Safety case content and level of detail

Core concepts

- The safety case for an offshore facility that an operator submits to NOPSEMA must comply with the contents requirements of the Offshore Petroleum and Greenhouse Gas Storage (Safety) Regulations *2009* [OPGGS(S)] for each stage in the life of the facility in respect of which the safety case is submitted.
- This guidance note, 'Safety Case Content and Level of Detail', provides guidance on the content and level of detail expected to be included in relation to each of the major aspects of a safety case submission (Facility Description, Safety Management System Description, Formal Safety Assessment Description) such that it complies with requirements of the OPGGS(S) Regulations.
- The safety case must be appropriate to the facility and to the activities conducted at that facility.
- Only by inclusion of a sufficient level of detail in the safety case will NOPSEMA be able to make a judgement on the appropriateness of the safety case in accordance with OPGGS(S) Regulation 2.26 (for new safety cases) or Regulation 2.34 (for revised safety cases).
- The safety case must be a stand-alone document that is sufficient to meet the contents and level of detail requirements of the OPGGS(S) Regulations without need to refer to other documents external to the safety case.
- The safety case that the operator prepares for an offshore facility must identify the safety-critical aspects of the facility, both technical and managerial, with respect to major accident events.
- The adopted control measures for any particular identified major accident event must be shown to collectively eliminate, or reduce to a level that is as low as is reasonably practicable, the risk to health and safety of people at the facility.
- In order to provide evidence that the SMS is comprehensive and integrated for all aspects of the control measures, it needs to be shown to fully support and maintain the performance of the control measures within an integrated management framework.
- The descriptions within the safety case must provide evidence that risks are reduced to a level that is ALARP.
- Overall, a well-structured, coherent safety case will facilitate an operator's ability to demonstrate to others that they have a clear understanding of the factors that influence risk and the controls that are critical to minimising risk to people on their facility.
- It must be demonstrated that in the development or revision of a safety case there has been effective consultation with, and effective participation of, members of the workforce in order to facilitate informed opinions about the risks and hazards to which they may be exposed on the facility.
- Licensed pipelines are facilities – From 1 January 2010, under amendments made to form the *Offshore Petroleum and Greenhouse Gas Storage (Safety) Regulations 2009*, licensed pipelines are facilities requiring a safety case.

Table of contents

1 Introduction 7
1.1 Intent and purpose of this guidance note 7
1.2 Summary of legislative requirements 8
1.3 Presentation of OPGGS(S) Regulations within this guidance note 9
2 General considerations 11
2.1 Safety case must be appropriate 11
2.2 Safety case preparation – Involvement of members of the workforce 12
2.3 Standalone document 13
2.4 Common weaknesses 14
2.4.1 Insufficient detail 14
2.4.2 Too much detail 14
2.5 Safety case structure 15
3 Facility description 17
3.1 General 17
3.1.1 Scope of the safety case 17
3.1.2 Level of detail 18
3.1.3 Drawing set 19
3.1.4 Standards to be applied 19
3.1.5 Performance standards 21
3.2 General Description and layout of the facility 21
3.2.1 General description 21
3.2.2 Facility layout 22
3.3 Activities, machinery and equipment 23
3.3.1 General considerations 23
3.3.2 Wells and sub-sea operations 26
3.3.3 Production operations 27
3.3.4 Utility operations 27
3.3.5 Marine operations 28
3.3.6 Drilling and well intervention operations 28
3.3.7 Diving and ROV operations 29
3.3.8 Lifting operations 29
3.3.9 Pipe-lay operations 30
3.3.10 Pipe operations 30
3.3.11 Logistical support 31
3.3.12 Construction, installation, and other operations 31
3.4 Technical and other control measures 32
3.4.1 General considerations 32
3.4.2 Command structure 34

3.4.3 Medical and pharmaceutical supplies and services 35
3.4.4 Emergency communication systems 36
3.4.5 Control systems 37
3.4.6 Piping systems 37
3.4.7 Vessel and aircraft control 37
3.5 Common weaknesses 38
4 Formal Safety Assessment description 39
4.1 General considerations 39
4.2 Hazard identification 41
4.3 Risk assessment 43
4.4 Control measures 45
4.4.1 The ALARP argument 46
4.5 Supporting studies 47
4.5.1 Evacuation, escape and rescue analysis 47
4.5.2 Fire and explosion risk analysis 48
4.6 Common failings in Formal Safety Assessment 50
4.6.1 FSA process 50
4.6.2 Hazard identification stage 51
4.6.3 Risk assessment stage 51
4.6.4 Control measure identification 51
4.6.5 Evidence of ALARP 51
5 Safety Management System description 53
5.1 General requirements 53
5.1.1 Description of the SMS 53
5.1.2 Level of detail 54
5.1.3 Comprehensive and integrated 55
5.1.4 Scope of the SMS 56
5.1.5 Hazard identification and risk management 56
5.1.6 Inspection, testing and maintenance 57
5.1.7 Communications 58
5.1.8 Objects of the regulations 58
5.1.9 Performance standards 59
5.1.10 SMS implementation 60
5.1.11 Standards to be applied 61
5.1.12 Means to ensure on-going integrity of technical and other control measures (5 Year revisions) 61
5.2 Safety measures 62
5.2.1 Command structure 62
5.2.2 Members of the workforce must be competent 63
5.2.3 Permit to work system for safe performance of various activities 64

5.2.4 Workforce involvement – provisions of the SMS 65
5.2.5 Design, construction, installation, maintenance and modification (SMS) 65
5.2.6 Drugs and intoxicants 66
5.3 Emergencies 67
5.3.1 Emergency preparedness 67
5.3.2 Pipes 69
5.3.3 Vessel and aircraft control 69
5.4 Arrangements for records 70
5.5 Common weaknesses in the SMS descriptions 71
5.6 Evidence of compliance 71
6 Critical factors for acceptable safety cases 72
7 References, acknowledgments & notes 72

Abbreviations/acronyms

ALARP	as low as reasonably practicable
AOP	associated offshore place
EER	evacuation, escape and rescue analysis
ESD	emergency shutdown
FD	facility description
FSA	formal safety assessment
HAZID	hazard identification (study)
HAZOP	hazard and operability (study)
JHA/JSA	job hazard analysis / job safety analysis
LOPA	layers of protection analysis
MAE	major accident event
MoC	management of change
MODU	mobile offshore drilling unit
MPD	managed pressure drilling
NOPSEMA	National Offshore Petroleum Safety and Environmental Management Authority
NORM	naturally occurring radioactive material
OHS	occupational health and safety
OPGGSA	*Offshore Petroleum and Greenhouse Gas Storage Act 2006*
OPGGS(S)	Offshore Petroleum and Greenhouse Gas Storage (Safety) Regulations 2009
P&IDs	piping and instrumentation diagrams
PSMP	pipeline safety management plan
PTW	permit to work
QRA	quantitative risk assessment
ROV	remotely operated vehicle
SAR	search and rescue
SMS	safety management system
TEMPSC	totally enclosed motor propelled survival craft
UBD	under balance drilling
UPS	uninterruptible power supply

Key definitions for this guidance note

Major Accident Event	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) Regulation 1.5)
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) subregulation 2.11(3))
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) Regulation 1.5)

Following are some useful definitions for verbs & nouns used in the regulations (The Macquarie Dictionary Online © 2007). They are a suggested starting point only and are not prescriptively defined.

Adequate:	equal to the requirement or occasion; fully sufficient, suitable or fit
Appropriate:	suitable or fitting for a particular purpose, person, occasion, etc.
Comprehensive:	inclusive; comprehending much; of large scope
Consider:	to make allowance for; to regard with consideration or respect
Demonstrate:	to describe and explain with the help of specimens; to manifest or exhibit
Describe:	to set forth in written or spoken words; give an account of
Detail:	particulars collectively; minutiae; item by item
Evidence:	ground for belief; that which tends to prove or disprove something; proof
Identify:	to recognise or establish as being a particular person or thing
Include:	to contain, embrace, or comprise, as a whole does parts or any part or element; to contain as a subordinate element; involve as a factor
Integrated:	to make up or complete as a whole, as parts do
Provide for:	to make arrangements for supplying means of
Specify:	to mention or name specifically or definitely; state in detail
Summary:	a brief and comprehensive presentation of facts or statements; an abstract, compendium, or epitome
Systematic:	having, showing, or involving a system, method, or plan

1 Introduction

1.1 Intent and purpose of this guidance note

This document is part of a suite of documents that provide guidance on the preparation and use 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 where powers have been conferred on NOPSEMA.

Figure 1 – Safety case guidance note map illustrates the scope of the NOPSEMA safety case guidance notes overall, and their inter-related nature. The guidance notes are available on the NOPSEMA website, along with guidance on other legislative requirements, such as nomination of operator, validation, and notifying and reporting accidents and dangerous occurrences.

Figure 1 – Safety case guidance note map

The purpose of the guidance is to explain the objectives of the regulations, to identify the general issues that should be considered, and to provide practical examples to illustrate the concepts and potential approaches that can be taken in the preparation of safety cases. The guidance is intended for use by industry and NOPSEMA inspectors in the preparation and assessment of safety cases. It is not, however, the intention of the guidance to provide detailed approaches or detailed regulatory assessment criteria.

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.

This guidance note in particular, 'Safety Case Content and Level of Detail', provides direction on the content and level of detail expected to be included in relation to each of the major aspects of a safety case submission (Facility Description, Safety Management System Description, Formal Safety Assessment Description) such that it complies with the requirements of the OPGGS(S) Regulations and provides evidence that risks are reduced to a level that is ALARP. The guidance will be of use to those with responsibility for safety at offshore facilities, and specifically to those developing the facility safety case.

The aim of this guidance note is essentially threefold:

- to provide a common basis for the preparation and assessment of safety cases in accordance with the requirements of the OPGGS(S) Regulations;
- to facilitate the operator in giving appropriate descriptions via the safety case so as to provide all stakeholders with assurance that the operator has or will have appropriate control measures and satisfactory safety management systems; and
- to provide clarification as to what elements would support a suitable and sufficient demonstration of meeting the intent of the regulations in order to facilitate safety case acceptance by NOPSEMA.

If this guidance note does not cover a particular aspect in respect to safety case content, or if further clarification is required, operators are encouraged to contact NOPSEMA directly.

This Guidance Note is not a substitute for legal advice on interpretation of the regulations or the Acts under which the regulations have been made.

1.2 Summary of legislative requirements

Summary tables of the legislative requirements are included as a quick reference throughout this document. ***However, the reader is encouraged to work directly from the regulations themselves.***

With respect to safety case contents aspects of this guidance note the elements of the OPGGS(S) regulations covered by this are as follows:

Contents requirements (Safety case)

Part 2 Division 1 of the OPGGS(S) Regulations sets out the contents requirements for safety cases:

- Subdivision A covers contents of a safety case. In particular, regulation 2.5 covers the major elements to be included in a safety case submission:
  - a description of the facility;
  - a detailed description of the formal safety assessment; and
  - a detailed description of the safety management system.
- Subdivision B covers safety measures
- Subdivision C covers emergencies
- Subdivision D covers arrangements for record keeping

These elements are also two of the four elements of the acceptance criteria detailed in OPGGS(S) Regulations 2.26 and 2.34, for new and revised safety cases respectively.

With respect to the level of detail aspect of this guidance note, the relevant OPGGS(S) Regulations are simply the requirements for a safety case to be appropriate to the facility and to the activities conducted at the facility which comprises the 1st element of the acceptance criteria in OPGGS(S) Regulations 2.26 and 2.34, for new and revised safety cases respectively. The remaining acceptance criteria relates to validation, where relevant.

Safety case acceptance criteria	
Reg 2.26(1)	NOPSEMA must accept a safety case if: (a) the safety case is appropriate to the facility and to the activities conducted at the facility; and (b) the safety case complies with Subdivisions A, B and C of Division 1 for each stage in the life of the facility in respect of which the safety case is submitted; and (c) the safety case complies with Subdivision D of Division 1; and (d) in a case in which NOPSEMA has requested a validation of the facility: (i) the person, or each person, undertaking the validation meets the criteria specified in subregulation 2.40(5); and (ii) the validation complies with regulation 2.40.

In general terms the level of detail required in a safety case to satisfy NOPSEMA the case is appropriate to the facility and the activities conducted at the facility is a function of a number of factors such as the level of risk, complexity, uncertainty.

Given the over-arching nature of the appropriateness requirements, an operator should apply this test to all the contents requirements as the case is being developed, e.g. with respect to OPGGS(S) Regulation 2.20 – "Have I included sufficient detail in the description of the emergency response plan to demonstrate the safety case is appropriate to my facility and the activities the conducted at the facility?" The subject of level of detail is expanded upon specifically at the start of each major section of this guidance note (i.e. with respect to the facility description, detailed description of the formal safety assessment and detailed description of the safety management system).

1.3 Presentation of OPGGS(S) Regulations within this guidance note

This guidance note is structured to contain specific guidance on the content and level of detail expected by NOPSEMA for OPGGS(S) Regulations 2.5 through 2.23. In order to provide for a logical flow and structure, the order in which specific guidance is presented does not always mirror the order in which the regulations appear in OPGGS(S). Instead the regulations and parts thereof are dealt with more in line with how they could be addressed in a safety case. For clarity, an OPGGS(S) concordance table is included as an appendix to this Guidance Note to show where the OPGGS(S) Regulations are discussed.

The OPGGS(S) Regulations contain a large number of explicit content requirements which are reproduced within this guidance note in the following format:

EXAMPLE content requirement	
Reg 2.13	**The safety case for a facility must specify** the medical and pharmaceutical supplies and services, sufficient for an emergency situation, that must be maintain on, or in respect of, the facility.

There are also a number of places where the regulations require the safety case to contain a description of a particular item which is followed by one or more requirements for the item

itself. In order for NOPSEMA to be assured that such requirements are met, these requirements set level of detail requirements for the safety case. In the example shown below there is an explicit preceding content requirement for the safety case to contain a description of an emergency response plan:

EXAMPLE Level of detail requirement

Reg 2.20(2)(b) **The plan must specify** the performance standards that it applies.

In order for NOPSEMA to be assured the plan specifies the performance standards it applies, there is an implicit level of detail requirement that the description includes appropriate coverage of performance standards associated with emergency response (refer to section 5.3.1, p67) of this Guidance Note for further guidance associated with this regulation).

2 General considerations

2.1 Safety case must be appropriate

Safety case acceptance criteria	
Reg 2.26(1)(a)	**NOPSEMA must** accept the safety case if the safety case is appropriate to the facility and to the activities conducted at the facility.

In order to meet the 1st acceptance criteria, descriptions within the safety case must be relevant to the facility and activities. That is, there should be a suitable level of detail that accurately explains the physical characteristics of the facility, its operating envelope, the management systems in place and the activities that take place at or in connection with the facility.

There is also an element of proportionality with respect to the level of detail: a higher level of risk or uncertainty should result in an equivalently higher level of detail in the safety case.

Example

The safety case must specify the medical and pharmaceutical supplies and services sufficient for an emergency situation that must be maintained on, or in respect of, the facility [OPGGS(S) Regulation 2.13]. Whether or not these supplies and services are suitable and fit-for-purpose will vary depending on facility location, number of personnel on board, types of activities being carried out, access to other supporting services, etc. The risks and extent to which these supplies and services are responsible for significant risk reduction should provide a guide to the level of detail the safety case requires.

Consequently, the medical and pharmaceutical supplies and services that would be appropriate for a facility with minimal manning, located close to a major population centre undertaking activities with very low risk of hydrocarbon fire or explosion may be quite different to a facility located a long way from shore undertaking complex hydrocarbon processing with high inventories and a larger workforce. Appropriate supplies and services to provide initial treatment and potentially keep casualties stabilised on-board pending evacuation are just a few of the considerations that would need to be made.

Similarly, the emergency response plan that the operator describes to address possible emergencies will be expected to differ according the location of the facility, and therefore must be specific and appropriate in each case.

The test of appropriateness applies to each and every aspect of OPGGS(S) Regulations 2.5 to 2.23.

OPGGS(S) Regulation 2.45 makes it clear that a person must not construct, install, operate, modify, carry out maintenance, decommission or do any other work at a facility in a manner that is contrary to the safety case that is in force for the facility. Operators should be mindful that the safety case is a ‘permissioning tool’ and therefore, statements made within the document need to be clear and unambiguous as these become commitments that the operator must comply with once the safety case is accepted by NOPSEMA.

2.2 Safety case preparation – Involvement of members of the workforce

Requirement	
Reg 2.11(1)(a)	The **operator of a facility must demonstrate** to NOPSEMA, to the reasonable satisfaction of NOPSEMA, that 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.

Documentation requirement	
Reg 2.11(2)	A demonstration for the purposes of subregulation (1)(a) **must be supported** by adequate documentation.

Definition	
Reg 2.11(3)	In subregulation (1) ***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.

Note: regulation 2.11(1)(b) is addressed in the SMS section 5.2.4, p65.

Operators should think carefully about the level of involvement of the workforce that is necessary to constitute full compliance with the requirements of OPGGS(S) Regulation 2.11 with respect to safety case development.

In order to achieve the objectives of producing a safety case that accurately reflects the reality of activities and operations on the facility, the operator needs an appropriate level of involvement of members of the workforce. It is essential the operator uses the specific knowledge that the workforce has in identifying hazards, assessing risks, and adopting control measures.

In the development of a safety case (or revised safety case), the operator of a facility must demonstrate to NOPSEMA's satisfaction that there has been effective consultation with, and participation of, members of the workforce. This particular demonstration does not necessarily need to be included within the safety case itself; but it must be supported by adequate documentation. However, as the safety case is the key health and safety document for the facility, it may be the best place to document the demonstration required.

A documented demonstration for the purposes of this regulation could include a combination of a description of the process by which the workforce was involved in safety case development inclusive of specific references to the actual SMS document(s) (a copy of applicable documentation could also be submitted with the safety case) supported by actual records clearly identifying which participants were members of the workforce as defined above.

As per the note to OPGGS(S) Regulation 2.11, the broad consultative arrangements provided for in Part 3 of Schedule 3 to the Act should be used in this context.

NOPSEMA recognises that in some instances a safety case may be developed before the entire workforce is recruited. This means that the expectation to consult with 'members of the workforce' is seen as being difficult to achieve. NOPSEMA suggests that in such cases it is incumbent on the operator to consult as much as is reasonably practicable. This can be done in a number of ways – seeking input from the workforce on other facilities of a similar type; consulting with those members of the workforce who are available; seeking input from organisations who typically employ or represent the workforce, and so on. In any event, the operator of the facility should ensure that they have satisfied NOPSEMA about how they have attempted to meet these expectations, what results were achieved and if there are any remaining steps they intend to take once further members of the workforce are available for consultation.

Further guidance is available in the NOPSEMA guidance note:
'Involving the Workforce'

2.3 Standalone document

The safety case is a roadmap to ongoing health and safety processes and, as such, it must be a standalone document that is sufficient to meet the contents and level of detail requirements of the OPGGS(S) Regulations without need to refer to other documents external to the safety case. This means that there may be references to other documents in the safety case, but if these documents are mentioned in order to meet a content or level of detail requirement of the OPGGS(S) Regulations, they must be described in sufficient detail within the safety case to meet the specific regulatory requirement. The reference documents themselves are not part of the safety case, only the descriptions are.

During a safety case assessment, a request for further written information may be made by NOPSEMA with regard to the description of a reference document, but the document itself would not be requested.

The regulations are very clear in that operators are to supply *descriptions* of elements in the safety case, as opposed to copies of the documents themselves. The description of an element should:

- distil the points of value, the relevant features of the element
- outline its potential deficiencies and how these may be overcome
- outline the reasoning or the background thinking to the development of the element
- explain how it is connected to, or supports, other elements.

For supporting studies, the safety case should summarise the key findings and explain their significance. Assumptions should also be specifically noted, i.e. the description should include an understanding of the limitations that apply.

Further guidance is available in the NOPSEMA guidance note:
'Supporting Safety Studies'

In the case of SMS procedures, the summary should be such that the safety case describes the essential elements of how these documented systems contribute to the management of safety at the facility. As with any formal document relying on other material, the safety case should employ a robust referencing system that is applied both internally and externally to the document. The referencing system should uniquely identify source documents (e.g. include the version or edition and year of publication for external design standards or internal design philosophies applied to the facility).

For complex subjects that need to be described in the safety case, operators should consider providing examples to help explain the issues where possible.

2.4 Common weaknesses

There are two types of recurring problems that have been noted with respect to content and level of detail in safety case submissions:

2.4.1 Insufficient detail

Simply listing elements or referencing documents will generally not provide a sufficient level of detail. Examples of this include:

- details in relation to formal safety assessments limited to either a reference to a study performed or, in some cases, simply a commitment to conduct a study
- details provided in relation to the summary of an operator's safety management system limited to listing of policies and procedures
- facility descriptions limited to the physical plant and equipment, with little or no detail on the activities that will, or are likely to, take place at or in connection with a facility
- only partial details of the technical or other control measures identified as a result of the formal safety assessment.

2.4.2 Too much detail

Submitting complete standalone documents within the safety case does not necessarily provide evidence that it complies with OPGGS(S) regulatory requirements. Common examples of this are the inclusion of:

- the complete facility SMS or parts thereof
- the actual Emergency Response Plan
- the evacuation, escape and rescue analysis
- the fire and explosion risk analysis.

For each of these examples the OPGGS(S) Regulations explicitly require the safety case to contain a description of rather than the actual system, study or plan.

For example, the facility Management of Change (MoC) procedure should not be reproduced in the safety case in full, but the MoC systems should be described, including features such as scope of changes managed by the system, the manner in which hazards are identified, how recommendations to reduce risk are managed through allocation of responsible parties, provision of resources, etc. – in other words, the main features of the MoC system and associated commitments to reduce the risk to as low as reasonably practicable must be documented in the safety case.

Example (Introductory text only)

The final two areas of the Safety Management System are the Management of Change and the Audit and Review Process. Management of Change is a series of procedures to ensure that any change to the facility equipment or systems, to operational or emergency procedures or to personnel is assessed so that hazards are not introduced or the risk to personnel is not increased because of the change. It ensures that changes are properly scrutinised, assessed, documented and communicated. The MoC process consists of…

2.5 Safety case structure

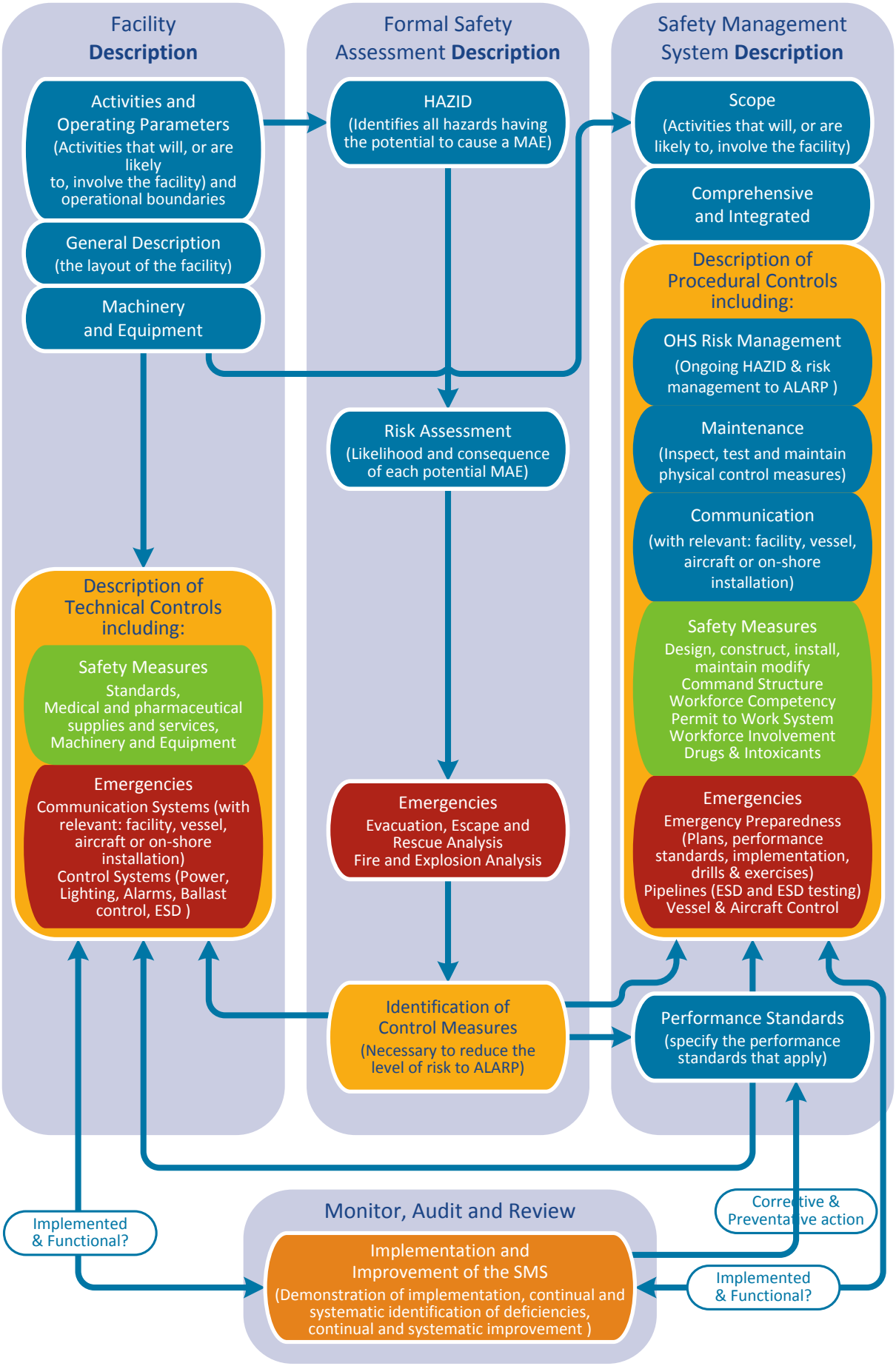
The safety case should have a coherent, integrated overall structure: there should be logical flow to the process to create strong links between the causes and consequences of major accident events, their associated risks, the selection of strategies and measures to control the risks, and the performance required from specific measures to maintain risk levels to ALARP.

The process of developing a safety case is an iterative one. In order to achieve the overall linkage between the elements and ensure consistency throughout, the safety case development process should involve several review loops in order to close gaps and achieve a quality document.

The use of good editorial practice is essential: duplication of information (and the potential for contradiction) can be avoided by using effective internal cross-referencing within the safety case document itself. For instance, something may be identified as a control measure in several places but there should only be a single detailed description of the control, usually this will be in the facility description section.

Overall, a well-structured, coherent safety case will facilitate an operator's ability to demonstrate to others that they have a clear understanding of the factors that influence risk and the controls that are critical to minimising risk on their facility. Figure 2 shows the main elements of a safety case and their inter-relationship as they are set out in the OPGGS(S) Regulations. It is a visual representation of what the regulations require to be included in each of the various parts of the safety case. It is NOT intended to be read as a process diagram.

Figure 2 – A graphical representation of the OPGGS(S) Regulations



3 Facility description

3.1 General

Content requirement	
Reg 2.5(1)	**The safety case for a facility must contain a description of the facility** that gives details of: (a) the layout of the facility; (b) the technical and other control measures identified as a result of the formal safety assessment; and (c) the activities that will, or are likely to, take place at, or in connection with, the facility; and (d) for a facility that is a pipeline: (i) the route corridor of the pipeline and the pipeline's interface start and end positions; and (ii) the compositions of petroleum that are to be conveyed through the pipeline when it is operating; and (iii) the safe operating limits for conveying those compositions through the pipeline; and (e) any other relevant matters.

The facility description structure need not be constrained by the order of elements as they are laid out in the regulations or guidance. Provided all the elements are covered, operators are encouraged to structure the facility description such that the description 'tells a story' in a sensible and usable format. The facility description must document the factual information about the facility that provides the basis for the formal safety assessment and some elements of the safety management system. In the sense that development of the FSA may result in a decision to modify the physical facility, the facility description also documents some of the outputs of the FSA development processes.

The requirements for provision of detail within the facility description section may inter-link. For instance, elements of the facility layout required to be described under subregulation 2.5(1)(a) may also be functional control measures as per subregulation 2.5(1)(b). These should be specifically mentioned as controls within the facility description text when describing the element.

3.1.1 Scope of the safety case

The facility description defines the intended range or scope of operation of the facility, the physical arrangements of the facility, all of the activities on the facility, surrounding activities near the facility, and the numbers of people present involved in each type of activity. The facility description fixes the envelope or range within which the operator is, or will, operate the facility. It is vital that this scope is clearly specified since operation contrary to the safety case in force is not permitted.

The purpose of the facility description is to provide the factual information regarding the physical layout, the controls and proposed activities required to understand the major accident events that have been identified and assessed in the FSA, the arrangements for managing the risks of those MAEs and the interactions between those risk control measures and the safety management system. This information should be sufficient to gain a full appreciation of the major accident hazards and risk management strategies from the FSA. The facility description should highlight any novel or unusual conditions, engineering solutions or technologies to be encountered or used at the facility.

The facility description should describe both the design and the operating envelopes for facility systems, considering that the safety case covers normal and emergency operations anywhere within the set of conditions described. These descriptions will link to performance standards set for control measures and demonstration that machinery and equipment is fit for its function.

In order to provide an effective basis for, and documentation of the output of, the other parts of the safety case, it is generally required that the design basis and philosophy are described, rather than just the output of the design process. The description of the design basis and philosophy of the facility should thoroughly address potential uses of the facility i.e. what the facility is physically capable of. This philosophy is consistent with that encouraged for activities. The implications of these decisions may result in residual risks and controls that will be discussed in the other sections of the safety case. The facility description also describes the physical systems in place to ensure that the design envelope is not breached, or if it is, the measures in place for bringing the situation back under control

3.1.2 Level of detail

Preparation of the facility description involves finding a balance between providing a readable document that contains useful information, and including so much detail that the document becomes quickly out of date and/or requires frequent revisions. In managing the content of the document, it is important to remember that the focus of the facility description is on the design and operating philosophy and envelope. These things are unlikely to be subject to frequent changes.

The facility description is not intended to be a simple regurgitation of technical specifications. The safety case must explain how the facility works and why particular safety design solutions were adopted. This means the facility description must include, or describe, the design and operating philosophies for the facility, and it must reference the design standards that have been used.

Example

The process facilities have been designed to the maximum Shut-in Tubing Head Pressure of the reservoir up to a point on the separator outlet to crude storage. The separator is provided with full flow relief against failure of level controls or process isolation valves.

A description of this nature provides a sound context for the FSA (and a lead-in to discussion of the potential for overpressure of the tanks and the associated controls), than would a simple listing of the design pressure of various parts of the process system.

An operator can provide information such as engineering drawings, maps, renderings, photographs, specifications, technical descriptions, databases, etc. however adequate linkages should be given between descriptions provided in the text of the facility description and the associated drawings, photographs, maps, etc. For instance, it is not sufficient to simply include drawings without an accompanying description of the parts of the facility shown in those drawings. However, using diagrams, figures and pictures to describe aspects of elements required for the facility description can be very helpful. In any case, care must be taken to ensure diagrams are clear and legible in the format provided within the safety case document. Operators also need to be careful that any drawings included in the safety case are those which are least likely to require change. For example, P&IDs are drawings that are generally subject to regular and relatively frequent change, and therefore can quickly become obsolete in the context of a safety case.

Operators are encouraged to keep details such as tag numbers, line/valve numbers within safety case documentation to a minimum. These details should be maintained current within data bases and hazard registers and NOPSEMA may inspect against up-to-date printouts of these registers and data bases during facility inspections.

Operators should find that the facility description can be a useful document in its own right, to provide internal and external stakeholders with an introduction to the facility and an insight into the operation of the facility. For the purpose of the facility description a description can include text, data, drawings, diagrams, schematics, photographs or any other means of conveying information about the facility and activities to be conducted at the facility.

3.1.3 Drawing set

A drawing set can be very beneficial to gaining an understanding of the facility. The drawings provided within the safety case should be sufficiently comprehensive and detailed to enable NOPSEMA's assessment, but need not contain all engineering details. A typical drawing set could include:

- development location map
- general arrangement drawings (deck plot plans and elevations)
- major equipment/facilities layout (including sub-sea)
- marine systems
- fire and blast protection
- fire and safety equipment
- hazardous area drawings
- escape routes/emergency assembly area/temporary refuge
- mooring layout if applicable
- process schematic
- emergency shut-down logic

Other drawings may be necessary to illustrate complex or novel designs. These should only be included if they are required to gain an understanding of the system from a safety or risk perspective. In general, operators are discouraged from including P&IDs in a safety case as provision of too much operational detail makes the document difficult to keep up to date.

3.1.4 Standards to be applied

Content requirement	
Reg 2.7	**The safety case for a facility must specify** all Australian and international standards that have been applied, or will be applied, in relation to the facility or plant used on or in connection with the facility for the relevant stage or stages in the life of the facility for which the case is submitted.

Note: regulation 2.7 is also addressed in the SMS description section 5.1.11, p61.

For some facilities, compliance with industry standards (including Australian and international standards, codes of practice, etc.) may play an important role in providing evidence that necessary and appropriate control measures have been identified. In principle, such standards may be Australian Standards, equivalents from overseas organisations, international industry practices such as those from the American Petroleum Institute, or company-specific standards. However, whichever standards are being used, these standards, and the control measures that they apply, should all be shown to be suitable and appropriate to the specific facility, taking account of its type, scale, activities, location, etc. It is common for an operator to adopt a suite of standards, perhaps taken from a number of different organisations. In such cases, significant effort may be necessary to show that this overall suite of standards is suitable and appropriate, as well as the individual parts.

Operators should also be mindful of the potential complications that use of multiple standards can cause. For example, there are a number of different standards available for hazardous area electrical equipment, however if different standards are used for different parts of a facility, this can create different ongoing maintenance and inspection regimes for similar equipment on the same facility.

For initial safety cases, or revised safety cases where the reason for revision is a modification to the facility, a scope of validation must be agreed prior to submission. This agreed scope of validation will have already addressed much of the requirement to select appropriate standards since the scope of the safety case, and activities and equipment/hardware it covers, determines which equipment must be validated. The focus should be on equipment, a failure of which, would pose a high risk to personnel at that stage in the life of the facility (e.g. result in an MAE). For a proposed facility, the legislation requires that design, construction and installation of the facility are consistent with the FSA for the facility.

Further guidance is available in the NOPSEMA guideline:
'Validation'

The descriptions of systems, plant and equipment within the facility description should include reference to the standards that have been applied so that the specified standard is seen in context. Simply providing a listing of standards without discussing the relevance of the standards in their application does not provide the evidence required to demonstrate appropriateness of the control measures they apply. Operators may choose to put a consolidated list of applied standards in the safety case document reference section, but this list should not live by itself in the text of the safety case.

The regulatory requirement is to *specify* the standards that are applied. References therefore should include the version or edition and year of publication for external design standards or internal design philosophies or standards applied to the facility. Alternately, operators may choose to maintain their facility and plant to the most current standard and this should then be stated in the safety case. Whatever standard or set of standards is used, the operator should take care to justify applicability and recognise limitations of those standards.

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.

Example: MODU code

A number of MODUs operating in Australian waters are only classed to the 1979 MODU Code (rather than the 1989 or 2001 Codes). One area of significant difference with later versions of this code is considerations for ballast control following the Ocean Ranger incident in which a MODU and all on board were lost. Any ALARP argument for the management of ballasting related MAEs should explicitly consider the limitations of the older code and implementation of the current code unless it can be demonstrated not to be reasonably practicable to do so.

3.1.5 Performance standards

Whilst it is a requirement that the SMS specifies the performance standards that apply (see section 5.1.9), references to specific performance standards should be made where appropriate in the facility description, in particular for technical and other control measures.

3.2 General Description and layout of the facility

3.2.1 General description

Content requirement	
Reg 2.5(1)(e)	**The safety case for a facility must contain a description** of the facility that gives details of any other relevant matters.

In general, "other relevant matters" pertains to operational boundaries and information required in support of the FSA and SMS. It provides for the what, where, when and how, in general terms, in order to set the scene and support the overall safety case structure. Other relevant matters may include, but are not limited to, the following types of information:

The facility description should contain all the necessary administrative particulars such as:

- operator's details including contact details
- permit and/or licence number (including pipeline licence numbers)
- block details.

There could be a description of the petroleum location that also shows the applicable legal jurisdiction(s). The location information should be primarily concerned with the environmental hazards the facility will be exposed to, and which have influenced its design. The location information may cover:

- geographical location
- meteorological conditions, including return period data for limiting environmental conditions
- geotechnical conditions
- marine data in regard to shipping and navigational hazards
- transport data in regard to the basis for assessing transportation risks (e.g. flight times).

There could be a brief description of reservoir fluids and conditions to help NOPSEMA gain an appreciation of the hazards and risks that will be associated with the wells and the production fluids. This information may cover matters such as:

- number and location of wells
- production profiles
- changes to well fluid characteristics, e.g. pressure, compositions, souring
- NORMs
- well intervention arrangements
- drilling and well work-over plans.

Note that the information listed here is also required for safety case revisions to specific campaigns of MODUs as these revisions are intended to address the site and well-specific risks.

The facility description should provide an overview of the facility type e.g. fixed platform with steel jacket and integrated deck, floating production platform, column-stabilised semi-submersible drilling unit, etc. The description should define the extent of the facility; for instance does it include wells, any pipes from a well or secondary lines associated with the facility. There should be a description of the foundation design, or mooring design for floating facilities. There needs to be a description of the structural design of the facility, including a discussion of the design values and return periods selected for environmental loadings such as wind, wave and seismic events.

The operator must describe the manning philosophy for the facility and give estimates for the numbers of personnel that will be present on the facility, the personnel distributions according to the layout of the facility, and the shift-working arrangements for day and night working. If the manning is likely to vary, for example because there will be campaigns for maintenance or drilling and the like, then details should be given for the maximum and minimum numbers expected.

Recognising that there are many different types of facilities requiring a safety case, and 'one size does not fit all', the preceding sections should only be used as a guide by operators to consider what content is appropriate in their specific circumstances.

3.2.2 Facility layout

Content requirement	
Reg 2.5(1)(a)	The **safety case for a facility must contain a description** of the facility that gives details of the layout of the facility.

The facility layout should provide an effective overview of the location of key physical elements of the facility, their spatial distribution and relative locations. The details of the facility layout should include descriptions of items including, but not limited to, the following:

- Structure
- foundations or mooring systems (as appropriate)
- petroleum processing and storage equipment or packages e.g. wellheads, separators and other vessels, compressors, subsea systems, etc.
- isolation valves
- risers and caissons, flow-lines, control umbilicals
- control room
- hazardous areas
- safety systems e.g. fire pumps, deluge, fire and gas detection, etc.
- utility equipment or packages e.g. main, emergency and UPS power supplies
- accommodation
- helideck and/or boat landing arrangements for personnel transfer
- cranes
- emergency and evacuation equipment e.g. temporary refuge(s), TEMPSC, fast rescue craft etc.
- drilling/work-over plant and equipment
- heavy construction equipment
- diving related equipment.

3.3 Activities, machinery and equipment

3.3.1 General considerations

Activities

Content requirement	
Reg 2.5(1)(c)	**The safety case for a facility must contain a description** of the facility that gives details of the activities that will, or are likely to, take place at, or in connection with, the facility.

The safety case should list all of the activities that are likely to take place over the stages for which the safety case is submitted. The list must be specific and the operator must make an effort to anticipate the different work activities that may reasonably be expected to happen in connection with the facility. This means the safety case must not only describe what functions the facility has been designed to perform, but the operator must anticipate any unplanned, or unusual, or contingency activities that might be reasonably expected to happen during the course of facility operations.

There is benefit to all parties if the safety case addresses the reasonably foreseeable activities likely to take place, as this will limit the need for future safety case revisions. It is not sufficient to claim that the SMS is suitable to be applied to any activity that might be necessary as the formal safety assessment will also have to give due consideration to the activities to be performed with respect to potential MAEs.

The level of detail expected in the facility description includes those activities which expose people to hazards with the potential to lead to a major accident event. This includes from arrival at the facility (e.g. helicopter landing), normal operation, maintenance activities, etc., up to departure from the facility.

If an activity which introduces hazards having the potential to cause a major accident event is not contemplated within the safety case, it cannot be conducted until there is a safety case in force that addresses that activity.

Combined and simultaneous operations with other facilities and vessels

Operators should consider the potential for activities involving other facilities, in other words combined or simultaneous operations such as might happen with drilling rigs, construction vessels, ROV inspections, diving support vessels, major maintenance support vessels, or construction operations at facilities that have phased expansion plans. If these activities are not anticipated and described in the safety case that is in force then the operator will need to prepare and submit a revised safety case for acceptance.

Example: Jack-up Drilling Rig over a fixed platform

In the case of a jack-up drilling rig undertaking work over a fixed platform, the rig is considered to be a facility not only when it is being used for offshore petroleum activities, but from the time it arrives at the site where it is being prepared for use until it has ceased its operations and is in a navigable form that enables it to relocate from the site. Both of the facilities therefore will need safety cases which should describe the activities involved in mobilising and moving onto location, jacking up, cantilevering over a platform as well as the drilling or well intervention activities that might be performed.

Mobile facilities

Mobile facilities like drilling rigs and construction vessels must consider carefully what activities need to be included in the safety case. These facilities are essentially designed to perform specific tasks, but the locations and circumstances of each job will be different.

The operators of these facilities therefore need to think carefully about how to identify and describe these activities so that they are applicable to each new job the facility undertakes.

Example: Construction vessel

In the case of a construction vessel, the vessel is considered to be a facility not only when it is being used for offshore petroleum activities, but from the time it arrives at the site where it is being prepared for use until it has ceased its operations and is in a navigable form that enables it to relocate from the site. (OPGGSA Schedule 3, Clause 4)

Construction and installation phase submissions

Content requirement	
Reg 2.5(4)	If an operator of a facility submits to NOPSEMA a safety case for the construction or installation stage in the life of the facility, **the safety case must contain** the matters mentioned in subregulation (1), (2) and (3) in relation to: (a) the facility at that stage in the life of the facility; and (b) the activities that will, or are likely to, take place at, or in connection with, the facility during that stage in the life of the facility; and (c) to the extent that it is practicable — the facility and the activities that will, or are likely to, take place when the facility is in operation.

The concept of 'stages in the life of a facility' provides flexibility through staged safety case submission, it does not impose any restrictions and limitations on what activities may be conducted during any particular stage. It is up to the operator to choose what assets and activities are involved in any particular stage, and as long as the accepted safety case adequately addresses those assets and activities, the operator can conduct those activities.

Experience has shown that facility commissioning activities can pose difficulties from a safety case perspective in that they typically overlap both construction and operation stages. Operators should consider how best to address this, particularly in the case of 'hot' commissioning where hydrocarbons are being introduced into new, untested systems.

Example: Commissioning

The original safety case for the facility covers construction and installation activities and addresses pre-commissioning, hook-up and cold commissioning activities.

The facility safety case is then revised to cover operations. This revised safety case comes into effect in line with project handover to the operations group (prior to hot commissioning). The revised safety case covers hot commissioning and activities carried out by a commissioning team addressing 'punch list' items including performance testing. The commissioning activities are expected to carry on for 3 to 6 months into operations (from project handover).

There is a requirement to conduct well test / well clean up via a test separator, which may require the commissioning team to install test equipment and re-instate process equipment for normal operations. These activities are covered within the revised safety case for the operations phase.

The facility description must be appropriate to the stage or stages in the life of the facility for which the safety case is being prepared. The facility description for the operations stage of a facility should normally address any planned future development at the facility, so far as it is practicable to do so at the time.

Example: phased development of a gas project

An operator plans a phased development of a gas project with high, medium and low pressure operational phases and that this will require compression modules to be added in later years. It would be appropriate for the facility description to describe these different phases of operation, the changes to the facility that will be made to accommodate them, any changes to safety critical systems, measures, procedures, etc., as required.

Further guidance is available in the NOPSEMA guidance note: '**Safety Case Lifecycle Management**'

Machinery and equipment

Content requirement	
Reg 2.14(1)	**The Safety case for a facility must specify** the equipment required on the facility (including process equipment, machinery and electrical and instrumentation systems) that relates to, or may affect, the safety of the facility.

There is a broad requirement here to specify the equipment required on the facility that may affect the safety of the facility. This is linked to one of the fundamental purposes of the facility description, which is to provide of the factual information required to be able to gain an understanding of the activities to be carried out at the facility.

In general terms, the equipment referred to in this instance should not be solely the equipment or systems necessary to control MAE risks (which is addressed in section 3.4, p32) but rather equipment required for the functional operation of the facility. This is equipment (e.g. process equipment, drilling equipment etc.), which will be taken into consideration in the hazard identification but may not necessarily be carried further into the detailed risk assessment stage with respect to MAEs.

If machinery and equipment which could introduce hazards having the potential to cause a major accident event are not appropriately described within the safety case, such machinery and equipment cannot be used until there is a safety case in force in which they are appropriately addressed. Both proposed physical changes to a facility, and modifications to a facility description to include use of existing items currently excluded from the safety case (along with the associated activities), would trigger the requirement to revise and re-submit a safety case. The submission of this revised safety case can only be made after gaining agreement from NOPSEMA on a scope of validation. The validation provides NOPSEMA with assurance that the facility, *as described in the safety case*, incorporates measures that will protect the health and safety of persons at the facility.

Example: MPV

A multipurpose vessel enters the regime and has a safety case accepted that only includes some of the activities the facility is capable of and explicitly excludes a range of machinery and equipment from detailed description in the facility description. The operator subsequently wants to revise the safety case to address a wider range of activities and bring some of the equipment into operation. The operator contends the revision is only required to address the new activities. NOPSEMA however determines the facility as described by the facility description has also been modified and hence there is a requirement to agree a scope of validation.

Level of detail requirement – Machinery and equipment	
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 requirement of regulation 2.14(2) serves as a reminder of the requirements specified elsewhere in the regulations and can be linked to the more general requirement of subregulation 2.12(1) (discussed in the SMS description section 5.2.5, p65) with respect to design, construction, installation, maintenance and modification.

The facility description describes the design and operating envelope for facility systems, considering that the safety case covers normal operations anywhere within the set of conditions described. When considering equipment functioning under normal operating conditions, it can be argued that any equipment which fails or fails to operate correctly has the potential to affect safety.

For the purposes of demonstration required in the safety case for regulation 2.14(2)(a), evidence that equipment is fit for purpose can be provided with reference to design standards, risk assessment, function testing, certification, maintenance and inspection regime, etc.

The requirements of regulation 2.14(2)(b) are linked to the performance standards that apply as required under regulation 2.20 (see section 5.1.9, p59). Operators may wish to conduct survivability studies for key equipment and systems to provide evidence that the requirements of Regulation 2.14(2) are met.

The following sections provide guidance on the level of detail for activities, machinery and equipment in broad operational groupings.

3.3.2 Wells and sub-sea operations

The facility description should provide a description of the well and sub-sea systems and their operation including design data. Although wells are subject to the separate regulations (i.e. Part 5 of the Commonwealth Offshore *Petroleum and Greenhouse Gas Storage (Resource management and Administration) Regulations 2011*), the safety case should provide information about wells and well operations so that their hazard potential can be understood as an input to the FSA. The content and level of detail needs to be adequate for NOPSEMA to gain an appreciation of the hazards posed by these systems and associated activities.

The information should include production wells and other types of wells provided for reservoir management, such as gas injection, water injection, disposal of fluids and returns, etc.

The information must be appropriate to the facility and the activities to be conducted at the facility and may address, but is not necessarily limited to, the following:

- completion design and construction
- wellheads and Christmas trees
- shutdown and control philosophy and equipment
- down-hole equipment
- gas lift
- cuttings re-injection.

If the facility produces from subsea wells, then the information should include details of the key subsea components, such as:

- flowlines, manifolds, and risers
- subsea structures
- control systems
- umbilicals
- for pipes refer to section 3.3.10, p30.

The facility description should describe the planned methods for drilling and completing the wells, if relevant, including descriptions of the facilities that will be used to do this work. For subsea installations which are connected to a facility, the facility description should also cover the planned methods for constructing and installing the subsea structures and equipment, if relevant, including details of the vessels or facilities doing the work.

For subsea developments that are connected by licensed pipeline, all of this detail will need to be addressed in a safety case for the pipeline.

Where there is the potential for an overlap in the boundaries between two facilities (such as the case between licensed pipelines and production facilities), operators need to ensure that the overlap is recognised and that the FSA for each facility is compatible.

3.3.3 Production operations

The facility description should provide a description of the hydrocarbon production systems and their operation including design data. The content and level of detail needs to be adequate to gain an appreciation of the hazards posed by these systems and activities.

The information must be appropriate to the facility and the activities to be conducted at the facility and may address, but is not necessarily limited to, the following:

- process flow diagrams or utility flow diagrams
- stream data and mass balance information
- inventory data, including volumes of isolatable sections
- pressure vessel specifications
- equipment specifications e.g. pumps, compressors, etc.
- cause and effect charts
- process control
- related hazardous substances inventory data, including volumes of isolated and isolatable sections.

3.3.4 Utility operations

The facility description should provide a description of the utility systems and their operation including design data. The content and level of detail needs to be adequate to gain an appreciation of the hazards posed by these systems.

The information must be appropriate to the facility and the activities to be conducted at the facility and may address, but is not necessarily limited to, the following:

- power generation and distribution
- waste processing and disposal (sewerage, food, etc.)
- lighting (navigation, work area, etc.)

- communications (internal and external, voice and data)
- drains, sumps, caissons
- consumable production (potable water, nitrogen, rig air, etc.)
- heating, ventilation and air-conditioning
- laundry, galley and mess
- fuel storage and distribution (helicopter fuel, diesel, compressed gases, etc.)
- related hazardous substances inventory data, including volumes of isolated and isolatable sections.

Content requirement	
Reg 2.18(2)(a)	In particular, **the safety case must provide for** the communications systems of the facility to be adequate to handle: (i) a likely emergency on or relating to the facility; and (ii) the operation requirements of the facility.

This information is also required to give an understanding of any dependencies between safety systems and general utility systems, for example with regard to emergency electrical power.

3.3.5 Marine operations

The facility description should provide a description of the marine systems and their operation including design data. The content and level of detail needs to be adequate to gain an appreciation of the hazards posed by these systems and activities.

The information must be appropriate to the facility and the activities to be conducted at the facility and may address, but is not necessarily limited to, the following:

- stability management including: means of stability control, deck load limitations, draft limitations, damage stability, watertight integrity, software used to control/monitor stability and deck loading)
- ballast and bilge
- mooring
- jacking
- propulsion and steering
- dynamic positioning/station keeping
- cargo and offload (including workboat operations)
- related hazardous substances inventory data, including volumes of isolated and isolatable sections.

3.3.6 Drilling and well intervention operations

The facility description should provide a description of the drilling and well intervention systems and their operation including design data. The content and level of detail needs to be adequate to gain an appreciation of the hazards posed by these systems and activities.

The information must be appropriate to the facility and the activities to be conducted at the facility and may address, but is not necessarily limited to, the following:

- drill floor and derrick
- drilling fluid – mud storage, mixing, treatment, pumping, etc.

- tubular lifting and handling
- well testing
- coiled tubing
- Hydraulic work-over
- snubbing unit
- wireline
- HPHT well
- surface BOP
- under balance drilling (UBD) & managed pressure drilling (MPD)
- related hazardous substances inventory data, including volumes of isolated and isolatable sections.

3.3.7 Diving and ROV operations

The facility description should provide a description of the diving and ROV systems, this should extend to all associated key items of plant and equipment and their operation including design data. The content and level of detail needs to be adequate to gain an appreciation of the hazards posed by these systems and activities.

The information must be appropriate to the facility and the activities to be conducted at the facility and could address (but not be limited to):

- surface diving
- air diving
- mixed gas diving
- saturation diving
- mooring/diving from vessels in DP mode
- remotely Operated Vehicles
- related hazardous substances inventory data, including volumes of isolated and isolatable sections.

Examples of key plant and equipment to be described, include, but are not limited to launch and recovery systems, deck decompression/living chambers, bell handling systems, hyperbaric evacuation systems, diver breathing gas mixing/production systems, fire detection/protection systems, primary and secondary power systems, communications systems, (where appropriate to include communications between dive control and bridge/DP control/control room, ROV control, deck, crane, etc.), alarms, (to include DP status alarms where appropriate).

3.3.8 Lifting operations

The facility description should provide a description of the lifting systems and their operation including design data. The content and level of detail needs to be adequate to gain an appreciation of the hazards posed by these systems and activities.

The information must be appropriate to the facility and the activities to be conducted at the facility and may address, but is not necessarily limited to, the following:

- fixed lifting appliances – General purpose and specific purpose e.g.:
  - general Deck Cranes (offshore)
  - process train gantry cranes

  - BOP Cranes
  - stores cranes (shipboard)
  - forklifts
  - construction cranes
  - utility winches
  - man-riding winches (personnel transfer)
- portable and re-locatable lifting appliances (e.g. cherry picker)
- personnel lifting devices – e.g. man-riding cages, Billy Pugh's, lifting baskets, etc.
- davits dedicated to a craft (fast rescue craft, survival craft or workboats) should be described as part of the description of the craft.

3.3.9 Pipe-lay operations

The facility description should provide a description of the pipelay systems and their operation including design data. The content and level of detail needs to be adequate to gain an appreciation of the hazards posed by these systems and the associated activities.

The information must be appropriate to the facility and the activities to be conducted at the facility and may address, but is not necessarily limited to, the following:

- racking systems
- conveyors
- transfer modules
- bevelling systems
- line-up stations
- welding tunnels
- ramps
- field jointing systems
- tensioners
- NDT stations
- coating stations
- stern rollers
- stingers
- diving activities
- abandonment and recovery winches
- related hazardous substances inventory data, including volumes of isolated and isolatable sections.

3.3.10 Pipe operations

The facility description should provide a description of the piping systems connected to the facility and their operation including design data. Note that licensed pipelines are facilities in their own right, requiring a safety case. Therefore, both safety cases must describe the interfaces between the two facilities as well as the hazards posed by one facility on the other.

The content and level of detail needs to be adequate to gain an appreciation of the hazard potential of the pipeline systems to people at or near the facility. Pipeline safety cases must provide details of activities, including diving operations, which are envisaged to take place at or in connection with the facility.

In respect of pipes not requiring a license, these must be addressed in the safety case for the facility. The information must be appropriate to the facility and the activities to be conducted at the facility and may address, but is not necessarily limited to, the following:

- numbers, locations and battery limits
- diameters (internal and external) & lengths
- construction details (materials, wall thicknesses, pressure rating and schedule, etc.)
- process conditions across the expected range of production modes
- pressures and temperatures
- fluid compositions and flow rates
- related hazardous substances inventory data, including volumes of isolated and isolatable sections.

It should be noted that Regulation 2.21 contains specific requirements for controls associated with pipes as discussed in Section 3.4.6, p37.

3.3.11 Logistical support

The facility description should provide a description of the logistical support systems and their operation including design data. The content and level of detail needs to be adequate to gain an appreciation of the hazards posed by these systems and the associated activities.

The information must be appropriate to the facility and the activities to be conducted at the facility and may address, but is not necessarily limited to, the following:

- support vessel interaction (standby vessels, accommodation vessels, etc.)
- station-keeping capability
- aircraft interaction
- helidecks.

It should be noted that Regulation 2.22 contains specific requirements for controls associated with vessel and aircraft operations as discussed in Section 3.4.7, p37.

3.3.12 Construction, installation, and other operations

It is acknowledged that there is a range of specific activities utilising specialised machinery and equipment that is not covered elsewhere in this section.

The facility description should provide a description of such other systems and their operation including design data. The content and level of detail needs to be adequate to gain an appreciation of the hazard potential of the systems.

The information must be appropriate to the facility and the activities to be conducted at the facility and may address, but is not necessarily limited to, the following:

- construction, installation and retrieval of:
  - platform jacket and topsides
  - riser Turret, and Single Point Moorings
  - subsea infrastructure

- commissioning and decommissioning systems for facilities and parts thereof
- disconnection systems for FSOs and FPSOs
- petroleum product offloading systems
- related hazardous substances inventory data, including volumes of isolated and isolatable sections

3.4 Technical and other control measures

3.4.1 General considerations

Content requirement	
Reg 2.5(1)(b)	**The safety case for a facility must contain** a description of the facility that gives details of the technical and other control measures identified as a result of the formal safety assessment.

The extent to which the descriptions of technical and other controls are incorporated in the broader description of activities, machinery and equipment as discussed in the preceding section or separately described (in terms of a specific feature or sub-system) is not prescribed.

The descriptions of the control measures in the facility description should correspond to the functionality identified in the FSA as being required to ensure the control measure will effectively contribute to reducing risk to a level that is ALARP. (note; procedural control measures should be described in the SMS as discussed in section 5, p53).

The facility description must provide a description of the technical and other control measures and should include their operation and design data. The content and level of detail needs to be sufficient to gain an appreciation of the control measures identified in the FSA and, in general, should include:

- type of equipment used
- specification of the individual elements
- location of the equipment
- activation – how the various elements of the system are activated: automatically, by manual activation of ESD, or by local manual activation, etc.

Special cases or unusual arrangements should be clearly discussed as should the interdependencies between control measures.

Fire and explosion related systems

The following considerations are informed by the outcomes of the FERA, which is discussed in Section 4.5.2, p48.

The information must be appropriate to the facility and the activities to be conducted at the facility and may address, but is not necessarily limited to, the following:

- loss of containment prevention
- detection systems (fire, gas, smoke. etc.)
- ignition prevention (Hazardous Area Equipment, shutdown on gas detection, etc.)
- flammable atmosphere prevention (layout/congestion, ventilation etc.)
- fire and explosion protection – both passive and active (e.g. structural coatings, deluge, water curtain, water mist, CO_2, portable fire extinguishing equipment, support vessel equipment, fire walls, blast walls, etc.)

- emergency shutdown / blowdown / depressurisation / isolation
- pipeline isolation
- well control systems – blow out preventers, diverter, choke & kill, Koomey unit, etc.

Escape, evacuation and rescue equipment

The following considerations are informed by the outcomes of the EERA, which is discussed in section 4.5.1, p47.

The information must be appropriate to the facility and the activities to be conducted at the facility and may address, but is not necessarily limited to, the following:

- escape routes (primary and secondary) and muster points
- temporary safe refuges
- survival craft – lifeboats & life rafts (including float free capability where applicable)
- rescue craft e.g. Fast Rescue Craft, etc.
- hyperbaric evacuation/rescue systems
- communication systems (see also Section 3.4.4, p36)
- support vessels e.g. standby vessels
- mooring or dynamic positioning including emergency disconnection/move-off.

Mobile facilities

Mobile facilities must also specify the systems in place for shut down and disconnect, where relevant, in the event of an emergency within the facility description. It should also describe the systems for providing audible and visible warnings on shutting down or disconnect.

Content requirement	
Reg 2.20(6)	**The safety case for a mobile facility must also specify** systems that: (a) in the event of emergency, are adequate to shut down or disconnect all operations on the facility that could adversely affect the health or safety of persons at or near the facility; and (b) are adequate to give appropriate audible and visible warnings of the shutting down or disconnecting of those operations.

Design, construction, installation, maintenance and modification

Content requirement	
Reg 2.12(1)	**The safety case for a facility must describe** the means by which the operator will ensure the 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.

This is a very general requirement and is related to the safety management system description. This is discussed in the SMS section 5.2.5, p65.

However, subregulation 2.12(2) requires that the information provided in the facility description of the safety case should be sufficient to gain a full appreciation that the arrangements are adequate, or in other words 'equal to the requirement or occasion; fully sufficient, suitable or fit' for the stage or stages in the lifecycle of the facility for which the safety case is submitted.

The information must be appropriate to the facility and the activities to be conducted at the facility.

Level of detail requirement	
Reg 2.12(2)	In particular, the design, construction, installation, maintenance and modification of the facility must provide for: (a) adequate means of inventory isolation and pressure relief in the event of an emergency; and (b) adequate means of gaining access for servicing and maintenance of the facility and machinery and other equipment on board the facility; and (c) adequate means of maintaining the structural integrity of a facility; and (d) implementation of the technical and other control measures identified as a result of the formal safety assessment.

As highlighted earlier, the referencing of applicable standards and performance standards should be made with respect to technical and other control measures.

Guidance on control measures and the development of performance standards is given in the NOPSEMA Guidance Note: "Control Measures and Performance Standards".

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

In addition to the general requirements of OPGGS(S) subregulation 2.5(1)(b), subdivisions B and C (Safety Measures and Emergencies, respectively) also prescribe a number of content requirements.

3.4.2 Command structure

Reg 2.8(1)	For a facility that is manned, **the safety case must specify**: (a) an office or position at the facility, the occupant of which is in command of the facility and responsible for its safe operation when on duty; and (b) an office or position at the facility, the occupant of which is responsible for implementing and supervising procedures in the event of an emergency at the facility; and (c) the command structure that will apply in the event of an emergency at the facility. *Note: The same person may occupy both of the offices or positions mentioned in paragraph 1 (a) and (b).*

Note: regulation 2.8(2) is addressed in the SMS description Section 5.2.1, p62.

The safety case, usually the facility description, must provide a description of the command structure. The content and level of detail needs to be sufficient to gain an appreciation of the control measures identified in the FSA. The information must be appropriate to the facility and the activities to be conducted at the facility and may address, but is not necessarily limited to, the following:

- Emergency response organisation charts:

- facility level organisational structure (e.g. Station Bills)
- assets level organisational structure (e.g. incorporating the local support structure and interrelationship(s) with the facility level command structure)
- corporate level organisational structure (e.g. command structure for crisis management support for major emergencies).

For self-propelled mobile facilities such as some FPSOs and MODUs consideration needs to be given to the transition from facility to vessel / vessel to facility, and a discussion in the facility description of the command structures that apply, supported by applicable processes described in the SMS (see section 5.2.1, p62).

3.4.3 Medical and pharmaceutical supplies and services

Content requirement	
Reg 2.13	**The safety case for a facility must specify** the medical and pharmaceutical supplies and services, sufficient for an emergency situation, that must be maintained on, or in respect of, the facility.

The facility description must provide a description of specific medical and pharmaceutical supplies and services and should include their operation and design data, where relevant. The content and level of detail needs to be sufficient to gain an appreciation of the control measures identified in the FSA.

The information must be appropriate to the facility and the activities to be conducted at the facility and may address, but is not necessarily limited to, the following:

On the facility:

- hospital and/or sick bay fit out and equipment
- portable and field first aid stations and equipment
- hyperbaric medical equipment
- types of pharmaceutical supplies
- medical and first aid personnel resources
- medical and first aid services available on-board (personnel & facility combination).

In the field (e.g. from supply and standby vessels, etc.):

- hospital or sick bay
- medical and first aid personnel resources
- medical and first aid services available on-board (Personnel & vessel combination)

Arrangements with:

- local, regional and/or major hospitals
- providers of medical air transport services

3.4.4 Emergency communication systems

Content requirement	
Reg 2.18(1)	**The safety case for a facility must provide for** communications systems that, in the event of an emergency in connection with the facility, are adequate for communication: (a) within the facility; and (b) between the facility and: (i) appropriate on-shore installations; and (ii) appropriate vessels and aircraft; and (iii) other appropriate facilities.

The facility description must provide a description of the emergency communication systems and should include their operation and design data, where relevant. The content and level of detail needs to be sufficient to gain an appreciation of the control measures identified in the FSA.

The information must be appropriate to the facility and the activities to be conducted at the facility and may address, but is not necessarily limited to, the following:

Types of communication systems could include:

- radio (VHF, UHF, GMDSS, etc.)
- satellite
- internal telephone and Public Address
- data
- VOIP (video and voice).

Content requirement	
Reg 2.18(2)	In particular, **the safety case must provide for** the communications systems of the facility to be: (a) adequate to handle: (i) a likely emergency on or relating to the facility; and (ii) the operation requirements of the facility; and (b) protected so as to be capable of operation in an emergency to the extent specified in the Formal Safety Assessment relating to the facility.

In addition to the description of the communication systems themselves the above subregulation also requires the protection arrangements to be described. The description provided must be consistent with the requirements specified in the FSA. The information must be appropriate to the facility and the activities to be conducted at the facility and may address, but is not necessarily limited to, the following:

- provision of independent systems (fixed and/or portable)
- redundancy of systems (internal and external)
- passive and active protection
- location (and the extent to which the location provides protection to the system)
- EPIRBs and associated float free systems

3.4.5 Control systems

Content requirement	
Reg 2.19	**The safety case for a facility must make adequate provision for** the facility, in the event of an emergency, in respect of: (a) back-up power supply; and (b) lighting; and (c) alarm systems; and (d) ballast control; and (e) emergency shutdown systems.

The facility description must provide a description of the abovementioned control systems which should include their operation and design data. The content and level of detail needs to be sufficient to gain an appreciation of the control measures identified in the FSA.

The information must be appropriate to the facility and the activities to be conducted at the facility and may address, but is not necessarily limited to, the following:

- redundancy
- black start capabilities
- battery powered capabilities
- emergency power distribution (including what equipment is on the emergency switchboard).

3.4.6 Piping systems

Content requirement	
Reg 2.21(3)	**The safety case for a facility must also specify**: (a) adequate means of mitigating, in the event of emergency, the risks associated with each pipe connected to the facility; and (b) a frequency of periodic inspection and testing of pipe emergency shut-down valves that can reasonably be expected to ensure they will operate correctly in an emergency.

Note: regulation 2.21 is also addressed in the SMS description section 5.3.2, p69.

The facility description must provide descriptions that specify pipe risk mitigation controls and should include their operation and design data. The facility description must also specify the inspection and testing frequency of emergency shut-down valves associated with those pipes. The content and level of detail needs to be sufficient to gain an appreciation of the control measures identified in the FSA.

The information must be appropriate to the facility and the activities to be conducted at the facility and may address, but is not necessarily limited to, the following:

- emergency shut-down arrangements
- subsea isolation valves
- planned inspection schedules.

3.4.7 Vessel and aircraft control

Content Requirement	
Reg 2.22(1)	**The safety case for a facility must describe** a system, that is implemented or will be implemented, as part of the operation of the facility that ensures, as far as reasonably practicable, the safe performance of operations that involve vessels or aircraft.

Level of Detail Requirement	
Reg 2.22(2)	The system must be able to meet the emergency response requirements identified in the Formal Safety Assessment in relation to the facility and be described in the facility's Safety Management System.
Reg 2.22(3)	The equipment and procedures for ensuring safe vessel and aircraft operations must be fit for purpose.

Note: regulation 2.22 is also addressed in the SMS description section, 5.3.3, p69.

The facility description must provide a description of the vessel and aircraft control systems and should include their operation and design data. The content and level of detail needs to be sufficient to gain an appreciation of the control measures identified in the FSA.

The information must be appropriate to the facility and the activities to be conducted at the facility and could address (but not be limited to):

- radar/ARPA/AIS
- VHF/UHF radio.

3.5 Common weaknesses

The most common weaknesses in a facility description are:

- inclusion of vague statements, rather than specific facts about the facilities
- facility descriptions that are not aligned with the FSA
- including assertions about the overall acceptability of the facility design features independent of the risk assessment
- provision of too much operational detail so that the document is difficult to keep up to date
- discrepancies in facts provided
- discrepancies between text and figures/drawings
- poor cross-referencing internal to the document
- lack of QA
- illegible drawings/figures.

4 Formal Safety Assessment description

4.1 General considerations

Content requirement (FSA Overall)

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.

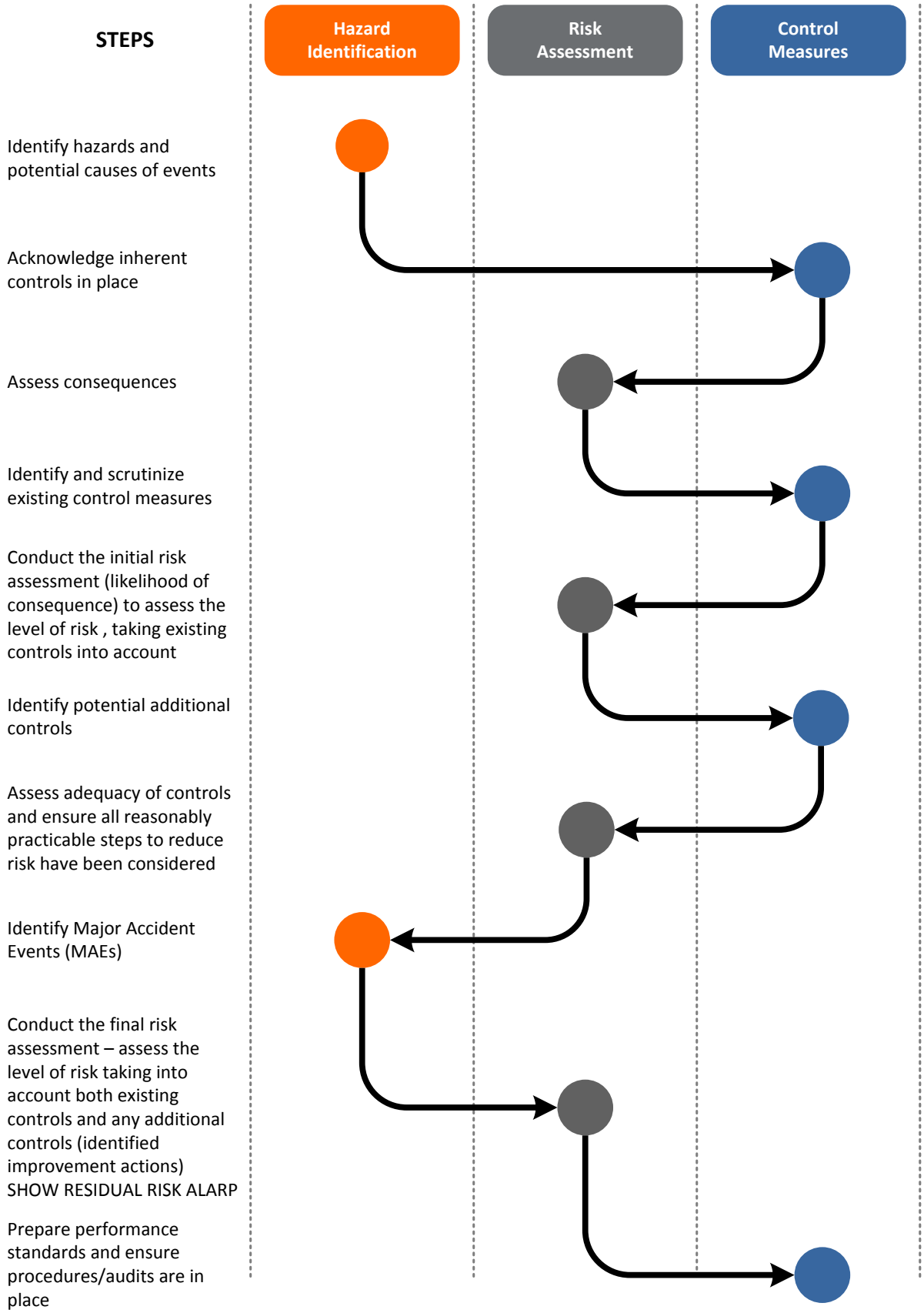
The formal safety assessment (FSA) is focused on major accident events (MAEs). Providing a well-considered, detailed description of a suitable and sufficient formal safety assessment within the safety case will enable operators to provide evidence of:

- an understanding of the factors that influence risk and the controls that are critical to managing risk
- the magnitude and severity of the consequences arising from major accident events for the range of possible outcomes
- the likelihood of potential major accident events
- clear linkages between hazards, the major accident events, control measures and the associated consequences and risk
- a prioritised list of actions that reduce risks to a level that is ALARP.

The steps for developing a safety case 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.

Because of this 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. The safety case should have a consistent, integrated overall structure: there should be logical flow to the assessment process to create strong links between the causes and consequences of major accident events, their associated risks, the selection of strategies and measures to control the risks, and the performance required from specific measures to maintain risk levels to ALARP. The intent here is to emphasise that the FSA must be a coherent, integrated assessment of major accident events. Spending time getting the structure right will greatly enhance an operator's ability to present evidence in a robust way that others can follow and understand. The FSA description in the safety case then is a description of the methodologies employed and a summary of the results: this would be a list of the MAEs and their controls. The actual description of the controls must then be described in be in the facility description (for technical controls) or the SMS description (for procedural based controls), as applicable.

Figure 3 – The FSA process



4.2 Hazard identification

Level of detail 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.

It is important to identify all hazards having the potential to cause a major accident event at the facility. Operators must apply appropriate hazard identification techniques, and in most cases a combination of different techniques will be required in order to ensure that the full range of factors is properly considered. The methodologies employed should be described in the safety case.

It is expected that the hazards are described in sufficient detail to allow differentiation between their impacts on different parts of a facility. That is, there must be sufficient links between a hazard and a MAE to show paths by which a MAE can be realised. Those hazards that may apply to many aspects/areas of a facility, e.g. corrosion of pipe work, may be grouped where appropriate. However, where the control measures used in relation to a hazard differ, these hazards should be detailed separately.

For any particular incident there may be several independent hazards or combinations of hazards, each of which could lead to that incident, as well as several control measures which may be particularly important because they may impact on one or more of those hazards. The description of the formal safety assessment should give an understanding of the likelihood of each incident and the relative importance of each control measure relating to a hazard. Operators may wish to consider using a matrix to show these inter-relationships.

A key output of the hazard identification is the documentation records, such as a hazard register, that lists all hazards identified with the potential to cause a major accident event, along with the underlying causes, control measures and any assumptions. This documentation should contain sufficient information to support later steps in the safety case development process; this will be especially important in cases where:

- the identified hazard is particularly complex;
- there is uncertainty as to the underlying causes of an incident;
- there is little or no operating experience in relation to the identified hazard; or
- the potential consequences of the MAE are particularly significant.

In any case, the information that is contained in the safety case must:

- identify all hazards with the potential to cause a major accident event (irrespective of likelihood or existing control measures)
- provide evidence that the operator and the workforce have sufficient knowledge, awareness and understanding of the causes of major accident events to be able to prevent and deal with emergencies
- provide a basis for identifying, evaluating, defining and justifying the selection (or rejection) of control measures for eliminating or reducing risk
- show clear links between hazards, causes and the potential major accident events
- provide a systematic record of all identified hazards and major accident events, together with any assumptions.

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

4.3 Risk assessment

Level of detail 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: (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.

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.

Whatever approach is used, it must be detailed and systematic. 'Detailed' in this instance is taken to mean the risk assessment must cover all hazards having the potential to cause a major accident event and must address all parts of the facility (identified in the hazard identification), and must address all of the aspects of risk for each MAE (nature, likelihood, consequence, etc.). The requirement to be systematic relates to the need to employ a logical, transparent and reproducible process, which enables the operator to compare the range of undesirable events and identify which are the most important contributors to the overall risk profile of the facility.

The risk assessment should use assessment methodologies (quantitative and/or qualitative) that are appropriate to the hazards being considered. Regardless of the methodologies employed, operators must clearly understand and describe the uncertainty present in the risk assessment. Uncertainty cannot always be eliminated, and it will be necessary to make assumptions in some areas. 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 each assumption
- explicitly recognise where the main gaps or uncertainties exist
- seek to reduce the level of uncertainty by testing assumptions, conducting more detailed studies as required, etc.

These aspects should be clearly described in the safety case. Where the level of uncertainty is high, operators should consider using sensitivity analysis to test the robustness of the risk assessment results against variations within the key areas of uncertainty.

If risk criteria are used as part of the assessment process, then operators will need to justify the selection of the risk criteria and show a clear linkage between the criteria and the arguments made that adopted controls are appropriate to reduce risk to a level that is ALARP.

It is important that the safety case shows that the risk associated with each hazard is considered. Consequently, the demonstration that the risks are eliminated or reduced to ALARP may need to be made for hazards individually and in groups. This has several aspects:

- The effects of several hazards occurring in combination must be considered, i.e. any chain of events, causes and contributing factors leading to an incident. In relation to this, the operator must give consideration to the possibility of common mode failure mechanisms which can cause several failures to occur simultaneously, significantly increasing the chances of an undesirable event.
- For any MAE there may be several independent hazards or combinations of hazards, each of which could lead to that event, and several control measures which may be particularly important because they may impact on one or more of those hazards. The risk assessment should give an understanding of the total likelihood of each MAE and the relative importance of each separate hazard and control measure.
- The potential for escalation of major accident events needs to be considered, i.e. the cumulative consequences of apparently separate events that may be triggered by each other.

These issues can be illustrated in the form of 'bow tie' diagrams that show how a range of causes, controls and outcomes can be linked together and associated with each MAE scenario. 'Full-blown' bowties can be very detailed and therefore should not be included in the safety case, however high level bowties can be very helpful to illustrate links.

Overall, the information that is contained in the safety case with respect to risk assessment must provide evidence that:

- the risk assessment addresses all potential major accident events and the hazards that could cause or contribute to causing those potential MAEs
- the risk assessment supplies the information necessary to determine which control measures to adopt and the necessary functioning of the safety management system with regard to major accident event hazards
- the risk assessment is detailed, systematic, rigorous and transparent
- appropriate members of the workforce are actively involved in safety case development
- the knowledge is kept up to date, through necessary processes of review and revision
- the information is provided to persons who require it in order to work safely, and respond and react appropriately during an emergency
- the risk assessment is used as a basis for adoption of control measures, including emergency planning.

MAEs should be assessed in a consistent manner and (as far as possible) using a common methodology. In this way the measure of risk will be expressed in common terms and the operator will be better able to make meaningful comparisons and objective decisions about the allocation of resources for risk reduction.

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

4.4 Control measures

Level of detail 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: (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.

Bear in mind that the physical description of plant and equipment identified in the FSA should be covered in the facility description section of the safety case and not repeated in the FSA section. The FSA should cross-reference to the appropriate facility description section. Similarly, the FSA section should cross-reference to the systems descriptions in the SMS section of the safety case for detailed descriptions of organisational or procedural controls.

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 should include discussion of the control measures selected (including how they contribute to reducing the risk) and those considered and rejected, and the reasons for not adopting these controls. In relation to technical control measures, the safety case should:

- provide evidence that control measures and their effects on risk are explicitly addressed
- provide evidence that a range of control measures was considered including existing and potential new control measures
- include sufficient detail to describe the circumstances in which these controls measures will be effective, including any associated limitations, for example, a deluge system may be suitable and effective for certain fire scenarios, however may not be effective for others. It may well be the limitations of the control measures which most influence the emergency response to any given scenario – therefore, it is important to have a good understanding of any shortcomings
- include discussion on the robustness of control measures, such as fault tolerance or safety integrity levels where appropriate
- for the description of procedural controls (e.g. PTW, JSA/JHA and MoC) – include sufficient detail of the main steps to describe how these processes contribute to reduction of risk
- reference applicable standards and performance standards.

The OPGGS(S) Regulations require the operator to make a commitment to ongoing improvement of all aspects of the operator's safety management system. Further, the regulations require the operator to implement control measures that reduce risks as low as reasonably practicable.

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

4.4.1 The ALARP argument

The concept of 'reasonably practicable' is central to the safety case regime. It allows operators and NOPSEMA to set goals for safety performance rather than be prescriptive. Determining whether a measure is reasonably practicable requires the operator to weigh up, on the one hand, the likelihood of the hazard causing harm to people, and the gravity of that harm, against the cost, time and trouble of removing or reducing the risk.

The formalised descriptions within the safety case must provide evidence that the control measures reduce risk to a level that is as low as reasonably practicable (ALARP), and that the SMS provides for reduction of risks to ALARP. A safety case must achieve this in a transparent and robust manner such that it will meet regulatory requirements to the reasonable satisfaction of NOPSEMA.

There is no prescribed methodology for demonstrating that the necessary control measures have been identified to reduce risks to ALARP. However there are several basic approaches which may be used to support an operator's provision of justification within the safety case. These include:

- case law
- risk acceptance criteria
- comparative assessment of risks, costs and benefits
- comparison with recognised codes and standards
- benchmark against good practice
- best available technology
- clear description and justification for rejection of control measures
- performance of control measures
- LOPA (Layers of Protection Analysis)
- engineering judgement approach
- practical tests of equipment or systems in situ.

In practice, it is likely that most operators will need to use a combination of approaches in their demonstration of ALARP.

For safety case acceptance purposes, NOPSEMA will evaluate the operator's approach in terms of its robustness, transparency and appropriateness to the facility. The operator should therefore define the underlying rationale, criteria and decision-making basis for the case. The description must be convincing; this means that the rationale for deciding the completeness of the process should be supported and accompanied by all assumptions made and conclusions drawn. Where appropriate, it should present the results of supporting studies that have been performed. The description should provide evidence that the process was systematic which means that it followed a fixed and pre-established scope. Finally, the degree of analysis in support of the demonstration should be proportionate to the risk and to the complexity of the facility, hazards and the control measures.

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

4.5 Supporting studies

There are many types of risk studies that can be carried out in support of a safety case (e.g. survivability studies, human factors, dropped objects, marine operations, etc.) however both a fire and explosion risk analysis, and an evacuation, escape and rescue analysis are specifically required by the OPGGS(S) Regulations. 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. As noted in the OPGGS(S) Regulations in so far as both of these prescribed studies address major accident events, they form a part of the formal safety assessment.

4.5.1 Evacuation, escape and rescue analysis

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

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) subregulation 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)	(a)	The evacuation, escape and rescue analysis must 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 hazard identification outputs.

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; and
	(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; and
	(f)	consider a range of amenities and means of emergency communication to be provided in a temporary refuge; and
	(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.

Note that a *range* of measures must be considered as specified in this subregulation. The content and level of detail needs to be sufficient to gain an appreciation of the scope and process for undertaking the consideration including sources of data and rationale for excluding or discounting items from consideration.

The considerations must be appropriate to the facility and the activities to be conducted at the facility and address all potential major accident events that could require evacuation, escape and/or rescue.

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.

The content and level of detail needs for these controls are essentially the same as the more general requirement discussed in section 0, p45.

Note that the detailed description of the control measures identified belong in the facility description (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.

4.5.2 Fire and explosion risk analysis

For fire and explosion risks, the OPGGS(S) Regulations call for an analysis to be carried out as part of the FSA, and for detailed descriptions of these analyses to be in the safety case.

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

Similarly, it is important that the description in the safety case provides enough information to give assurance to NOPSEMA that all the requirements of the analysis, as given in OPGGS(S) subregulation 2.17(2), have been met.

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 content and level of detail needs to be adequate for NOPSEMA to gain an appreciation that the study is aligned with the hazard identification outputs.

The information must be appropriate to the facility and the activities to be conducted at the facility and address all potential fire and explosion related major accident events.

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

(iii) leaks or escapes of flammable greenhouse gas; 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; and

(f) consider the evacuation, escape and rescue analysis, in so far as it relates to fires and explosions.

Note that a *range* of measures must be considered as specified in this subregulation. The content and level of detail needs to be adequate for NOPSEMA to gain an appreciation of the scope and process for undertaking the consideration including sources of data and rationale for excluding or discounting items from consideration.

The considerations must be appropriate to the facility and the activities to be conducted at the facility and address all potential fire and explosion related major accident events.

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 content and level of detail needs for these controls are essentially the same as the more general requirement discussed in section 0, p45.

Note that the detailed description of the control measures identified belong in the facility description or SMS description sections of the safety case which relevant parts of the FSA description should cross-reference.

Further guidance is available in the NOPSEMA guidance note:
'Supporting Safety Studies'

4.6 Common failings in Formal Safety Assessment

4.6.1 FSA process

Common failings in the FSA include:

General

- inadequate linkages to the facility description and layout drawings
- The FSA not addressing all of the expected activities at the facility
- no consideration of organisational failure potential: An effective safety case will include consideration of the organisation as a whole, not just the operational engineering aspects, in determining causes of hazards and risk control strategies. Many safety cases are excessively focussed on engineering hardware and systems
- inadequate or weak linkages between separate studies within the FSA
- inadequate links between hazards, risks, control measures (hardware and software) and the safety management system: Since the safety management system is the primary way in which risks are controlled during the operational phase of a facility, the links between the hazards, main risk contributors and measures in place to control them must be detailed and explicit. Some safety cases make very general statements about how risks are managed, and do not provide links between the FSA and the SMS.

Insufficient detail

- in relation to risk studies conducted as part of a formal safety assessment, it is not sufficient to simply list and reference the various HAZID and HAZOP workshops and indicate that the outcomes from these workshops have been addressed. Likewise, it is not sufficient to simply indicate in the safety case that a risk study will be conducted (other than where these relate to every-day risk assessment tasks such as Job Safety Analysis, Permit To Work, etc.)

Too much detail

- it is not appropriate to include all of the risk studies in full within the safety case. This does not constitute a 'detailed description'
- it is expected that a summary of a risk study within the formal safety assessment will include:
  - details of personnel involved in the risk study, clearly demonstrating involvement by members of the workforce (where appropriate) and involvement of personnel with experience and knowledge appropriate to issues being considered
  - a description of the major outcomes of the risk studies, including identification of hazards with the potential to lead to MAEs, control measures considered and rejected/adopted, and major recommendations
- while a summary of a risk study within a description of the FSA may identify action items to be completed (as identified at that stage in the process), the safety case must also address how all of these items have been, or will be, appropriately closed out before activities commence
- in summary, the description of the formal safety assessment should include a sufficient level of detail for the safety case to be considered a 'stand-alone' document.

Further information in relation to tools and techniques for hazard identification and risk assessment can be found in ISO17776.

4.6.2 Hazard identification stage

Common failings in the Hazard Identification include:

- not considering human error as a potential cause of hazardous events
- failing to consider the hazardous events that may arise during maintenance
- failing to consider common mode failure
- failing to consider escalation
- assuming that events that have never occurred cannot occur
- assuming that MAEs are no longer considered MAEs if appropriate risk control measures are in place (e.g. engine room fire for vessels).

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

4.6.3 Risk assessment stage

Common failings in risk assessment include:

- underestimating the risk by assuming that all risk control measures function perfectly
- results of supporting studies that have been performed are not presented (where appropriate)
- the description does not provide evidence that the process was systematic which means that it followed a fixed and pre-established scope
- failure to provide evidence that a range of measures for risk reduction have been considered in the fire and explosion analysis
- failure to provide evidence that a range of measures for risk reduction have been considered in the evacuation, escape and rescue analysis.

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

4.6.4 Control measure identification

Common failings in control measure identification include:

- Only trivial or inappropriate risk reduction measures considered for implementation: Risks are not considered to be ALARP until they have been subjected to the ALARP process. This means that additional risk controls must be identified, if possible, and considered explicitly.
- Insufficient workforce involvement: The safety case must address the actual condition of risk controls on the facility, including the implementation of the safety management system. Consequently, workforce involvement is essential.

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

4.6.5 Evidence of ALARP

Common failings in demonstrating ALARP include:

- no justification is provided; the operator has not defined the underlying rationale, criteria and decision-making basis for the case
- the description is not convincing; i.e. the rationale for deciding the completeness of the hazard identification and the adequacy of the measures employed is not supported and accompanied by all assumptions made and conclusions drawn

- the operator's approach to providing evidence is not robust or transparent and/or appropriate to the facility
- the degree of analysis in support of the demonstration is not proportionate to the risk and to the complexity of the facility, hazards and the control measures
- over-reliance on QRA results to show that risks are ALARP, or arguing that ALARP is achieved because the QRA gives numerical results below a certain number. An argument aimed at showing that risk is as low as reasonably practicable requires a broad consideration of risk and safety management issues, not just a numerical calculation
- simply stating that the risk is ALARP because it falls within the 'ALARP Region' of the 'ALARP triangle'. This simply serves to show that further consideration of potentially practicable risk reduction options is required. Only after all other potential risk reduction measures have been exhausted (considered and either adopted or rejected on the basis of reasonable practicability) can an operator hope to claim that the risk has been reduced to a level that is ALARP
- over-reliance on codes and standards as evidence that risks are ALARP: Codes and standards are important in managing risk as they represent the industry knowledge in order to prevent past accidents from being repeated. The role of the safety case is to try to minimise the potential for all incidents, including those that have not occurred previously and those that are unique to a particular site or facility. Compliance with codes and standards alone cannot address risk management for the full range of things that might go wrong.

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

5 Safety Management System description

5.1 General requirements

5.1.1 Description of the SMS

Content requirement	
Reg 2.5(3)	**The safety case for the facility must also contain a detailed description** of the safety management system that: (a) is comprehensive and integrated; and (b) provides for all activities that will, or are likely to, take place at, or in connection with, the facility; and (c) provides for the continual and systematic identification of hazards to health and safety of persons at or near the facility; and (d) 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; 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; and (f) provides for inspection, testing and maintenance of the equipment and hardware that are the physical control measures for those risks; and (g) provides for adequate communications between the facility and any relevant: (i) facility; or (ii) vessel; or (iii) aircraft; or (iv) on-shore installation; and (h) provides for any other matter that is necessary to ensure that the safety management system meets the requirements and objects of these Regulations; and (i) specifies the performance standards that apply.

Note that this is taken to mean that the SMS itself must meet the requirements of items (a) to (i), not necessarily the detailed description. It is the intent of the regulations that the detailed description provides evidence that all these matters are addressed in the SMS, using samples/examples where appropriate. It is not intended that the detailed description of the SMS in the safety case include the entire SMS.

Example: Performance standards that apply

It is the SMS itself which must specify the performance standards that apply, not the detailed description of the SMS in the safety case. However, the detailed description of the SMS in the safety case must provide sufficient evidence to demonstrate to NOPSEMA that the SMS specifies the performance standards that apply.

5.1.2 Level of detail

The safety case must provide sufficient information to describe the major aspects of the safety management system and explain how these aspects contribute to reducing the risks to health and safety of people at and near the facility. The description should provide a summary of processes specific to the operations that are in place, or will be in place. These include, but are not limited to:

- training and competency
- communications
- hazard identification and risk assessment
- management of change
- permit to work
- inspection, testing, maintenance and repair
- evacuation, escape and rescue
- performance standards applied

It is expected that the detailed description will provide sufficient information to demonstrate that the safety management system is comprehensive and integrated, using samples/examples where appropriate.

The safety case should also describe how the safety management system is or will be implemented, and how deficiencies are continually and systematically identified and addressed to achieve ongoing improvement. The description of the SMS should provide adequate linkages between the hazards identified in the formal safety assessment and the elements of the safety management system used to manage the risks from those hazards.

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 major accident events. While specific OHS risk control measures are not required to be presented in detail in the safety case, evidence must be provided for NOPSEMA to be assured that the safety management system for a facility meets the requirements of OPGGS(S) subregulation 2.5(3) with respect to OHS hazards and risks. Operators should therefore describe the systems in place for effective risk management of OHS hazards within the SMS description including, for example, how they are identified, analysed, evaluated, treated, communicated and monitored such that OHS risks are managed to a level that is ALARP. By way of evidence, operators may choose to provide specific examples of how this is done in practice. However, emphasis should be on the system description rather than provision of detailed plans or procedures within the safety case.

It is recommended that rather than including full policies and procedures within the SMS section of the safety case, operators simply include a detailed description and provide references to the SMS documents. Any subsequent inspection by a NOPSEMA inspector will be of the SMS itself (i.e. the referenced documents) rather than of the description provided in the safety case. One exception to this recommendation is the OHS policy required to be developed under clause 9(2)(i) of Schedule 3 to the Act.

An operator's duties under Schedule 3 to the OPGGSA include agreement on an occupational health and safety policy that will enable the operator and the workforce to develop measures to ensure health and safety at the facility. The policy includes providing adequate mechanisms for reviewing the effectiveness of measures to ensure health and safety. The policy must be available to the workforce, and as the safety case is the primary safety document for the facility, operators may wish to include it within the safety case however there is no regulatory requirement to do so.

Applicable SMS documents and performance standards should be referenced.

Further guidance is available in the NOPSEMA guidance note:
'Safety Management Systems (SMS)'

5.1.3 Comprehensive and integrated

Level of detail requirement	
Reg 2.5(3)	**The safety case for the facility must also contain a detailed description** of the safety management system that: (a) is comprehensive and integrated.

The content and level of detail needs to be adequate for NOPSEMA to gain an appreciation of coverage and extent to which the elements of the SMS are linked in a logical manner.

The information must be appropriate to the facility and the activities to be conducted at the facility and may address, but is not necessarily limited to, the following:

- a description of the overall structure of the SMS including hierarchy and dependencies as well as key system policies
- interrelationships and dependencies between the various aspects of the SMS
- relationships between the facility, local, regional and/or corporate elements of the SMS.

Example: SMS that is insufficiently comprehensive

A safety case contains a description of the SMS that includes a detailed description of how changes to hardware and processes are managed to ensure any new hazards are identified, risks assessed and appropriate control measures identified necessary to ensure risk are reduced to ALARP. There is however no coverage of a similar process applied to personnel / position change.

On the basis that both temporary and permanent changes in personnel and/or positions have a range of implications for the management of safety on a facility, this aspect of the SMS is unlikely to be considered as comprehensive.

Example: SMS that is insufficiently comprehensive

A safety case for simultaneous drilling and diving operations contains a description of the SMS that includes a detailed description of the drilling operator's facility SMS, however it only makes reference to the diving contractor having a NOPSEMA accepted Diving Safety Management System (DSMS) in place, and fails to detail the steps taken by the operator to determine the suitability and sufficiency of the or how conflicts between the safety case and the DSMS will be managed.

Not describing the diving contractors SMS and the interface between operations can result in confusion and lack of clarity with respect to roles and responsibilities for safety management.

5.1.4 Scope of the SMS

Level of detail requirement	
Reg 2.5(3)	**The safety case for the facility must also contain a detailed description** of the safety management system that: (b) provides for all activities that will, or are likely to, take place at, or in connection with, the facility.

An operator must be able to describe an SMS that will ensure effective control of health and safety across all stages in the life of the facility for which the safety case is submitted. The SMS itself must be sufficiently broad and detailed to cover all aspects of the management of health and safety.

The information must be appropriate to the facility and the activities to be conducted at the facility and may address, but is not necessarily limited to, the following:

- well and subsea operations
- production operations
- utility operations
- marine operations
- drilling and well intervention operations
- diving and ROV operations
- lifting operations
- pipe-lay operations
- pipe-line operations
- logistical support
- occupational health and hygiene.

5.1.5 Hazard identification and risk management

Level of detail requirement	
Reg 2.5(3)	**The safety case for the facility must also contain a detailed description** of the safety management system that: (c) provides for the continual and systematic identification of hazards to health and safety of persons at or near the facility; and (d) 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; 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 description of the SMS must provide descriptions of actual planned arrangements (policies, procedures, etc.) for hazard identification and risk management. The content and level of detail needs to be adequate to gain an appreciation of hazard identification and risk management processes for all hazards. The information must be appropriate to the facility and the activities to be conducted at the facility and may address, but is not necessarily limited to, the following:

- HAZID and HAZOP processes
- JSA/JHA processes
- observational hazard identification programs
- qualitative and quantitative risk assessment processes
- risk reduction and control evaluation processes
- inclusion of non-MAE examples (e.g. Noise, Fatigue, NORMs, etc.)

The operator should be able to demonstrate that, by following the SMS, each hazard has a cohesive set of control measures, and these are further defined in performance standards for each measure.

5.1.6 Inspection, testing and maintenance

Level of detail requirement	
Reg 2.5(3)	**The safety case for the facility must also contain a detailed description** of the safety management system that: (f) provides for inspection, testing and maintenance of the equipment and hardware that are the physical control measures for those risks.

Content requirement	
Reg 2.21(3)	**The safety case for a facility must also specify:** (b) a frequency of periodic inspection and testing of pipe emergency shut-down valves that can reasonably be expected to ensure that they will operate correctly in an emergency.

The description of the SMS must provide descriptions of actual planned arrangements (policies, procedures etc.) for inspection, testing and maintenance. The content and level of detail needs to be adequate to gain an appreciation of inspection, testing and maintenance processes.

The information must be appropriate to the facility and the activities to be conducted at the facility and may address, but is not necessarily limited to, the following:

- criticality and prioritisation
- planning
- maintenance management software
- pipe ESD inspection and testing program

5.1.7 Communications

Level of detail requirement

Reg 2.5(3) **The safety case for the facility must also contain a detailed description** of the safety management system that:

(g) provides for adequate communications between the facility and any relevant:

(i) facility; or

(ii) vessel; or

(iii) aircraft; or

(iv) on-shore installations

(iv) onshore installation.

The description of the SMS must provide descriptions of actual planned arrangements (policies, procedures, etc.) for communications. The content and level of detail needs to be adequate to gain an appreciation of communication processes.

The information must be appropriate to the facility and the activities to be conducted at the facility and may address communication protocols for:

- simultaneous and combined operations
- managing vessels offloading supplies to the facility or offloading petroleum from a facility
- flight following
- liaison with connected onshore facilities.

5.1.8 Objects of the regulations

Level of detail requirement

Reg 2.5(3) **The safety case for the facility must also contain a detailed description** of the safety management system that:

(h) provides for any other matter that is necessary to ensure that the safety management system meets the requirements and objects of these Regulations.

Reg 1.4(1) *An object of these Regulations is to ensure that offshore petroleum facilities are designed, constructed, installed, operated, modified and decommissioned in Commonwealth waters only in accordance with safety cases that have been accepted by NOPSEMA.*

(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.

(3) *An object of these Regulations is to ensure that the risks to the health and safety of persons at offshore petroleum facilities are reduced to a level that is as low as reasonably practicable.*

The description of the SMS should provide descriptions of planned arrangements (policies, procedures, etc.) for any other activities that may contribute to meeting the objects of the regulations. The content and level of detail needs to be adequate to gain an appreciation of such processes.

It should be recognised that this is effectively a 'catch all' and as such is a reminder to operators to carefully consider the extent to which the case for safety effectively addresses all the objects, notwithstanding the prescribed content and level of detail requirements imposed by regulations 2.5 through 2.23.

It should be noted that OPGGS(S) subregulation 1.4(2)(d) is effectively a reminder of the some of the considerations that should be taken into account when addressing the requirements of Regulation 2.6 relating to SMS implementation and improvement (see 5.1.10, p60).

5.1.9 Performance standards

Level of detail requirement	
Reg 2.5(3)	**The safety case for the facility must also contain a detailed description** of the safety management system that: (i) specifies the performance standards that apply.

The description of the SMS should provide descriptions of actual planned arrangements (policies, procedures etc.) for developing and setting performance standards. The content and level of detail needs to be adequate to gain an appreciation of the processes that are applied.

The information must be appropriate to the facility and the activities to be conducted at the facility and may address, but is not necessarily limited to, the following:

- process for development of performance standards
- structure and content, e.g. the extent to which the following aspects are considered:
  - functionality
  - reliability / availability
  - survivability, and
  - maintainability
- listing of actual standards
- usage of performance standards (e.g. linkages into inspection, testing and maintenance programs and routines, emergency response plans etc.).
- examples of the content of selected performance standards (e.g. samples for both hardware related and procedural controls).

A complete set of performance standards is not required as part of a safety case submission. However, as with the facility description, references to applicable performance standards should be explicitly included throughout the SMS description.

5.1.10 SMS implementation

Content requirement	
Reg 2.6	**The safety case for a facility must demonstrate** that there are effective means of ensuring: (a) the implementation of the safety management system; and (b) continual and systematic identification of deficiencies in the safety management system; and (c) continual and systematic improvement of the safety management system.

The description of the SMS should provide descriptions of actual planned arrangements (policies, procedures etc.) for implementation of the SMS. The content and level of detail need to be adequate to gain an appreciation of SMS implementation processes. The information must be appropriate to the facility and the activities to be conducted at the facility and may address, but is not necessarily limited to, the following:

- induction and training in the SMS
- key performance indicators for the SMS
- audit and review processes
- corrective and preventative action management
- management of change processes for the SMS
- organisational learning processes

In the case of new facilities, facilities that have changed operator, or facilities new to Australian waters, there may be a transition period required before the operator's safety management system is fully implemented as per the safety case. In the case of a new workforce, this transition period may also apply to the requirement for the safety case to provide 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 me exposed on the facility [OPGGS(S) subregulation 2.11(b)]. This proposed transition period does not mean operators can operate their facilities at an increased risk level; activities not covered by the SMS in place should not be carried out until such time as the corresponding SMS elements are fully implemented. There are some instances where planned future activities such as diving, well interventions, etc. may be described in the safety case without the accompanying SMS controls being in place. This is illustrated by the following example.

Example: Diving activities

Diving operations are envisaged to be required by an operator at his facility at some time in the foreseeable future, however work involving diving is not planned to take place within the next 12 months. Although details of the planned diving activities are described within the facility's safety case, as the work is not to be carried out immediately, the associated SMS controls do not necessarily need to be in place until the activities are to be conducted. However, the safety case should clearly state that a revision to the safety case will be submitted to NOPSEMA (and accepted) prior to conducting any diving activities.

In practice, there are very few activities that can be carried out without the SMS being fully implemented. Operator commitments made in the safety case will be verified during NOPSEMA planned inspections and the operator is reminded that NOPSEMA may withdraw acceptance of the safety case for a facility on the grounds of non-compliance with Schedule 3 to the Act [OPGGS(S) Regulation 2.37].

5.1.11 Standards to be applied

Content requirement	
Reg 2.7	**The safety case for a facility must specify** all Australian and international standards that have been applied, or will be applied, in relation to the facility or plant used on or in connection with the facility for the relevant stage or stages in the life of the facility for which the case is submitted.

Note: regulation 2.7 is also addressed in the facility description Section 3.1.4, p19.

Similarly to the facility description, the description of SMS in the safety case should include references to the standards that have been applied. Simply providing a listing of standards without discussing the relevance of the standards in their application does not provide the evidence required to demonstrate appropriateness of the control measures they apply. Operators may choose to put a consolidated list of applied standards in the safety case document reference section, but this list should not live by itself in the text of the safety case.

Whatever standard or set of standards is used, the operator should take care to justify applicability and recognise limitations of those standards.

The information must be appropriate to the facility and the activities to be conducted at the facility and may address, but is not necessarily limited to, the following:

- Standards that address topics such as:
  - training and competency
  - management systems
  - auditing
  - operational activities
  - maintenance and servicing
  - testing and inspection
  - design, construction and installation.
- Published by bodies such as:
  - National and International Standards Associations
  - NOHSC
  - OLF
  - IADC
  - OGP
  - APPEA.

5.1.12 Means to ensure on-going integrity of technical and other control measures (5 Year revisions)

Content requirement	
Reg 2.32(2)	**A revised safety case submitted under this regulation must describe** the means by which the operator will ensure the on-going integrity of the technical and other control measures identified by the formal safety assessment.

This requirement is specific to 5 yearly revisions. The description of the SMS should provide descriptions of actual planned arrangements (policies, procedures, etc.) for ensuring the ongoing integrity of technical and other control measure. The content and level of detail needs to be adequate to gain an appreciation of SMS implementation processes.

The information must be appropriate to the facility and the activities to be conducted at the facility and may address, but is not necessarily limited to, the following processes that consider and act on the outcomes of periodic reviews of:

- major hazards
- performance standards and deviations from them
- manual override System data
- planned maintenance system data
- SMS audits and reviews
- class and other third party survey and inspection results

5.2 Safety measures

As well as the safety case content requirements called for under OPGGS(S) Regulations 2.5 and 2.6, there are various specific content requirements detailed under regulations 2.7 through 2.23 that are somewhat more prescriptive in nature.

It is useful to note at this point that OPGGS(S) Regulations 2.7 to 2.23 all impose requirements for the safety case to describe or specify or make provision for certain matters, but only regulations 2.10 (PTW) and 2.22 (vessel & aircraft control) explicitly state that the relevant matters must be part of the SMS.

In practice, however, all the relevant matters should be addressed in the SMS in order to meet the requirement that the SMS is "comprehensive and integrated". Thus the SMS should contain or refer to the methods of conducting a fire and explosion risk analysis and an evacuation, escape and rescue analysis. Similarly, the SMS should contain or refer to the design standards for the facility, as well as standards relevant to the stage(s) in the life of the facility for which the safety case is submitted.

Depending on the nature of the safety measures, some descriptions may sit better within the facility description rather than the SMS description in the safety case. A compliance matrix, or table, detailing which section(s) of the safety case submission address each of the requirements of OPGGS(S) Regulations 2.5 to 2.23; can assist in locating the information and in demonstrating that all of the regulatory requirements for the submission have been met. Operators may wish to compile a compliance matrix to check the completeness of their safety case submission and to facilitate the assessment process. An example of a simple concordance table is shown in Appendix A; a comprehensive and editable version is available to download from the NOPSEMA website (www.nopsema.gov.au).

5.2.1 Command structure

Content requirement	
Reg 2.8(2)	**The safety case must also describe**, in detail, the means by which the operator will ensure that, as far as reasonably practicable: (a) the offices or positions mentioned in subregulation (1) are continuously occupied while the facility is in operation; and (b) the person who occupies each office or position mentioned in subregulation (1) has the necessary skills, training and ability to perform the functions of the office or position; and (c) the identity of the persons who occupy each office or position, and the command structure can, at all times, be readily ascertained by any person at the facility.

Where Reg 2.8(1) states:

For a facility that is manned, the safety case must specify:

(a) an office or position at the facility, the occupant of which is in command of the facility and responsible for its safe operation when on duty; and

(b) an office or position at the facility, the occupant of which is responsible for implementing and supervising procedures in the event of an emergency at the facility; and

(c) the command structure that will apply in the event of an emergency at the facility.

Note The same person may occupy both of the offices or positions mentioned in paragraph 1 (a) and (b).

Note: regulation 2.8(1) is addressed in the facility description Section 3.4.2, p34.

The description of the SMS should provide descriptions of actual planned arrangements (policies, procedures etc.) associated with the command structure. The content and level of detail needs to be adequate to gain an appreciation of command structure management processes.

The information must be appropriate to the facility and the activities to be conducted at the facility and may address, but is not necessarily limited to, the following:

- Human resource processes (recruitment, retention etc.)
- Training and competency processes
- Applicable job descriptions
- Training and competency requirements for the positions

5.2.2 Members of the workforce must be competent

Content requirement

Reg 2.9 **The safety case for a facility must describe** the means by which the operator will ensure that each member of the workforce at the facility has the necessary skills, training and ability:

(a) to undertake routine and non-routine tasks that might reasonably be given to him or her:

(i) in normal operating conditions; and

(ii) in abnormal or emergency conditions; and

(iii) during any changes to the facility; and

(b) to respond and react appropriately, and at the level that might be reasonably required of him or her, during an emergency.

The description of the SMS should provide descriptions of actual planned arrangements (policies, procedures etc.) workforce competency. The content and level of detail needs to be adequate to gain an appreciation of workforce competency processes.

The information must be appropriate to the facility and the activities to be conducted at the facility and may address, but is not necessarily limited to, the following:

- recruitment and retention
- training and competency
- links with emergency response plans

- links with drill and exercises
- compliance monitoring
- training and competency management software
- example records of:
  - job descriptions
  - training and competency requirements.

5.2.3 Permit to work system for safe performance of various activities

Content requirement	
Reg 2.10(1)	**The safety case for a facility must provide for** the operator of the facility to establish and maintain a documented system of coordinating and controlling the safe performance of all work activities of members of the workforce at the facility, including in particular: (a) welding and other hot work; and (b) cold work (including physical isolation); and (c) electrical work (including electrical isolation); and (d) entry into, and working in a confined space; and (e) procedures for working over water; and (f) diving operations.

Level of detail requirement	
Reg 2.10(2)	**The system must**: (a) form part of the Safety Management System described in the safety case in force for the facility; and (b) identify the persons having responsibility to authorize and supervise work; and (c) ensure that members of the workforce are competent in the application of the permit to work system.

The description of the SMS should provide descriptions of actual planned arrangements (policies, procedures etc.) for the permit to work system. The content and level of detail needs to be adequate to gain an appreciation of the permit to work system.

The information must be appropriate to the facility and the activities to be conducted at the facility and may address, but is not necessarily limited to, the following:

- overview of the system (objects, roles and responsibilities, etc.)
- permit types and uses
- management and operation of the system
- links with training and competency systems
- examples of a selection of permits types

5.2.4 Workforce involvement – provisions of the SMS

Content requirement	
Reg 2.11(1)	**The operator of a facility must demonstrate** to NOPSEMA, to the reasonable satisfaction of NOPSEMA, that: (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.

The workforce needs to be provided with information so they understand what actions to take to support safe operation, and to minimise the effect on health and safety of people in the event of an emergency. Involvement of employees in the specified activities supports the following key objectives:

- An understanding is developed of the hazards and risks, and informed decisions are made concerning the control measures and safety management systems implemented to control these risks.
- Members of the workforce are fully informed about the risks to which they may be exposed, about the control measures and safety management system which provide the means of eliminating or reducing those risks, and about the safety case which presents the demonstrations and arguments for adequacy of the SMS and control measures.

Meeting the above objectives can expect to result in members of the workforce who have an active role in implementing the controls and safety management systems, and are also better aware of their own responsibilities.

The description of the SMS should provide descriptions of actual planned arrangements (policies, procedures etc.) for involving members of the workforce. The content and level of detail needs to be adequate to gain an appreciation of the workforce involvement arrangements.

The information must be appropriate to the facility and the activities to be conducted at the facility and may address, but is not necessarily limited to, the following:

- safety case development processes
- inductions
- hazard identification and risk management process (project and task level)
- workplace arrangements.

5.2.5 Design, construction, installation, maintenance and modification (SMS)

Content requirement	
Reg 2.12(1)	**The safety case for a facility must describe the means** by which the operator will ensure the 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.

Note: subregulation 2.12(2) is addressed in the facility description Section, 3.4.1, p32.

The information provided in the description of the SMS should give descriptions of actual and planned arrangements (policies, procedures, etc.) for design, construction and installation of the facility in the first place, and maintenance and modification of the facility on an ongoing basis.

The content and level of detail needs to be adequate to gain an appreciation of the processes employed and how hazard identification and risk assessment are incorporated such that risks are reduced to a level that is ALARP in the original design and maintained ALARP throughout the lifecycle of the facility.

The descriptions should describe both the design and the operating considerations for facility systems, taking into account applicable standards and codes of practice where appropriate as a means of addressing adequacy. These descriptions will link to performance standards set for control measures and demonstration that machinery and equipment is fit for its function, that systems function as intended, and that they are adequately maintained.

The SMS description should also give details of the procedures and administrative controls in place to ensure that the design envelope is not breached, or if it is, the measures in place for bringing the situation back under control. The maintenance management system description and the management of change procedure description are of particular importance here and care should be taken to describe them in sufficient detail to give NOPSEMA satisfaction that they are adequate and appropriate for the facility and the activities to be conducted at the facility.

ISO 10418 provides further guidance on basic surface process safety systems for offshore petroleum production facilities.

5.2.6 Drugs and intoxicants

Content requirement	
Reg 2.15	**The safety case for a facility must describe the means** by which the operator will ensure that there is in place, or will be put in place, a method of: (a) securing, supplying, and monitoring the use of, therapeutic drugs on the facility; and (b) preventing the use of controlled substances (other than therapeutic drugs) on the facility; and (c) preventing the use of intoxicants on the facility.

The description of the SMS should provide descriptions of actual planned arrangements (policies, procedures, etc.) for managing drugs and intoxicants. The content and level of detail needs to be adequate to gain an appreciation of the drugs and intoxicant management processes.

The information must be appropriate to the facility and the activities to be conducted at the facility and may address, but is not necessarily limited to, the following:

- responsibilities and authorities, training and competency requirements
- dispensary processes
- pharmaceutical management processes including stock takes, disposal and auditing
- drug and alcohol testing processes

5.3 Emergencies

5.3.1 Emergency preparedness

Emergency Response Plan

Content requirement	
Reg 2.20(1)	**The safety case for a facility must** (a) **describe** a response plan designed to address possible emergencies, the risk of which has been identified in the formal safety assessment for the facility; and (b) **provide for** the implementation of that plan.

Level of detail requirement	
Reg 2.20(2)	**The plan must:** (a) **specify** all reasonably practicable steps to ensure the facility is safe and without risk to the health of persons likely to be on the facility at the time of the emergency; and (b) **specify** the performance standards that it applies.

The safety case should provide sufficient information to describe the major aspects of the emergency response plan and explain how these aspects contribute to reducing the risks from possible emergencies at the facility. The information must be appropriate to the facility and the activities to be conducted at the facility.

The description of the response plan should provide adequate linkages between the types of emergencies identified in the formal safety assessment and the elements of the response plan used to control the risks from those hazardous events.

The description should be sufficient to give NOPSEMA reasonable assurance that the plan specifies all reasonably practicable steps to ensure the facility is safe and without risk to the health of persons likely to be on the facility at the time of the emergency, and assurance that it meets the requirements of subregulation 2.20(2).

The requirements of OPGGS(S) Regulation 2.20 are closely linked with the requirements of subregulation 2.5(3) discussed in the SMS section 5.1. The emergency response plan, and the personnel and resources that it calls upon, are treated as control measures under the regulations. The emergency plan must be properly incorporated within the overall facility safety management system as a control measure subject to the same regime as all other control measures. The development of the emergency response plan therefore needs to include processes for testing, review, training and informing. There should be consideration of the performance standards with reference to the general discussion of this topic elsewhere in the case (see also section 5.1.9).

The safety case must also describe how the response plan is, or will be, implemented. This should include that it is understood by the workforce and other potentially affected people; and that it is subject to review, testing and update.

Operators should note that the response plan itself is not part of the safety case; only a description of it is required. During a safety case assessment, a request for further written information may be made with regard to the description of an emergency response plan, but the document itself would not be requested.

The content and level of detail needs to be adequate for NOPSEMA to gain an appreciation of the emergency response plan, its relationship with the FSA and how it will be implemented and contribute to risk reduction.

All aspects of the emergency plan need to be realistic, workable and agreed to by the relevant parties. This includes assumptions regarding actions required, timing, effectiveness of detection methods, decision-making processes, etc. The emergency plan should be robust and take into account the less than ideal conditions that may prevail in a real emergency which often make it difficult to achieve ideal responses in practice.

The safety case should describe a response plan that is appropriate to the hazards and risks at the facility and that mitigate these so far as practicable. The response plan should be shown to be specific to the facility, and to the identified major accident event hazards; and effective in addressing the consequences of a major accident event occurring. The plan should be compatible with relevant studies (e.g. fire and explosion risk analysis).

ISO 15544 provides further guidance on emergency response for offshore petroleum production facilities.

For the majority of facilities, there is a spectrum of potential major accident events of varying nature, likelihood and severity, each of which could lead to different emergency planning areas. The emergency planning process needs to consider the full spectrum of incidents, and also uncontrolled events which could lead to major incidents, so that the plan can be put into effect for any major accident or uncontrolled event.

Example:
An emergency response plan may be based around natural disasters that may arise between once per year and once every 50 years. In this case, it may be meaningless to develop an emergency response plan around a scenario which is not likely to occur in 100 years. Rather, it may be more appropriate to base the emergency response plan primarily on a less severe but more likely major incident, and then include contingency plans and actions to take if more severe events occur.

Hence the emergency response plan and associated training drills should reflect the full range of scenarios but could place different levels of emphasis and detail on different scenarios according to their relative risk or significance to emergency planning.

Drills and exercises

Content requirement	
Reg 2.20(3)	**The safety case must make adequate provision** for escape drill exercises and fire drill exercise by persons on the facility.

Level of detail requirement	
Reg 2.20(4)	In particular, those exercises must ensure that those persons will be trained to function in the event of emergency with an adequate degree of knowledge, preparedness and confidence concerning the relevant emergency procedures.

Content requirement	
Reg 2.20(5)	**The safety case must provide for** the operator of the facility to ensure, as far as reasonably practicable, that the escape drill exercises and fire drill exercises are held in accordance with the safety case relating to the facility.

The description of the SMS must provide descriptions of actual planned arrangements (policies, procedures etc.) for managing escape drills and exercises and fire drills and exercises. The content and level of detail needs to be adequate to gain an appreciation of the drills and exercise processes.

The information must be appropriate to the facility and the activities to be conducted at the facility and may address, but is not necessarily limited to, the following:

- coverage of the drills and exercise program with reference to both the FERA and EERA
- processes for evaluation the success of drill and exercises and the management of and subsequent corrective and preventative actions
- relationship with performance standards specified in the emergency response plan
- schedule of drills and exercises
- processes for monitoring and maintaining compliance with the schedule
- involvement of parties not at the facility (e.g. logistics providers, onshore management, titleholders etc.)
- requirements for participation / grounds for exemption.

5.3.2 Pipes

Content requirement	
Reg 2.21(1)	**The safety case for a facility that is:** (a) connected to or one or more pipes; or (b) proposed to be connected to one or more pipes; that convey, or will convey, petroleum to the facility **must specify** adequate procedures for shutting down or isolating, in the event of emergency, each of those pipes so as to stop the flow of petroleum into the facility through the pipe.

Level of detail requirement	
Reg 2.21(2)	In particular, **the procedures must include**: (a) effective means of controlling and operating all relevant emergency shut-down valves for a pipe; and (b) a fail-safe system of isolating a pipe in the event of failure of other safety devices for the pipe.

Note: regulation 2.21 is also addressed in the facility description Section 3.4.6, p37.

The description of the SMS must provide descriptions of procedures that specify the management pipeline shutdown or isolation. The content and level of detail needs to be adequate to gain an appreciation of the pipeline shutdown or isolation processes.

The information must be appropriate to the facility and the activities to be conducted at the facility.

5.3.3 Vessel and aircraft control

Content requirement	
Reg 2.22(1)	**The safety case for a facility must describe** a system, that is implemented or will be implemented, as part of the operation of the facility that ensures, as far as reasonably practicable, the safe performance of operations that involve vessels or aircraft.

Level of detail requirement	
Reg 2.22(2)	The system must be able to meet the emergency response requirements identified in the Formal Safety Assessment in relation to the facility and be described in the Safety Management System.
Reg 2.22(3)	The equipment and procedures for ensuring safe vessel and aircraft operations must be fit for purpose.

Note: regulation 26 is also addressed in the SMS description Section 3.4.7, p37.

The description of the SMS must provide descriptions of the vessel and aircraft procedural control and their operation. The content and level of detail needs to be adequate for NOPSEMA to gain an appreciation of how the activities are managed.

The information must be appropriate to the facility and the activities to be conducted at the facility and may address, but is not necessarily limited to, the following:

- Helicopter operations
  - flight following
  - helicopter refuelling
  - inside and outside helicopter landing officer activities.
- Vessel operations
  - general control of activity within safety zone
  - tandem or side-by-side petroleum offloading
  - bulk fluid transfers.

5.4 Arrangements for records

Content requirement	
Reg 2.23(2)	**The safety case for a facility must include arrangements for**: (a) making a record of the documents; and (b) securely storing the documents and records: (i) at an address nominated for the facility; and (ii) in a manner that facilitates their retrieval as soon as practicable.

Level of detail requirement	
Reg 2.23(1)	This regulation applies to the following documents: (a) the safety case in force for the facility; (b) a revision to the safety case for the facility; (c) a written audit report for the safety case; (d) a copy of each report given to NOPSEMA in accordance with subregulation 2.42 (2).
Reg 2.23(3)	A document mentioned in paragraph (1)(a) or (b) must be kept for 5 years after the date of acceptance of the document by NOPSEMA.
Reg 2.23(4)	A report mentioned in paragraph (1)(c) must be kept for a period of 5 years after the date of receipt by the operator.
Reg 2.23(5)	A copy mentioned in paragraph (1)(d) must be kept for a period of 5 years after the date the report was given to NOPSEMA.

The description of the SMS must provide descriptions of actual planned arrangements (policies, procedures etc.) for records management. The content and level of detail needs to be adequate to gain an appreciation of the records management processes. These arrangements must address explicitly safety cases, audit reports and reports of accidents and dangerous occurrences.

The information must be appropriate to the facility and the activities to be conducted at the facility and could address such items as retention and disposal schedules and storage, security and retrieval.

5.5 Common weaknesses in the SMS descriptions

Common weaknesses in SMS descriptions include:

- the safety case presents SMS documentation without any evidence to the effect that the SMS complies with requirements
- the safety case focuses on operational SMS matters and ignores the operator's organisational structure as an aspect of the SMS
- the description of the SMS focuses on the high level system without adequately describing how the SMS actually will work in the field (i.e. at the facility) to control risks associated with identified hazards
- the SMS consists of many procedures with no clear system, structure or integration
- the SMS does not provide clear linkages to corporate health and safety policies, or it does not demonstrate how it delivers against those policies
- there are gaps identified but no system in place for prioritisation and close out. For example, the operator has recognised that an audit program is required, and is "under development"
- there is an absence of meaningful performance standards e.g. systems are reviewed 'periodically' or 'frequently' or 'kept under constant review'
- there is poor integration between the SMS and other relevant business systems such as human resources, particularly when it comes to change management: Some organisations prepare a safety case outside of their business systems to meet a specific business need for safety case acceptance. This is likely to be unacceptable in the longer term if the requirements for hazard management identified in the safety case are not integrated with day-to-day operations. This is because gaps are likely to develop between what is actually done and what the safety case says is being, or should be done.

5.6 Evidence of compliance

Operators have the responsibility for ensuring that the SMS complies with the OPGGS(S) regulatory requirements. NOPSEMA is required to evaluate the safety case and decide, on the basis of the material presented in the documentary submission, if the operator has presented a convincing case that the SMS complies. As mentioned previously, operators may wish to fill out a concordance table (compliance matrix that shows where each aspect of the OPGGS(S) Regulations is addressed in the safety case) to check the completeness of their safety case submission and to facilitate the assessment process. The demonstration of compliance with the regulatory requirements may be thought of in another way. In order to comply with the OPGGS(S) Regulations, the operator must have reached the conclusion that all the measures that could be applied to reduce health and safety risks have been adopted and nothing that is reasonably practicable still remains to be done. In effect, the safety case describes the management processes by which the operator has reached that conclusion.

6 Critical factors for acceptable safety cases

NOPSEMA will expect safety cases to address at least the following specific factors:

- safety case content that is consistent with the OPGGS(S) Regulations
- description with an appropriate level of detail that accurately explains the physical characteristics of the facility, its operating envelope, the activities that take place at or in connection with the facility and its technical safety-related control systems
- a consistent, integrated overall structure to the safety case such that there is a logical flow through the assessment process with links between the causes and consequences of MAEs, their associated risks, the selection of strategies and measures to control the risks, and the performance required from specific measures to maintain risk levels to ALARP
- description with an appropriate level of detail that explains the hazards and MAEs identified and the risk assessment conducted
- description with an appropriate level of detail that explains the means by which the operator ensures adequacy of the design, construction, installation, operation, maintenance or modification of the facility
- a transparent and robust argument to show that the adopted control measures reduce risk to ALARP
- a transparent and robust provision of evidence that the SMS provides for reduction of risk to ALARP, and that it is comprehensive and integrated
- a description of the processes by which the workforce are consulted and involved in preparation or revision of the safety case
- consideration for interrelatedness of the information being presented
- implementation of appropriate referencing techniques for both SMS documents and external material the case relies on (e.g. standards, codes, data, etc.).

7 References, acknowledgments & notes

Offshore Petroleum and Greenhouse Gas Storage Act 2006

Offshore Petroleum and Greenhouse Gas Storage (Safety) Regulations 2009

ISO 15544 Petroleum and natural gas industries - Offshore production installations - Requirements and guidelines for emergency response

ISO 10418 Petroleum and natural gas industries - Offshore production platforms - Basic surface process safety systems

ISO 17776 Petroleum and natural gas industries - Offshore production installations - Guidelines on tools and techniques for hazard identification and risk assessment

NOPSEMA 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 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.

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

APPENDIX A – OPGGS(S) Concordance Table for this guidance note

	Reg	Topic	FD	FSA	SMS
Facility description	2.5(1)(a)	Layout	3.2.2, p22		
	2.5(1)(b)	Technical & other control measures	3.4, p34		
	2.5(1)(c)	Activities	3.3, p23		
	2.5(1)(d)	Facility that is a pipeline			
	2.5(1)(e)	Other relevant matters	3.2.1, p21		
Formal Safety Assessment	2.5(2)(a)	Hazard Identification		4.2, p41	
	2.5(2)(b)	Risk assessment		4.3, p43	
	2.5(2)(c)	Controls to achieve ALARP		4.4, p45	
Safety Management System	2.5(3)(a)	Comprehensiveness and integration			5.1.3, p55
	2.5(3)(b)	Scope			5.1.4, p56
	2.5(3)(c)	Hazard Identification			5.1.5, p56
	2.5(3)(d)	Assessment of OHS hazards & risks:			5.1.5, p56
	2.5(3)(e)	Risk reduction (ALARP)			5.1.5, p56
	2.5(3)(f)	Provide for inspection, testing and maintenance			5.1.6, p57
	2.5(3)(g)	Provisions for adequate communications			5.1.7, p58
	2.5(3)(i)	Performance standards.	3.1.5, p21		5.1.9, p59
	2.6	Implementation and improvement			5.1.10, p60
Safety measures	2.7	Standards to be applied	3.1.4, p19		5.1.11, p61
	2.8	Command structure	3.4.2, p34		5.2.1, p62
	2.9	Members of the workforce must be competent			5.2.2, p63
	2.10	Permit to work system			5.2.3, p64
	2.11	Involvement of members of the workforce [1]			5.2.4, p65
	2.12	Design, construct, install, maintain and modify	3.4.1, p33		5.2.5, p65
	2.13	Medical and pharmaceutical supplies and services	3.4.3, p35		
	2.14	Machinery and equipment	3.3, p25		
	2.15	Drugs and intoxicants			5.2.6, p66
Emergencies	2.16	Evacuation, escape and rescue analysis		4.5.1, p47	
	2.17	Fire and explosion risk analysis		4.5.2, p48	
	2.18	Emergency communications systems	3.4.4, p36		
	2.19	Control systems	3.4.5, p37		
	2.20	Emergency preparedness			5.3.1, p67
	2.21	Pipes	3.4.6, p37		5.3.2, p69
	2.22	Vessel and aircraft control	3.4.7, p37		5.3.3, p69
Records	2.23	Arrangements for records			5.4, p70
5 Year revision	2.32(2)	Means to ensure ongoing integrity of technical and other control measures			5.1.12, p61

Notes: 1 For provisions with respect to safety case preparation see Section 2.2.