

## Risk assessment

Document No: N-04300-GN0165 A122420

Date: 24/06/2020

---

### Core concepts

- The operator of an offshore facility must conduct a detailed and systematic formal safety assessment, which includes the assessment of risk in relation to all potential major accident events (MAEs) and all hazards that could cause or contribute to causing those potential major accident events. The operator also has a duty to manage non-MAE health and safety risks. This guidance note is concerned with risk assessment in both contexts.
- The risk assessment process is central to the overall formal safety assessment and therefore should be linked to the hazard identification process and control measure selection process.
- The purpose of the risk assessment is to provide the operator with a detailed understanding of all aspects of the risks to people that may arise at or near the facility.
- Operators are encouraged to broaden the scope of risk assessment activities to incorporate risk assessment of all health and safety related hazards as the safety management system (SMS) must provide for all hazards and risks, not just risks of MAEs.
- The following aspects of MAEs must be understood as a result of the risk assessment:
  - The likelihood of each potential MAE; and
  - The consequences of each potential MAE.
- Although all types of risk assessment tools or methods are intended to provide some 'structure' for determining the level of risk, it should be recognized that all involve subjective and arbitrary judgements, and provide no absolute determination of risk.
- Operators should clearly understand and describe the uncertainty present in their risk assessment. Where the level of uncertainty is high, sensitivity analysis should be considered to test the robustness of the risk assessment results against variations within the key areas of uncertainty.
- The results of the risk assessment should be used in decision-making regarding the identification of technical and other control measures that are necessary to reduce the risk to a level that is as low as reasonably practicable.
- Hazards should not be ignored or discounted simply because control measures are, or will be, in place to reduce the associated risks.
- Operators should develop a role for the workforce in risk assessment, so that the workforce can contribute to the assessment of MAEs. Widespread awareness and understanding of the management measures for reducing the risks of MAEs is essential for safety improvement.
- The operator should select risk assessment tools appropriate to the facility and its risks. For many facilities, a combination of tools may be needed. The risk assessment may be tiered, initially using

relatively simple techniques to assess the risks associated with identified hazards, in order to identify the areas of high risk or uncertainty that require more detailed and specific assessment. This approach ensures assessment effort is targeted in critical areas.

- The operator must provide a detailed description of the formal safety assessment, including the risk assessment, for the facility in the safety case. The matters to be included in the formal safety assessment and described in the safety case are set out in the OPGGS(S) Regulations.

## Table of contents

Core concepts.....	1
Table of contents.....	3
Abbreviations/acronyms .....	4
Key definitions for this guidance note.....	5
1. Introduction.....	6
1.1. Intent and purposes of this guidance note .....	6
1.2. The risk management process applied in the safety case.....	7
1.3. Formal safety assessment .....	8
1.4. Involving the workforce.....	11
2. Risk assessment.....	12
2.1. The aims and outcomes of risk assessment .....	12
2.2. Features of a risk assessment.....	12
2.3. The role of codes, standards and classification society rules .....	13
3. Planning and preparation for risk assessment .....	14
3.1. Scope .....	14
3.2. General approach .....	14
3.3. Selecting risk assessment techniques .....	15
3.4. Qualitative or quantitative risk analysis.....	15
3.4.1. Use of a tiered approach .....	17
3.4.2. Detailed risk assessment studies.....	18
3.5. Organisation and personnel requirements .....	19
4. The risk assessment process .....	20
4.1. Likelihood analysis.....	21
4.1.1. Likelihood estimation .....	21
4.2. Consequence analysis.....	21
4.2.1. Consequence estimation .....	22
4.3. Nature of injury or illness .....	23
4.4. Control measure assessment .....	23
4.5. Determining and interpreting the risk results.....	24
4.5.1. Managing risk uncertainty and error.....	25
4.5.2. Providing evidence that risks are reduced to a level that is ALARP .....	26
5. Outputs.....	26
5.1. Risk assessment outputs .....	26
5.2. Uses of risk assessment outcomes.....	27
5.3. Review and revision of risk assessment .....	27
6. Quality assurance .....	29
7. Critical success factors for risk assessment.....	29
8. Common weaknesses.....	30
9. References, acknowledgements and notes.....	31
Appendix A: Structures risk assessment techniques .....	33
A.1: Risk matrix.....	33
A.2: Fault and event trees .....	34
A.3: Hazard and operability analysis (HAZOP).....	35
A.4: Quantitative or quantified risk assessment (QRA).....	36
A.5: Layers of protection analysis (LOPA) and safety integrity levels (SIL).....	37

## Abbreviations/acronyms

ALARP	As Low As Reasonably Practicable
CFD	Computational Fluid Dynamics
EER	Evacuation, Escape and Rescue Analysis
FD	Facility Description
FSA	Formal Safety Assessment
HAZID	Hazard Identification Study
HAZOP	Hazard and Operability Study
JHA	Job Hazard Analysis
JSA	Job Safety Analysis
LOPA	Layers of Protection Analysis
MAE	Major Accident Event
MoC	Management of Change
NOPSEMA	National Offshore Petroleum Safety and Environmental Management Authority
OHS	Occupational Health and Safety
OPGGGS Act	<i>Offshore Petroleum and Greenhouse Gas Storage Act 2006</i>
OPGGGS(S) Regulations	Offshore Petroleum and Greenhouse Gas Storage (Safety) Regulations 2009
QRA	Quantitative Risk Analysis
SMS	Safety Management System

## Key definitions for this guidance note

The following are some useful definitions for terms used in this guidance note. Unless prescriptively defined in the Commonwealth Offshore Petroleum and Greenhouse Gas Storage (Safety) Regulations 2009 [OPGG(S) Regulations] [as indicated by the square brackets] they are a suggested starting point only.

ALARP	This term refers to reducing risk to a level that is As Low As Reasonably Practicable. In practice, this means that the operator has to show through reasoned and supported arguments that there are no other practicable options that could reasonably be adopted to reduce risks further.
Control Measure	A Control Measure is any system, procedure, process, device or other means of eliminating, preventing, reducing or mitigating the risk of hazardous events arising at or near a facility. Control measures are the means by which risk to health and safety from events is eliminated or minimised. Controls can take many forms, including physical equipment, process control systems, management processes, operating or maintenance procedures, emergency response plans, and key personnel and their actions.
Formal Safety Assessment	A formal safety assessment, in the context of the OPGGS(S) Regulations, is an assessment or series of assessments that identifies all hazards having the potential to cause a major accident event. It is a detailed and systematic assessment of the risk associated with each of those hazards, including the likelihood and consequences of each potential major accident event. It identifies the technical and other control measures that are necessary to reduce that risk to a level that is as low as reasonably practicable [OPGG(S) subregulation 2.5(2)(c)].
Hazard	A Hazard is defined as a situation with the potential for causing harm to human health or safety.
Hazard Identification	Hazard Identification is the process of identifying potential hazards. In the context of the OPGGS(S) Regulations, hazard identification involves identifying all hazards having the potential to cause a major accident event [OPGG(S) subregulation 2.5(2)(a)], and the continual and systematic identification of hazards to health and safety of persons at or near the facility [OPGG(S) subregulation 2.5(3)(c)].
Major Accident Event	A Major Accident Event is an event connected with a facility, including a natural event, having the potential to cause multiple fatalities of persons at or near the facility [OPGG(S) Regulation 1.5].
Performance Standard	Performance standard means a standard, established by the operator, of the performance required of a system, item of equipment, person or procedure which is used as a basis for managing the risk of a major accident event [OPGG(S) Regulation 1.5].
Risk Assessment	Risk assessment is the process of estimating the likelihood of an occurrence of specific consequences (undesirable events) of a given severity.
Workforce	Members of the workforce include members of the workforce who are: <ul style="list-style-type: none"> <li>(a) identifiable before the safety case is developed; and</li> <li>(b) working, or likely to be working, on the relevant facility.</li> </ul> [OPGG(S) subregulation 2.11(3)].

## 1. Introduction

### 1.1. Intent and purposes of this guidance note

This document is part of a series of documents that provide guidance on the preparation of safety cases for Australia's offshore facilities, as required under the Commonwealth *Offshore Petroleum and Greenhouse Gas Storage (Safety) Regulations 2009* [the OPGGS(S) Regulations] and the corresponding laws of each State and of the Northern Territory.

This guidance note, *Risk Assessment*, forms part of a suite of guidance notes which are designed to help operators through the process of conducting risk assessments in the context of both formal safety assessment and other occupational health and safety risks in support of the evidence to be provided in the safety case that risks are reduced to a level that is as low as reasonably practicable (ALARP). The suite of guidance notes includes:

- Hazard Identification
- Supporting Safety Studies
- Risk Assessment
- ALARP
- Control Measures and Performance Standards

Section 1 of this guidance note gives an overview of the Formal Safety Assessment process, and the balance of the guidance note discusses risk assessment aspects in particular.

The purpose of risk assessment is to help all stakeholders understand the risks to health and safety and address potential major accident events (MAEs) in a structured manner. The guidance note will explain risk assessment approaches which might apply to offshore facilities and activities, and demonstrate that there are a wide range of analysis types, including qualitative, semi-qualitative and quantitative approaches that can be used to help operators understand the risk levels at their facilities. Only once hazards have been identified and the associated risks have been assessed will operators will be able to manage them properly.

This guidance note will be of use to those with responsibility for planning and developing the facility safety case, and those involved in safety case implementation, maintenance, and ongoing risk management.

Figure 1 illustrates the scope of the NOPSEMA safety case guidance notes overall, and their interrelated nature. This guidance note on *Risk Assessment* should be read in conjunction with the other relevant guidance notes; the full set is available on the NOPSEMA website along with guidance on other legislative requirements such as operator nomination, validation, and notifying and reporting accidents and dangerous occurrences.

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**, while other cases are indicated by the words **should**, **may**, etc. NOPSEMA acknowledges that what is good practice and what approaches are valid and viable will vary according to the nature of different offshore facilities and their hazards. Whilst this guidance note puts forward a selection of the possible approaches that operators may choose to explore in addressing the risk assessment requirements of the OPGGS(S) Regulations, the selection is not exhaustive and operators may choose to use other techniques not covered by this guidance note.

This guidance note is not a substitute for detailed advice on the regulations or the Acts under which the regulations have been made.



Figure 1 – Safety case guidance note map

## 1.2. The risk management process applied in the safety case

The Australian/New Zealand Standard on Risk Management AS/NZS ISO 31000:2009 provides a generic framework for establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk. The requirements under the OPGGS(S) Regulations reflect the current thinking on risk management and hence call for application of the key elements of risk management. These are outlined in subregulation 1.4(2) *Objects* summarised below.

### OPGGS(S) Regulation - Objects

- Reg 1.4(2) An object of these Regulations is to ensure that safety cases for offshore petroleum facilities make provision for the following matters in relation to the health and safety of persons at or near the facilities:
- (a) the identification of hazards, and assessment of risks;
  - (b) the implementation of measures to eliminate the hazards, or otherwise control the risks;
  - (c) a comprehensive and integrated system for management of the hazards and risks;
  - (d) monitoring, audit, review and continuous improvement.

## 1.3. Formal safety assessment

### OPGGS(S) Regulation - Formal Safety Assessment Requirement

- Reg 2.5(2) The safety case for the facility must also contain a detailed description of the formal safety assessment for the facility, being an assessment, or series of assessments, conducted by the operator that:
- (a) identifies all hazards having the potential to cause a major accident event; and
  - (b) is a detailed and systematic assessment of the risk associated with each of those hazards, including the likelihood and consequences of each potential major accident event; and
  - (c) identifies the technical and other control measures that are necessary to reduce that risk to a level that is as low as reasonably practicable.

*Note A formal safety assessment relates only to major accident events*

The Formal Safety Assessment is focused on Major Accident Events (MAEs). Providing a well-considered, detailed description of a suitable and sufficient formal safety assessment within the safety case will enable operators to provide evidence of:

- an understanding of the factors that influence risk and the controls that are critical to controlling risk;
- the magnitude and severity of the consequences arising from MAEs for the range of possible outcomes;
- the likelihood of potential MAEs and the range of possible outcomes from it; and
- clear linkages between hazards, the MAEs, control measures and the associated consequences and risk.

Risk is a function of both likelihood and consequence. For the purposes of this guidance note, risk assessment is defined as the process of estimating the likelihood of an occurrence of specific consequences (undesirable events) of a given severity. Figure 2 below provides a diagrammatic representation of the primary focus of the OPGGS(S) Regulations on high consequence low frequency events.

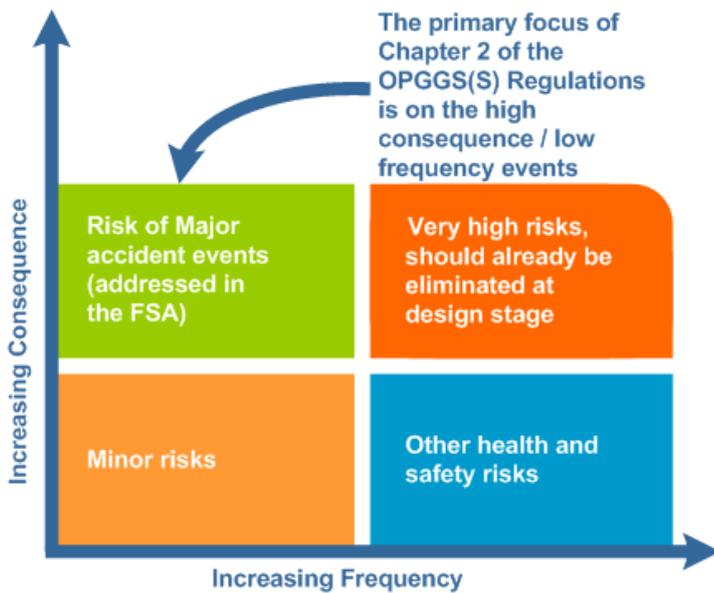


Figure 2 – Formal Safety Assessment to focus on MAEs

For the purposes of a safety case submission, the hazard identification and risk assessment need only relate to MAEs. However, it should be noted that the detailed description of the safety management system in the safety case must provide for all hazards and risks to persons at the facility, including risks to health and safety. Therefore, operators may wish to consider broadening the scope of hazard identification and risk assessment studies to address other hazards not necessarily linked to MAEs e.g. noise, exposure to exhaust fumes, etc.



Further guidance is available in NOPSEMA guidance note:

**“Safety Management System”**

The formal safety assessment should have a consistent, integrated overall structure; there should be logical flow to the assessment process to create strong links between the hazards, the causes and consequences of MAEs, their associated risks, the selection of strategies and measures to manage the risks, and the performance required from specific measures to maintain risk levels to a level that is ALARP.

The intent here is to emphasise that the FSA must be a coherent, integrated assessment of MAEs. Spending time getting the structure right will greatly enhance an operator’s ability to present evidence in the safety case in a robust way that others can follow and understand.

The steps for developing a formal safety assessment are integrally linked. For this reason the process is not a strictly linear one, and some steps can overlap. Identifying and assessing control measures, for instance, cuts across all areas of the FSA process as shown in Figure 3. Due to this potential overlap, it is particularly important to organise and construct linkages through the process. This is best done at the hazard identification phase, as this phase sets the scene for the later steps of formal safety assessment development.



Further guidance is available in NOPSEMA guidance note:

**“Hazard Identification”**



Further guidance is available in NOPSEMA guidance note:

**“Control measures and performance standards”**

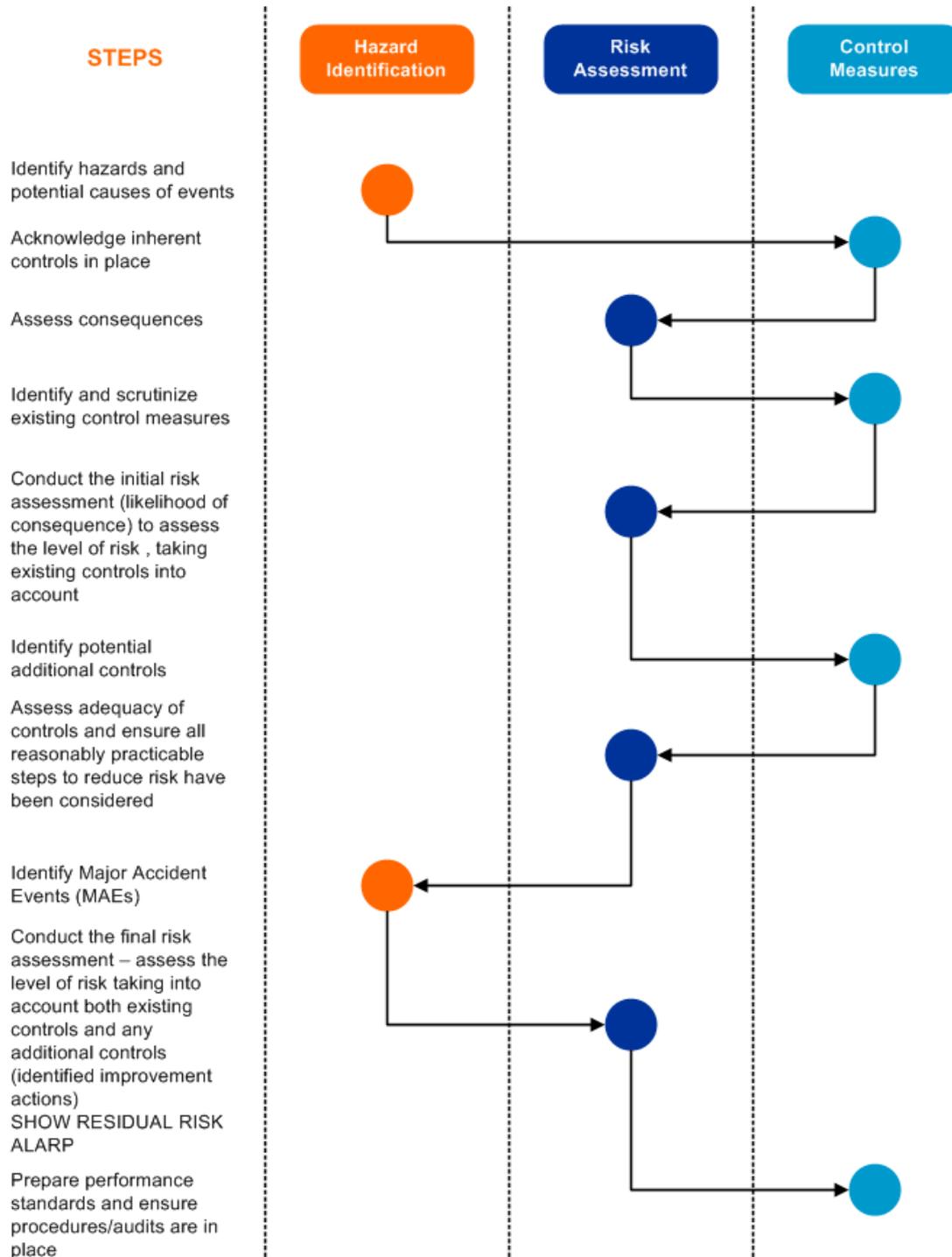


Figure 3 – The FSA process

*Note:* Figure 3 is included as an example only and is not intended to prescriptively dictate the steps to be followed in a formal safety assessment process. Operators may choose to conduct different steps at different stages depending upon their own circumstances.

## 1.4. Involving the workforce

OPGGS(S) Regulation - Involvement of members of the workforce	
Reg 2.11 (1)	The operator of a facility must demonstrate to NOPSEMA, to the reasonable satisfaction of NOPSEMA, that: <ul style="list-style-type: none"> <li>(a) in the development or revision of the safety case for the facility, there has been effective consultation with, and participation of, members of the workforce; and</li> <li>(b) the safety case provides adequately for effective consultation with, and the effective participation of, the members of the workforce, so that they are able to arrive at informed opinions about the risks and hazards to which they may be exposed on the facility.</li> </ul>
(2)	A demonstration for paragraph (1) (a) must be supported by adequate documentation.
(3)	In subregulation (1): <p><i>members of the workforce</i> includes members of the workforce who are:</p> <ul style="list-style-type: none"> <li>(a) identifiable before the safety case is developed; and</li> <li>(b) working, or likely to be working, on the relevant facility.</li> </ul>

Formal safety assessment is the process of debating, analysing, creating and sharing views, information and knowledge on the risk of MAEs and their means of control. It must include the participation of people at the 'coal face' who influence safe operation, and hence members of the workforce should play a role in hazard identification and risk assessment. Formal safety assessment can include any activity the operator employs to understand the facility and its risks. For example, it could incorporate information from incident investigations, discussions during safety meetings regarding hazards and ways of controlling them, condition monitoring programs, analysis of process behaviour, evaluation of trends or deviations from critical operating parameters, procedure reviews, etc.

The knowledge generated by the formal safety assessment should be captured, managed and disseminated to ensure it remains up-to-date and is used in the design, operation and maintenance of the facility. The effective management of knowledge generated in the hazard identification and risk assessment will also greatly assist the efficient development of a safety case for the facility, for example, by handling assumptions, actions arising, etc. through the development process.

It is not practical to involve everyone in the hazard identification and risk assessment processes; therefore, it is important that feedback is provided to the rest of the workforce. This feedback should take the form of communicating the hazards that are present, the risks associated with those hazards, the controls in place and any recommendations arising. The workforce should also be provided with an opportunity to review and comment on the risk assessment output. This is both an important quality control activity and part of the mandatory consultation and participation required by the OPGGS(S) Regulations. It can also promote a feeling of ownership among personnel not directly involved in the risk assessment process.



Further guidance is available in NOPSEMA guidance note:

***“Involving the workforce”***

## 2. Risk assessment

### 2.1. The aims and outcomes of risk assessment

The aims of risk assessment in the context of the OPGGS(S) Regulations are as follows:

- To provide the operator and the workforce with sufficient knowledge, awareness and understanding of the risks from health and safety hazards and, in particular, the risks from MAEs to be able to manage the facility safely.
- To provide a basis for identifying, evaluating, defining and justifying the selection (or rejection) of control measures for eliminating or reducing risk, and to lay the foundations for demonstrating that the risks have been reduced to a level that is as low as reasonably practicable (ALARP).
- To provide the specific information required by the regulations.

While the risk assessment provides an important link between the identified hazards, the adopted control measures and the demonstration of ALARP within the safety case, risk assessment is also a means of generating an understanding and knowledge of risk. A deficiency in risk assessment may make it difficult to demonstrate appropriateness of control measures, but more significantly it may indicate a lack of sufficient knowledge to conduct activities safely. The operator should therefore approach risk assessment as an objective learning process, and not simply as a means of justifying the control measures already in existence.

Good and practical risk assessment, carried out at a time when it can affect decisions of significance for the risk level, are a key precondition for being able to design and operate a facility safely. The development, implementation, use and follow-up of risk assessment in a systematic and traceable way is thus an important contribution towards managing risk through all stages of a facility's lifecycle.

Finally, the risk assessment creates knowledge, awareness and preparedness within the organisation. Knowledge of hazards and their implications is necessary to prevent and deal with dangerous occurrences; therefore this knowledge is in itself an important control measure, which should be properly managed.

### 2.2. Features of a risk assessment

#### OPGGS(S) Regulation - FSA and SMS Risk Assessment Requirements

- |               |  |
|---------------|--|
| Reg 2.5(2)(b) | The safety case for the facility must also contain a detailed description of the formal safety assessment for the facility, being an assessment, or series of assessments, conducted by the operator that is a detailed and systematic assessment of the risk associated with each of those hazards, including the likelihood and consequences of each potential major accident event. |
| Reg 2.5(3)(d) | The safety case for the facility must also contain a detailed description of the safety management system that <i>[provides evidence that the Safety Management system]</i> ; provides for the continual and systematic assessment of:   |

- (i) the likelihood of the occurrence, during normal or emergency situations, of injury or occupational illness associated with those hazards; and
- (ii) the likely nature of such injury or occupational illness.

OPGGS(S) subregulation 2.5(2)(b) requires risk assessment, as part of the FSA, to be **detailed** and **systematic**. In addition, OPGGS(S) subregulation 2.5(3)(d) requires risk assessment, as part of the SMS, to be **continual** and **systematic**.

A '**detailed**' risk assessment means covering the requirements of OPGGS(S) in all areas. It should as a minimum:

- cover all potential MAEs and all of the aspects of risk to people for each identified potential MAE (consequence, likelihood, etc.);
- cover all risks associated with emergencies;
- cover all risks associated with fires and explosions;
- cover all aspects of the facility design, construction, installation, maintenance and modification; and
- cover all activities included within the scope of the safety case.

A '**systematic**' risk assessment should methodically employ a logical, transparent and reproducible process, which enables the operator and workforce to understand the risks.

A '**continual**' risk assessment is assessment of risk that is carried out on a regular and ongoing basis.

### 2.3. The role of codes, standards and classification society rules

The safety case regime enables the operator to choose which established and appropriate codes and standards to apply, which provides for a more flexible basis for managing safety. The safety case should show that the risk assessment is based on sound science and good risk management decisions that are appropriate to the facility. The approach taken depends on the nature of the activities, the operator's capabilities and the risk management decisions they face.

The risk assessment should reflect the operator's safety case philosophy. That is, if the operator intends to base the safety case largely on the facility's compliance with specific codes or standards, the risk assessment should address corresponding issues such as the basis of the codes and standards, their applicability to the facility, and the issues associated with compliance or non-compliance. Any risk assessment carried out in developing the standards may be useful in support of this. However, the operator would need to evaluate whether the proposed standards fully address the requirements of the OPGGS(S) Regulations, and then address any gaps between the two. For example, if the standard did not consider a certain type of hazard then additional control measures may be required over and above those prescribed by the standard. This may be particularly relevant in respect of marine hazards; the safety of offshore installations against marine hazards has traditionally relied on International Maritime Organisation legislation and classification society rules. These rules have been developed by expert judgement, responding to previous accident experience and, in general, prescribe specific design solutions. They are only rarely based on risk assessment, and do not necessarily satisfy the requirement to perform a risk assessment [ref HSE report 2001/063]. In addition, marine related classification society rules do not necessarily address all of the hazards faced by a vessel operating in the offshore petroleum industry.

Conversely, if the operator intends to base the safety case on fundamental engineering or management systems, the risk assessment should be structured accordingly. In particular, if the operator intends to diverge from established codes or standards, or if the codes and standards do not apply fully to the facility, the risk assessment should address these issues. Some operators may be faced with situations where there is a need for dynamic change, new technology is developing, there are numerous options available for managing the risks, there may be no established standards, or existing standards may be unnecessarily constraining the business. These operators may use the risk assessment as a way of identifying alternative and more effective/efficient means of managing risk. In this situation the operator is using risk assessment to establish the most appropriate controls for their facility.



*Further guidance is available from NOPSEMA guidance note:*

**“ALARP”**

### 3. Planning and preparation for risk assessment

#### 3.1. Scope

Operators and their workforce may carry out safety assessments such as job safety analyses (JSA) or job hazard analyses (JHA) as part of established routine and non-routine activities, e.g. in deciding on shift teams, planning an activity, etc. However, the formal safety assessment (FSA) required by the OPGGS(S) Regulations is a distinct, formal exercise undertaken by the operator (and members of the workforce, as appropriate) to assess risk across the entire facility.

For the purposes of a safety case submission, the hazard identification and risk assessment carried out as part of the formal safety assessment need only relate to MAEs. However, it should be noted that the safety management system must provide for all hazards and risks to persons at the facility, not just risks of MAEs. Therefore, operators may wish to consider broadening the scope of hazard identification and risk assessment studies to address other hazards not necessarily linked to MAEs, e.g. noise, exposure to exhaust fumes, etc.

The risk assessment is linked to the hazard identification phase in the first instance. All identified hazards should be subject to a ‘screening’ process to determine if there is any potential for the hazard to lead to an MAE. Once this has been done, the areas of high risk or uncertainty may be subjected to more detailed and specific assessment to better understand the mechanisms by which a MAE (or other hazardous event) may occur.

The risk assessment provides information necessary to determine which control measures to adopt and the necessary functioning of the safety management system with regard to each identified hazard. The scope of the risk assessment should therefore be linked to these issues also.

#### 3.2. General approach

It must be recognised that assessing risk is not the same as managing risk, and risk assessment therefore is only worthwhile if it informs and improves the operator’s decision-making and seeks to reduce risk to a level that is as low as reasonably practicable (ALARP). The purpose of risk assessment is to understand the nature of risks and what might be needed to eliminate or minimise them.

Risk assessment should be a rigorous process of gathering information in order to understand the nature of the hazard(s), the mechanisms by which the hazard(s) could give rise to injury or ill-health and the magnitude and severity of the risk. On the basis of such a risk assessment, the operator can then determine what preventive or mitigation action is required. Thus, the assessment of risks should be focussed on making well informed decisions about suitable risk control measures, rather than putting effort into subjectively estimating risk.

Risk assessment should be instigated by the safety management system as required in order to maintain a comprehensive and up-to-date understanding of risk as the facility changes; hence risk assessment may typically be triggered via the process for formal management of change at the facility.

The results of risk assessment would be expected to be fed into the development of the safety management system, e.g. where the risk assessment indicates operational procedures need to be developed. In addition, the results of risk assessment would be expected to provide input for engineering design to ensure that the appropriate level of performance is incorporated into engineered barriers that may be required.

### 3.3. Selecting risk assessment techniques

Operators must select appropriate techniques for conducting risk assessment. Brief descriptions of some of these techniques are provided in Appendix A. Selection will depend on the desired level of information required to better understand the risk and to manage it.

The main considerations that should be taken into account when selecting risk assessment techniques are:

- they should be suitable for the type and complexity of facility and the nature of the hazards present;
- they should assist in understanding and selecting control measures;
- they should adequately differentiate between MAE outcomes on a risk basis (i.e. likelihood and consequence); and
- they should be capable of assessing the potential effect of risk reduction measures.

Depending on the different types of hazards and their potential outcomes, several techniques to develop a complete understanding of the hazards and risks at the facility may need to be employed. No single assessment tool is able to meet all of the requirements for risk assessment, as all tools have limitations and weaknesses. Therefore, some of the questions that will need to be answered when planning for risk assessment are:

- What risk analysis method(s) (e.g. qualitative, semi-quantitative, quantitative, etc.) and risk criteria will be used?
- What risk assessment technique(s) will be used (e.g. risk matrix, bow-tie, QRA, etc.)?
- What level of detail is required?
- What resources are available?

### 3.4. Qualitative or quantitative risk analysis

Risk analysis may be carried out using qualitative, semi-quantitative and/or quantitative approaches. There are numerous qualitative approaches to ranking risks that apply descriptive scales (such as extreme, major,

moderate, minor) to rate the magnitude of consequences or rate the likelihood of occurrence (very likely, likely, unlikely, remote). There is also a multitude of semi-quantitative and quantitative methods which use numerical values rather than descriptive scales for both the magnitude of consequences and the likelihood of adverse outcomes. A range of data sources might be used to determine these numerical values, including past incident data, or data obtained from modelling events or experimental studies. Although all types of risk assessment tools or methods are intended to provide some 'structure' for determining the level of risk, all involve subjective and arbitrary judgements, and provide no absolute determination of risk. Unreliability can creep in, either in determining the descriptor or numerical values assigned to risk (qualitative and semi-quantitative analysis), or in selecting or processing data to use for analysing risk (quantitative assessment). Clearly, risk assessment is not an exact science. The concern is that more time and effort may go into applying these methods than goes into determining or developing preventive measures.

In selecting a risk assessment process, the objective of the risk assessment, the anticipated level of risk, and the detail needed in the assessment results, should all be considered. If risks are complex, the process of assessing them will need to have sufficient depth to understand those risks. Operators are urged to 'do what it takes' to ensure they fully understand the risks of their operations and activities, and to identify and take appropriate preventive measures on the basis of that assessment. The most common risk assessment techniques and the key points of each approach are listed in Table 1 below.

*Table 1 – Risk analysis techniques – Key aspects*

Technique	Risk Assessment Method	Key Aspects of the Risk Analysis Technique
<b>Qualitative</b>	Risk matrix method	<p>Likelihood and consequence expressed on a scale described in words.</p> <p>Risk output is not expressed as a numerical value.</p> <p>Emphasis is placed on relative grouping of hazards (e.g. into acceptable, tolerable and unacceptable) or on rough ranking of hazards from highest to lowest.</p> <p>The workshop participants estimate the risk resulting in greater ownership of the risk results. Site/facility specific.</p> <p>Based on subjective judgement so a higher potential for uncertainty.</p> <p>Coarse level of risk assessment in general with little risk ranking capacity.</p> <p>Difficult to calculate cumulative risk.</p> <p>Often used as a preliminary risk assessment or screening tool.</p> <p>Often used for operations or task based risk assessments.</p> <p>Suitable for simple facilities or where the exposure of the workforce is low.</p> <p>Rapid assessment of risk.</p> <p>Relatively easy to use.</p> <p>Can take into account intangible issues such as public outrage and company reputation.</p>

Technique	Risk Assessment Method	Key Aspects of the Risk Analysis Technique
<b>Semi-quantitative</b>	Risk matrix method Layers of protection analysis (LOPA)	<p>Generates a numerical risk value (although this value is not an absolute value of risk).</p> <p>Provides greater capacity to discriminate between hazards on the basis of risk.</p> <p>Better for assessing cumulative risk although still coarse and difficult for large facilities. Caution is required to ensure that only like data is combined.</p> <p>Some methods provide a more structured technique for understanding the effectiveness of controls.</p>
<b>Quantitative</b>	Quantitative risk assessment (QRA) Fault tree Event tree Layers of protection analysis (LOPA) Computational fluid dynamics (CFD) Gas dispersion analysis	<p>Based on calculated estimates of consequence (usually software modelling) and likelihood (estimates based on failure rate data – site or industry).</p> <p>Provides a calculated value of risk.</p> <p>Better suited to more complex decision making or where risks are relatively high.</p> <p>Some quantitative techniques (i.e. fault and event trees) can provide a more detailed knowledge of the causal chain and the influence of controls.</p> <p>More rigorous, detailed and objective than other methods and can better assist choice between different control options.</p> <p>More time intensive and expensive than other methods.</p> <p>QRA can provide risk levels if necessary for demonstrating exposure and effect. Does not necessarily provide a full understanding of the impact of controls.</p>

Risk assessment needs to be planned and suitably resourced. It is appropriate that the time and resources spent on the risk assessment are comparative to the types of hazardous events to be considered and the level of risk associated with those hazardous events. Resources are frequently limited and spending excess time on hazardous events which are of a low level of risk may take resources away from the more critical events.

### 3.4.1. Use of a tiered approach

The tiered or multi-level approach to risk assessment may see relatively simple techniques (e.g. a qualitative or semi-quantitative approach) used initially to assess hazards as part of a 'screening' process to determine if they can result in a MAE. Once this has been done, the areas of high risk or uncertainty may be subjected to more detailed and specific risk assessment.

For many operators, a combination of approaches may be required. For example, quantitative consequence modelling may be used to justify the consequence analysis category selected in a risk matrix approach. Alternatively, qualitative assessment is used for simpler processes, while quantitative risk assessment may be employed for higher risks or more complex processes. The complexity of the process or facility in itself does not necessarily dictate that quantitative risk assessment is required.

The onus is on the operator to select and conduct assessment appropriate to their facility and activities to be carried out. Further guidance is provided in Table 1 above.

The results of the preliminary hazard evaluation should provide guidance towards the types of detailed risk studies required. Clearly, the greatest attention should be directed towards those areas where there are gaps in knowledge, and where the risks may be high. For example, if a qualitative risk assessment shows a high level of risk then further analysis may be required, including a quantitative risk assessment, to examine the risks in more detail.

### 3.4.2. Detailed risk assessment studies

Detailed analyses of the facility and / or activities may be required to better understand the mechanisms by which a hazardous event may occur and the controls in place to prevent this. In particular, where there is insufficient knowledge of causes, likelihoods, etc. in key areas, consideration should be given to using more detailed studies to reduce this uncertainty. These analyses supplement the overall risk assessment and may be required to accurately assess the risk at a facility.

Note that the OPGGS(S) Regulations specifically require the safety case to include a detailed description of an evacuation, escape and rescue analysis [OPGGS(S) Regulation 2.16] and a fire and explosion risk analysis [OPGGS(S) Regulation 2.17] for the facility. These analyses form part of the FSA in so far as they address MAEs.

Additionally, the OPGGS(S) Regulations require the safety case to provide for operational and emergency communication systems and control systems [OPGGS(S) Regulation 2.18 and Regulation 2.19]. This may require operators to conduct emergency system survivability studies, in particular in relation to emergency communications and control systems such as back-up power, lighting, alarm systems, ballast control and emergency shut-down systems.



*Further guidance is available in NOPSEMA guidance note:*

***“Supporting safety studies”***

Detailed assessments may involve the application of more quantitative techniques such as fault tree techniques. However, there are other types of detailed studies that may be appropriate to fully investigate and understand a hazard. Some of these are shown in Table 2 below.

The studies listed in the table are given as an example only and should not be taken to be an exhaustive listing of studies and reviews that may be applicable.

**Table 2 – Types of detailed studies**

Key identified risk driver	Potential Studies for Investigation and Understanding of a Hazard
<b>Aging equipment and associated mechanical integrity problems</b>	<ul style="list-style-type: none"> <li>• Mechanical integrity</li> <li>• Corrosion rates</li> <li>• Breakdown data</li> <li>• Reliability</li> <li>• Inspection / testing / maintenance issues</li> </ul>

Key identified risk driver	Potential Studies for Investigation and Understanding of a Hazard
<b>Changing process conditions</b>	<ul style="list-style-type: none"> <li>• Process HAZOP</li> <li>• Procedure HAZOP</li> <li>• Mechanical integrity</li> </ul>
<b>Dropped or swinging load impact</b>	<ul style="list-style-type: none"> <li>• Dropped object study</li> <li>• Layout study</li> <li>• Mechanical and materials handling</li> </ul>
<b>Human error</b>	<ul style="list-style-type: none"> <li>• Task analysis</li> <li>• Human reliability analysis</li> <li>• Detailed analysis of operating procedures</li> </ul>
<b>Hazardous gas/vapour accumulation</b>	<ul style="list-style-type: none"> <li>• Natural ventilation</li> <li>• Gas dispersion</li> <li>• Gas/smoke ingress study</li> <li>• Wind tunnel modelling</li> <li>• Explosion overpressure study</li> <li>• Layout study</li> </ul>
<b>Potential ignition of flammable materials</b>	<ul style="list-style-type: none"> <li>• Electrical zoning</li> <li>• Equipment compliance status</li> <li>• Inspection programs</li> <li>• Hazardous area studies</li> </ul>
<b>Control system reliability</b>	<ul style="list-style-type: none"> <li>• Reliability of power supply</li> <li>• Common mode failures</li> <li>• Safety Integrity Level assessment</li> </ul>

Through use of common sense and good engineering judgement, some detailed studies may readily be identified as being required prior to conducting any risk assessment activity. As some studies (asset integrity studies, hazardous area studies) can take time, it makes sense to identify the required studies and plan for them to be conducted as early as possible.

### 3.5. Organisation and personnel requirements

Risk assessment is normally and best performed by a team. There can be desk-top studies that are done by one person, however in this case a broader group of people will generally need to be available to inform the person undertaking the assessment. It should also be reviewed by appropriate people to validate it. The effectiveness of the risk assessment depends on the skills, knowledge and efforts of the people doing the work. The number of people involved and the range of experience should be determined by the size and complexity of the facility or operation being analysed.

The risk assessment should be carried out by people, or groups of people, who are skilled in the techniques involved and knowledgeable about the design, operation and maintenance of the facilities under

consideration or the activities to be undertaken. In order to capture the skills and knowledge typically required, the risk assessment team should:

- include all relevant work groups. Each work group will tend to bring a different experience base and perspective to the process;
- include a representative from operations who has a thorough and detailed knowledge of the facility or similar facilities;
- include a mix of scientific and engineering disciplines. Hazards not evident to individual work groups may be identified due to the interaction between the various disciplines;
- include a representative from maintenance who has a thorough and detailed knowledge of the facility, or similar facilities, and the maintenance history; and
- involve contractors and suppliers as necessary.

The involvement, from an early stage, of workforce representatives with 'hands-on' experience has been shown to be particularly beneficial. Operators should develop a role for the workforce in the risk assessment process that allows them to contribute, and gain an understanding of the hazards and controls present on the facility. Widespread awareness of these issues is essential for safe operation of the facility and is also an essential part of the workforce involvement requirements.



Further guidance is available in NOPSEMA guidance note:

***"Involving the workforce"***

It may be the case that an organisation does not have appropriate risk assessment skills in-house. If people outside of the operator's organisation are used to conduct risk assessment, it is essential that the facility operator manages and monitors the process, and understands the results. There is no value in commissioning a risk assessment from a contractor only to then file the results away on a shelf. Equally, there is no value in having someone carry out a 'generic' risk assessment that does not fully address the issues pertinent to the facility. In any case, operators have the ultimate responsibility for any risk assessment carried out for their facility and therefore are responsible for:

- setting the scope of the risk assessment; defining the elements to be included and the approach to be taken;
- providing the necessary supporting information, resources, inputs and members of the risk assessment teams;
- reviewing the outputs to ensure that details of the facility and its operation are appropriate; and
- making use of the results of the risk assessment to reduce risks to a level that is ALARP [OPGGS(S) subregulation 1.4(3)] and as part of continuous improvement [OPGGS(S) subregulation 1.4(2)(d)].

## 4. The risk assessment process

OPGGS(S) subregulation 2.5(2)(b) requires the risk assessment to consider the **likelihood** and **consequences** of each potential MAE, whilst OPGGS(S) subregulation 2.5(3)(d) requires the risk assessment to consider the **likelihood** and **nature** of injury or occupational illness. These aspects are considered in the following

sections. For offshore petroleum production facilities, guidance on tools and techniques for hazard identification and risk assessment can be found in ISO 17776.

## 4.1. Likelihood analysis

Risk assessment requires an estimate of the likelihood of the event occurring. For qualitative risk assessment this may simply require the selection of a category on a risk matrix. This selection is based on the experience and judgement of those conducting the assessment but can be justified, if necessary, with historical accident event data.

In more complex quantitative risk assessment the estimated frequency of an event occurring may be determined by using historical accident event or failure databases. Event tree analysis is often used to determine the likely probability of escalating events, such as fires or explosions, following an initiating event.

### 4.1.1. Likelihood estimation

To ensure consistency across a risk assessment, it is recommended that standard guidance material is developed for likelihood estimation. It is also suggested that risk matrix likelihood categories are assigned to quantitative frequencies (e.g. at least once per year, 1 in 10 years, 1 in 100 years, etc.) so they can be correlated with accident event history and failure databases. It can be very difficult and unreliable for persons to estimate very low frequency events.

Options to aid in the estimation of the likelihood of occurrence for extremely low frequency events include:

- stating the frequencies in terms of experience on the facility, within the company, within the industry, in all industries, etc.
- referring to industry guidance material or failure frequency databases; and
- use of fault trees to analyse the combination of contributing factors that may lead to a hazardous event. Fault trees are described in more detail in Appendix A.

The basis, including relevant references, for determining likelihood including all the assumptions that have been made should always be recorded. This helps ensure a robust analysis and will be beneficial for future reviews. Care must be taken that likelihood is determined on the basis of the hazard and not based on the reliability of the controls that are in place. Otherwise, the likelihood may be determined to be low due to an assumption that the control is very reliable when, in fact, it may not be.

## 4.2. Consequence analysis

When carrying out risk assessment with respect to MAEs, the assessment needs to evaluate the consequences of each MAE in terms of the severity as well as the magnitude of the MAE. It is important to consider both aspects.

- The severity of a MAE in the context of OPGGS(S) Regulations is an event connected with a facility having the potential to cause multiple fatalities.
- The magnitude of the MAE is the size or scale of the effect created by the major accident event, within which a number of fatalities could arise.

Assessment of the possible outcomes needs to include consideration of what may go wrong if measures to eliminate or prevent accident events are not present, are wrongly implemented, or fail to function as intended.

The risk assessment should consider escalation, i.e. the possibility of the event intensifying or accelerating or the possibility of one event triggering another, as well as considering the most likely events as this may affect the adequacy of control measures in place. Consideration of escalation is particularly important when assessing the adequacy of emergency response arrangements.

Whatever consequence analysis is conducted, it must be conducted to a level both sufficient for the estimation of risk and which is appropriate to the facility.

In the end, what is important is how the results from the consequence analysis are used to improve the operator's decision-making. For example, results from the consequence analysis could be used in influencing aspects of design, defining emergency response arrangements, and/or influencing operational procedures and controls.



*Further guidance is available in the NOPSEMA guidance note:*

***“Control measures and performance standards”***



*Further guidance is available in the NOPSEMA guidance note:*

***“Emergency planning”***

#### **4.2.1. Consequence estimation**

Consequence analysis assesses the severity of an accident event. Qualitative estimates of consequence tend to be based on accident event history and workforce experience. For qualitative risk evaluation this requires selecting a consequence category, for example on a risk matrix, such as “lost time injury”, “single fatality” or “multiple fatalities”.

Quantitative estimates of consequence are produced through consequence modelling. More detailed analysis of consequences can be achieved with complex computerised modelling techniques. Successful application requires that the models are used by personnel with adequate training and experience. Some examples of consequences that can be modelled include:

- pool fires
- jet fires
- confined and partially confined explosions
- flash fires
- toxic releases and their effects
- gas dispersion (flammable or toxic)
- dropped objects
- collision impact
- loss of structural stability

- loss of hull integrity
- helicopter ditching
- search and rescue

The results of consequence modelling can be used in conjunction with qualitative or semi-quantitative risk analysis to justify the consequence categories selected. In a QRA, consequence modelling is used in conjunction with event tree analysis to determine the risk of fatality or injury.

### 4.3. Nature of injury or illness

When carrying out risk assessment with respect to potential injury or occupational illness, the OPGGS(S) Regulations require that risk assessment considers the nature of injury or occupational illness as well as its likelihood of occurrence. 'Nature' in this context refers to the essential properties or characteristics of a particular type of injury or illness.

Assessing the nature of injuries or illnesses from hazardous events requires knowledge of what may go wrong at the facility (including process upsets, operator errors, external events, mechanical integrity failures, unwanted reactions, etc.) if measures to eliminate or prevent incidents are not present, are wrongly implemented, or fail to function as intended. It also requires knowledge of the whole range of possible outcomes, taking account of possible combinations of the success or failure of measures for reduction and mitigation of incidents. Depending on the different types of hazards and potential outcomes, the operator may need to employ a combination of techniques to develop a complete understanding.

Again, the assessment needs to evaluate the consequences of each hazardous event in terms of the magnitude (the potential number of personnel impacted) as well as the severity of the injury or illness, including fatal and non-fatal injuries.

### 4.4. Control measure assessment

Control measures are the means of reducing the risk associated with hazardous events. They eliminate, prevent, reduce or mitigate the hazards and/or consequences. The Hazard Identification process can assist in the identification of control measures. Control measures may also be identified during the risk assessment process.

Recording of existing and/or potential new control measures during the process of determining causes, likelihood, consequences, etc. should be done throughout the risk assessment process. It is essential to be explicit about what control measures are being included, and how they are considered to influence risk. There is also a need to be aware of the potential for control measures to experience common mode failures.

When conducting the risk assessment, careful consideration needs to be given to each control measure. For example, it is important to consider how reliable the control is and how effective it might be for particular situations (i.e. during an accident event).

The risk assessment process should provide the following in relation to control measures:

- identification or clarification of existing and potential control measure options;
- evaluation of control measure influence on risk;

- a basis for selection or rejection of control measures; and
- information useful to the setting of performance standards for control measures.

These will all be factors that will feed into an operators' demonstration within the safety case that the risks have been reduced to a level that is ALARP.

ISO 13702 provides guidance on control and mitigation of fires and explosions on offshore petroleum production facilities.



*Further guidance is available in NOPSEMA guidance note:*

***"ALARP"***

Regarding control measure performance standards, typical considerations that might arise from the risk assessment are:

- control measures associated with high risk hazards or MAEs may require rigorous performance standards; and
- the required reliability or number of control measures should reflect the risk of the corresponding MAEs or other hazardous events.

Through the risk assessment process operators should gain an understanding of which controls have the most influence on reducing risk. Those controls which have the most influence may need to be assessed in greater detail.



*Further guidance is available in NOPSEMA guidance note:*

***"Control measures and performance standards"***

With respect to the information to be included in the safety case, the OPGGS(S) Regulations require operators to provide a detailed description of the FSA [OPGGS(S) subregulation 2.5(2)]. This should be a description of the methodologies employed and a summary of the results, such as a list of the MAEs and the associated controls. The controls would generally be described in the facility description section of the safety case for hardware-related controls or the safety management system description section of the safety case for management system or procedure-related controls.



*Further guidance is available in NOPSEMA guidance note:*

***"Safety case content and level of detail"***

## 4.5. Determining and interpreting the risk results

After analysing the consequences and likelihood of a potential hazardous event, the risk can be determined.

The risk assessment process described in the safety case must show that the operator has considered each hazard with MAE potential, as well as the risk of each individual MAE. The risk associated with each MAE can then be assessed in the context of proposed additional control measures. Improvements (or further

controls) should always be considered and must be adopted or implemented if it is reasonably practicable to do so.

A means of satisfying the requirements of OPGGS(S) subregulation 2.11(1)(b) (see Section 1.4 of this guidance note) would be to determine risk levels for different areas of the facility and/or different worker groups according to the potential for exposure, so that the workforce are able to arrive at informed opinions about the risks and hazards to which they may be exposed at the facility. Facility operators may determine both the risk contribution from each individual MAE and the overall profile of risks from all of the identified MAEs. This will enable the operator and the workforce to gain an understanding of the most important risk contributors.

#### **4.5.1. Managing risk uncertainty and error**

Operators should clearly understand and describe the uncertainty present in their risk assessment. Uncertainty cannot always be eliminated, and it will be necessary to make assumptions in some areas. It should be noted that the reasons for uncertainty are different to the reasons for error however both will need to be managed. The presence of uncertainty and/or error can be due to any of the following reasons (refer to Wells, 1997):

- invalid assumptions made;
- incomplete hazard or consequence identification and analysis;
- inappropriate or inadequate models or methods used (e.g. model not within its validity range);
- incomplete, inadequate or irrelevant data used;
- absence of process or safety related information;
- out of date documentation or drawings;
- poor knowledge of changes in equipment or operations;
- limited understanding of the effectiveness, performance or even the identification of control measures;
- difference in opinion between members of the workforce regarding how a specific hazard or dangerous condition should be dealt with;
- lack of information on the underlying reasons for specific procedures, measures, training etc.; and
- lack of awareness of hazards, causes and the associated control measures.

In general, the uncertainty present is directly proportional to the assumptions made. The key to understanding the uncertainty and managing it, in the context of the safety case, is to:

- record any assumptions made and the basis for the assumptions;
- explicitly recognise where the main gaps or uncertainties exist; and
- seek to reduce the level of uncertainty by testing assumptions, conducting more detailed studies, etc. as required.

Where the level of uncertainty is high, sensitivity analysis should be considered to test the robustness of the risk assessment results against variations within the key areas of uncertainty.

#### 4.5.2. Providing evidence that risks are reduced to a level that is ALARP

The adopted control measures for any particular identified MAE must be shown to collectively eliminate, or reduce the risk to a level that is as low as is reasonably practicable (ALARP). This must be described in the detailed description of the formal safety assessment within the facility safety case.

The safety case must also contain a description of the SMS that provides evidence that the SMS arrangements (such as policies, procedures, etc.) with respect to hazard identification and risk assessment provide for risk reduction to a level that is ALARP.

There is no prescribed methodology for demonstrating that the necessary control measures have been identified to reduce risks to ALARP. However, risk assessment is integral to the process in order to establish the 'base case' and thereafter to assess the residual risk once control measures have been applied. By evaluating options for control measures within the risk assessment it should be possible to determine what additional benefit (if any) is gained from introducing additional and/or alternative control measures.

Risk assessment should consider a range of control measures, and provide a basis for the selection or rejection of control measures as appropriate to the nature of the facility and its hazards. It is important to explain the reason for selection or rejection of alternatives. The reasons for rejection or selection should be derived from the findings of the risk assessment, in particular findings regarding effectiveness and viability.

'Risk acceptance criteria' are the targets or standards some operators use to provide a basis for judging the risks that have been analysed, and for deciding the urgency or priority with which any identified hazard or risk should be addressed.

Operators may opt to use any criteria they determine appropriate in order to meet internal or company requirements. However, it is important to bear in mind that the OPGGS(S) regulatory requirements for a facility safety case encompass the requirement to reduce risk to a level that is ALARP.



*Further guidance is available in NOPSEMA guidance note:*

**"ALARP"**

## 5. Outputs

### 5.1. Risk assessment outputs

At the end of the risk assessment process the following information will be available for input into the formal safety assessment and the safety management system, as appropriate:

- an understanding of the factors that influence risk and the controls that are critical to reducing risk; and in particular, an understanding of the risk controls required to ensure adequacy of the design, construction, installation, maintenance or modification of the facility for the relevant stage or stages in the life of the facility for which the safety case has been submitted.
- the likelihood of potential MAEs and other hazardous events with potential to affect health and safety of people at or near the facility;
- the magnitude and severity of the range of possible consequences arising from identified hazards that could lead to MAEs;

- the magnitude and severity of the consequences arising from other hazardous events with potential to affect health and safety of people at or near the facility, including the nature of injury or occupational illness; and
- clear linkages between hazards, the associated consequences, likelihood and risk, and the associated control measures.

Facility operators should consider providing some examples in the safety case of the risk assessment process for a few specific MAEs, as this will help those reading it (both facility personnel and the NOPSEMA assessor) to understand the process taken and any linkages that are present.

## 5.2. Uses of risk assessment outcomes

Outputs of risk assessment can be used in the following ways:

- as an input to engineering design to ensure the appropriate level of performance is incorporated into engineered barriers, particularly at front end engineering and detailed design stages;
- to ensure that the workforce understand the hazards and risks associated with the facility, the control measures in place to manage these risks, and their role in the prevention of MAEs and other hazardous events;
- to provide evidence that risks are reduced to a level that is ALARP;
- to assist in the development of emergency response plans;
- to enable priorities and resource allocations to be based on appropriate information and assessment, resulting in a cost-effective improvement of risk;
- to assist in the improvement of procedures and management systems;
- as an input into 'training needs' analyses; and
- to assist with other processes such as management of change and accident and dangerous occurrence investigation.

## 5.3. Review and revision of risk assessment

Operators of facilities have an ongoing responsibility to understand and reduce risks to a level that is ALARP, including risks associated with proposed changes to the facility. The risk reduction involves learning from experience, including improved standards where industry expectations have changed or where new technology has become available, and looking for new ways to reduce risk.

OPGG(S) Regulation - SMS Ongoing Assessment Requirements	
Reg 2.5(3)	The safety case for the facility must also contain a detailed description of the safety management system that <i>[provides evidence that the safety management system]</i> : <ul style="list-style-type: none"> <li>(c) provides for the continual and systematic identification of hazards to health and safety of persons at or near the facility; and</li> <li>(d) provides for the continual and systematic assessment of:</li> </ul>

- (i) the likelihood of the occurrence, during normal or emergency situations, of injury or occupational illness associated with those hazards; and
- (ii) the likely nature of such injury or occupational illness; and
- (e) provides for the reduction to a level that is as low as reasonably practicable of risks to health and safety of persons at or near the facility including but not limited to:
  - (i) risks arising during evacuation, escape and rescue in case of emergency; and
  - (ii) risks arising from equipment and hardware.

The ongoing management and use of the information developed during hazard identification and risk assessment is of fundamental importance to ongoing risk reduction. Conditions on offshore facilities are dynamic, with changes in operating parameters often being reflected in changed operating procedures and equipment. Therefore, it is important to clearly state the range of conditions for which the hazard identification and risk assessment are valid, and that the criteria triggering the need for re-evaluation are defined.

As discussed in Section 3.2, risk assessment should be instigated by the safety management system, as required, in order to maintain a comprehensive and up-to-date understanding of risk as the facility or its activities changes.

The following points highlight some of the possible triggers for risk assessment review. Depending on their significance they also may trigger a safety case revision submission under OPGGS(S) Regulation 2.30:

- Further information has come to light that can help to refine the risk assessment. This particularly applies to areas of uncertainty in the previous risk assessment.
- Accident or near-miss investigation identifies further hazards or indicates the risk may be higher than previously thought. Safety alerts from other facilities and operators should be reviewed for their relevance to the facility in this respect.
- Where changes have occurred to the plant or equipment in terms of hardware or software since the safety case was submitted.
- Changes in the workforce could lead to changes in work practices or in knowledge of the facility, and hence can alter the level of risk. Additional control measures may be necessary.
- New hazards are identified.
- Industry developments have occurred with respect to technology, or systems of work that may be applied to reduce risk. Operators should bear in mind that the OPGGS(S) Regulations seek continuous improvement [OPGGS(S) subregulation 1.4(2)(d)].



*Further guidance is available in the NOPSEMA guidance note:*

***“Safety case lifecycle management”***

## 6. Quality assurance

At the completion of the risk assessment phase it is important that operators have a quality assurance process in place. The following table outlines the key activities and checks that should be undertaken to ensure quality in the risk assessment process.

*Table 3 – Key activities and checks for quality assurance*

Activity	Check
<b>Validate Hazards/Major Accident Events</b>	<p>Check accident event and near miss history on the facility.</p> <p>Check industry accident event history.</p>
<b>Validate Likelihood and Control Measures</b>	<p>Verify that control measures are as reliable as thought. Inspection records for equipment should be reviewed.</p> <p>Ask personnel who were not part of the risk assessment process to verify that assumptions make sense.</p> <p>Verify identified control system reliability versus industry data and maintenance records.</p> <p>Verify that procedural controls exist and contain guidance to address the specific hazard/cause in question.</p>
<b>Validate Consequence</b>	<p>If not already done, verify consequences by conducting consequence modelling.</p> <p>Check that inputs have been linked back to authoritative sources?</p>
<b>Risk Analysis</b>	<p>Ask personnel to provide an indication of which hazards they perceive to be most likely to cause each accident event. Compare this with the risk results.</p> <p>If not already done, conduct sensitivity analysis to test the robustness of the risk assessment results against variations within the key areas of uncertainty where the level of uncertainty is high</p> <p>Have an independent person not involved in the risk assessment read the output from the risk assessment. The person should review the risk assessment including the assumptions and ask:</p> <p>Do I agree with the basis for the risk evaluation?</p> <p>Does each assumption, and its basis, make sense? If assumptions do not make sense to the person, there is the possibility that they are poorly defined in the first place as well as being difficult for the reader to understand.</p>

## 7. Critical success factors for risk assessment

Some of the factors critical for success of risk assessment include:

- There is full understanding of the consequence and likelihood of all potential MAEs;
- The risk assessment should be rational and relevant to the facility. It should reflect the safety philosophy adopted for the facility;
- A fresh view should be taken of any existing knowledge, and personnel should not automatically assume that no new knowledge is required;
- The information is provided to persons who require it in order to work safely;

- An appropriate number of members of the workforce is actively involved in the risk assessment process and consultation with others occurs;
- Uncertainties are explicitly identified;
- All methods, results, assumptions and data are documented;
- Control measures and their effects on risk are explicitly addressed;
- Risk assessment outcomes are used as a basis for adoption of control measures, including improvements to the safety management system and emergency planning; and
- The risk assessment is regularly maintained and used as a 'live' document.

## 8. Common weaknesses

Although risk assessment is a potentially powerful tool, as with all tools, if it is not used with care and understanding, the outcomes may well be incorrect and this could lead to poor decisions being made that are not supportable in reality.

A report by the HSE in the UK (Good practice\* and pitfalls in risk assessment, 2003) examined a range of assessments and identified the following pitfalls:

- Carrying out a risk assessment to attempt to justify a decision that has already been made;
- Using a generic assessment when a site-specific assessment is needed;
- Carrying out a detailed quantified risk assessment without first considering whether any relevant good practice\* was applicable, or when relevant good practice\* exists;
- Carrying out a risk assessment using an inappropriate good practice\*;
- Only considering the risk from one activity;
- Dividing the time spent on the hazardous activity between several individuals - the 'salami slicing' approach to risk estimation;
- Not involving a team of people in the assessment or not including members of the workforce with practical knowledge of the process/activity being assessed;
- Ineffective use of consultants;
- Failure to identify all hazards associated with a particular activity;
- Failure to fully consider all possible outcomes;
- Inappropriate use of data;
- Inappropriate definition of a representative sample of events;
- Inappropriate use of risk criteria;
- No consideration of ALARP or further measures that could be taken;
- Inappropriate use of cost benefit analysis;
- Using 'Reverse ALARP' arguments (i.e. using cost benefit analysis to attempt to argue that it is acceptable to reduce existing safety standards);

- Not doing anything with the results of the assessment;
- Not linking hazards with risk controls; and
- Using JHA in place of risk assessment.

\***Note**– within the HSE and their ALARP guidance documentation, **good practice** is the term used for those standards for controlling risk which have been judged and recognised by HSE as satisfying the law when applied to a particular relevant case in an appropriate manner. This is not the case in Australia. NOPSEMA have not endorsed any ‘approved codes of practice’ or standards to allow them a special legal status. The term ‘good practice’ in NOPSEMA guidance documentation therefore is taken to refer to any well-defined and established standard practice adopted by an industrial/occupational sector, including ‘learnings’ from incidents that may not have filtered down into standards yet Good practice generally represents a preferred approach; however it is not the only approach that may be taken. While good practice informs, it neither constrains, nor substitutes for, the need for professional judgement. Good practice may change over time because of technical innovation, or because of increased knowledge and understanding.

## 9. References, acknowledgements and notes

*Offshore Petroleum and Greenhouse Gas Storage Act 2006*

Offshore Petroleum and Greenhouse Gas Storage (Safety) Regulations 2009

WorkSafe Victoria (2006) Major Hazard Facilities Regulations – Guidance Note GN -14 – Safety Assessment, MHD GN-14, Rev 1, February 2006

AS/NZS ISO 31000:2009 Australian/New Zealand Standard “Risk Management – Principles and Guidelines” (AS/NZS ISO 31000:2009)

ISO 17776 International Standard “Petroleum and natural gas industries – Offshore production installations – Guidelines on tools and techniques for hazard identification and risk assessment”

ISO 13702 International Standard “Petroleum and natural gas industries – Control and mitigation of fires and explosions on offshore production installations -- Requirements and guidelines”

IEC standard 61511, 2004 "Functional safety - Safety instrumented systems for the process industry sector". (IEC 16511:2004)

NORSOK Standard Z-013 “Risk and emergency preparedness analysis”, Rev 2, 2001-09-01

HSE Research Report 151 “Good practice and pitfalls in risk assessment” Prepared by the Health & Safety Laboratory for the Health and Safety Executive 2003

HSE Information sheet “Guidance on Risk Assessment for Offshore Installations” Offshore Information Sheet No 3/2006

Wells, G., *Hazard Identification and Risk Assessment*, Institution of Chemical Engineers, Rugby, 1997

Offshore Technology Report 2001/063 “*Marine Risk Assessment*”, prepared by Det Norske Veritas for the Health and Safety Executive

NOPSEMA would like to acknowledge WorkSafe Victoria for their assistance in the preparation of this guidance documentation.

For more information regarding this guidance note, contact the National Offshore Petroleum Safety and Environmental Management Authority (NOPSEMA):

Telephone: +61 (0)8 6188-8700, or

E-mail: [safetycaseguidance@nopsema.gov.au](mailto:safetycaseguidance@nopsema.gov.au)

Note: All regulatory references contained within this Guidance Note are from the Commonwealth *Offshore Petroleum and Greenhouse Gas Storage Act 2006* and the associated Commonwealth Offshore Petroleum and Greenhouse Gas Storage (Safety) Regulations 2009. For facilities located in designated coastal waters, please refer to the relevant State or Northern Territory legislation.

## Appendix A: Structures risk assessment techniques

This appendix is not intended to be a detailed or comprehensive description of risk assessment techniques. The methods and figures shown below are selected examples to illustrate different approaches; however, other approaches may be taken. There are many published references on this subject; operators are advised to review these. NOPSEMA does not promote any particular technique. The onus is on the operator to select methodologies and conduct a risk assessment or series of assessments appropriate to the facility.

### A.1: Risk matrix

A risk matrix is a common approach used for qualitative risk assessment. The risk matrix is used to assess individual accident events in terms of descriptive categories (e.g. “low”, “moderate”, “significant” or “high” risk) based on their expected consequences and likelihood. A basic risk matrix approach places each of the hazards considered into a region of the matrix. In the matrix shown in Fig A1, risks are classified in terms of low, moderate, or high risk as indicated by the shaded areas.

V (highest)					
IV					
III					
II					
I					
Frequency per year	A	B	C	D	E(highest)
	Consequence				

Figure A1 – Example Risk Matrix

The risk matrix can also be used in a semi-quantitative format by placing numbers in each box of the matrix. This can provide greater resolution in risk ranking. In the risk matrix example, a simple scoring system can be introduced to represent the combined result of likelihood and consequence. The risk score or risk index can be calculated by multiplying the numbers representing the likelihood rows and consequence columns. Note that these numbers increase with increasing likelihood and consequence.

Corporate risk matrices may need to be tailored to the requirements for assessing MAEs in order to segregate the risks into the categories. Corporate risk matrices will often result in all analyses involving death being located in the ‘high risk’ category due to a limitation in the number of frequency categories. Additional lower frequency categories are often needed.

If a risk matrix is chosen to assess the risk at the facility, care should be taken to ensure that it provides sufficient differentiation between risks. For simpler facilities, a risk matrix may provide sufficient differentiation.

## A.2: Fault and event trees

A fault tree may be used to provide an estimate of the likelihood of failure occurring. The starting point is the main event of interest (referred to as the top event) and the analyst works down in order to identify the sequences of events required to produce the top event. The technique is useful both for the quantification of likelihood and as a method for identifying which event sequences and hazards could lead to an MAE. It is also useful for identifying the major contributors to the likelihood of the top event. For example, it may be used to show how low-level failures, combined with external aspects such as a loss of power supply, operator error, etc. may combine to cause overall system failure. An example fault tree is shown in Figure A2.

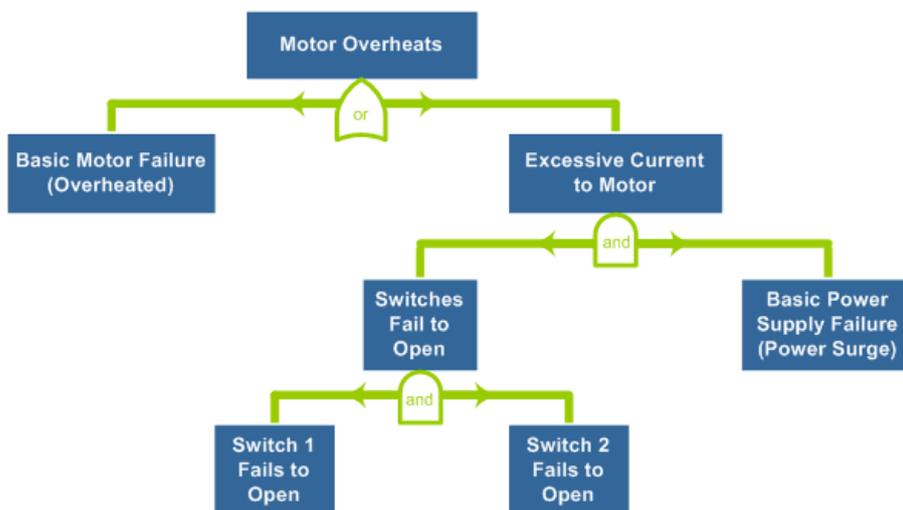


Figure A2 – Example Fault Tree

Similarly, an event tree can be used in the process of estimating likelihood. Event trees start with a single accident event (e.g. fire starts) and then fan out to the possible outcomes (e.g. fire detected and extinguished, fire undetected etc.). Any point in the event tree can be characterised by a particular consequence and an associated likelihood.

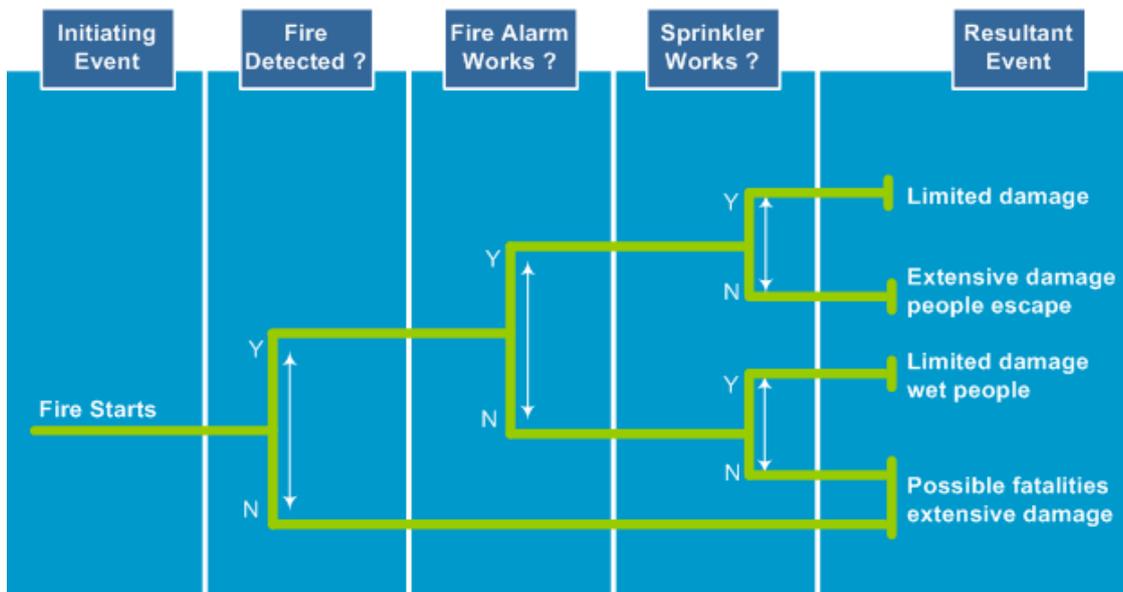


Figure A3 – Example Event Tree

The benefits of applying these techniques are that they provide:

- an in-depth analysis of the potential causal chains that result in the final outcomes;
- a clear demonstration as to the value of each control measure with respect to preventing or mitigating the accident event; and
- a reproducible and justifiable estimate of likelihood.

The use of these techniques is very time-consuming and should realistically only be applied to those hazardous events where a more formal method is required to analyse risk. Examples are accident events with high risk or where there is significant uncertainty as to the likelihood or the hazards which could lead to the accident event.

### A.3: Hazard and operability analysis (HAZOP)

In HAZOP analysis, an interdisciplinary team uses a systematic approach to identify hazards and operability problems occurring as a result of deviations from the intended range of process conditions. An experienced team leader systematically guides the team through the plant design, using a fixed set of “guide words” which are applied to specific “process parameters” at discrete locations or “study nodes” in the process system. The team analyses the effects of any deviations at that point in question and determines possible causes for the deviation, the consequences of the deviation and the safeguards in place to prevent the deviation. If causes and consequences are significant and the safeguards are inadequate, the details are recorded so that follow-up action can be taken.

HAZOP is not strictly speaking a risk assessment technique, but rather a hazard identification technique with some degree of qualitative risk assessment. The objective of the HAZOP study is to identify possible problem areas and to make recommendations as to how the particular problems may be resolved. It is therefore critically important that clear procedures and responsibilities are established to ensure the HAZOP recommendations are reviewed and action taken by the appropriate personnel.

## A.4: Quantitative or quantified risk assessment (QRA)

The application of quantitative methods is considered to be desirable when:

- several risk reduction options have been identified whose comparative effectiveness is not obvious;
- the exposure to the workforce is high, and reduction measures need to be evaluated;
- equipment spacing provides for significant risk of escalation;
- novel technology is involved resulting in a perceived high level of risk for which no historical data is available; and
- demonstration of relative risk levels and their causes is needed to make the workforce more aware of the risks.

A QRA seeks to:

- provide numerical estimates (for all hazards) of both consequences and their likelihood of occurrence based on historical data and computer simulations; and
- develop a quantified analysis of risk for the entire facility (generated using the cumulative effects of the individual hazards).

The analysis of risk incorporates the various effects from a range of applicable meteorological conditions, as well as from various hydrocarbon release conditions, types and sizes. It also allows for consideration of workforce distribution in the work area being considered and other areas of the facility. The output is typically in the form of individual risk of fatality contours.

A number of software tools are available to assist with some or all of the calculations that may be required in a QRA. The accuracy and usefulness of such tools depends heavily on the knowledge and skill of the user and the accuracy of the input data.

The results of a QRA can offer greater consistency, however there are a number of potential shortcomings:

- the output may be misleading if the selection of failure statistics is not well considered;
- there is a lower involvement of the workforce in the risk analysis;
- the industry data may not reflect how well, or poorly, the facility is managed; and
- on its own, it does not provide sufficient understanding of the full range of controls present on a facility.

A QRA is typically best suited to differentiating design, layout, location and engineering options. However, the application of QRA should not be limited to large, complex and expensive studies. It is a technique that can be used quickly and cheaply to help structure the solution to problems for which the solution is not immediately obvious. A sensitivity analysis may be necessary covering any assumptions made or data utilised during the analysis of the risk. This should illustrate the sensitivity of the results to changes in the data and assumptions, and identify any inputs that significantly affect the results. This analysis is an essential part of a QRA, as it ensures that the user fully understands the results of QRA and how they were developed.

## A.5: Layers of protection analysis (LOPA) and safety integrity levels (SIL)

LOPA is one of a number of techniques developed in response to a requirement within the process industry to be able to assess the adequacy of the layers of protection provided for an activity. The technique uses simplifying rules to evaluate initiating event frequency, independent layers of protection, and the impact of consequences to provide order of magnitude estimates of risk.

The LOPA process normally follows these steps:

- identify hazardous event – this includes both the hazard and outcome (consequence);
- identify the frequency of initiation;
- estimate the inherent likelihood of a fatality – this includes the level of exposure for an individual, the likelihood of ignition, etc.;
- identify the independent preventative layers of protection and the risk reduction factors that apply to each layer;
- identify the independent consequence mitigation layers of protection and the risk reduction factors that apply to each layer; and
- calculate the estimated likelihood of the consequence.

The results may be plotted on a risk matrix if required. This may assist members of the workforce to understand the calculated risk, especially if they are used to using risk matrices, e.g. for Job Safety Analysis (JSA). A further step that can be applied is to compare the estimated likelihood against a target likelihood (e.g. company risk acceptance criteria) which has been defined for each consequence category. Any difference may then be altered by the identification or implementation of additional control measures.

This process may be conducted using a quantitative approach that references initiation frequencies and control measure failure rate data. Alternatively, it may be conducted using an index approach where protection layer credits are applied to the risk reduction measure. These figures are indicative of the level of protection provided by a control. Benefits of this approach are:

- there is a rigorous assessment of likelihood;
- the effectiveness of control measures is explicitly shown;
- cumulative risk can easily be shown; and
- the technique helps define the level of performance required from additional or alternative control measures to meet all relevant criteria. These requirements can then be used as performance specifications when designing or purchasing new control measures.

Safety Integrity Level (SIL) determination for control measures is another aspect of LOPA. SIL application for process industries is well established; if instrumentation is to be effectively used for safety instrumented functions, it is essential that this instrumentation achieves certain minimum standards and performance levels. The objective is to establish a system design to lower the overall risk to a level that is ALARP. IEC standard 61511, 2004 provides further guidance and examples.