan="2">Source study:</td></tr>
<tr><td colspan="4">Plant location:</td></tr>
<tr><td colspan="4">Hazard description:</td></tr>
<tr><td colspan="4">Hazard scenario:</td></tr>
<tr><th>Risk assessment</th><th>Worst case</th><th>With existing safeguards</th><th>With proposed safeguards</th></tr>
<tr><td>Consequences:</td><td></td><td></td><td></td></tr>
<tr><td>Severity:</td><td></td><td></td><td></td></tr>
<tr><td>Likelihood:</td><td>N/A</td><td></td><td></td></tr>
<tr><th colspan="2">Risk reduction measures</th><th colspan="2">Performance criteria</th></tr>
<tr><td colspan="2">In place:
1.
2.
...</td><td colspan="2">1.
2.
…</td></tr>
<tr><th colspan="2">Proposed risk reduction measures</th><th colspan="2">Timing</th></tr>
<tr><td colspan="2">1.
2.
...</td><td colspan="2">1.
2.
…</td></tr>
<tr><th colspan="2">Rejected risk reduction measures</th><th colspan="2">Justification</th></tr>
<tr><td colspan="2">1.
2.
...</td><td colspan="2">1.
2.
…</td></tr>
<tr><td colspan="2">Supporting SMS components:</td><td colspan="2"></td></tr>
<tr><td colspan="2">Emergency mitigation measures:</td><td colspan="2"></td></tr>
</table>

12.1 Summary of occupier's requirements

The occupier may use the following as a checklist.

As a minimum, the occupier should include the following information in the SRA report to be submitted to the regulatory authority:

	Tick Box
General information	
• The consultation mechanism between the occupier and employees.	☐
• The degree of employee involvement.	☐
• The standards of competency of those involved in the SRA.	☐
• The techniques and methodologies used in the SRA and justification for their selection.	☐
• Any assumptions made and the logic behind them.	☐
• The sources, suitability and reliability of all data and information used.	☐
• Evidence that all information/drawings/etc. relevant to the facility are up to date.	☐
• The methods used to verify results.	☐
• Transparent linkages to the SMS, emergency plans and community consultation.	☐
• Evidence that the SRA is commensurate with the nature and scale of the facility, the type of operations carried out and its location.	☐
Specific information	
• The objectives of the SRA.	☐

- Evidence that the current plant integrity and the original design, selection and construction of the facility has been accounted for in the SRA. ☐
- Current facility information (land-use plan, process description, process flow diagrams, hazardous materials location map and properties list, other relevant information). ☐
- Hazards list for the entire facility operating under normal and abnormal conditions during start-up, shut-down and routine operations. ☐
- The worst case consequences for each major accident scenario ☐
- The sequence of events leading to all possible major accidents. ☐
- Sensitivity analyses for critical variables. ☐
- The likelihood and consequences of all major accidents with existing safeguards. ☐
- Evidence that the major accident scenarios identified are consistent with referenced studies from similar facilities. ☐
- The major accident scenarios. ☐
- A comparison of the risks against acceptable risk criteria (establish a level of risk that is as low as reasonably practicable). ☐
- The degree of uncertainty in the results. ☐
- A map of the area requiring community consultation. ☐
- All the risk reduction measures considered and their link to the relevant hazard. ☐
- Justification for the selection or rejection of risk reduction measures over alternatives. ☐
- The degree of diversity and independence of the risk reduction measures. ☐

- The effectiveness, reliability and survivability f the risk reduction measures, including those already in place.
- The operating parameters of the critical risk reduction measures adopted including those already in place.
- The likelihood and consequences of all major accidents with all proposed risk reduction measures in place
- The effects of the risk reduction measures on the overall facility risk.
- Justification for the overall facility risk being acceptable.
- Evidence that the SRA incorporates the current and proposed risk reduction measures.
- Clear linkages between the SRA and the SMS.
- Clear linkages between the SRA and the emergency plans.
- Clear linkages between the SRA and the community consultation process.
- The risk reduction measures implementation plan.
- The final date by which an acceptable level of risk will be achieved.
- The justification that the short term risk of the facility is acceptable while proposed risk reduction measures are being implemented.
- Evidence that risk reduction measures that impact upon the process have been adequately reviewed prior to implementation.
- The responsibilities for the completion of studies into identified knowledge gaps, the timeframe and the proponent carrying out the study.
- A summary table of the major accident scenarios.

13 Further reading

This section is not intended to be an exhaustive list of references but simply a list of useful reference texts concerning risk assessment.

Department of Employment, Training and Industrial Relations – Workplace Health and Safety
Workplace Health and Safety Risk Management Advisory Standard 2000
Available at: www.whs.qld.gov.au/advisory/adv027v1.pdf

National Occupational Health and Safety Commission
National Code of Practice for the Control of Major Hazard Facilities
[NOHSC:2016(1996)]
Australian Government Publishing Service Canberra
ISBN 0 644 45926 3
Available at:
www.nohsc.gov.au/OHSInformation/NOHSCPublications/fulltext/toc/01497-01.htm

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

National Occupational Health and Safety Commission
National Standard for the Control of Major Hazard Facilities
[NOHSC:1014(1996)]
Australian Government Publishing Service Canberra
ISBN 0 644 45926 3
Available at:
www.nohsc.gov.au/OHSInformation/NOHSCPublications/fulltext/toc/01397-01.htm

New South Wales Department of Urban Affairs and Planning
Hazardous Industry Planning Advisory Paper No. 3 (HIPAP No. 3), 1997
Environmental Risk Impact Assessment Guidelines
Department of Urban Affairs and Planning, Sydney

ISBN 0 7310 3042 7

New South Wales Department of Urban Affairs and Planning
Hazardous Industry Planning Advisory Paper No. 4 (HIPAP No. 4), 1997
Risk Criteria for Land Use Safety Planning
Department of Urban Affairs and Planning, Sydney
ISBN 0 7305 7130 0

New South Wales Department of Urban Affairs and Planning
Hazardous Industry Planning Advisory Paper No. 6 (HIPAP No. 6), 1992
Guidelines for Hazard Analysis
Department of Urban Affairs and Planning, Sydney
ISBN 0 7305 7125 4

New South Wales Department of Urban Affairs and Planning
Hazardous Industry Planning Advisory Paper No. 8 (HIPAP No. 8), 1995
Hazard and Operability Studies
Department of Urban Affairs and Planning, Sydney
ISBN 0 7310 3080 X

New South Wales Department of Urban Affairs and Planning
Multi-level risk assessment, 1997
Department of Urban Affairs and Planning, Sydney
ISBN 0 7310 9053 5

Standards Australia
Risk analysis of technological systems – Application guide
AS/NZS 9931:1998
Standards Australia and Standards New Zealand
ISBN 0 7337 1711 X

Standards Australia
Risk Management
AS/NZS 4360:1999

Standards Australia and Standards New Zealand

ISBN 0 7337 2647 X

Victorian Workcover Authority

Major hazard guidance material guidance notes

GN 14 Safety Assessment

Available from

http://www.workcover.vic.gov.au/vwa/home.nsf/pages/so_majhaz_guidance/$File/GN14_MHFR.pdf

14 (i) Sections of the Act relevant to this guideline

Dangerous Goods Safety Management Act 2001

PART 2—SAFETY OBLIGATIONS

Division 2—Obligations of occupiers and others

Obligations of occupiers

(1) The occupier of a major hazard facility or dangerous goods location has the following obligations—

(a) as far as practicable, to minimise the risk associated with the major hazard facility or dangerous goods location by—

(i) eliminating or minimising hazards at the facility or location; and

(ii) implementing measures to minimise the likelihood of a major accident at the facility or location; and

(iii) implementing measures to limit the consequences if a major accident happens at the facility or location;

Part (b) not directly relevant

(c) to record or be able to demonstrate the way the occupier has complied with the occupier's obligations under paragraph (a);

Parts (d) and (e) not directly relevant

PART 4—MAJOR HAZARD FACILITIES

Division 3—Other obligations of occupiers of major hazard facilities

41 Occupier must carry out systematic risk assessment

(1) The occupier of a major hazard facility must, in consultation with the employees at the facility, carry out, document, review and update a systematic risk assessment that as far as practicable—

(a) identifies all hazards that may lead to a major accident at the facility; and

(b) assesses the likelihood of a major accident happening at the facility and its effects if it does happen; and

(c) assesses the overall risk from the major hazard facility.

(2) The systematic risk assessment must be carried out and documented—

(a) *not directly relevant*

(b) for a facility classified as a major hazard facility more than 12 months after the commencement of this section—within 3 months after classification.

(3) The systematic risk assessment for a major hazard facility must be reviewed and updated before the facility is modified in a way that significantly alters the risk associated with the facility.

PART 6—AUTHORISED OFFICERS AND DIRECTIVES

Division 3—Directives by authorised officers

Subdivision 2Matters for which directives may be given

93 Directive to review systematic risk assessment

If an authorised officer reasonably believes the systematic risk assessment for a major hazard facility is inadequate, the authorised officer may give a directive to review the systematic risk assessment.

PART 1—PRELIMINARY

Division 4—Interpretation

13 Meaning of "major accident"

"Major accident" means a sudden occurrence (including, in particular, a major emission, loss of containment, fire, explosion or release of energy) leading to serious danger or serious harm to persons, property or the environment, whether immediate or delayed.

SCHEDULE 2

DICTIONARY

"serious harm" is harm that—
(a) causes the death of a person; or
(b) impairs a person to such an extent that because of the harm the person becomes an overnight or longer stay patient in a hospital; or
(c) results in costs of more than $50 000 being incurred to prevent, minimise or repair harm to property or the environment.

15 (ii) Sections of the Regulation relevant to this guideline

Dangerous Goods Safety Management Regulation 2001

PART 3—SAFETY OBLIGATIONS FOR OCCUPIERS

Division 1—Obligations applying to occupiers of major hazard facilities and dangerous goods locations

Subdivision 2—Hazard identification and risk assessment

17 Identification of hazards

(1) The occupier must ensure that a hazard associated with the storage or handling of dangerous goods or combustible liquids at the occupier's facility or location is, to the extent possible having regard to the current state of knowledge about the hazard, identified and recorded.

Maximum penalty—

(a) for a major hazard facility—100 penalty units;

(b) for a dangerous goods location—30 penalty units.

(2) For subsection (1) and without limiting the subsection, the occupier, when identifying hazards for dangerous goods or combustible liquids, must have regard to—

(a) the chemical and physical properties of the goods or liquids; and

(b) the MSDS and any other information about the hazardous properties of the goods or liquids; and

(c) any manufacturing and transport processes involving the goods or liquids at the occupier's facility or location; and

(d) the structures, plant, systems of work and activities used in the storage or handling of the goods or liquids at the occupier's facility or location; and

(e) the physical location and arrangement of areas, structures and safety and health systems at the occupier's facility or location; and

(f) the structures, plant, systems of work and activities that are not used to store or handle the goods or liquids but could interact with the goods or liquids at the occupier's facility or location; and

(g) the chemical and physical reaction between the goods or liquids and other substances and articles with which the goods or liquids may come into contact at the occupier's facility or location; and
(h) any previous incidents involving the goods or liquids.

18 Risk assessment

(1) If a hazard is identified under section 17, the occupier must ensure that—

(a) an assessment is made of the risks associated with the hazard (a **"risk assessment**"); and

(b) a dated written record is kept of the risk assessment.

Maximum penalty—

(a) for a major hazard facility—100 penalty units;

(b) for a dangerous goods location—30 penalty units.

(2) For subsection (1), the occupier must—

(a) have regard to the matters stated in section 17(2); and

(b) in the risk assessment, state the methods considered and those implemented to control the risks associated with the hazard to achieve an acceptable level of risk.

19 Review of risk assessment

(1) The occupier must review a risk assessment and keep a dated written record of the review—

(a) if there is a significant change to a process, system or procedure in relation to the storage or handling of dangerous goods or combustible liquids at the occupier's facility or location; or

(b) if there is evidence to indicate that the risk assessment no longer adequately assesses the risk associated with a hazard.[3]

Maximum penalty—

(a) for a major hazard facility—100 penalty units;

[3] Section 47 requires the review of the risk assessment under this section after an accident involving stated dangerous goods or combustible liquids causing material harm.

(b) for a dangerous goods location—30 penalty units.

(2) A risk assessment must be reviewed at least once every 5 years.
Maximum penalty—

(a) for a major hazard facility—100 penalty units;

(b) for a dangerous goods location—30 penalty units.

20 Copy of risk assessment to be available to persons likely to be exposed to a hazard

(1) This section applies if a risk assessment has been made for a hazard at an occupier's facility or location.

(2) The occupier must make a copy of the written record of the risk assessment available to persons likely to be exposed to the hazard while working at the facility or location.

Maximum penalty—

(a) for a major hazard facility—100 penalty units;

(b) for a dangerous goods location—30 penalty units.

Subdivision 9—Accidents

46 Investigation of accident

If an accident at an occupier's facility or location involves stated dangerous goods or combustible liquids and causes material harm, the occupier must ensure that—

(a) the accident is investigated; and

(b) the investigation, as far as practicable, determines the cause or likely cause of the accident; and

(c) a dated written record of the investigation is—
- (i) made; and
- (ii) kept for the life of the facility or location; and
- (iii) if requested, readily available to the chief executive.

Maximum penalty—

(a) for a major hazard facility—100 penalty units;

(b) for a dangerous goods location—30 penalty units.

47 Risk assessment and control after accidents

The occupier of a facility or location where an accident mentioned in section 46 has happened must as soon as reasonably practicable—

(a) review the risk assessment under section 19, taking into account the results of the investigation into the accident; and

(b) if the review identifies that risk is not at an acceptable level, take the action necessary to achieve an acceptable level of risk.

Maximum penalty—

(a) for a major hazard facility—100 penalty units;

(b) for a dangerous goods location—30 penalty units.