Supporting Safety Studies

Core concepts

- Requirements under the *Offshore Petroleum and Greenhouse Gas Storage (Safety) Regulations 2009* (OPGGS(S) Regulations) to which supporting safety studies may contribute include those related to hazard identification, risk assessment, adoption of control measures and emergency planning.
- There is a direct requirement in the OPGGS(S) Regulations for the safety case for a facility to include a detailed description of a fire and explosion risk analysis.
- There is a direct requirement in the OPGGS(S) Regulations for the safety case for a facility to include a detailed description of an evacuation, escape and rescue analysis.
- There is a direct requirement for the safety case for a facility to demonstrate that equipment required to function in an emergency is fit for its function or use in the emergency.
- The regulations require that the risks are reduced to a level that is as low as reasonably practicable (ALARP) and therefore the supporting safety studies should not simply assume that industry codes and standards are suitable by default.
- The demonstrations and evidence required to be in the safety case impose a requirement for transparent and auditable processes for all studies that support the safety case.
- The hierarchical approach of risk management should be followed; studies should not concentrate on mitigation measures alone.
- The results of the risk assessment carried out in supporting safety studies 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 ALARP.
- Operators should develop a role for the workforce in contributing to, and reviewing, supporting safety studies 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 the continual and systematic assessment of risk and improvement of the safety management system.
- The operator of a facility must provide a detailed description of the formal safety assessment, including the results of supporting safety studies, 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

1 Introduction 6
1.1 Intent and purpose of this guidance note 6
2 Supporting Safety Studies 8
2.1 History 8
2.2 Scope 8
2.3 The Aims and Outcomes of the FSA 9
2.4 Formal Safety Assessment 9
2.5 Features of a Supporting Safety Study 10
3 Fire and Explosion Risk Analysis (FERA) 11
3.1 Identification of Fires and Explosions 11
3.1.1 Stage 1: HAZID) 13
3.1.2 Stage 2: Understand the Hazard 14
3.2 Consider control measures 15
3.2.1 Inherent safety 16
3.2.2 Controls Pre-ignition 16
3.2.3 Controls Post-Ignition 17
3.3 Consider Evacuation, Escape and Rescue Analysis 18
3.3.1 Escalation 18
3.3.2 Smoke Impairment Analysis 18
3.3.3 Impairment of the Temporary Refuge via Smoke Ingress 19
3.3.4 Gas Impairment Analysis 20
3.3.5 Impairment of the Temporary Refuge via Gas Ingress 20
3.3.6 Toxic Gas Analysis 20
3.4 Demonstrating fire and explosions related risks have been reduced to a level that is ALARP 21
4 Evacuation, Escape and Rescue (EER) Analysis (EERA) 21
4.1 Identification of Emergencies 22
4.2 Consideration of evacuation routes 23
4.3 Consideration of procedures and equipment 23
4.4 Consideration of temporary refuge(s) 24
4.5 Consideration of life saving equipment 25
4.6 Demonstrating evacuation, escape and rescue risks have been reduced to ALARP 26
5 Survivability Studies 27
6 Other types of supporting studies 28
7 References, Acknowledgements & Notes 29

Abbreviations/Acronyms

ALARP	*As Low As Reasonably Practicable*
CFD	*Computational Fluid Dynamics*
EER	*Evacuation, Escape and Rescue*
EERA	*Evacuation, Escape and Rescue Analysis*
ESSA	*Emergency Systems Survivability Analysis*
FD	*Facility Description*
FERA	*Fire and Explosion Risk Analysis*
FMEA	*Failure Mode Effects Analysis*
FMECA	*Failure Mode Effects and Criticality Analysis*
FSA	*Formal Safety Assessment*
HAZID	*Hazard Identification*
HAZOP	*Hazard and Operability Study*
LEL	*Lower Explosive Limit*
MAE	*Major Accident Event*
NOPEMSA	*National Offshore Petroleum Safety and Environmental Authority*
OHS	*Occupational Health and Safety*
OPGGS(S)	*Offshore Petroleum and Greenhouse Gas Storage (Safety) Regulations 2009*
QRA	*Quantitative Risk Analysis*
SMS	*Safety Management System*
UEL	*Upper Explosive Limit*

Key Definitions for this Guidance Note

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

The definitions used for emergency response in this guidance note are from the ISO guidelines for emergency response (ISO 15544:2000(E)).

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.*
Escape	*The act of personnel moving away from a hazardous event to a place where its effects are reduced or removed (ISO 15544:2000(E) 2.1.14).*
Escape route	*A route leading to the place where people muster, or to an area from which people may leave the installation in an emergency (ISO 15544:2000(E) 2.1.15).*
Evacuation	*A planned method of leaving the installation in an emergency (ISO 15544:2000(E) 2.1.17).*
Evacuation, escape and rescue (EER)	*A range of possible actions in an emergency. Such actions may include escape, muster, refuge, evacuation, escape to the sea and rescue/recovery (ISO 15544:2000(E) 2.1.18).*
Evacuation route	*An escape route which leads from the muster area to the place(s) used for primary or secondary evacuation from the installation (ISO 15544:2000(E) 2.1.20).*
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 [OPGGS(S) 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 [OPGGS(S) 2.5(2)(a)], and the continual and systematic identification of hazards to health and safety of persons at or near the facility [OPGGS(S) 2.5(3)(c)].*
Major Accident Event	*A major accident event (MAE) 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 [OPGGS(S) 1.5].*

Muster	*The movement of people to a designated area so that the person in overall charge can account for all people and thereby facilitate subsequent emergency response actions (ISO 15544:2000(E) 2.1.28).*
Muster area	*A designated area to which personnel report when required to do so in an emergency (ISO 15544:2000(E) 2.1.29).*
Performance Standard	*A 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 [OPGGS(S) 1.5].*
Rescue	*The process by which those who have entered the sea directly or in survival craft/liferafts are retrieved to a place where medical assistance is available (ISO 15544:2000(E) 2.1.32).*
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 includes members of the workforce who are:* *(a) identifiable before the safety case is developed; and* *(b) working, or likely to be working, on the relevant facility.* *[OPGGS(S) 2.11(3)]*

1 Introduction

1.1 Intent and purpose 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 or Territory where powers have been conferred on NOPSEMA.

This guidance note, Supporting Safety Studies, 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 (FSA) and other occupational health and safety (OHS) risks in support of the evidence that risks are reduced to a level that is ALARP. The suite of guidance notes includes:

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

The guidance note will explain the requirements for supporting safety studies to be carried out as part of the FSA in support of a facility safety case. 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 National Offshore Safety and Environment Management Authority (NOPSEMA) safety case guidance notes overall, and their interrelated nature. This guidance note on *Supporting Safety Studies* 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.

2 Supporting Safety Studies

2.1 History

Piper Alpha was a United Kingdom North Sea oil production platform operated by Occidental Petroleum (Caledonia) Ltd. On the 6th of July 1988, an explosion and resulting fire occurred, which destroyed the facility and killed 167 men. Only 61 men survived the incident. The death toll includes two crewmen of a rescue vessel.

A large pool fire formed which engulfed the accommodation. Of the resulting fatalities, 109 of the 167 fatalities died as a result of inhaling smoke. 81 men perished in the accommodation and tests indicate that these men had very high levels of carbon monoxide in their blood. It was later found that the accommodation provisions were not smoke-proofed, and the lack of training caused people to repeatedly open and shut doors which worsened the problem. Conditions got so bad in the accommodations area that some people realised that the only way to survive would be to escape the installation [facility] immediately. They, however, found that all routes to lifeboats were blocked by smoke and flames. Escaping to sea via ladders or jumping were the only options left [[1]].

The Cullen Inquiry was set up in November 1988 to investigate the cause of the disaster. It was recognised that the inquiry would be a lengthy process; however preliminary findings revealed significant issues and these were published early, so that industry could learn from the unfortunate issues.

<u>Cullen 'Forthwith' Studies</u>

The Cullen report recommended that operators carry out four key studies 'forthwith' without waiting for the final report to be issued, or for legislative change to be completed. These included:

1. A fire risk analysis
2. As assessment of the risk of ingress of smoke or gas into the accommodation
3. A review of the ability of emergency systems to withstand severe accident conditions
4. An evacuation, escape and rescue package.

The findings from the Piper Alpha disaster shaped the development of offshore petroleum safety legislation in many countries, including Australia.

2.2 Scope

There are many types of supporting studies that can be carried out in support of a safety case, however a detailed description of both a fire and explosion risk analysis, and an evacuation, escape and rescue analysis are specifically required to be included in a safety case by the OPGGS(S) Regulations.

As noted in the OPGGS(S) Regulations in so far as both of these prescribed studies address MAEs, they form a part of the FSA.

1 Fire and Blast Information Group, http://www.fabig.com/Accidents/Piper+Alpha.htm

2.3 The Aims and Outcomes of the FSA

The aims of the FSA (including the supporting safety studies) 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 ALARP.
- To provide the specific information required by the regulations.

2.4 Formal Safety Assessment

OPGGS(S) – 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 FSA is focused on MAEs. Providing a well-considered, detailed description of a suitable and sufficient FSA 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;
- clear linkages between hazards, the MAEs, control measures and the associated consequences and risk;

For the purposes of a safety case submission, the HAZID and risk assessment need only relate to MAEs. However, it should be noted that the detailed description of the safety management system (SMS) in the safety case 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 HAZID and risk assessment studies to address other hazards not necessarily linked to MAEs e.g. noise, exposure to exhaust fumes, etc.

2.5 Features of a Supporting Safety Study

OPGGS(S) – FSA Risk Assessment Requirement	
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.

OPGGS(S) sub-regulation 2.5(2)(b) requires risk assessment, as part of the FSA, to be **detailed** 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.

Often FSAs and their supporting studies are discrete/separate documents, therefore they are likely to describe the process undertaken (i.e. how the team went about the task), who was involved etc., and they are likely to describe the physical equipment provided. Legislation is quite clear that a detailed description is what is required in the safety case. Therefore the analysis of the FSA and other supporting documents should be described in the safety case, and this should be a summary of the process that was followed including the main findings, rather than the document itself.

Duplication of information should be avoided, and equipment descriptions (for example) should be summarised in the facility description (FD) section.

Operators should not simply include copies of these analyses within the safety case, but rather should provide a detailed description of theses analyses, including key outcomes and linkages to other sections of the safety case e.g. facility description and SMS description (SMSD).

3 Fire and Explosion Risk Analysis (FERA)

Content Requirement	
Reg 2.17(1)	The safety case for a facility must contain a detailed description of a fire and explosion analysis.

The Macquarie dictionary defines 'analysis' as *a method of studying the nature of a thing or of determining its essential features*. Therefore a fire and explosion risk analysis should be the process of studying the potential for fires and explosions on a facility, and this process should fully explore the 'nature' and 'essential features' of these fires and explosions. As the FERA forms part of the FSA, the description should focus on potential 'MAEs'.

The content and level of detail of the detailed description of the FERA in the safety case needs to be adequate for NOPSEMA to gain an appreciation of the scope and process for undertaking the FERA including sources of data and rationale for excluding or discounting items from consideration.

The control measures identified in the FERA must be clearly described in the FD or SMSD of the safety case as appropriate.

The intent of this guidance is to describe what is considered to be the 'nature' and 'essential features' of fires and explosions, and includes guidance on identifying the potential sources of fires and explosions and their likely outcomes.

The legislation goes on to provide further details as to what should be included in the analysis as follows.

3.1 Identification of Fires and Explosions

Level of Detail Requirement	
Reg 2.17(2)	The fire and explosion risk analysis must: (a) identify the types of fires and explosions that could occur at the facility.

The legislation requirement can be interpreted as a detailed, risk-based, fire and explosion analysis. There is a wide range of fire and explosion related events that could occur on a facility, and the safety case should describe those hazards that could have the potential to cause a major accident event. The content and level of detail needs to be adequate for NOPSEMA to gain an appreciation that the information provided meets the intent of the legislation.

A variety of fires and explosions may be experienced, including (but not limited to) those shown in Table 1 below.

Table 1 – Types of Fires and Explosions

	Fires	Explosions
Process Hydrocarbon	• Blowouts • Jet fires • Two phase fires • Pool fires • Fire balls • Flash fires • Compartment fires • Cargo tank fires • Sea fires • Loading/offloading	• Ignited Blowouts (e.g. moonpool) • BLEVEs • Confined explosions • Semi -confined explosions • Unconfined explosions • Atomised sprays/mists
Non Process Hydrocarbon	• Engine room/machinery room/pump room/workshops/storeroom room • Lube oil • Diesel/ fuel oil • Paints • Heli-fuel • Bottled gas • Solvents	
Non hydrocarbon	• Accommodation fires • Laundry room • Galley • Electrical equipment (e.g. circuit boards, switchgear room etc.) • Paints • Inhibitors • Cables • Cellulosic • Explosives • Batteries	

Considering the Macquarie Dictionary definition, the safety cases should describe the essential features of the assessment of fires and explosions applicable to the facility. Due to the nature of the industry, the fire and explosion analysis should primarily be focused on hydrocarbon fires; however other types of fire also have the potential to escalate into MAEs. The types and fires expected on a facility vary according to several parameters , therefore a risk assessment process is required to enable a comprehensive and systematic assessment to be undertaken which prioritises those events that could cause a major accident hazard.

Further guidance is available in the NOPSEMA guidance note:
"Risk Assessment"

When assessing fires and explosions a range of issues should be considered, and the following staged process may allow for the appropriate prioritisation of risks.

3.1.1 Stage 1: HAZID)

The FERA should identify the ways (credible and foreseeable) in which fires and explosions could occur for all areas of operation including commissioning, operation, shutdown, maintenance and decommissioning, as relevant to the safety case to be submitted.

The FERA should allow for the identification of those hazards that could lead to a fire or explosion. These hazards can then be screened to identify those hazards that have the potential to cause a major accident event.

Things to consider include:

Considerations	Tools/Equipment
• What is the fuel? e.g. composition. • How stable is the fuel? • How can it be released? e.g. impacts, corrosion; maintenance activities, construction defect; operator error, exceeding design conditions, etc. • What type? Immediate or delayed ignition - fire/explosion? Pool fire/confined explosion etc. • Can the event escalate? • etc.	• Plot plans • Plant layouts • Process Flow Diagrams (PFDs) • Process and Instrument Diagrams (P&IDs) • Cause and Effect Diagrams • Platform walk around; • Process data sheets • MSDS • etc.

There are a variety of ways to identify those hazards that could lead to a fire or explosion. For example;

- Checklist Analysis
- Brainstorming
- What-If Analysis
- Hazard and Operability Analysis (HAZOP)
- Failure Modes and Effects Analysis (FMEA)
- Failure Mode Effects and Criticality Analysis (FMECA)
- etc.

Further guidance is available in the NOPSEMA guidance note:
"Hazard Identification"

Some of the practical factors for success of hazard identification include:

- Appropriate members of the workforce have been actively involved in the hazard identification process and others have been given the opportunity to provide input.
- The operator has conducted early planning on how to link the various aspects of the safety case to provide information to the FSA process in a timely manner.
- The hazard identification processes chosen are appropriate to the facility and the operator is able to justify why particular hazard identification processes have been chosen.
- Any hazard identification technique selected is systematic and structured, fosters creative thinking about possible hazards that have not previously been experienced, and has included consideration of which approach will extract the maximum quantity of useful information.
- The operator has considered the scope of hazard identification studies in to ensure that of the hazards identified those with the potential to cause an MAE are clearly identified.

- The operator has based the hazard identification process on a comprehensive and accurate description of the facility, including all necessary drawings, process information, existing conditions, modifications, procedures and work instructions, hazardous materials information, etc.
- The operator has not screened out hazards simply because they have a very low likelihood.
- The hazard identification process has included involvement and/or input from designers, manufacturers, contractors and suppliers, where appropriate, as well as members of the workforce.
- Assumptions and uncertainties are explicitly identified and recorded so that these can be verified or analysed later.
- The hazard identification has produced sufficient documented records which list at least all potential major accident events and hazards along with the underlying causes, control measures and any assumptions.
- The hazard identification documentation has recorded properly worded "SMART" actions (specific, measurable, attainable, realistic and timely) that can be managed and closed out in an auditable manner.
- The operator can justify why certain control measures have been adopted while others have been rejected.
- Once the hazard identification workshop(s) have been completed, the operator conducts a review on the information gathered.

3.1.2 Stage 2: Understand the Hazard

This is a fundamental part of the process to demonstrate that the nature of fires and explosion and their essential features/characteristics are understood, so that the outcomes can be managed appropriately. This will allow the operator to fully comprehend the different fire and explosion scenario applicable to their facility.

For example, process conditions will determine the nature of a process fire and/or explosion, therefore the differences in process conditions should be understood. Determining these differences will help prioritise risks.

Things to consider include (but are not limited to):

Considerations	Tools/Equipment
• Leak frequency from systems/components • Inventory volume (isolated/not isolated) • Ignition potential of hydrocarbon/flash point (e.g. density, temperature, flammability) • Release frequency/size/duration • Direction of event • Ignition probability • Flame effects (emissivity/surface extent/dimensions/radiation levels/fuel or ventilation controlled/smoke • Overpressures expected (congestion/enclosed vs open areas) • Toxicity	• Qualitative Risk Assessment • Quantitative Risk Assessment (QRA) • Smoke Ingress Analysis • Gas Ingress Analysis • Escalation Analysis • Temporary Refuge Impairment Analysis

Many of these factors are often determined using technical modelling methods including computational fluid dynamics (CFD) techniques. Various modelling techniques are available and can be categorised as:

- Discharge modelling - typically determines:
    - The release rate depending on various parameters (e.g. phase of release [gas, liquid, two phase], hole size, volume, etc.).

    - The likely dispersion effects (e.g. gas dispersion, liquid release characteristics, etc.)
- Consequence modelling –
    - Fire modelling to determine whether a jet fire, flash fire or pool fire will be created.
    - Explosion modelling to determine the type of explosion: (confined; semi-confined; external).
- Impact assessment, e.g.
    - Impairment criteria for equipment, e.g.
        - Direct flame impingement of an "A"-rated firewall will be penetrated after 15 minutes.
        - Direct flame impingement of an "H"-rated firewall will be penetrated after 60 minutes.
    - Impairment criteria for personnel, e.g.:
        - Thermal radiation of 6.3 kW/m^2 – personnel exposed for 1 minute are very likely to be able to egress from the area to other areas/evacuation routes.
        - Thermal radiation of 12.6 kW/m^2 – personnel may escape, but only in the first few seconds. The pain threshold is likely to be reached within 4 seconds, and there is a 50% chance of death after 80 seconds.
        - Thermal radiation of 37.5 kW/m^2 – pain threshold is instantaneous, and there is a 50% chance of death after 20 seconds.

Important factors for "understanding the hazard" include:

- Document assumptions - In determining the nature or extent of possible fire/explosion, assumptions are often made e.g. in fire modelling. It is important to document these assumptions so that the basis for the results is known, and an analysis can be performed to ensure they are appropriate for the facility (i.e. justifiable).
- Document any source material for any information used.
- Use appropriate data - appropriate to the type, standard/design, use and operating conditions of the equipment.
- Effective use of workforce involvement as a "reality check" of input assumptions, modelling results and process conditions.

3.2 Consider control measures

Level of Detail Requirement	
Reg 2.17(2)	The fire and explosion risk analysis must: b) consider a range of measures for detecting those fires and explosions in the event that they do occur; and (c) consider a range of measures for eliminating those potential fires and explosions, or for otherwise reducing the risk arising from fires and explosions; and (d) consider the incorporation into the facility of both automatic and manual systems for the detection, control and extinguishment of: (i) outbreaks of fire; and (ii) leaks or escapes of petroleum; and (e) consider a range of means of isolating and safely storing hazardous substances, such as fuel, explosives and chemicals that are used or stored at the facility.

Note that this sub-regulation specifies that a range of measures must be considered for:

- Detecting fires and explosions;
- Eliminating or otherwise reducing the risks of fires and explosions; and
- Detection, control and extinguishment of fires and petroleum and gas leaks or escapes.

It is not sufficient to only consider one or two control measures. Range means an array of choice, variety, and assortment. Operators are encouraged by the regulations to examine multiple possible options for mitigation and control – it is not enough to simply adopt the same solution that was employed the last time around; operators need to review what is most appropriate under current particular circumstances.

The guidance note for 'Control measures and Performance Standards' describes how the hierarchy of controls is used to address a preferential order when considering/selecting controls to manage risks. The hierarchy of control measures typically includes elimination and prevention controls over reduction and mitigation controls. Applying a hierarchy of control measures involves for example designing out or removing hazards at the source and then controlling any residual risks by other control measures.

Further guidance is available in the NOPSEMA guidance note:
"Control Measures and Performance Standards"

3.2.1 Inherent safety

This is the process of hazard management that considers ways *to avoid or eliminate hazards or reduce their magnitude, severity or likelihood of occurrence.*

The greatest opportunity to eliminate hazard is at the design stage for new facilities, but it can it can easily be applied to projects where (e.g.) new production equipment is being added.

One example of considering inherent safety is via constructive questioning, for example:

- Why so much inventory? Can inventory be minimised?
- How can it be made simpler?
- How can systems be segregated?
- Can the process pressure/temperature be reduced?
- Can the material be substituted with a less flammable material?
- Can the amount of human involvement be minimised?
- Is it too complex/too simple (with respect to human intervention)?
- etc.

Whilst codes and standards are often used to design process systems, it is quite clear that just meeting these design codes does not necessarily mean that risks are reduced ALARP.

Further guidance is available in the NOPSEMA guidance note:
"ALARP"

3.2.2 Controls Pre-ignition

To generate a fire or explosion, ignition needs to occur. There are however, precursors to fires/explosions that can be identified and these should be considered in the FERA. Typical fire and explosion precursors include:

- Leakage of combustible fluids
- Ignition sources
- Accumulations of combustible/explosive fluids

Control measures associated with these precursors include:

- Leak prevention via equipment integrity (e.g. welded joints, corrosion monitoring; appropriate material selection)
- Leak detection

- Segregation of systems
- Ignition control (rated (e.g. EX) equipment/management of open flames/hot surfaces and rotating equipment/welding/cutting/sparks (e.g. violent failure of equipment)/ static electricity
- Procedural controls - e.g. trained staff
- Minimise dead areas/ confined spaces around process plant
- Gas detection (lower explosive limit (LEL)/upper explosive limit (UEL)
- HVAC/Ventilation
- Likely gas dispersion patterns e.g. into TR or other critical control areas
- Procedural controls - e.g. trained staff.

The actions to be taken once precursor(s) to a potential fire or explosion have been realised should also be considered. For example:

- Effects of unignited releases
  - e.g. narcotic/asphyxiate effects of unignited releases
  - potential for gas to migrate into other areas e.g. via HVAC into Temporary Refuge
- Isolation/ESD systems in place once a leak is detected
- Blowdown/pressure relief on confirmed HLG and corresponding hazards associated with the flare
- Deluge on high level gas (HLG)
- Process alarms to alert personnel of the fire/explosion
- Release containment e.g. drains/ bunds
- Expected personnel reactions to process alarms – e.g. manual intervention/firefighting; muster in TR; immediate evacuation.

The control measures should be considered for their suitability to control the event, and any limitations should be recognised such that other control measures can be considered.

The intended function of control measures identified in the FERA as being controls for MAEs must be clearly described in the formal safety assessment description within the safety case. The detail of the adopted controls must be described in the FD section or in the SMS description in the safety case as appropriate. For MAE controls, the regulations require that the SMS specifies the performance standards that apply.

Further guidance is available in the NOPSEMA guidance note:
"Control Measures and Performance Standards"

3.2.3 Controls Post-Ignition

There are various controls measures available to identify and manage the products of a fire an explosion, and the FERA should describe these systems. Examples include:

- Confirmed smoke detection
- Confirmed heat detection
- Smoke dispersion
- How it affects evacuation e.g. time to incapacitate personnel? Visibility of escape routes?
- Into TR or other critical control areas
- Emergency Shutdown System (for 'leaking' system; ESD of other inventories)
- Blowdown (for 'leaking' system; of other inventories)
- Fire protection systems
- Active (deluge, sprinklers/portable firefighting)

- Passive
- Purging with inert gas
- Venting of confined spaces
- Hydrocarbon management e.g. drains/bunds
- etc.

The actions to be taken a fire or explosion is realised should also be considered. For example:

- Process alarms to alert personnel of the fire/explosion.
- Expected personnel reactions once fire/explosion has occurred e.g. evacuation requirements.

The consequences should a fire and/or explosion occur should also be considered including the immediate impact of fire/explosions on personnel within area, as well as the potential for escalation (refer to section 3.3.1), and survivability of the systems (refer to section 5).

Estimates of, or assumptions made about, the availability, reliability and response time of protective systems (including any human components thereof) should be realistic and adequately justified.

3.3 Consider Evacuation, Escape and Rescue Analysis

Level of Detail Requirement	
Reg 2.17(2)	The fire and explosion risk analysis must: (f) consider the evacuation, escape and rescue analysis, in so far as it relates to fires and explosions.

3.3.1 Escalation

There are a variety of ways in which fires and explosions can escalate or develop further, and the FERA should examine these in sufficient detail to allow an appreciation of the risks such that they can be managed. Examples include:

- Prolonged smoke dispersion can impair evacuation routes and can ingress or migrate to critical areas including the TR (e.g. via TR HVAC system)
- BLEVEs may occur resulting in knock-on effects and potentially further explosions
- Escalation to other hydrocarbon inventories may occur. An explosion is likely to cause small bore pipework to be displaced and rupture. The FERA should consider the impact on other adjacent hydrocarbon equipment and safety critical systems
- Impairment of adjacent walls or other structural components may occur under certain loads, therefore these need to be assessed with respect to firewalls and other critical structural components
- Hydrocarbon management by means of drains and bunds to limit inventory and contain pool fires
- The likelihood that the Temporary Refuge or evacuation systems become unavailable within their required endurance times should be examined
- etc.

3.3.2 Smoke Impairment Analysis

The findings from the Piper Alpha disaster highlighted the importance of understanding the effects of smoke from fires and explosions. Smoke usually consists of three elements as follows:

- Combustion gases – the gases are dependent on the material composition but generally could include carbon dioxide, carbon monoxide, nitrogen, and water vapour. Understanding the concentration of these components is important due to their impact on personnel.
- Soot - solid carbon particles, entrained in the combustion gases.
- The smoke filled area is deficient in oxygen.

The main consequences form smoke production includes:

- Combustion gases are toxic to personnel – both carbon monoxide (CO) and carbon dioxide (CO2) can impair the performance of personnel.
- Carbon monoxide (CO) combines with haemoglobin in the blood which reduces the delivery of oxygen to body tissues. Examples of the effects of excessive CO include:
  - 1500 ppm - headache after 15 minutes, collapse after 30 minutes, death after 1 hour
  - 12800 ppm - immediate effect, unconscious after 2 to 3 breaths, danger of death in 1 to 3 minutes
- Carbon dioxide (CO2) can stimulate the respiration rate (hyperventilation) and high volumes cause confusion, for example:
  - 65000 ppm – dizziness and confusion after 15 minutes exposure
  - 200000 ppm – unconsciousness in less than 1 minute
  - Often personnel become unconscious from the gas (narcosis - where the gas has affected the nervous and cardio-vascular system) and then they asphyxiate (due to the lack of oxygen).
- Soot impairs visibility – therefore access to evacuation routes may become impaired.
- Oxygen depletion can cause hypoxia (deprivation of oxygen). Ambient air comprises 21% oxygen. Reducing the oxygen content to 17% can cause the respiration rate to increase, reduces muscular coordination and attention/thinking process need more effort. If the oxygen content were to reduce to 6% or below, death is expected after 6 to 8 minutes [6].

A smoke impairment study will inform the operator on factors that will influence the risk and this information then needs to be used in helping to identify control measures to manage the risk.

The smoke study should consider the hazards to personnel both at the time of the fire/explosion, and for a pre-determined time after ignition of the event. An assessment should be undertaken to establish the expected behaviours for personnel for these events, including their ultimate destination should these events occur.

3.3.3 Impairment of the Temporary Refuge via Smoke Ingress

The Smoke Impairment Analysis should:

- Understand how smoke impairment can cause an MAE
- Identify and evaluate potential scenarios for smoke ingress
- Consider the design of the TR and other congregation areas (e.g. muster areas) and the expected response to smoke ingress.

> ***Example – Smoke Ingress***
>
> *Smoke ingress is likely to occur if the pressure outside the TR is greater than inside. Air pressure can be affected by (for example):*
>
> - *Wind effects*
> - *Chimney/stack effect (hot air rises)*

- Assess the leakage rate/seepage of the TR through doors, windows, openings, HVAC dampers etc.
- Evaluate those control measures required to ensure risks are reduced ALARP.

> ***Example – HVAC shutdown***
>
> *HVAC shutdown on confirmed gas detection, consider – consider the actual time it takes to close the damper etc.*

Therefore these elements need to be considered in the FERA so that their associated risks can be reduced ALARP.

3.3.4 Gas Impairment Analysis

Hydrocarbon releases if not ignited can present a significant hazard. The main consequences of un-ignited gas include:

- They are hazardous to health and can impair personnel performance – as with the combustion gases from smoke, personal may, very quickly depending on the composition of gas, cause unconsciousness (via narcosis) before they asphyxiate.
- Gas volumes may migrate to other areas, for example, where, for example, electrically rated equipment is less controlled, therefore causing an explosion.

A gas impairment study will inform the operator on factors that will influence the risk and this information then needs to be used in helping to identify control measures to manage the risk.

The gas study should consider the hazards to personnel both at the time of the release, and for a pre-determined time after the initial release. An assessment should be undertaken to establish the expected behaviours for personnel for these events, including their ultimate destination should these events occur

3.3.5 Impairment of the Temporary Refuge via Gas Ingress

The Gas Impairment Analysis should:

- Understand how gas impairment can cause an MAE
- Identify and evaluate potential scenarios for gas ingress
- Consider the design of the TR and other congregation areas (e.g. muster areas) and the expected response to gas ingress.
- Assess the leakage rate/ seepage of the TR through doors, windows, openings, HVAC dampers, etc.
- Evaluate those safety systems required to ensure risks are reduced ALARP.

3.3.6 Toxic Gas Analysis

Other than combustion gases from fires, facilities may be exposed to the release of Hydrogen Sulphide (H_2S). The following is extracted from the UK HSE's Offshore Information Sheet No. 6/2009:

The gas is toxic in relatively low concentrations and the risks to the workforce need to be addressed as soon as its' presence becomes known. Hydrogen sulphide is considered a broad-spectrum poison, meaning that it can poison several different systems in the body, although the nervous system and respiratory systems are most affected. Besides being highly toxic H_2S is a flammable gas. It is heavier than air and hence tends to accumulate in low-lying areas. It is pungent but rapidly destroys the sense of smell.

Production of liquid and gaseous hydrocarbons containing hydrogen sulphide in significant amounts can be hazardous to people. H_2S in hydrocarbon fluids has the potential to form sulphur dioxide (SO2) via combustion. Flaring hydrocarbon gas containing measurable quantities of H_2S needs to be managed to ensure the SO2 produced does not present a toxic hazard. Combinations of H_2S, SO2 and hydrocarbon gaseous mixtures also need to be considered in terms of their accumulated toxic load.

3.4 Demonstrating fire and explosions related risks have been reduced to a level that is ALARP

Level of Detail Requirement	
Reg 2.17(2)	The fire and explosion risk analysis must: (g) identify, as a result of the above considerations, the technical and other control measures necessary to reduce the risks associated with fires and explosions to a level that is as low as reasonably practicable.

The ultimate goal of the safety case is to improve the safety at the facility and to demonstrate that risks have been reduced to a level that is as low as reasonably practicable. The adopted control measures for any particular identified MAE must be shown to reduce the risks associated with fires and explosions to a level that is ALARP, i.e. that the cost to implement further control measures is grossly disproportionate to the risk reduction they would provide.

Depending on the circumstances, the approach employed in providing the required evidence of ALARP may include:

- comparison with standards, codes and industry practices;
- analysis of the risks, and of the benefits and costs of alternative/additional control measures;
- assessment of the appropriateness of control measures and their performance standards;
- comparison with benchmarks for risk and for management performance;
- comparison with good practice management system frameworks; and
- demonstration of past and planned improvements.

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

There is no prescribed methodology for demonstrating that the necessary control measures have been identified to reduce risks to ALARP, however in any case, 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 and make the argument for why further risk reduction is not practicable.

Further guidance is available in the NOPSEMA guidance note:
"ALARP"

4 Evacuation, Escape and Rescue (EER) Analysis (EERA)

Content Requirement	
Reg 2.16(1)	**The safety case for a facility must contain a detailed description** of an evacuation, escape and rescue analysis.

In a similar way to the fire and explosion risk analysis the evacuation, escape and rescue analysis should be the process of studying the potential for evacuation, escape and rescue associated with a facility, and this process should fully explore the 'nature' and 'essential features' of such evacuation, escape and rescue. As the EERA forms part of the FSA, the description should focus on potential MAEs.

The content and level of detail of the detailed description of the EERA in the safety case needs to be adequate for NOPSEMA to gain an appreciation of the scope and process for undertaking the EERA including sources of data and rationale for excluding or discounting items from consideration.

The control measures identified in the EERA must be clearly described in the FD or SMSD of the safety case as appropriate.

The intent of this guidance is to describe what is considered to be the 'nature' and 'essential features' of evacuation, escape and rescue analysis.

The EER arrangements should be appropriate for the protection of personnel on the facility for the expected MAEs in that they facilitate effective evacuation, escape or rescue, to a place of safety. Things to consider include:

- Provision of suitable and sufficient equipment to ensure successful ERR when required, and as a minimum, for all MAEs; and
- As evacuation and escape are two different activities, there should be clear distinction between means of evacuation and means of escape.

Example – Means of Evacuation and Escape
The primary mean of 'evacuation' is via a helicopter. The secondary means of evacuation is via the lifeboats. The equipment used for escape includes ladders, knotted ropes, etc.

Note that as with the FERA a number of the EERA sub-regulations specify that a range of items must be considered for evacuation and escape of persons at the facility. Range means an array of choice, variety, and assortment. Operators are encouraged by the regulations to examine multiple possible options need to review what is most appropriate for the facility and the range of emergencies identified.

The legislation goes on to provide further details as to what should be included in the analysis as follows.

4.1 Identification of Emergencies

It is important that the description in the safety case provides enough information to provide assurance to NOPSEMA that all the requirements of the analysis as given in OPGGS(S) Reg 2.16(2) have been met. The information must be appropriate to the facility and the activities to be conducted at the facility, and address all potential major accidents.

Level of Detail Requirement	
Reg 2.16(2)	The evacuation, escape and rescue analysis must: (a) identify the types of emergency that could arise at the facility.

The content and level of detail needs to be adequate to gain an appreciation of the extent to which the study is aligned and consistent with the HAZID outputs.

The FSA, including the FERA should provide sufficient detail of the MAEs to identify the types of emergencies for a facility. Examples include:

- hydrocarbon release resulting in fire/explosion
- oil spill
- helicopter incidents
- loss of well control
- ship collision
- adverse weather
- loss of ballast control, stability and station keeping
- subsea hydrocarbon releases, for example: pipelines or flowlines
- diving emergencies
- confined space emergencies
- toxic release

4.2 Consideration of evacuation routes

Level of Detail Requirement	
Reg 2.16(2)	The evacuation, escape and rescue analysis must: (b) consider a range of routes for evacuation and escape of persons at the facility in the event of an emergency; and (c) consider alternative routes for evacuation and escape if a primary route is not freely passable.

Considerations for routes for evacuation and escape include:

- appropriateness for the environment they need to function within
- Location of temporary refuges and means of evacuation and escape
- impact MAEs may have:
    - Can the evacuation routes withstand the effects of fire/smoke/gas/heat/impact?

Example – Impairment criteria for evacuation/escape routes

- *Heat flux exceeds 4 kW/m2*
- *Visibility – less than 5m for those routes involving staircases, 2m for others*
- *H2S concentrations – exceeding 15 ppm*

    - What happens if the evacuation route is impaired?
    - What happens if people become injured?
- Distribution of personnel in a range of conditions

4.3 Consideration of procedures and equipment

Level of Detail Requirement	
Reg 2.16(2)	The evacuation, escape and rescue analysis must: (d) consider different possible procedures for managing evacuation, escape and rescue in the event of an emergency; and (e) consider a range of means of, and equipment for, evacuation, escape and rescue.

Effective planning and communication is vital in an emergency. Consideration of a range of procedures for managing EER should include:

- Consideration of the time required for evacuation and rescue and provide appropriate provisions accordingly, for example:
    - Time to muster
    - Time for helicopters to arrive/ land/ take-off
    - Time to load/ embark lifeboats/ life rafts
    - Time to descend the Lifeboat
    - Time to recover personnel from lifeboats
    - How personnel are recovered from lifeboats
    - Time to recover personnel from water
    - How to recover personnel from water
    - Time to survive if in water

    - etc.
- Consideration of the command structures to handle emergencies. This includes
    - Considering the roles and responsibilities of all key personnel involved in emergency response:
        - Who is in command during an incident? What are their required tasks?
        - How is communication between the different parties managed?
        - The minimum number of persons required for key roles (e.g. the emergency response team).
        - Who is responsible for maintaining EER equipment?
        - etc.
    - Any interface arrangements with for example, onshore and other support agencies (e.g. maritime agencies).
- Noting that whilst there is legislative provision for communication within the TR (see 4.4 below), to ensure effective evacuation, consideration should be given to how information is communicated to all populated areas on a facility more generally.
- Consideration of the actions to be taken in the event of an MAE. For example:
    - the operator may wish to monitor (for example) a fire, and may choose to have non–essential personnel muster in the TR before attempting a platform evacuation.
    - The helideck may be unavailable due to the effects of fire or explosion.
    - The facility should be clear of the actions required for all potential MAEs.
- Consideration of emergency policies and procedures in place to support EER activities including those to:
    - account for all personnel during an emergency.
    - perform regular drills/ exercises for all scenarios, in order to regularly determine their effectiveness.
    - manage change to EER arrangements.
    - provide for contingency processes, for example, if equipment becomes unavailable, e.g. the helideck becomes impaired by smoke, heat radiation.
    - provide for testing/ maintaining/ repairing EER equipment.
- Ensure the competency for all personnel to respond appropriately if the need for EER is required.

Consideration of procedures associated with procedures for managing evacuation, escape and rescue in the event of an emergency should also feed into the response plan as required under OPGGS(S) Regulation 2.20.

Further guidance is available in the NOPSEMA guidance note:
"Emergency Planning"

4.4 Consideration of temporary refuge(s)

Level of Detail Requirement	
Reg 2.16(2)	The evacuation, escape and rescue analysis must: (f) consider a range of amenities and means of emergency communication to be provided in a temporary refuge.

- Consideration should be given to fundamental aspects of a temporary refuge (TR) such as:
    - sufficient in size including the provision to support any casualties/ injuries;
    - muster areas to be located in protected areas;

  - have suitable equipment to support EER activities (for example life vests, suitable lighting, smoke hoods); and
  - ability to withstand the effects of fire/ smoke/ gas/ heat/ impact etc. should be provided.
- The range of TR amenities that should be considered include:
  - Muster areas within the TR of sufficient size to accommodate required personnel;
  - First aid provisions;
  - Water and sanitary amenities; and
  - Breathable air of a suitable temperature and humidity for the endurance period.
- Consider the equipment required to ensure effective communication. For example:
  - Telephones
  - Radios
  - PA system
  - etc.

4.5 Consideration of life saving equipment

Level of Detail Requirement	
Reg 2.16(2)	The evacuation, escape and rescue analysis must: (g) consider a range of life saving equipment, including: (i) life rafts to accommodate safely the maximum number of persons that are likely to be at the facility at any time; and (ii) equipment to enable that number of persons to obtain access to the life rafts after launching and deployment; and (iii) in the case of a floating facility — suitable equipment to provide a float-free capability and a means of launching.

The consideration of a range of life-saving equipment must include life rafts but is not limited to them. For facilities where emergencies have been identified associated with fires and explosions at or near sea level consideration should be given to the use of totally enclosed motor propelled survival craft (TEMPSC) complete with external deluge with an appropriate level of redundancy, particularly for normally attended facilities.

- Consider the limitations of any equipment provided; For example:
  - Adequate clearance from the structure so that launching of lifeboats is successful.
  - Weather limitations.
- Consider what go wrong with EER provisions. For example:
  - Premature release of lifeboats
  - Ability of lifeboats to move away from the facility (depending on the weather, wind and wave may push the boat back onto the facility).

The International Convention for the Safety of Life at Sea (SOLAS) is often used as the standard for lifesaving appliances offshore. As discussed in the guidance note for ALARP, reliance on codes and standards does not necessarily mean that risks are reduced ALARP.

It may be, for example, that:

- the codes or standard may not address the types of incident that are of prime concern to the facility;
- there may be gaps in the standards, such that the particular standard does not govern all aspects of hazards and risks at a facility; and

- the standard has fallen behind current good practice, or the facility has fallen behind the standard as that has been further developed.

Example: Lifeboat Capacity

An operator may decide to comply with the Life-Saving Appliances (LSA) IMO code for all lifeboats on a specific facility, since LSA is an internationally recognised standard for lifeboats on vessels. The operator should recognise according to the LSA code, lifeboat capacity is based on a person having an average mass of 75kg. If the average weight for the personnel on the operators' facility is typically 90kg then the operator should identify the limitation of the LSA code and ensure their lifeboat capacities are reclassified accordingly.

4.6 Demonstrating evacuation, escape and rescue risks have been reduced to ALARP

Level of Detail Requirement	
Reg 2.16(2)	The evacuation, escape and rescue analysis must: (h) identify, as a result of the above considerations, the technical and other control measures necessary to reduce the risks associated with emergencies to a level that is as low as reasonably practicable.

Note that the detailed description of the control measures identified belong in the FD (for technical controls) or SMS description (for procedural controls) sections of the safety case which the relevant parts of the FSA description should cross-reference.

Measures that could improve EER and the performance of temporary refuges for the specified endurance time should be considered as part of the ALARP demonstration. Typical control measures include those that:

- Prevent damage to EER arrangements from the effects of MAEs
- Mitigate the effects of risks resulting from EER arrangements, for example:
    - Lifeboat assist systems
    - Individual Escape Devices
    - Multiple Personnel Escape Devices
    - Increasing recovery times from water, for example
        - Dacon scoop
        - Fast Rescue Craft
        - Standby Vessels with lower freeboards
        - Re-breathers for helicopter ditching
        - etc.

The adopted control measures for any particular identified MAE must be shown to reduce the risks associated with emergencies to a level that is ALARP, i.e. that the cost to implement further control measures is grossly disproportionate to the risk reduction they would provide.

Depending on the circumstances, the approach employed in providing the required evidence of ALARP may include:

- comparison with standards, codes and industry practices;
- analysis of the risks, and of the benefits and costs of alternative/additional control measures;
- assessment of the appropriateness of control measures and their performance standards;

- comparison with benchmarks for risk and for management performance;
- comparison with good practice management system frameworks; and
- demonstration of past and planned improvements.

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

There is no prescribed methodology for demonstrating that the necessary control measures have been identified to reduce risks to ALARP, however in any case, 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 and make the argument for why further risk reduction is not practicable.

Further guidance is available in the NOPSEMA guidance note:
"ALARP"

5 Survivability Studies

Lord Cullen identified the need to 'review the ability of emergency systems to withstand severe accident conditions' (one of the 'Forthwith' studies).

Whether or not a control measure is able to survive a potentially damaging event such as an MAE is relevant for all control measures that are required to function after an incident has occurred. Survivability performance should therefore be considered for those systems (e.g. blow-down & ESD systems, fire protection systems (passive and active) and emergency evacuation/ escape systems).

Operators should conduct survivability studies for key equipment and systems to provide evidence that the requirements of Regulation 2.14(2) are met.

Level of Detail Requirement	
Reg 2.14(2)	The safety case must demonstrate that: (a) the equipment is fit for its function or use in normal operating conditions; and (b) to the extent that the equipment is intended to function, or to be used, in an emergency – the equipment is fit for its function or use in the emergency.

The overall aim of an emergency systems survivability analysis (ESSA) is to determine the vulnerability of emergency systems against MAEs. Understanding their vulnerability to operate as expected will allow judgements to be made as to their effectiveness/survivability.

It is important to consider the following for any equipment required in an emergency for the required endurance time:

- Identify and assess the criticality of the system in terms of their vulnerability to MAEs. For example, if it is expected that the deluge system will contain the fire, the deluge system should also be able to withstand the effects from the fire;
- Determine the functionality of critical components e.g. firewater pump for deluge system;
- Understand whether the components of the system are fail-safe. For those that do not fail safe, consider how the performance of that component/system will behave in an MAE. For example, the failure mechanism may allow the event to escalate further;
- Consider redundancy of systems/components;
- Consider additional risk reduction measures to increase the survivability of emergency systems, particularly for those that may be impaired by MAEs, and are neither fail-safe nor have redundancy. This is an important step in the risk management process as it aids the demonstration that risks are reduced to a level that is ALARP.

Information to determine the survivability of safety systems can be sourced from other studies conducted, including the FSA, EERA, and performance standards. The requirements of OPGGS(S) Regulation 2.14(2)(b) are linked to the studies and performance standards that apply as required under Regulation 2.20(2)(b) for the emergency response plan.

Example – survivability of critical cable runs
A review was undertaken which established that the cable runs for main process control system are critical to allow the appropriate action to be taken – e.g. automatic shutdown of process valves. Whilst it was recognised that these cables are fail-safe, have redundancy, and are coated such that they can withstand the expected fire events, an additional risk reduction measure was implemented (as it was reasonably practical) which involved routing the cables in such a way that the facility structure provided dropped object protection.

6 Other types of supporting studies

The OPGGS(S) Regulations do not require further supporting safety studies to be undertaken or described in a safety case. However, factors such as the nature and frequency of certain activities, complexity and location of the facility and number of personnel on board may require detailed examination beyond the FERA and EERA studies. Consideration should be given, as appropriate to the facility and activities to be conducted, to undertaking studies on subjects such as:

- Dropped objects
- Cold Spills
- Ship Collisions
- Dispersion (smoke, gas, exhaust, cold vents)

7 References, Acknowledgements & Notes

Offshore Petroleum and Greenhouse Gas Storage Act 2006

Offshore Petroleum (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 17776:2000(E))

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

Australian Petroleum Production & Exploration Association Limited GUIDELINES FOR FIRE AND EXPLOSION MANAGEMENT, ISBN 0 908277 19 9

Health and Safety Executive, Improving Inherent Safety, OTH 96 521, Mansfield, D; Polter L; Kletz T, http://www.cieng.org/events/lectures%202010%20-%202011%20session/2011-05-10%20annual%20conference/presentations/jo%20fearnley_cie%20inherent%20safety.pdf

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

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 regulations. For facilities located in designated coastal waters, please refer to the relevant State or Northern Territory legislation.

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

- Telephone: +61 (0)8 6461-7000, or
- e-mail: safetycaseguidance@nopsema.gov.au.