NOPSEMA
Australia's offshore energy regulator

GUIDANCE NOTE

Control measures and performance standards

Document No: N-04300-GN0271 A336398

Date: 22/10/2025

Core concepts

- Control measures include the physical features of a facility, and elements of the operator's management system employed at the facility, that eliminate, prevent, reduce or mitigate the risk of major accident events and other hazardous events. They can take many forms including physical equipment, process control systems, management processes, operating or maintenance procedures, the emergency plan, key personnel and their actions.
- A range of control measures should be considered within the formal safety assessment for identified major accident events (MAEs). Operators must demonstrate that they have scrutinised existing control measures and considered an array of alternative control measures, which will vary depending on the scale and complexity of the facility and the nature of the risk profile.
- As part of the formal safety assessment process, operators need to demonstrate that the control measures in place for each identified hazard are effective (or will be effective) in reducing the risk to a level that is as low as reasonably practicable (ALARP).
- Control measures must be reviewed periodically to ensure risks remain ALARP. This is linked to lifecycle management, management of change and integrity assurance processes.
- The safety management system must provide for all activities that will, or are likely, to take place at the facility. Determination of control measures will therefore need to be applied to hazards with the potential to harm people at the facility, not just to those associated with MAEs.
- Control measure identification, assessment and selection should involve people who have a thorough knowledge of the use and possible failure modes of the control measures.
- Preferential order should be considered when selecting controls. The hierarchy of control measures typically includes, in order of priority, elimination, prevention, reduction and mitigation. Applying a hierarchy of control measures involves for example designing out or removing hazards at the source and then controlling any residual risks by engineering or organisational means.
- A range of different types of controls generally provides more effective protection than a single type as they help provide independence and layers of protection.
- The control measures should be understood in terms of their effectiveness; this will include consideration of a range of factors including their functionality, availability, reliability, independence, survivability, compatibility, maintainability, benefit and cost, and their ability to reduce risk.
- The operator's safety management system for a facility must specify the performance standards that apply. The performance standards are the parameters against which control measures for MAEs are assessed to ensure they reduce the risks to ALARP on an on-going basis.
- The operator's safety management system must be comprehensive and integrated, including consideration of all aspects of the control measures. As such, as part of the description provided in the safety case, the safety management system needs to be shown to fully support and maintain the performance standards of the control measures within an integrated management framework.

Table of contents

Abbreviations/acronyms

ALARP	As Low As Reasonably Practicable
API	American Petroleum Institute
AS	Australian Standard
BDV	Blowdown Valve
COP	Critical Operating Parameter
ESD	Emergency Shutdown
FMEA	Failure Mode Effects Analysis
FPSO	Floating Production Storage and Offloading
FSA	Formal Safety Assessment
GN	Guidance Note
HVAC	Heating Ventilation and Air Conditioning
ISO	International Standards Organisation
MAE	Major Accident Event
MHD	Major Hazards Division
MODU	Mobile Offshore Drilling Unit
NZS	New Zealand Standard
OPGGS(S) Regulations	Offshore Petroleum and Greenhouse Gas Storage (Safety) Regulations 2024
NOPSEMA	National Offshore Petroleum Safety and Environmental Management Authority
OHS	Occupational Health and Safety
PTW	Permit to Work
SDV	Shutdown Valve
SMS	Safety Management System
SSIV	Subsea Isolation Valve

Key definitions for this guidance note

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

ALARP	This term refers to reducing risk to a level that is as low as reasonably practicable. In practice, this means that the operator has to show through reasoned and supported arguments that there are no other practicable options that could reasonably be adopted to reduce risks further.
Control Measure	A control measure is any system, procedure, process, device or other means of eliminating, preventing, reducing or mitigating the risk of hazardous events at or near a facility. Control measures are the means by which risk to health and safety from events is eliminated or minimised. Controls can take many forms, including physical equipment, process control systems, management processes, operating or maintenance procedures, emergency response plans, and key personnel and their actions.
Formal Safety Assessment	A formal safety assessment, in the context of the OPGGS(S) Regulations, is an assessment or series of assessments that identifies all hazards having the potential to cause a MAE. It is a detailed and systematic assessment of the risk associated with each of those hazards, including the likelihood and consequences of each potential MAE. It identifies the technical and other control measures that are necessary to reduce that risk to a level that is as low as reasonably practicable [OPGGS(S) subregulation 2.5(3)(c)].
Hazard	A hazard is defined as a situation with the potential for causing harm to human health or safety.
Hazard Identification	Hazard identification is the process of identifying potential hazards. In the context of the OPGGS(S) regulations, hazard identification involves identifying all hazards having the potential to cause a MAE [OPGGS(S) subregulation 2.5(3)(a)], and the continual and systematic identification of hazards to health and safety of persons at or near the facility [OPGGS(S) subregulation 2.5(4)(c)].
Major Accident Event	A major accident event (MAE) is an event connected with a facility, including a natural event, having the potential to cause multiple fatalities of persons at or near the facility [OPGGS(S) Regulation 1.5].
Performance Standard	A performance standard means a standard, established by the operator, of the performance required of a system, item of equipment, person or procedure which is used as a basis for managing (controlling) the risk of a MAE [OPGGS(S) Regulation 1.5].
Risk Assessment	Risk assessment is the process of estimating the likelihood of an occurrence of specific consequences (undesirable events) of a given severity.
Workforce	Members of the workforce include members of the workforce who are: (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)]

1. Introduction

1.1. Intent and purpose of this guidance note

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

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

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

Section 1.3 of this guidance note gives an overview of the formal safety assessment process, and then the balance of the guidance note discusses aspects relating to control measures and performance standards in particular.

The purpose of control measure identification, assessment and selection is to help operators understand how the risks to health and safety are managed on their offshore facility. This guidance note is intended to assist operators through the process of identifying, selecting and assessing control measures in the context of MAE risks as addressed by the formal safety assessment, as well as other occupational health and safety risks covered by the safety management system, in support of the evidence that risks are reduced to a level that is as low as reasonably practicable (ALARP).

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

Figure 1 illustrates the scope of the NOPSEMA safety case guidance notes overall, and their interrelated nature. This guidance note on *Control Measures and Performance Standards* should be read in conjunction with the other relevant guidance notes; the full set is available on the NOPSEMA website.

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 respectively. 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. Whilst this guidance note puts forward a selection of the possible approaches that operators may choose to explore in addressing the FSA and safety management system requirements of the OPGGS(S) regulations, the selection is not exhaustive, and operators may choose to use other approaches not covered by this guidance note.

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.

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.**

1.2. The risk management process applied in the safety case

The Australian Standard on Risk Management AS ISO 31000 provides a generic framework for establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk. In addition, ISO 17776 "Petroleum and natural gas industries – Offshore production installations – Major accident hazard management during the design of new installations" also provides guidelines on tools and techniques for hazard identification and risk assessment for offshore production facilities.

The requirements under the OPGGS(S) regulations reflect the current thinking on risk management and hence call for application of the key elements of risk management. These objectives are outlined in subregulation 1.4(2) summarised below.

OPGGS(S) Regulation - Objects	
Reg 1.4(2)	An object of this instrument is to ensure that safety cases for facilities make provision for the following matters in relation to the health and safety of persons at or near the facilities: (i) the identification of hazards, and assessment of risks; (ii) the implementation of measures to eliminate the hazards, or otherwise control the risks; (iii) a comprehensive and integrated system for management of the hazards and risks; (iv) monitoring, audit, review and continuous improvement.

1.3. Formal Safety Assessment

OPGGS(S) Regulation - Formal Safety Assessment Requirement	
Reg 2.5(3)	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; (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; and (d) describes the emergency response plan required to be followed in the event of an emergency in connection with the facility.

For the purposes of a safety case submission, the identification of technical and other control measures that are necessary to reduce risk to ALARP and the FSA is focused on MAEs.

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

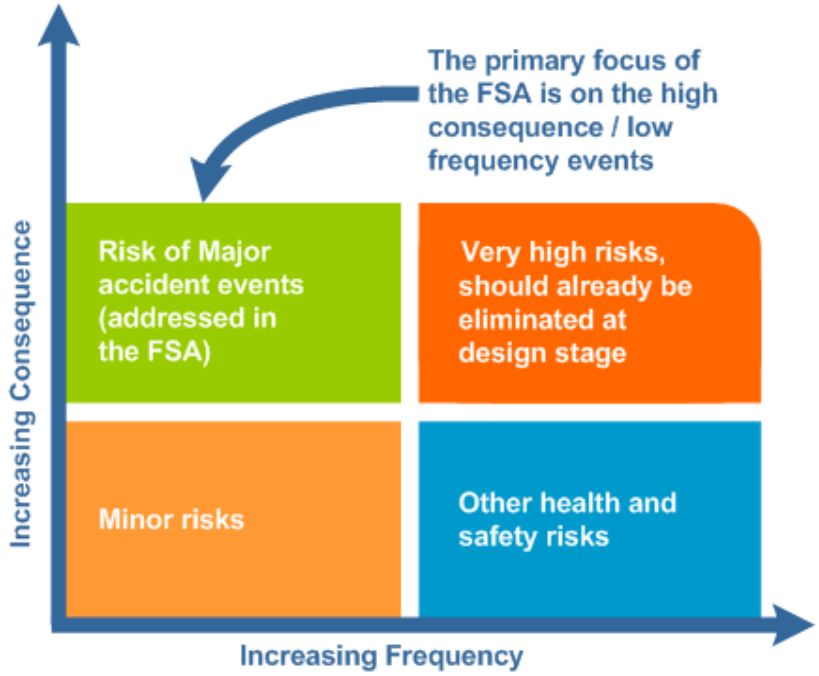

Figure 2 – Formal Safety Assessment to focus on MAEs

It should be noted that the detailed description of the safety management system in the safety case must provide for all hazards and risks to persons at the facility, not just risks of major accident events. Therefore, operators may wish to consider broadening the scope of hazard identification, risk and control measure assessment studies to address other hazards not necessarily linked to MAEs, e.g. noise, exposure to exhaust fumes, etc.

Further guidance is available in the NOPSEMA guidance note:
"Safety Management Systems"

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

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

Formal safety assessment should not be limited to desktop theoretical studies. It can include any activity the operator employs to understand the facility and its risks. For example, an FSA could incorporate information from incident investigations, discussions during safety meetings regarding hazards and ways of controlling them, condition monitoring programs, analysis of process behaviour, evaluation of trends or deviations from critical operating parameters, procedure reviews, etc.

The knowledge generated by the formal safety assessment should be captured, managed and disseminated to ensure it remains up to date and is used in the design, operation and maintenance of the facility. The management of knowledge generated through hazard identification and risk assessment will also greatly

assist the efficient development of a safety case for the facility. For example, these processes will assist in handling assumptions, actions arising, etc. through the safety case development process.

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

For offshore production facilities, ISO 17776 "Petroleum and natural gas industries – Offshore production installations – Major accident hazard management during the design of new installations" provides guidelines on tools and techniques for hazard identification and risk assessment.

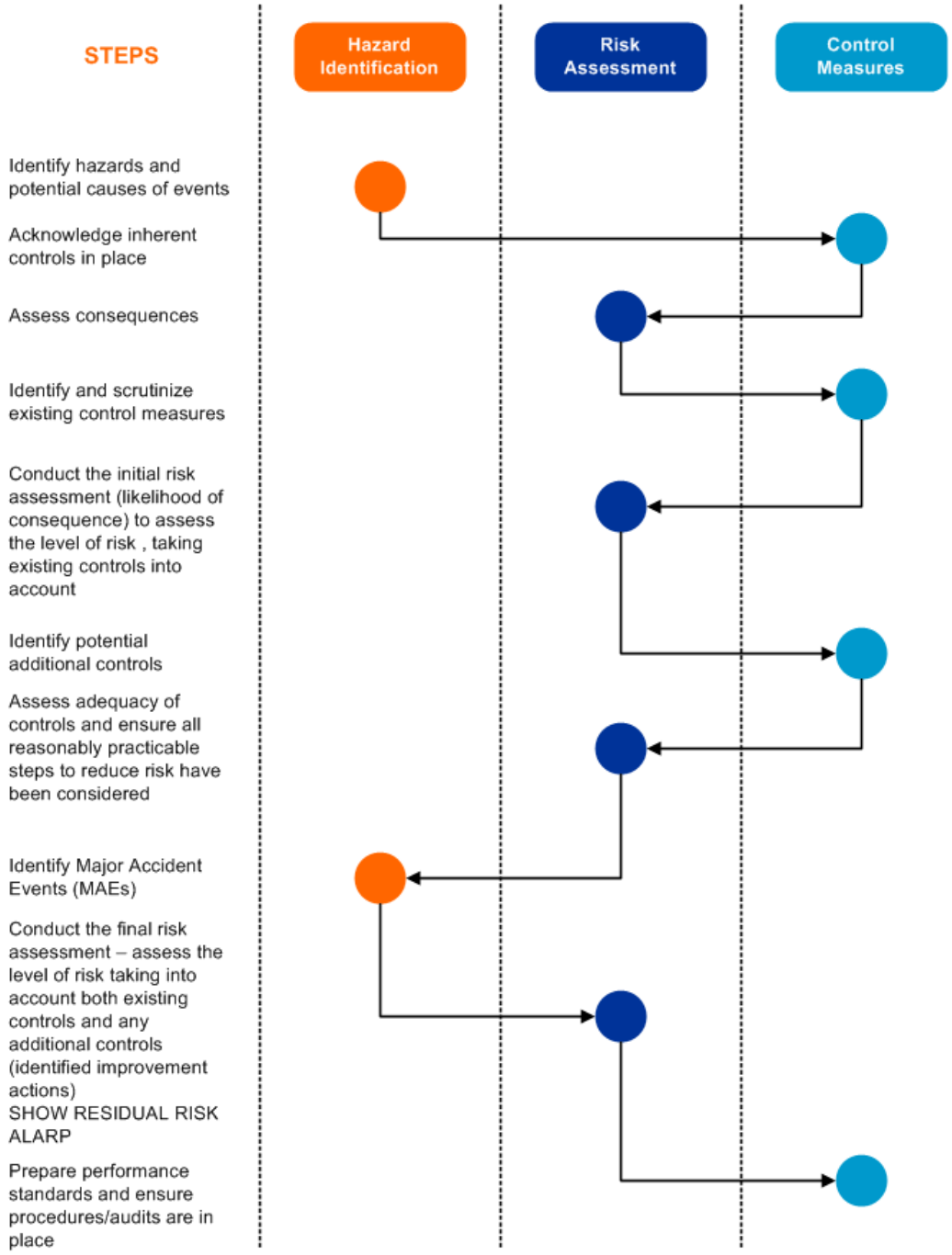

Figure 3 – The FSA process

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

Providing a well-considered, detailed description of a suitable and sufficient formal safety assessment within the safety case will enable operators to provide evidence of:

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

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

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

1.4. Involving the workforce

OPGGS(S) Regulation - Involvement of members of the workforce	
Reg 2.11(1)	The operator of a facility must demonstrate to NOPSEMA, to the reasonable satisfaction of NOPSEMA, that: (a) in the development or revision of the safety case for the facility, there has been effective consultation with, and participation of, members of the workforce; and (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.
Reg 2.11(2)	A demonstration for paragraph (1)(a) must be supported by adequate documentation.
Reg 2.11(3)	In subregulation (1): *members of the workforce* include 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.

Formal safety assessment is the process of debating, analysing, creating and sharing views, information and knowledge on the risk of MAEs and the means to prevent or mitigate them. It must include the active participation of people at the 'coal face' who influence safe operation, and hence hazard identification and risk assessment roles should be defined for members of the workforce

It is unlikely that everyone can be involved in the processes of hazard identification, risk assessment and control measure assessment. Therefore, it is important that regular feedback is provided to the rest of the workforce. This feedback should take the form of communicating the hazards that are present, the risks associated with those hazards, the controls in place and any recommendations arising.

The workforce should also be provided with an opportunity to review and comment on the risk and control measure assessment output. This is important both as a quality control activity and as part of the mandatory workforce consultation and participation required by the OPGGS(S) regulations. It can also foster a feeling of ownership among personnel not directly involved in the process.

Further guidance is available in the NOPSEMA guidance note:
"Involving the workforce"

2. Control measures

Control measures are the features of a facility that eliminate, prevent, reduce or mitigate the risk to health and safety associated with potential MAEs or other hazardous events. They are the means by which an operator reduces risk at their facility to a level that is ALARP.

Control measures can take many forms including physical equipment, process control systems, management processes, operating or maintenance procedures, the emergency response plan and key personnel and their actions.

2.1. Control of MAEs versus control of all health and safety risks

In accordance with the definition given in regulation 1.5, a MAE is an event connected with a facility, including a natural event, having the potential to cause multiple fatalities of persons at or near the facility. The relative rarity of events with catastrophic consequences may give rise to the situation where potential MAEs receive little attention, as compared with day-to-day operational issues. The safety case regime therefore is a regulatory initiative focused on addressing potential for MAEs, while continuing to address occupational health and safety.

Identifying MAEs is the backbone of the formal safety assessment required to be described in the facility safety case. All identified hazards should be subject to a 'screening' process to determine if they can result in a MAE. Those hazards which can lead to MAEs must be considered in the formal safety assessment, whereas those hazards that cannot result in a MAE but are a hazard to health and/or safety must be addressed by the operator's safety management system.

Example – Helicopter Operations:

An example of a health and safety risk on an offshore facility is the potential for an individual to be seriously injured or killed through coming into contact with the rotating blades on approach to helicopter during boarding. In this case only one person would be involved.

An example of a MAE for an offshore facility may include helicopter ditching whilst in transit to or from the facility. In this case there is potential for all on board the aircraft to perish at sea.

Because of the difference in the way these hazards are expected to be addressed in the safety case, it is practical to clearly differentiate between them at the outset and ensure that differentiation is maintained throughout the process. Correspondingly, controls associated with MAEs need to be clearly identified as such. The regulations require that the SMS specify the performance standards that apply, and the performance standards by definition are associated with controls used as a basis for managing the risk of an MAE.

Bearing in mind that the safety management system must provide for all activities that will, or are likely to take place at the facility, determination of control measures will need to be applied to all risks to health and safety of people at the facility. The SMS should therefore address both MAEs and other health and safety risks through procedural systems designed to reduce risks to a level that is ALARP.

Operators should note that mandatory controls specified in the regulations with respect to occupational health and safety risks, such as those pertaining to exposure to noise or hazardous substances for instance, must be implemented regardless of the methodologies suggested in this guidance.

Further guidance is available in the NOPSEMA guidance note:
"Safety Management Systems"

Figure 4 shows the variation in the regulations for the process as it applies to hazards with MAE potential and developing performance standards for those controls as compared to hazards with other potential health and safety outcomes.

For simplicity, the balance of this guidance note will refer to controls for MAEs only, however it is important to bear in mind that there is a distinction as described above. The principles behind control measure identification, assessment and selection are essentially the same whether a control is for an MAE or not, and although the regulations only require performance standards to be specified for MAE controls, this does not preclude operators from applying the principle to controls for other health and safety hazards.

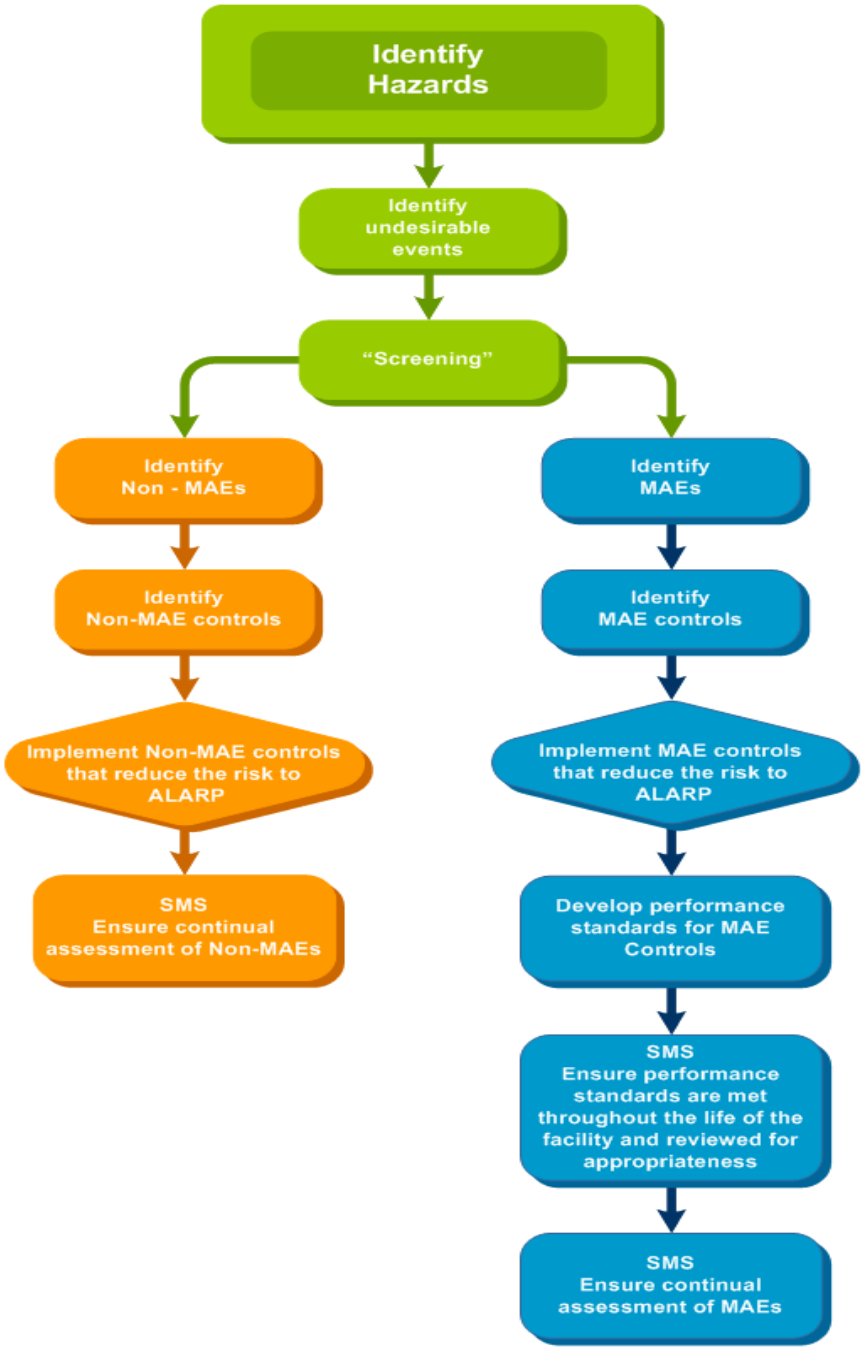

Figure 4 – MAE and non-MAE control measures

2.2. Control measures identification, selection and assessment aims

The aims of the control measure identification, selection and assessment process are to:

- provide operators and the workforce with sufficient knowledge, awareness and understanding of the control measures for MAEs and other hazardous events to be able to prevent and deal with dangerous occurrences
- identify all existing and potential control measures
- provide a basis for identifying, evaluating, defining and justifying the selection (or rejection) of control measures for eliminating or reducing risk

- lay the foundations for demonstrating within the safety case that the risks have been reduced to a level that is as low as reasonably practicable (ALARP)
- show clear links between control measures and the potential MAEs or other hazards they are intended to control
- understand the effectiveness of adopted control measures and their impact on risk
- provide a monitoring regime to ensure the ongoing effectiveness of the control measures.

2.3. Features of control measure identification and assessment

OPGGS(S) Regulation - FSA and SMS Control Measure Assessment	
Reg 2.5(3)(c)	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 identifies the technical and other control measures that are necessary to reduce that risk to a level that is as low as reasonable practicable.
Reg 2.5(4)(e)	The safety case for the facility must also contain a detailed description of the safety management system that 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 OPGGS(S) safety case content requirements with respect to control measures are qualified by the phrase "to reduce the risks to a level that is as low as reasonably practicable". This means that the operator has to show through reasoned and supported arguments within the safety case that there is nothing else that could reasonably be done to reduce risks further.

The risk assessment and consequently the associated control measure identification and assessment, should reflect the operator's safety case philosophy. For instance, if the operator intends to base the safety case largely on the facility's compliance with specific codes or standards, the risk assessment and control measure selection should address corresponding issues such as the basis of the codes and standards, their applicability to the facility, and the risks associated with compliance or non-compliance. Conversely, if the operator intends to base the safety case on fundamental engineering or management systems, the risk assessment and control measure selection should be structured accordingly.

In particular, if the operator intends to diverge from established codes or standards, or if the codes and standards do not apply fully to the facility, the risk assessment should address these issues. Operators should use the risk assessment as a way of identifying alternative and more effective/efficient means of managing risk and so use risk assessment to establish the most appropriate controls for their facility.

In either case the safety case should show that the risk assessment and control measure identification and selection is based on sound science and good risk management decisions which are appropriate to the facility. The approach taken depends on the nature of the activities and the risk management decisions they face.

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

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

2.4. Planning and preparation

2.4.1. General

The amount of work required to prepare a safety case requires a large commitment in terms of both onshore management and facility personnel at all stages, including control measure identification, assessment and selection.

There is a range of methodologies that can be employed in assembling the information required for a safety case. A facilitated workshop is a common way of gathering accurate information based on a diversity of viewpoints and may also generate buy-in to the safety case process.

However, when assessing the suitability of controls, another option is to have selected personnel prepare the control measure assessment and then run a workshop to validate their work. Personnel who are independent of the actual work but have similar relevant experience should be involved in the review, for instance an operator that has multiple facilities may have personnel from facility 'A' review the work done for facility 'B', or a company may involve a cross-section of different personnel from within the company in the review. The best approach will depend on the size and type of facility and the resources available.

2.4.2. Assessment team

When carrying out control measure identification, selection and assessment it is recommended to involve representatives from management, supervisors, operators, maintenance personnel and relevant technical personnel. As highlighted in section **Error! Reference source not found.** above, the regulations require the participation of members of the workforce in the development of the safety case.

The operator may also choose to employ a third party to provide guidance on the path to follow (i.e. a workshop facilitator), or bring in technical expertise in a specific area, however it is important that the operator maintains ownership of the entire process rather than 'farming the work out' to third parties simply to provide a result.

Aspects to consider when selecting team members to carry out this work are similar to those discussed with respect to carrying out hazard identification and risk assessment exercises.

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

2.5. Identifying and selecting control measures

2.5.1. Identifying control measures

The purpose of control measure identification is to identify the existing and potential control measures, for each hazard and associated outcomes. The regulations require operators to consider a ***range*** of control measures and to identify those that are necessary to reduce risks to a level that is ALARP, particularly in relation to fire and explosion risks, and evacuation, escape and rescue risks [OPGGS(S) regulation 2.16 and 2.17].

For this reason, it is important to have a structured methodical approach to identify and consider a variety of potential control measures, explore them sufficiently and be able to provide reasons why certain control measures were selected and others rejected.

For offshore production facilities, ISO 13702 "Petroleum and natural gas industries – Control and mitigation of fires and explosions on offshore production installations – Requirements and guidelines" provides guidance on the control and mitigation of fires and explosions.

OPGGS(S) Regulation - Safety Case Content Requirements	
Reg 2.16(1)	The safety case for a facility must contain a detailed description of an evacuation, escape and rescue analysis in the event of an emergency at the facility.

OPGGS(S) Regulation - Analysis Requirement	
Reg 2.16(2)	The evacuation, escape and rescue analysis must: (a) identify the types of emergency that could arise at the facility; and (b) evaluate a range of routes for evacuation and escape of persons at the facility in the event of an emergency; and (c) evaluate alternative routes for evacuation and escape if a primary route is not freely passable; and (d) evaluate different possible procedures for managing evacuation, escape and rescue in the event of an emergency; and (e) evaluate a range of means of, and equipment for, evacuation, escape and rescue; and (f) evaluate 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.

(h) identify, as a result of the above considerations, the technical and other control measures necessary to reduce the risks associated with emergencies to a level that is as low as reasonably practicable.

Note: In so far as it addresses major accident events, the evacuation, escape and rescue analysis forms part of the formal safety assessment.

The emergency plan must be treated as a control measure: a range of emergency planning provisions must be considered in the evacuation, escape and rescue analysis and reasons for selecting certain provisions and rejecting others must be documented.

ISO 15544 "Petroleum and natural gas industries – Offshore production installations – Requirements and guidelines for emergency response" provides further guidance on emergency response for offshore production facilities.

It is for the operator of a facility to carry out the analysis and determine a suitable emergency response plan which is appropriate to their facility and the activities to be conducted at the facility.

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

In practice, the provisions made for offshore emergency response are facility and location specific. They will change from one location to another dependant on a variety of factors including, but not limited to: types of emergencies that could be encountered, distance from shore and onshore support, meteorological conditions at the location and season in which the proposed activities are to take place, the type of offshore facility, and number of personnel on board.

OPGGS(S) Regulation - Safety Case Content Requirements

Reg 2.17(1) The safety case for a facility must contain a detailed description of a fire and explosion risk analysis for the facility in the event of a fire or explosion at the facility.

OPGGS(S) Regulation - Analysis 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; and

(b) evaluate a range of measures for detecting those fires and explosions in the event that they do occur; and

(c) evaluate a range of measures for eliminating those potential fires and explosions, or for otherwise reducing the risk arising from fires and explosions; and

(d) evaluate the incorporation into the facility of both automatic and manual systems for the detection, control and extinguishment of:

(i) outbreaks of fire; and

(ii) leaks or escapes of petroleum; and

(e) evaluate 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) evaluate the evacuation, escape and rescue analysis, in so far as it relates to fires and explosions; and

(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.

Note: In so far as it addresses major accident events, the fire and explosion risk analysis forms part of the formal safety assessment.

The regulations require the operator to identify control measures that are suitable for the specific facility and are adequate to reduce risks to a level that is ALARP, having considered alternatives.

Fire and explosion risk analysis and control measure identification must not simply concentrate on mitigation measures, but must also consider elimination, prevention and protection measures. Thus, the fire and explosion risk analysis should not simply assume that industry codes and standards are suitable by default; they must justify this for the specific situation and must assess whether alternative measures are reasonably practicable and more effective.

For any of the identified control measures which relate to control of potential MAEs, performance standards will be required.

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

2.5.2. Understanding control measures in relation to the hazards

Understanding the linkages between the control measure and the hazards giving rise to the MAE or other hazardous event will be critical in assessing the control measures that protect against each hazard.

The nature, scale and range of hazards and outcomes that each control measure is designed to address, and the relationship of the control measure to the hazard, the possible MAEs or undesirable health and safety outcomes and other control measures, will all need to be understood. That is, the mechanism by which the control works to prevent or manage risk associated with the potential MAE or hazardous event. These mechanisms for the range of operating conditions that might exist at the facility (i.e. normal, abnormal and emergency conditions) will need to be understood. It is also necessary to determine whether there are sufficient control measures for all possible hazards and outcomes and that the control measures in place are robust enough to reduce the risk associated with the potential MAE or hazardous event to a level that is ALARP.

One way to represent the relationships between hazards, outcomes, control measures and the potential MAE pictorially is a bowtie diagram (also called a cause-consequence diagram). The relationship between the proactive control measures, the event, the reactive control measures and the outcomes for each hazard is shown in **Figure 5**. Proactive controls can also be referred to as preventative controls and reactive controls referred to as mitigation controls.

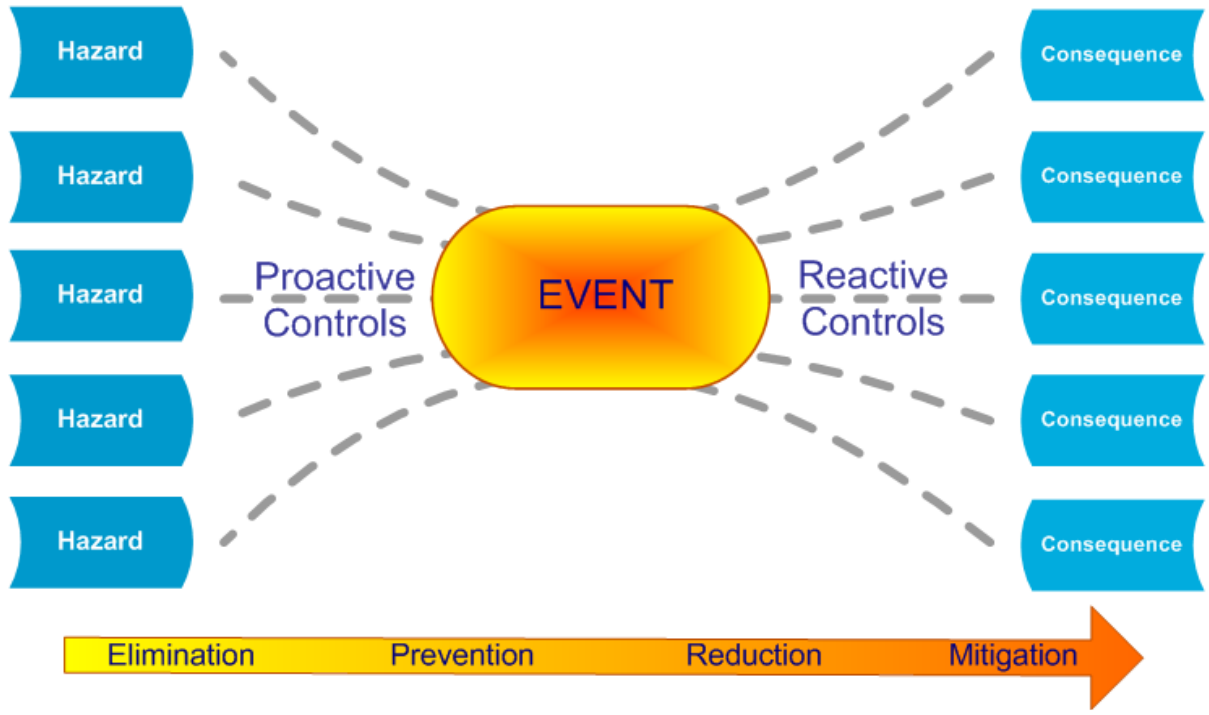

Figure 5 – Schematic Representation of a Bowtie Diagram

The benefit of using a bowtie diagram is that it is a transparent and easily accessible method of documenting and presenting information for stakeholders. However, this information or parts of this information can also be recorded in formats such as hazard registers, fault trees and event trees, or any other format which clearly shows linkages.

2.5.3. Assessment of control measures

As part of the formal safety assessment process operators must demonstrate that the full suite of control measures in place for each potential MAE are effective (or will be effective) in reducing the risk to a level that is ALARP.

When assessing the capability and effectiveness of the control measures under consideration the operator should think about whether the control measures:

- have been selected in accordance with the hierarchy of controls (order of preference)
- are distributed appropriately with representation of the different types of control namely; engineering, procedural and administrative
- have adequate layers of protection
- consider the full range of operating and emergency circumstances
- consider common mode failures
- are effective
- are reasonably practicable
- reduce the risk to a level that is ALARP.

When conducting the assessment, it is important to involve people who have a thorough knowledge of the use and possible failure modes of the control measures. Operators must demonstrate that they have considered a reasonable number of existing and alternative control measures, which will vary depending on the scale and complexity of the facility and the nature of the risk profile.

Figure 6 below shows possible stages of control measure assessment sequentially. During this process it may become evident that it is necessary to select additional control measures or identify improvement actions for current control measures. Each of these steps is described more fully throughout the following sections.

Applying a hierarchy of controls

It is good practice to consider applying a preferential order when selecting controls. A hierarchy of control measures typically includes, in order of priority: elimination, substitution, prevention, reduction and mitigation. Applying a hierarchy of control measures involves for example designing out or removing hazards at the source and controlling any residual risks by engineering or organisational means. An example hierarchy of control is shown in **Figure 6**.

This approach is considered the most effective as it takes account of the human factor, aiming to neutralise the effects of the idiosyncrasy and fallibility of human beings by making workplaces, work, equipment and substances inherently safe rather than relying on workers always being alert to and successfully avoiding risks. This is crucial as a variety of factors make safe behaviour strategies ineffective, including lack of awareness, human errors and mistakes, stress and fatigue, acting reflexively ('automatic pilot'), giving priority to production or operational demands, protecting job security and simply 'getting the job done'.

The hierarchy of control approach encourages operators to seek out opportunities to design or change work processes, equipment, substances and other aspects of the work environment to make them inherently safer and to meet human needs, rather than trying to modify human behaviour and practices to address shortfalls in plant or equipment design.

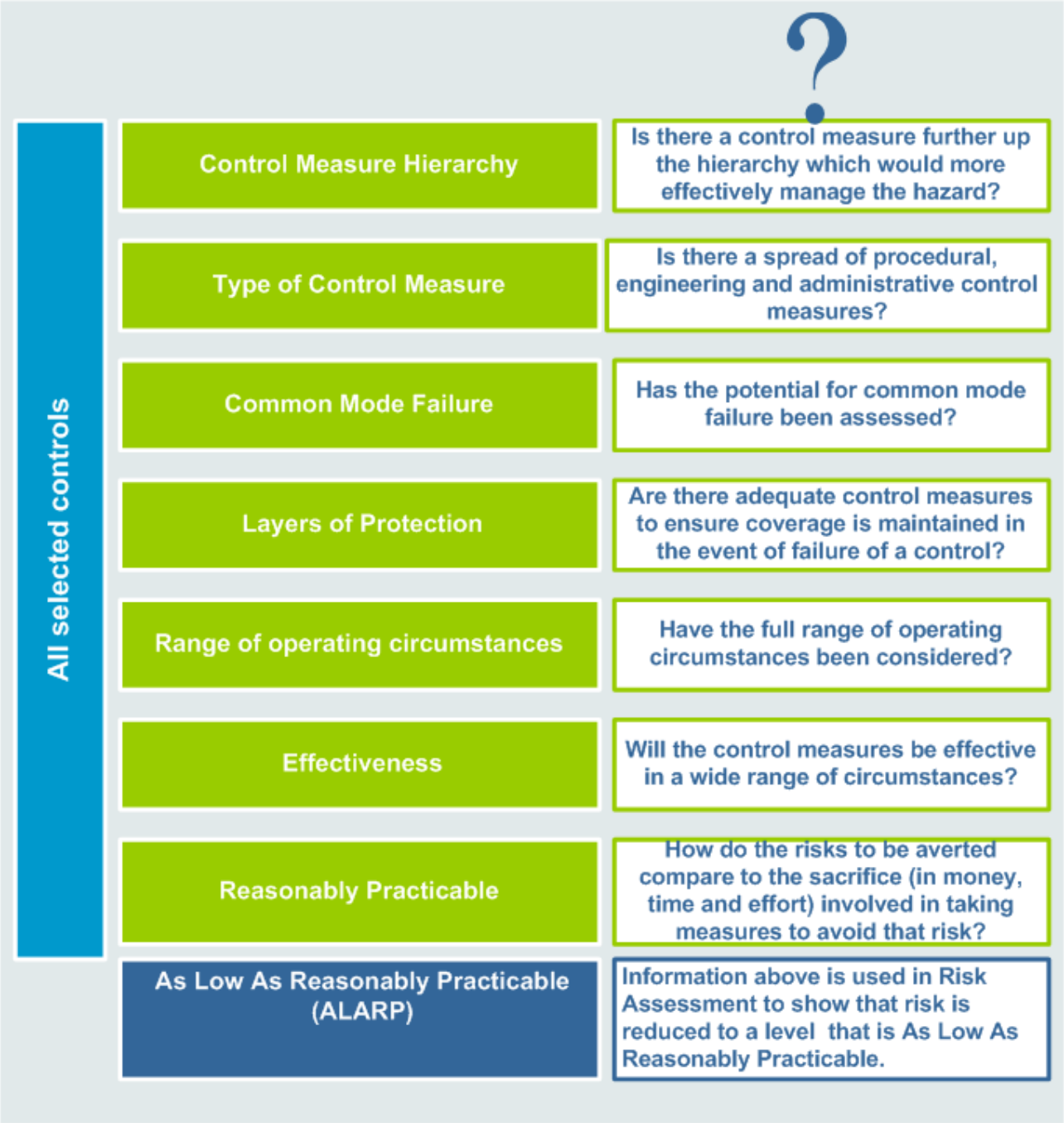

Figure 6 – Assessment of Control Measures

Elimination is the most effective control, however not all hazards can be eliminated. Where hazards cannot be eliminated, reducing the frequency and / or the consequences of the hazardous event are the next most effective routes of control. This is achieved by having robust prevention, reduction and mitigation controls in place.

Safe work practices, administrative procedures, or personal protective clothing and equipment are important to supplement the risk control measures already selected but should not be considered as the first or only means of reducing exposure to workplace hazards.

Figure 7 below outlines an example of hierarchy of control measures in preferential order. It should be noted that other models are in existence which incorporate different elements such as substitution, separation, engineering controls before administrative controls or personnel protective equipment, etc. Operators are entitled to apply these general principles as they see fit. However, NOPSEMA promotes removal of the hazard or the incorporation of inherently safer design features, where appropriate.

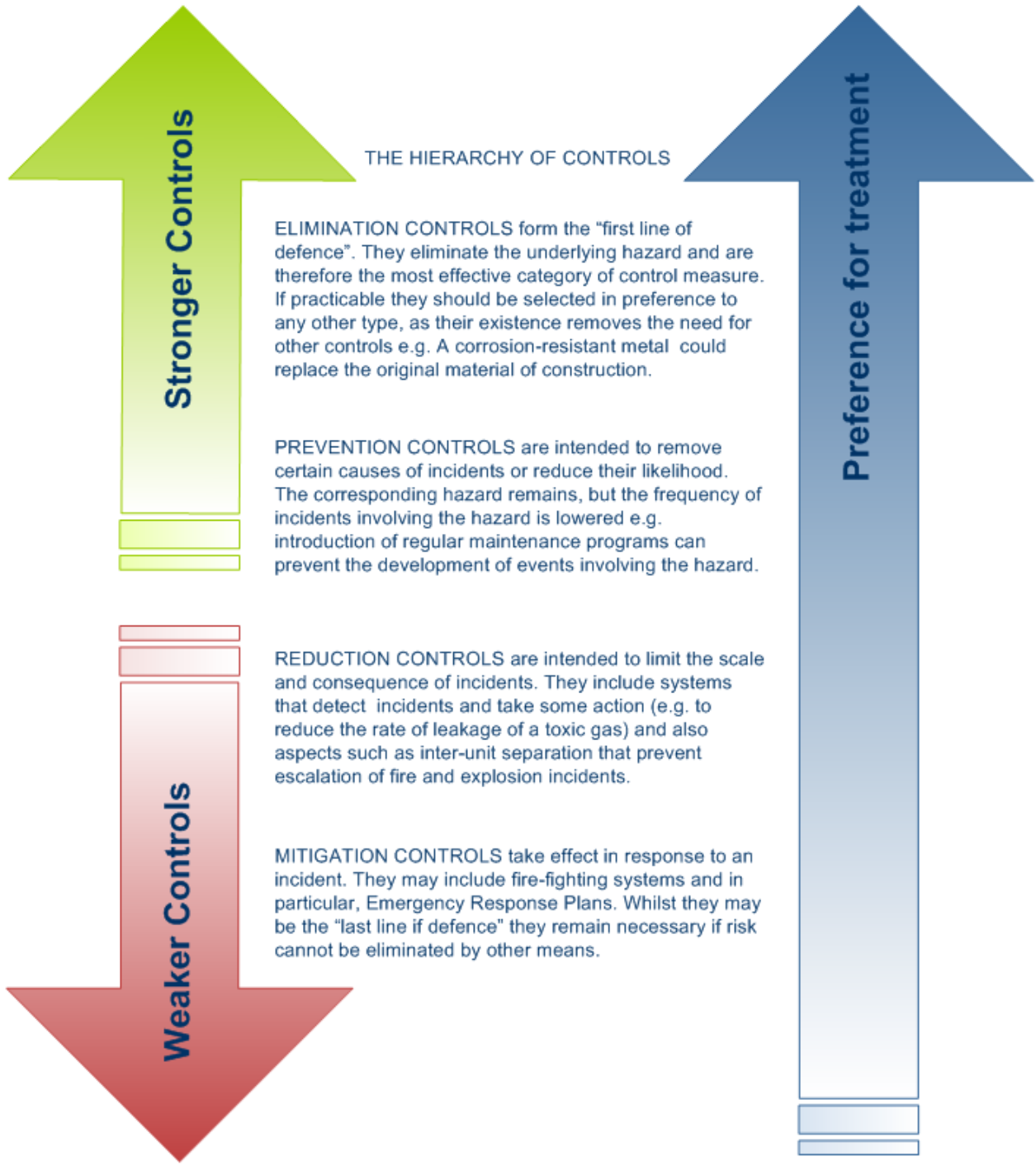

Figure 7 – Example of a Control Measure Hierarchy

Managing risk using different types of control measures

A range of different types of controls generally provides more effective protection as they help provide independence and layers of protection. The regulations refer to two main types of control; namely technical and 'other', where 'other' can be taken to include administrative and procedural controls:

- technical control measures involve hardware like shutdown valves, deluge systems and alarms
- administrative and procedural control measures may include general policy like facility inductions or a drug and alcohol policy, and specific procedures such as inspection and test check sheets and work instructions.

Common mode failures

A common mode failure is where two or more controls may fail as a result of a common cause. It is therefore essential this type of assessment be undertaken as the perceived degree of protection provided by the controls may be overly optimistic if this failure mode is not considered. Common mode failures should be considered for all types of control.

Example:

Examples of common mode failures for an oil storage tank on an FPSO are:

- the level transmitters for the control system and the shutdown system on a storage tank are the same type
- an instrument technician is employed to test all safety systems but calibrates them all incorrectly
- the power supply for a control system and the shutdown system fails impacting multiple controls.

Typical analytical techniques that could be used to identify common mode failures include:

- Failure Mode and Effect Analysis (FMEA)
- Fault Tree Analysis.

Applying 'Layers of Protection'

For many potential hazardous events there are numerous layers acting as barriers to prevent, reduce or mitigate them.

A robust control measure regime will feature a range of independent layers, the number and integrity of which should be scrutinised. Some layers considered for inclusion are: design standards; operating standards; control systems; safety devices; operating procedures, organisational aspects and emergency systems.

Figure 8 illustrates a situation were all technical, procedural and administrative controls have failed.

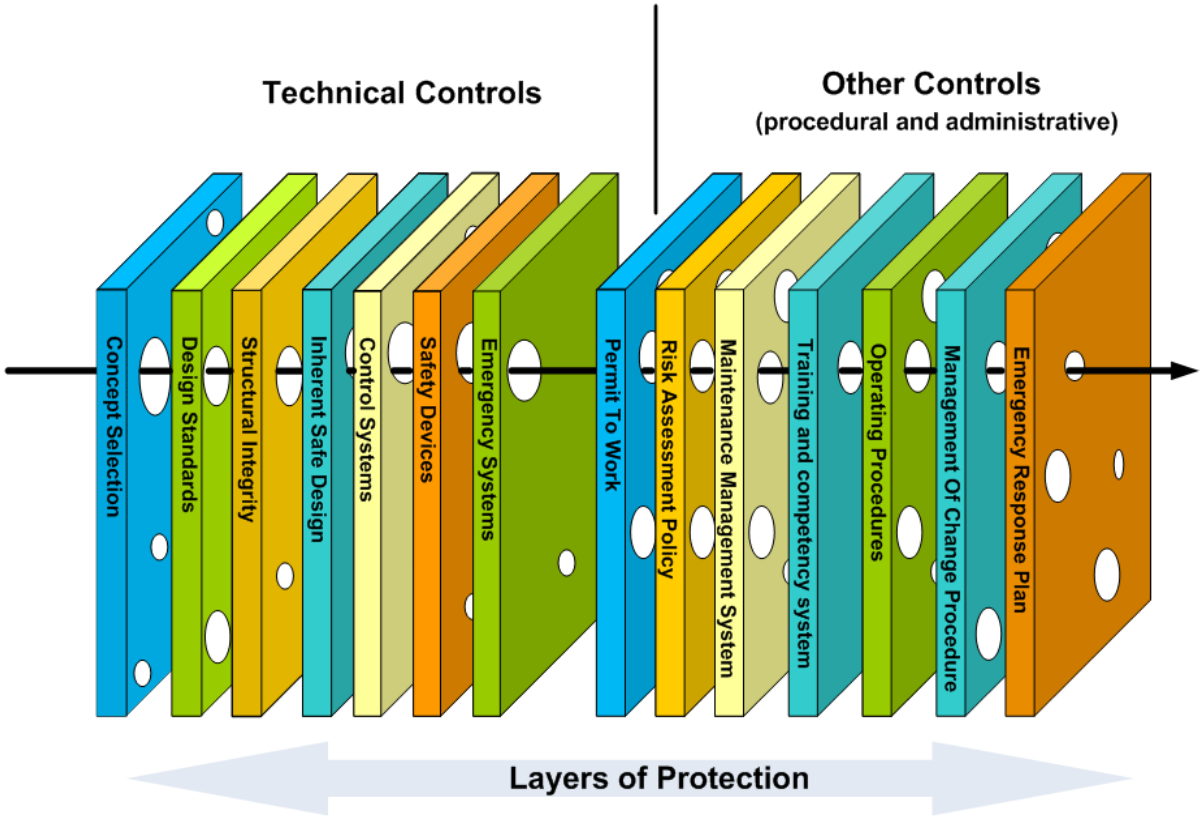

Figure 8 – Layers of Protection

Where some of these layers are not present, additional layers of protection may be required where:

- too much reliance is placed on too few control measures or even a single control measure
- controls are not fully independent, and a common cause could result in the 'loss of control' and a failure of more than one control measure.

The layers of protection provided for each hazard related to each hazardous event should be considered, and the associated risk reduction taken into account, to determine whether an adequate level of protection is provided.

Range of operating circumstances

Control measures may vary for different stages of the facility's lifecycle. For example, design and construction standards are important for new facilities, but as the facility ages more importance may need to be given to asset integrity management. Control measures may themselves have lifecycles that may need to be considered.

Operating circumstances caused by other factors also need to be considered, for example, environmental conditions such as low visibility or heavy winds, or changes to manning levels caused by periodic shutdowns for maintenance, survey and inspection activities. To determine control measure suitability, it is important to have an understanding of the circumstances in which these controls will be effective, including any associated limitations. For example, a deluge system may be effective under certain fire scenarios but not others.

It may well be the limitations of the control measures which most influence the emergency response to any given hazardous event and therefore it is important to have a good understanding of any shortcomings.

It should be noted that hazardous events often occur during commissioning, start-up, shut-down and simultaneous operations, when activity levels are high and operators are dealing with a complex array of interrelated activities. Therefore, it is important that appropriate attention is given to control measures relevant to these phases of operation. The types of control measures in place, or being considered, must be appropriate to the activities undertaken at the facility and the hazards that have been identified.

Focus on control measures

The level of protection control measures require should be considered both during the assessment process and later when assigning performance standards and maintenance regimes. It may become apparent that certain control measures warrant more detailed focus than others, and may justify a higher depth of scrutiny.

The level of attention given to each control measure should relate to the increase in risk if that control measure were to be disabled or not fully function as designed. The following factors are a useful guide in determining the focus given to a control measure:

- is the control measure relied on to control a number of different MAEs?
- is the control measure relied on to prevent the most likely hazards that cause MAEs?
- is the control measure relied on to reduce or mitigate incidents having very severe potential consequences, i.e. is it a MAE control?
- are other control measures, that provide 'back-up', known to be weak (e.g. of poor reliability or effectiveness)?
- is the total number of barriers or control measures for the hazard low?

Effectiveness

Effectiveness is a measure of how well the control measures perform their required function; consideration should be made for reliability, functionality, survivability and availability. This is discussed more in section 3 on Performance Standards.

2.6. Reasonably practicable

In order to comply with OPGGS(S) subregulation 2.5(3)(c) the operator has to identify the technical and other control measures that are necessary to reduce the risk to a level that is as low as reasonably practicable. Clearly, the balance between benefits in terms of reduced risk and the costs of further control measures will play a part in achieving and justifying ALARP. For example, if an option has a benefit that greatly outweighs the cost, this option will almost always have to be implemented, or very good reasons provided for not doing so. In contrast, if the cost greatly outweighs the benefit, demonstrating that the option is not appropriate is straightforward, as other options will almost certainly exist that are able to achieve a similar level of risk reduction at lower cost. If benefits and costs are both high, or are both low, more careful consideration may be required before selecting or rejecting control measures.

There is no defined or preferred way for an operator to demonstrate ALARP. However, it is expected that for each MAE or hazardous event identified for the facility, the demonstration would contain elements of the following process:

- identification and consideration of a range of potential measures for further risk reduction
- systematic analysis of each of the identified measures and a view formed on the safety benefit associated with each of them
- evaluation of the reasonable practicability of the identified measures and the implementation (or planned implementation) of the identified reasonably practicable measures
- recording of the process and results – these are summarised in the safety case.

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

2.7. Summary of considerations

As stated previously it is important to have a structured methodical approach to identify and consider a variety of potential control measures, explore them sufficiently and be able to provide reasons why certain control measures were selected and others rejected. **Table 1** provides a summary of control measure considerations.

Table 1 – Summary of control measure considerations

Methodology for understanding controls	**Points to Consider**
Control Measure Hierarchy • Elimination • Prevention • Reduction • Mitigation	Is there a control higher up the hierarchy that would more effectively manage the hazard? Where appropriate, is there a spread of controls across the hierarchy?
Types of Control Measure • Technical • Other	Is there an appropriate spread of technical and other controls?
Common Mode Failures	Have failure modes been identified for each control measure and then compared to identify common mode failures?
Layers of Protection • Design Standards • Control Systems • Operating Procedures • Safety Devices • Emergency Systems	Are the layers of protection provided adequate for the level of risk posed by the hazard?
Operating Circumstances • Environment • Operating conditions • Activities being carried out	Have the controls been assessed for effectiveness over the range of different operating circumstances they may have to operate in?

Focus of Control Measure	Does the relative importance or vulnerability of the control measure justify a higher depth of scrutiny than others
Effective • Reliability • Functionality • Survivability • Availability	Has the reliability, functionality, survivability, availability been established for each control measure? Have means of improving these aspects been considered?
ALARP	Has each control measure been assessed for practicability, and those found practicable been implemented while those found to be not practicable noted as such with sufficient justification?

NOTE: These types of assessments should not be applied generically across similar facilities. Facilities are rarely identical and therefore some may have, for example, common mode failures that others do not have.

3. Performance standards

The regulations require that the SMS specifies the performance standards that apply. The performance standards, by definition, are associated with controls used as a basis for managing the risk of an MAE. The performance standards are the parameters against which MAE controls are assessed to ensure they reduce risk to ALARP. They facilitate the transition from the theoretical to the practical in the MAE risk management process. In developing these standards for a facility, the operator should consider what level of performance it is reasonable to achieve from each control measure, considering:

- functionality
- availability
- reliability
- survivability
- dependency
- compatibility.

Performance standards enable the operator to measure, monitor and test the effectiveness of each control measure and take corrective action based on deviations or trends. They pertain equally to technical controls as well as to "other controls" such as administrative or procedural controls.

3.1. Contents of a performance standard

Not all aspects of any given control measure will require performance standards, only the key aspects. The following sections explore aspects of control measures which operators may choose to measure and set standards for, bearing in mind that these may not all apply to all control measures.

3.1.1. Aim

It is beneficial when developing the performance standards to state an overall goal or objective for the performance standard to achieve. For instance, in the case of a gas detection system, is the aim of the system to detect gas, or is it to detect gas above its lower explosive limit?

A well-defined aim statement will focus the elements of the performance standard on the important aspects to be addressed by the standard. It is also essential to understand if the performance standard is to apply to grouped elements as in an entire system (gas detection system with voting and redundancy), or individual discrete elements of a system (single gas detector). Both may be required.

3.1.2. Functionality

The functional performance of a control measure is what it is required to do. How does the control perform in order to achieve the required risk reduction? Functionality may include applicable standards to be met including a wide range of performance characteristics, for example, the performance standard for a firewater system would specify the quantity of firefighting water, the delivery rate per square metre, and the response time from onset of the fire to applying the water.

It may be important to establish critical operating parameters (COPs) of some control measures which should define the upper and lower performance limitations, for example temperatures and pressure, and also normal operational limits which should be safely within the COPs. The purpose of identifying a COP is to ensure that more robust monitoring and management of that parameter occurs.

COPs are best defined for those parameters where there is a high reliance on the operator to respond to a process or manage an activity appropriately. As such it is important to ensure that COP documentation is continuously available to operating personnel and that this documentation provides clear guidance as to how people should respond if a deviation occurs. In the event that a COP is exceeded, an investigation, including risk assessment, should be conducted and outcome documented (see **Figure 9** below).

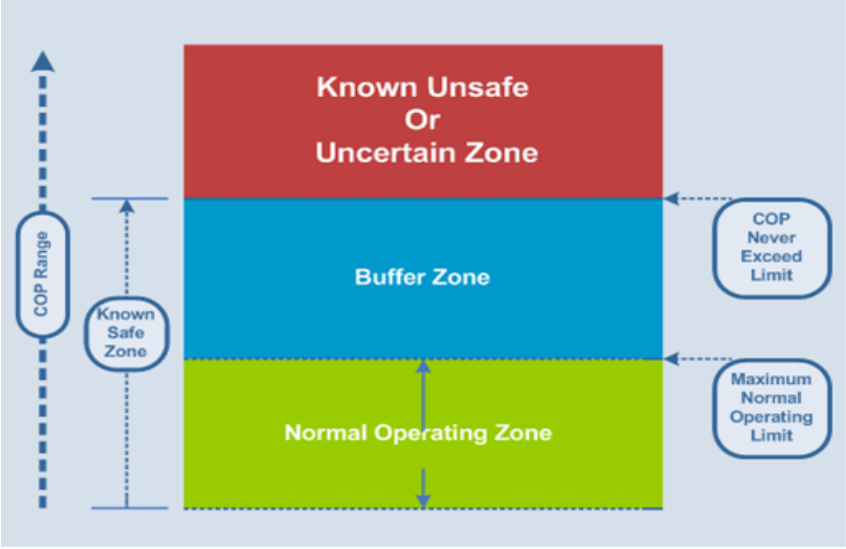

Figure 9 – Critical Operating Parameter zones

Example:

The hazard 'overpressuring of a vessel' has controls covering a range of layers of protection as follows:

- Design standards – Design standards dictate that the pump cannot deliver enough pressure to overpressure the vessel
- Operating procedures – Operator's procedure for filling the vessel
- Control systems – Process monitoring
- Safety devices – Pressure relief valves
- Emergency systems – Emergency Response Plan, Emergency Isolation Valve, Gas Detection.

In assessing these layers of protection the following can be noted:

While the pump can't overpressure the vessel, it can still be overfilled. The contents may then expand on a hot day and still overpressure the vessel. Hence the important controls are process monitoring and the filling procedures. These rely on a single level indicator and the attention of an operator who may get distracted. An alternative control considered was to add a high-level trip on the pump to the vessel.

The decision was then made to add the high-level trip based on the suite of control measures, their effectiveness, and the potentially significant consequences.

3.1.3. Availability

The availability of a control measure is the percentage of time that it is capable of performing its function (operating time plus standby time) divided by the total period (whether in service or not). In other words, it is the probability that the control has not failed or is undergoing a maintenance or repair function when it needs to be used. Therefore, a firewater pump available for 8585 hours per year has 98% availability.

The availability of the control measure should be assessed against the proportion of time it is actually required to operate. For example, the battery life on an emergency lighting system should be equal to, or more than, the intended length of time the lights would be used.

3.1.4. Reliability

The reliability of a control measure is the probability that at any point in time it will operate correctly for a further specified length of time. Reliability is all to do with the probability that the system will function correctly and is usually measured by the mean time between failure (MTBF).

Function testing should be sufficiently frequent to detect failures, and detected failures should be rectified promptly through maintenance or replacement.

Example:

Suppose maintenance becomes proficient at repairing a recurrent failure, reducing downtime. Availability will improve but reliability will not be improved.

3.1.5. Survivability

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

OPGGS(S) Regulation – Safety Case Requirements	
Reg 2.14(2)(b)	The safety case for a facility must demonstrate that, 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 requirements of OPGGS(S) subregulation 2.14(2)(b) are linked to the performance standards that apply as required under subregulation 2.20(2)(b) for the emergency response plan. Operators may wish to conduct survivability studies for key equipment and systems to provide evidence that the requirements of subregulation 2.14(2) are met.

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

3.1.6. Dependency

The dependency of the control measure is its degree of reliance on other systems in order for it to be able to perform its intended function. If several control measures can be disabled by one failure mechanism (common mode failure), or the failure of one control measure is likely to cause the failure of others, then the control measures are not independent, and it may not be appropriate to count such measures as separate.

Adopting a diverse range of control measures such as a combination of inherently safe features, hardware and procedural controls will assist in achieving independence.

Example – Accommodation module Temporary Refuge:

A temporary refuge on an offshore facility is required to maintain its integrity for 1 hour.

The integrity of the temporary refuge in the event of an uncontrolled gas release is supported and protected by a number of features including HVAC shutdown inter-linked to confirmed gas detection in air intakes. Further inherent safety is provided by gas-tight door seals on all doors leading to the accommodation module. Passive fire protection is provided on the exterior walls for protection in the event the gas release should ignite.

3.1.7. Compatibility

Whether or not a control measure is compatible takes into account how alternative control measures may interact with other controls and the rest of the facility, if introduced. Consideration should be given to whether new control measures are compatible with the facility and any other control measures already in use.

Example:

An operator may in the past have complied with AS 3000 Electrical Installations standard which has been revised in 2007 with respect to selection of cables for size and colour. The operator may assess that there is a risk arising from the use of two different cable colour schemes in the same system.

3.2. Defining parameters of a performance standard

A performance standard should state the key requirements (indicators) that the control measure has to achieve in order to perform as intended in relation to its functionality, availability, reliability, survivability and dependencies.

If a performance standard is based on industry standards and codes for the control measure to meet, then the performance standard should include the key requirements (some of which may be contained within the codes and standards) that the control measure will be measured against during its life and not simply list the codes and standards that apply. It is important that the parameters set in the performance standard are specific (well defined and not open to wide interpretation), measurable, appropriate, realistic and timely (SMART).

Specific	performance standards should well defined and not open to wide interpretation.
Measurable	whenever possible, performance standards should be based on quantitative measures such as direct counts, percentages, and ratios.
Appropriate	the performance standard should be in alignment with the overall goal of the control measure.
Realistic	performance standards should be achievable, but may be challenging, and attainable using resources available.
Timely	performance standards should be developed and made available in a timely manner. For example, operational performance standards should be available prior to start-up of operations.

Example:

API 521 is applicable to pressure-relieving and vapour-depressurising systems on oil and gas production facilities. The information provided is designed to aid in the selection of a system that is most appropriate for the risks and circumstances involved in various installations. API 521 specifies requirements and gives guidelines for examining the principal causes of overpressure; determining individual relieving rates; and selecting and designing disposal systems, including such component parts as piping, vessels, flares, and vent stacks.

For a specific FPSO with a process system designed in accordance with API 521, the system has been evaluated and a performance target set to be depressurised to 6.5 barg within 12 minutes. Typically, the blow-down is automatically initiated and blow-down valves are designed to fail open. In this case the pressure decay over time can be monitored and logged on the process control system e.g. it is measurable as “pressure versus time". The blow-down rate is designed to meet the objective of effective and safe disposal of hydrocarbons within the process system and, for a fire case, ensuing jet fire is within a quantifiable magnitude which is considered appropriately benign. The performance is achievable but can be compromised if the topside isolation shut-down valves (SDVs) are passing or the blow-down valves (BDVs) fail to open on demand. SDVs and BDVs have their own performance standards – typically SDVs are fire rated per API 607 / API 6FA or an equivalent standard; and they have defined closing speeds.

3.3. Utilising findings from the risk assessment

Risk assessment should generate information useful to the setting of performance standards for control measures. Typical considerations that might come from the risk assessment are:

- control measures associated with high risk MAEs may require rigorous performance standards
- the required reliability or number of control measures should reflect the likelihood and consequences of the corresponding MAEs
- the interdependence of control measures should be specifically noted and accounted for.

3.4. Performance standards for “other” controls

In general, the process of assigning performance standards to technical controls is straight forward when a control measure is viewed in terms of functionality, availability, reliability, survivability, dependency and compatibility. There are, however, certain procedures or administrative controls within the safety management system that are key hazard and risk management controls for MAEs.

When it comes to setting performance standards for administrative or procedural controls the same principles apply as for technical controls, but not all parameters may be relevant.

The consideration of “other” controls in the FSA process tends to be at a high level, (i.e. at a system level). It is in the development of performance standards that an appropriate level of detail is introduced. This level of detail should be commensurate with the complexity of the system being considered and must be adequate to allow the performance standards to be verifiable (i.e. quantifiable and measurable). They are the acceptance or test criteria for the verification of MAE controls; this applies equally to procedural and administrative controls as it does to technical controls.

Example:

The Permit to Work system will have the following functionality criteria as a minimum (drawn from requirements of OPGGS(S) regulation 2.10):

- the PTW system is a documented system
- the PTW system coordinates and controls safe performance all work activities at the facility, including in particular:
  - welding and hot work
  - cold work (including physical isolation)
  - electrical work (including electrical isolation)
  - entry into and working in a confined space
  - procedures for working over water
  - diving operations.
- permits are issued by the appropriate authorised person
- permit work is supervised by the appropriate authorised person
- personnel are trained and competent in the use of the PTW system.

Availability of the permit to work system may be an issue for a new facility, for facilities that have changed operator, or facilities new to Australian waters. In these cases there may be a transition period required before the operator's safety management system is fully implemented. 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 element (in this case the permit to work system) is fully implemented.

Reliability of the system would be related to workforce compliance with the system, and the required frequency by which this is tested (through audit functions) will be determined by reliability criteria set in the performance standard. When a functional aspect of the permit to work system is found to have failed then the frequency of the audit function should be reviewed and if necessary adjusted accordingly to increase testing of the system.

Interdependencies with other systems would include training and competency management. Compatibility with the facility shift roster system may be relevant for permit authority availability, etc.

Example:

A competency assurance system may be quite complex in that competence cannot be assured by a one-off test or examination in a training environment. Competence describes actual performance in the workplace (or valid simulation of the workplace) over time. It requires that a person has both the knowledge and the skill to perform a particular function and also the ability to apply these to unforeseen circumstances. Competency develops over time and therefore a competency assurance system should reflect various levels of attainment within any skill area ranging from minimum proficiency through to fully competent.

Functional requirements of a competency system will have elements of personnel selection according to qualifications required for the role, initial and on-going training to specified standards, and on-going coaching, supervision and assessment by personnel who are themselves deemed competent to do the assessments

Performance standards can be set against required recognised qualifications, timeframes set for completion of individual training needs analysis and the training itself, % completion of competency assessments at pre-set intervals, emergency response training drills and follow-up reviews, minimum manning level requirements against planned work scopes and emergency response requirements, audit and review schedules, number of non-conformities found, etc.

Performance measurement can be monitored through recruitment process records, competency-based training and assessment records, individual training needs analysis and plans prepared and implemented, job manuals including role competency requirements developed for each position, records of gap analyses conducted, review of training matrices, emergency response drills, audit findings.

3.5. Lifecycle and continual development

There are a number of ways in setting out performance standards. Operators may choose to have different performance standards set for the different stages in their facility's life, for example initial and ongoing suitability standards, or just one single performance standard to cover all. It is critical that whatever performance standards are established they remain relevant and effective for the life of the facility in managing risk to a level that is ALARP.

The appropriateness of individual performances standards may change during the life of the facility. The operator should therefore consider means of assessing their suitability throughout their facility's life in order to ensure compliance with OPGGS(S) subregulation 2.5(4)(e). Some examples noted for consideration are:

- conduct annual MAE reviews incorporating feedback from process / integrity monitoring
- conduct gap analyses and evaluate performance requirements for control measures
- introduce additional control measures as necessary
- adjust assurance tasks to incorporate changes
- apply a continuous monitoring and feedback loop.

Figure 10 shows the relationship between the FSA and ongoing operations and risk management. These are linked through the process of developing performance standards and their continual improvement over time.

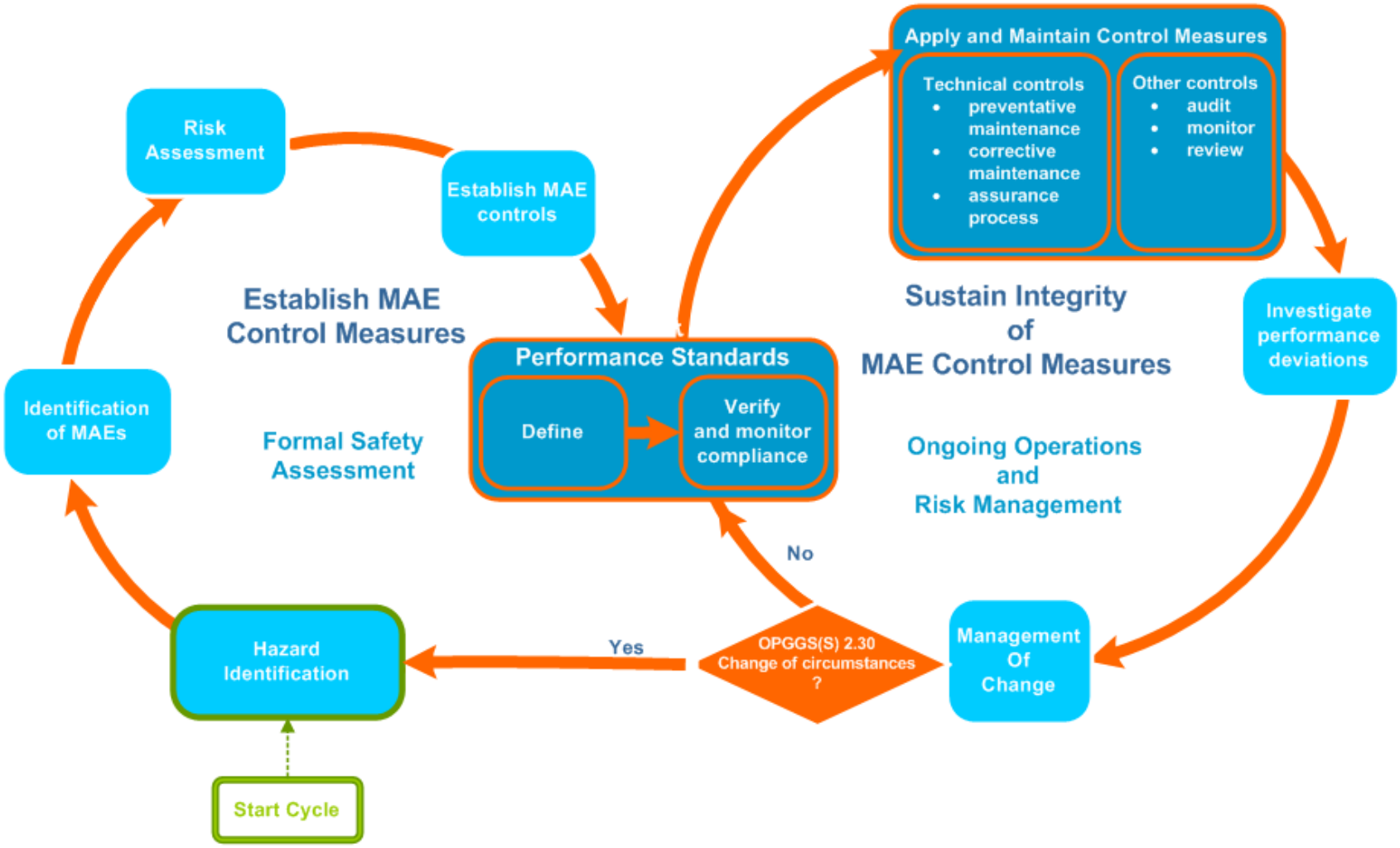

Figure 10 – Performance Standards and Continuous Improvement

4. Assurance of control measures

There are a number of different ways by which the regulations require the operator to provide assurance to NOPSEMA that control measures will eliminate the hazards or otherwise control the risks to health and safety of people at or near the facility. These are described in the sections that follow.

4.1. Validation

Validation is an assurance activity that may be requested by NOPSEMA as per OPGGS(S) regulation 2.40.

OPGGS(S) Regulation - Validation	
Reg 2.40(4)	The validation must establish, to the level of assurance reasonably required by NOPSEMA: (a) in the case of a proposed facility — that the design, construction and installation (including instrumentation, process layout and process control systems) of the facility incorporate measures that: (i) will protect the health and safety of persons at the facility; and (ii) are consistent with the formal safety assessment for the facility; and (b) in the case of an existing facility — that, after any proposed change or changes, the facility incorporates measures that will protect the health and safety of persons at or near the facility.

The validation process is therefore the first assurance activity in the lifecycle management of control measures. For new safety cases and for revised safety cases where the operator proposes to modify or decommission the facility, the operator must not submit the safety case or revised safety case before the operator and NOPSEMA have agreed on the scope of validation [OPGGS(S) subregulations 2.24(4) and 2.30(3)].

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

4.2. Ongoing assurance

The regulations also include a requirement for the safety case to describe the means by which the operator will ensure the ongoing adequacy of the design, construction, maintenance and modification of the facility. This obligation on the operator is detailed in regulation 2.12.

OPGGS(S) Regulation - Safety Case 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 have been submitted.

There is no prescribed methodology for demonstrating the adequacy of control measures, however there are several basic approaches which may be used to support an operator's provision of evidence and

justification within the safety case. Operators could consider using one or more of these approaches but should also be prepared to consider developing specific approaches appropriate to their facilities.

ISO 10418 "Petroleum and natural gas industries – Offshore production installations – Process safety systems" provides objectives, functional requirements and guidelines for techniques for the analysis, design and testing of surface process safety. This document is applicable to fixed offshore structures, floating production, storage and off-take systems for the petroleum and natural gas industries.

In practice, it is likely that most facilities will require a combination of approaches.

4.2.1. Comparison with Codes and Standards

Compare design, the safety management system framework and operational procedures against national or industry standards, codes of practice, guides etc. as these are revised.

4.2.2. Audit against good practice

Audit the basis and implementation of the management system, including operations and maintenance systems, against good practice for offshore facilities, vessels, or onshore major hazard facilities in the same or similar industries.

4.2.3. Technical Analysis

Evaluate control measures in technical terms, assess strengths and weaknesses, e.g. effectiveness, functionality, availability, reliability, technical feasibility, compatibility, survivability, correspondence of control measures to hazards and risks, appropriateness of performance standards, etc.

4.2.4. Performance Data

Evaluate safety-related performance data as evidence of adequacy or satisfactory levels of performance, e.g. data on the operational effectiveness or reliability of a control measure may support the demonstration of its appropriateness for that service.

4.2.5. Improvement Approach

Demonstrate the extent of relative improvements in performance for the facility based on past, present and planned modifications and enhancements.

4.2.6. Benchmarking and Judgement Approach

Present considered judgements as to the suitability of control measures and the management systems, or the perceptions of a cross-section of various stakeholders, e.g. key members of the workforce, senior management, plus independent observers.

4.2.7. Practical Tests

Demonstrate that the management system and/or control measures function effectively, using major incident simulations, management system tests, equipment breakdown and recovery tests, etc.

A periodic assessment of control measure effectiveness should form an integral part of the adequacy assurance process. For safety case purposes, the rationale for deciding the adequacy of the measures employed should be supported and accompanied by all assumptions made and conclusions drawn. Where appropriate, the results of supporting studies that have been performed should be described.

4.3. Sustaining technical integrity of control measures

OPGGS(S) Regulation - Safety Case Requirement	
Reg 2.14(2)(a)	The safety case must demonstrate that the equipment is fit for its function or use in normal operating conditions.

Once an operator has identified (and subsequently implemented) the technical and other control measures necessary to reduce risks to a level that is ALARP, the operator must then demonstrate that the control measures identified are, and will continue to be, adequate for their intended purpose. For technical control measures in particular, the regulations require the operator to provide a demonstration that equipment is fit for purpose. This is an important means of providing evidence that risks are controlled to a level that is ALARP in ongoing operations.

OPGGS(S) Regulation - Safety Case Requirement	
Reg 2.5(4)(f)	The safety case for a facility must also contain a detailed description of the safety management system that provides for inspection, testing and maintenance of the equipment and hardware that are the physical control measures for those risks.

The operator's safety management system must be comprehensive and integrated for all aspects of the control measures. As such it must be shown to fully support and maintain the performance standards of the control measures within an integrated management framework.

The performance standards should be clearly traceable to their associated control measures. They should also reference associated strategies, procedures, work instructions and other assurance related documentation within the facility safety management system. Having clear links enables the operator to measure, monitor and test the effectiveness of each control measure.

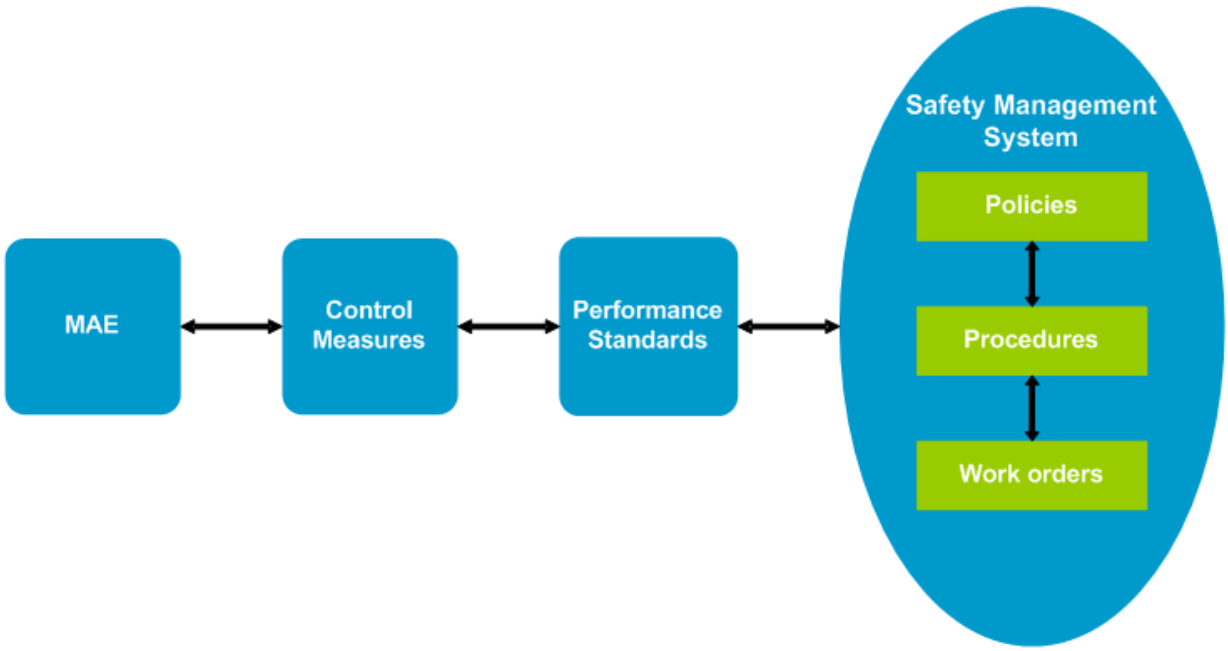

Figure 11 – Control Measure integration into the SMS

In order for the operator to assure control measures achieve performance standards there must be a clear link between performance standards and the operator's safety management system. In particular, the maintenance and testing systems need to be clearly aligned with the performance standards.

This may be achieved by undertaking a number of activities including but not limited to:

- developing and implementing inspection, testing, audits and maintenance tasks for control measures that are able to assure functionality as per the performance standard requirements
- making certain these assurance strategies are undertaken at the appropriate time
- maintaining a record of the activities and findings
- addressing any deficiencies or non-conformances and taking corrective action to maintain the risk to ALARP.

Example:

An example of an assurance activity is a 3 monthly function test and leak test for a sub-sea isolation valve (SSIV).

In this case it is expected that the SMS include a test routine to cycle the SSIV and record its closure time and additionally, monitor pressure build up to determine leak rates. The acceptable maximum closure time and leak rate parameters being verified are to be clearly stated in the performance standards.

4.4. Monitoring compliance with performance standards

The SMS procedures and administrative controls in place should ensure that once implemented, control measures continue to be fit for purpose on an ongoing basis. SMS controls should therefore be subject to monitoring, audit and review.

Monitoring comprises the routine checking that activities under the SMS are actually being conducted, the measurement of actual performance of the SMS elements, and the comparison of this performance with the defined performance standards or targets.

Audit is the process of checking that the overall established SMS is understood and is being used and that the management framework (in particular the monitoring and corrective action processes) is being implemented and is effective. It can also include evaluation of the degree of compliance against the defined standards. Both quality control and quality assurance are necessary: checks are required that activities occur, that the activities are being performed to a suitable standard; and that the systems, procedures, controls etc. are achieving the desired results.

Review is the regular but less frequent process of stepping back and asking if the entire system and the standards within it remain adequate, fit-for-purpose, and in-line with current good practice. A view should be taken as to whether or not the performance standards are appropriate once practical experience has been gained.

A combination of Monitoring, Audit and Review is necessary to ensure the ongoing effectiveness of the SMS, and to drive continual improvement.

Further guidance is available in the NOPSEMA guidance note:

"Safety management systems"

Performance standards of technical control measures are sustained by the maintenance management system to reduce risks to ALARP. For technical control measures, failure to meet required performance standards should result in a review of maintenance requirements. Measures such as decreased periods between scheduled maintenance, and increased testing and inspection frequencies may be required to ensure performance standards are met.

4.5. Contingency measures for control measure failure

"Failure" of a control measure can be present in several different ways:

- complete failure or absence of the control
- chronic failure or decline of performance over time
- marginal ability of the control to perform as intended from the outset due to inadequate design.

As part of the development of performance standards for safety-critical equipment and safety-critical procedures as part of the safety management system, the operator should consider the possible failure modes and develop associated contingency measures to apply if a performance measure is not met. For example, the operator's safety management system should address what action should be taken if a control measure is deemed to be impaired or compromised, i.e. unable to meet its performance standard(s). Such contingency measures could range from applying additional alternative control measures to ceasing operation of the facility, or parts of the facility, until the ability of the control measures to meet the performance standards is restored.

Contingency measures should be developed as part of the development of the safety case to avoid the situation where the operator needs to submit a revised safety case for each deviation from a specified performance standard. It also avoids the operator seeking consent to operate outside the safety case in these circumstances. NOPSEMA policy is to avoid issuing consent to operate outside the safety case in such circumstances, as these types of consent are reserved for emergency scenarios which are considered to be not reasonably foreseeable.

It is up to the operator to establish appropriate contingency measures for their facility and operations, based on assessment of the risks created by the control measure failure or deviation.

Operators should consider the extent to which a breach of the design envelope for technical control measures results in 'damage to safety-critical equipment'. Consideration should be given to whether such incidents are to be notified and reported to NOPSEMA under OPGGS(S) regulations 2.41 and 2.42 'Notification and Reporting of Accidents and Dangerous Occurrences'.

Example:

An example of a complete failure is an emergency generator that won't start on demand.

An example of chronic failure is marine growth on impellors or filters.

An example of marginal ability is the addition of emergency electrical systems over time which renders the original UPS system inadequate to be able to meet the increase in demand.

Further Information is available in the NOPSEMA paper:
"Notification and Reporting of Accidents and Dangerous Occurrences"

Further guidance is available in the NOPSEMA guideline:
"Operational Risk Assessment"

5. Outputs

At the end of the process of control measure identification, selection and assessment, the following information should be available:

- a list of the existing and potential control measures and an understanding of their relationship to MAEs
- identification of new control measures to be implemented
- effectiveness assessment information for existing controls and any new controls which are to be implemented
- a list of improvement actions recommended for existing control measures
- a list of hazards where additional control measures may be desirable
- performance standards for the MAE control measures.

These outputs should be documented with clear linkages between the hazard identification, the risk assessment and the outcomes from the control measure assessment. Good documentation at this stage will significantly help the demonstration that risks are reduced to a level that is ALARP.

The overall process of control measure assessment is shown schematically in Figure 12.

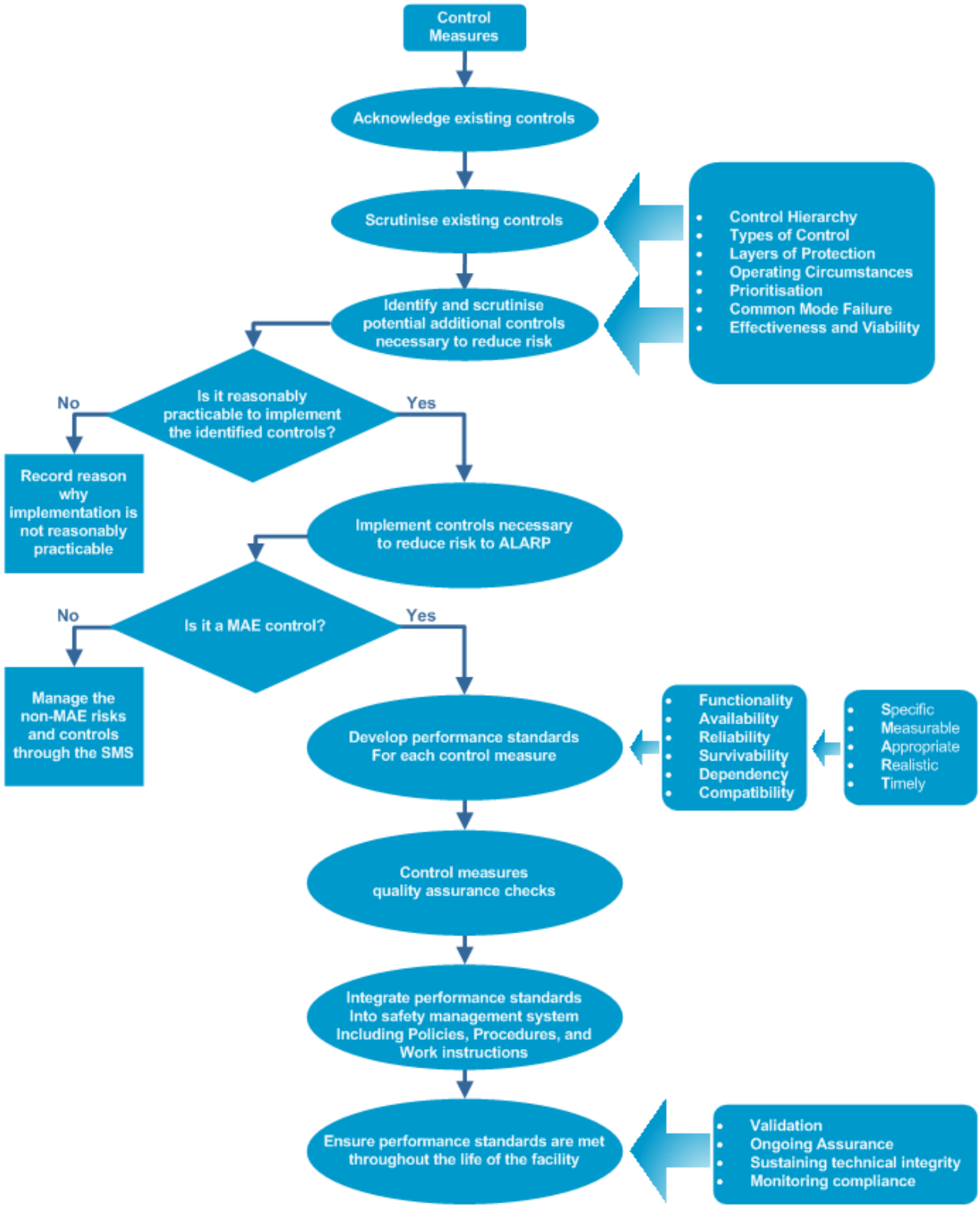

Figure 12 – Process of Control Measure Selection and Implementation

6. Quality assurance

At the completion of the control measure assessment phase, it is important that checks for quality assurance are conducted. The following table outlines the key activities and checks that should be undertaken to ensure quality in the control measure selection and assessment process. These checks will also assist to ensure that all control measures relevant to major accident events have been identified, selected and assessed.

Table 2 - Key Activities and Checks for Quality Assurance

Activity	Check
Verify all control measures have been identified	Use a checklist to confirm that all types of control measures have been identified.
	Have those personnel who were not present when control measures were identified review the hazard identification documentation and the bow-tie diagrams
	Review previous risk assessments to identify hazards and controls not identified during the hazard identification.
	Review other documents that may indicate additional control measures. For example: • Cause-effect diagrams for protective systems • Equipment manufacturer manuals, etc. • Codes and standards
Verify accuracy of information	There is a need to confirm that the control measures are in place. Experience shows that this is not always the case. An individual should be appointed to verify the control measure is in place and meets the description provided in the hazard register.
	A field check will identify whether a control measure has been changed over the life of the plant. Frequently it is found that the control measure has been modified and the documentation not updated to reflect the change.
	A review process is included to verify the output of control monitoring (e.g. adequacy assessments, criticality assessment).
	Where the adequacy assessment includes verifying the functionality for the control measure, is there documentary evidence? Is it linked with the safety case?
Verify the outcomes (assessment, performance indicators, critical operating parameters) have been communicated	Is there a communication/ training plan in place?
	Is there a requirement for this training to be signed off after completion?
	Is this training list available and does it confirm that all relevant personnel have been trained?
	Are written procedures in place where required (e.g. Critical operating parameters)?
	Have contingency measures been identified for the different possible performance standard failure types?

7. Common weaknesses

7.1. Control measures

The following are common weaknesses associated with control measures:

- a single control measure has been considered rather than a range of control measures
- concentrating effort on mitigation measures for fire and explosion risks rather than consideration of measures higher up the control hierarchy
- assuming that industry codes and standards are suitable by default, without justification of their application in the specific situation
- there is no direct link to clearly established performance standards for control measures
- "As Built" information is missing.

7.2. Performance standards

The following are common weaknesses associated with performance standards:

- performance standard has no defined performance parameters to facilitate the design of assurance tasks and supporting verification
- performance standard has no information on interdependencies
- performance standards fail to cross-reference to the source information
- performance standards provide no direction or link to what actions or processes should be followed if the performance standard is not met
- failure to conduct ongoing review of performance standards for production against actual well stream and process data
- failure to address degradation and lifecycle asset management issues using control measure performance standards
- blindly applying marine standard classification society provisions for shipping to MODU and platform applications without conducting review of the suitability of those standards.

8. References, acknowledgements and notes

8.1. Legislation

- *Offshore Petroleum and Greenhouse Gas Storage Act 2006*
- Offshore Petroleum and Greenhouse Gas Storage (Safety) Regulations 2024

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 2024. For facilities located in designated coastal waters, please refer to the relevant State or Northern Territory legislation.

8.2. Codes and Standards

- AS IEC 61511 – "Functional safety - Safety instrumented systems for the process industry sector"
- ISO 13702 – "Petroleum and natural gas industries – Control and mitigation of fires and explosions on offshore production installations – Requirements and guidelines"
- ISO 15544 – "Petroleum and natural gas industries – Offshore production installations – Requirements and guidelines for emergency response"
- ISO 17776 – "Petroleum and natural gas industries - Offshore production installations –Major accident hazard management during the design of new installations"

8.3. Publications

- AIChE CCPS – "Layer of Protection Analysis: Simplified Process Risk Assessment", ISBN 0-8169-0811-7, 2001
- WorkSafe Victoria – Guidance Note "Control measures for a major hazard facility – Advice for operators of major hazard facilities on identifying, selecting and managing effective risk control measures"

8.4. NOPSEMA publications

- N-03000-GN0099 - Notification and Reporting of Accidents and Dangerous Occurrences
- N-04200-GL0525 - Validation
- N-04300-GN0087 - Safety Case Lifecycle Management
- N-04300-GN0106 - Safety Case Content and Level of Detail
- N-04300-GN0107 - Hazard Identification
- N-04300-GN0165 - Risk Assessment
- N-04300-GN0166 - ALARP
- N-04300-GN1051 - Supporting Safety Studies
- N-04300-GN1052 - Safety Management Systems
- N-04300-GN1053 - Emergency Planning
- N-04300-GN1054 - Involving the Workforce
- N-04300-GN1668 - Safety Case GN Cross Reference
- N-04300-GN1733 - Vessel facilities subject to external hydrocarbon hazards
- N-04300-GN1818 - Operational Risk Assessment

8.5. Acknowledgement

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