Department of **Energy, Mines, Industry Regulation and Safety**

GOVERNMENT OF WESTERN AUSTRALIA

WorkSafe Western Australia Petroleum Safety

GUIDE

Identification of major accident events, control measures and performance standards

Disclaimer

The information contained in this publication is guidance material only. It is provided in good faith and believed to be reliable and accurate at the time of publication.

To ensure you understand and comply with your legal obligations, this information must be read in conjunction with the appropriate Acts and regulations which are available from the Parliamentary Counsel's Office www.legislation.wa.gov.au.

The State disclaims all responsibility and all liability (including without limitation liability in negligence) for all expenses, losses, damages and costs you might incur as a result of the information being inaccurate or incomplete in any way, and for any reason.

In this disclaimer:

State means the State of Western Australia and includes every Minister, agent, agency, department, statutory body corporate and instrumentality thereof and each employee or agent of any of them.

Information includes information, data, representations, advice, statements and opinions, expressly or implied set out in this publication.

Loss includes loss, damage, liability, cost, expense, illness and injury (including death).

Reference

WorkSafe Western Australia, 2024, Identification of major accident events, control measures and performance standards: Guide. Department of Energy, Mines, Industry Regulation and Safety, Western Australia, 33 pp.

This publication can be available on request in other formats for people with special needs.

Further details of safety publications can be obtained by contacting:

WorkSafe Group – Regulatory Support
Department of Energy, Mines, Industry Regulation and Safety
303 Sevenoaks Street
CANNINGTON WA 6107

Telephone: 1300 307 877
NRS: 13 36 77
Email: Safety@dmirs.wa.gov.au

Foreword

Western Australia's work health and safety (WHS) legislation came into force in March, 2022. This resulted in the amendment of the various petroleum Acts and the repeal of the associated regulations so that all onshore and offshore petroleum, pipeline and geothermal energy operations are now subject to the requirements of the:

- *Work Health and Safety Act 2020* (the WHS Act)
- Work Health and Safety (Petroleum and Geothermal Energy Operations) Regulations 2022 (WHS PAGEO Regulations).

A key responsibility for the WorkSafe Group (WorkSafe) of the Department of Energy, Mines, Industry Regulation and Safety continues to be the ongoing risk management and safety requirements for the onshore and offshore petroleum, pipeline and geothermal energy operations. To support these requirements, the guides previously developed have been updated to provide support and assist operators to meet their commitments under the WHS Act and WHS PAGEO Regulations.

Application

This Guide is a non-statutory document provided by WorkSafe to assist persons subject to duties under the WHS Act and requirements to conduct audits of the safety management system as prescribed by the WHS PAGEO Regulations.

It has been developed to provide advice and guidance to operators to meet the WHS Act and the WHS PAGEO Regulations requirements administered by WorkSafe.

Who should use this Guide?

You should use this Guide if you are:

- the operator of onshore or offshore petroleum, pipeline or geothermal energy operations under the WHS Act
- responsible for identification of major accident events, control measures and the development of performance standards (including bowties).

WHS legislation

Under the WHS Act, the WorkSafe Commissioner is responsible for performing the functions and exercising the powers of the regulator. Each safety document must be submitted for acceptance by the regulator.

WorkSafe assists the regulator in the administration of the WHS Act and the WHS PAGEO Regulations, including the provision of inspectors and other staff to oversee compliance with the legislation.

For facilities outside the Western Australian waters, the WHS Act does not apply and guidance should be sought from National Offshore Petroleum Safety and Environmental Management Authority (NOPSEMA). If a vessel does not fall under the definition of "facility" in the Act, operators should contact the Australian Maritime Safety Authority and Department of Transport.

No petroleum or geothermal operations can be conducted on any onshore or offshore petroleum, pipeline or geothermal energy operations unless the facility has an operator registered in accordance with the requirements of WHS PAGEO Regulations.

The WHS PAGEO Regulations provided for transitional provisions in relation to facility operators and safety cases in place or submitted before the commencement of the WHS legislation.

Contents

1 Introduction

WHS PAGEO Regulations r. 109
Managing risks to health and safety

The purpose of this Guide is to assist operators in identifying effective control measures of hazards that have the potential to cause major accident events (MAEs) and the development of performance standards.

For the purpose of this Guide, the term “safety case” is used to cover both the safety case and diving safety management system (DSMS) requirements.

The term “facility” covers offshore and onshore facilities and pipelines, including above ground structures.

The objective of this Guide is to provide clarity on areas of the legislation which may be ambiguous or open to interpretation.

1.1 Aims and outcomes of identification of major accident events

Identification of a major accident event (MAE), the subsequent control measures put in place and the performance standards developed create knowledge, awareness and preparedness within an organisation. Knowledge of the MAEs identified and their implications is necessary to prevent and deal with dangerous occurrences.

The aims and outcomes are to provide:

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

Risk assessments and the identification of possible MAEs carried out at a time when they can affect decisions of significance for the risk level are key for designing and operating a facility safely. The systematic development, implementation, use and follow up of risk assessment is an important contribution towards managing risk through all stages of a facility’s life cycle.

A detailed risk assessment for the facility and operations should cover:

- all potential MAEs and risks to people, property and environment for each identified potential MAE (consequence and likelihood)
- all risks associated with emergencies
- all risks associated with fires and explosions
- all aspects of the facility design, construction, installation, maintenance and modification
- the whole life cycle of a facility, or an explicitly defined period.

A continual risk assessment should be carried out on a regular and ongoing basis as a result of:

- problems reported by workers
- lessons learned from notifiable incident or notifiable occurrence reports both localised and external
- any significant changes or improvements that need to be made
- changes in technology that may provide more effective controls.

1.2 Linked guides

The following guides have been developed that will provide information to assist operators in the area of hazard identification and risk management and the development and implementation of a safety case:

- *Hazard identification*
- *Risk assessment and management including operational risk assessment*
- *Demonstration of risk reduction so far as is reasonably practicable (SFAIRP)*
- *Human factors fundamentals for petroleum and major hazard facility operators*
- *Human factors self-assessment guide and tool for safety management systems at petroleum and major hazard facility operations*

The above guides, together with this Guide, provide information for effective hazard identification, risk assessment and management including identification of MAEs and control measures.

Figure 1 gives an example of the overall formal safety assessment process which may be used by operators to identify and manage the hazards and risks within their organisations and also meet the requirements of the WHS PAGEO legislation.

1.3 Identifying hazards and potential causes

Reports from risk assessment consultations held prior to undertaking the control measure assessment and development of performance standards will identify MAE and non-MAE risks and hazards and assess current controls. The identification of hazards and their potential causes should have taken place during the hazard identification and risk assessment workshops held prior to undertaking the control measure assessment and development of performance standards, as shown in Figure 1.

The reports from these workshops form the basis of the identification of MAE and non-MAE risks, the controls already identified as being in place and the need for further control measures to be identified and assessed.

For further information, see the *Guides: Hazard identification* and *Risk assessment and management including operational risk assessment.*

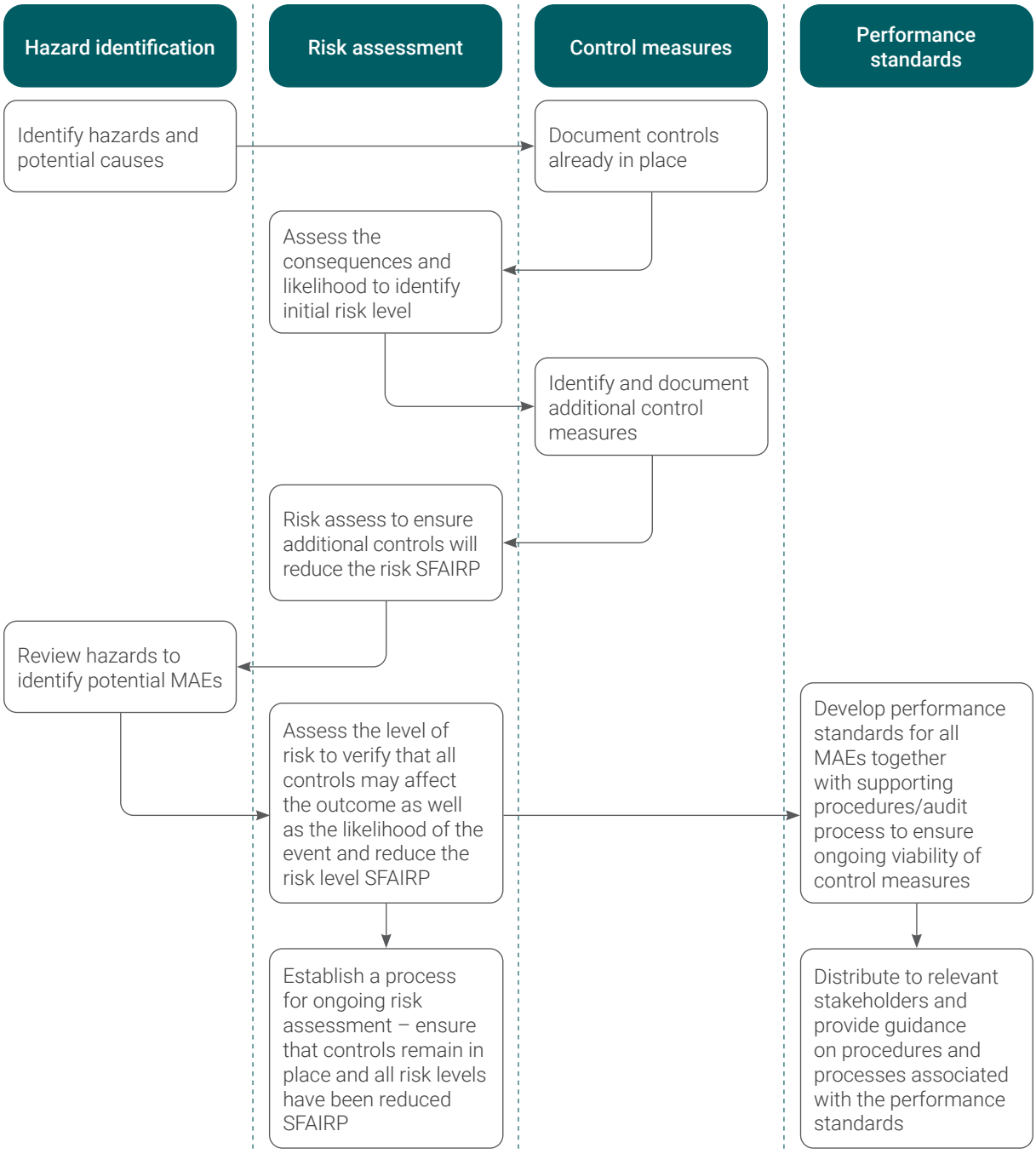

Figure 1 Formal safety assessment process

2 Control measure assessment

Control measures are applied to activities at a facility that eliminate or minimise the risk to health and safety associated with potential MAEs or other hazardous events. These are the means by which an operator reduces risk at their facility so far as is reasonably practicable (SFAIRP).

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

2.1 Control measure assessment team

When selecting participants, consider:

- the overall scope of the proposed process and the activities to be conducted during the phase of operation under review; i.e. design, construction, operational or decommissioning
- technical expertise; i.e. leadership, engineering, design, operational, or, if relevant decommissioning; this will allow identification of hazards not evident in individual workgroups to be identified through interaction between the workgroups
- workers with a thorough knowledge of the facility or similar facilities if appropriate, and its history
- areas of the general workforce that need to attend taking into account any interactive areas within the facility, shift rosters, simultaneous operations (SIMOPs) and third party impacts.

Consider the appointment of a facilitator. It is important the facilitator has the appropriate level of expertise and knowledge of the technique adopted for the hazard identification process and is able to manage the team so that all attendees have the opportunity to put forward their views and opinions.

The hazard identification and risk assessment reports already conducted on the facility must be available for the control measure assessment.

A facilitated workshop is a common way of gathering accurate information based on a diversity of viewpoints. However, when assessing the suitability of controls, another option is to have selected workers prepare the control measure assessment and then run a workshop to validate their work.

Where an operator has multiple facilities, it may be appropriate to involve independent workers from one facility to review the assessments completed in relation to another similar facility.

2.2 Worker involvement

WHS Act s. 47
Duty to consult workers

WHS Act. s. 48
Nature of consultation

WHS PAGEO Regulations r. 38
Involvement of workers

The operator of a facility must demonstrate that there has been effective consultation with, and participation of, workers in the hazard identification and risk assessment process leading up to the identification and application of control measures.

As well as including the subject matter experts, other workers can provide direct knowledge of the activities under consideration and the effectiveness of the controls that are being considered to reduce the level of risk. Operators should ensure that contributions from workers are considered on the basis of technical and working knowledge and not on the seniority of the contributor. Ensure opportunities to contribute are not dominated by individual persons or groups within the organisation.

Workers are entitled to take part in consultations and to be represented in consultations by a health and safety representative who has been elected to represent their work group. Consultation with workers and their health and safety representatives is required at each step of the hazard identification process.

In the event that a proposed hazard identification process relates to a new facility where the workforce has not yet been fully identified and put in place, involving workers from a similar facility should be considered.

By drawing on the experience, knowledge and ideas of workers, operators are more likely to identify all hazards and choose effective control measures.

Those workers invited to be part of hazard identification process should be involved in:

- development of the process
- forming the team and scheduling consultation, such as through meetings and workshops
- considering a range of methods for consultation such as via email, surveys, an intranet health and safety page, and conducting meetings via teleconference or video link up as well as in person
- conducting the consultations and reviewing any results or outcomes
- implementing of any actions arising from the process
- assisting in provision of feedback of the consultation outcomes to the rest of the workforce.

Those workers involved in this phase can then provide feedback to the general workforce to provide a better understanding of the controls in place. This inclusion and consultation also promotes a feeling of ownership among workers not directly involved in the process which enables the ongoing monitoring and where applicable reporting of any reduction in the level of control measures applied.

For more information, refer to the *Guide: Involvement of workers and the Code of practice: Work health and safety consultation, cooperation and coordination.*

2.3 Control of MAEs versus control of all health and safety risks

WHS PAGEO Regulations r. 32

Operation description, formal safety assessment, safety management system and emergency response plan

An MAE is defined in the WHS PAGEO Regulations as an event connected with a facility (including a natural event) that has the potential to cause multiple fatalities of persons at or in the vicinity of the facility.

Events that result in catastrophic consequences, such as the the explosion and fire on the Piper Alpha Platform in 1988, are rare and the resultant potential to become an MAE can be overlooked in the hazard identification process. The safety case regime provides a regulatory requirement to focus on addressing potential for MAEs as well as continuing to address work health and safety.

Identifying potential MAEs is crucial in the development of the formal safety assessment for a safety case. All identified hazards must be subject to a screening process to determine if they can result in an MAE. Those hazards identified as having the potential to lead to an MAE must be considered in the formal safety assessment, whereas those not likely to result in an MAE, but are a hazard to health and safety must be addressed in the operator's safety management system.

While MAEs are a key factor in the formal safety assessment, the safety management system (SMS) 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 must address both MAEs and other health and safety risks through procedural systems designed to minimise risks SFAIRP. Figure 2 depicts the screening process for MAE and non-MAE control measures.

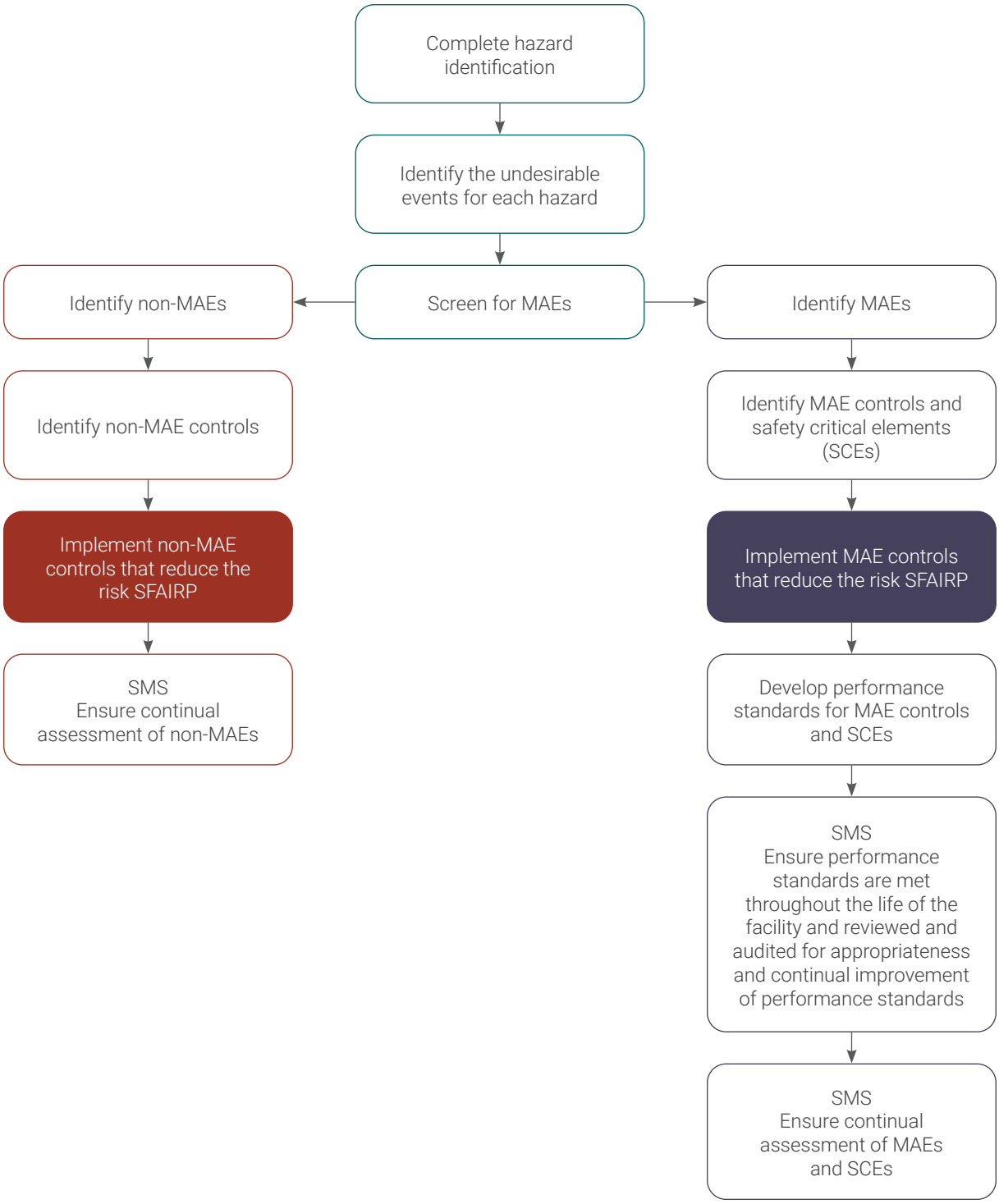

Figure 2 MAE and non-MAE control measures

2.4 Aims and outcomes of control measure assessment

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

- provide operators and workers 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 incidents
- 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 minimising risk
- lay the foundations for demonstrating within the safety case that the risks have been minimised SFAIRP
- 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.

3 Identifying and selecting control measures

3.1 Identifying control measures

WHS PAGEO Regulations r. 32(3)
Content of safety cases – Formal safety assessment

The purpose of control measure identification is to identify the existing and potential control measures for each hazard and associated outcomes. It is important to have a methodical approach to identify and consider a variety of potential control measures and to explore them sufficiently to be able to provide reasons why certain control measures are selected and others rejected.

3.2 Safety critical elements

A safety critical element (SCE), as defined within the WHS PAGEO Regulations, is any part of a facility, system, process, procedure, person or other control measure the purpose of which is to prevent, or mitigate, the effect of an MAE, or the failure of which might cause, or substantially contribute to an MAE.

The aims and outcomes of SCE identification, selection and assessment are to:

- provide sufficient knowledge, awareness and understanding of the SCEs for MAEs, to be able to prevent and manage significant hazardous events
- provide a basis for identifying, evaluating, defining and justifying the selection (or rejection) of SCEs
- lay the foundations for demonstrating within the safety case that the risks associated with MAEs have been minimised so far as is reasonably practicable (SFAIRP)
- show clear links between SCEs and the potential MAEs they are intended to control
- understand the effectiveness of adopted SCEs and their impact on risk
- provide a monitoring regime to ensure the ongoing effectiveness of the SCEs
- audit for continual improvement opportunities.

3.3 Safety critical element classification

It is important to recognise that SCEs can be general descriptions of a series of systems, components and sub-systems or sub-components used to perform the same or similar control actions and contribute to the overall effectiveness of the SCE, as in the example presented in Table 1. Performance requirements should be established at those levels that are deemed critical to ensuring the control of a particular MAE.

Table 1 Relationship between SCEs, systems, sub-systems, components and tag items

Category	Example
Safety critical element Typically are groups of systems on a facility which are used to achieve the same general outcome	Emergency shutdown
Safety critical systems The separate systems that fall within the general definition of each SCE that are used to achieve the SCE performance criteria	Instrument initiators
Safety critical sub-system Any part of the SCE system (including computer software) where the failure of which could cause or contribute substantially to an MAE, or a purpose of which is to prevent, or limit the effect of an MAEs	Instrument alarms, supervisory control and data acquisition (SCADA)
Safety critical component Component of a critical sub-system where the failure of the component will lead to failure of the critical sub-system	Actuated isolation valves
Safety critical tag item Individual elements of a critical component, having maintenance tags, where the failure of the tag item will lead to failure of the critical component and therefore the critical sub-system	Function testing of actuators through maintenance management system

SCE components and tag items will have performance requirements identified as part of the higher level SCE and should be linked to the relevant item in the facility maintenance system.

3.4 SCE identification and analysis

A robust and systematic process for the identification of SCEs is essential to ensure that MAE risks are managed and minimised SFAIRP.

Good practice requires application of the hierarchy of controls when determining the most effective risk mitigation. Applying hierarchy of control measures involves, as a priority, designing out or removing hazards at the source and then controlling residual risks by engineering or organisational means. The hierarchy of controls, as described within the safety case SMS, applies when it is not reasonably practicable to eliminate risks to health and safety and is structured from the highest to lowest levels of protection and the most to least reliable, as follows:

- elimination (of hazard at source)
- substitution (of materials/process)
- engineering methods (ventilation/guards, enclosure/isolation of materials/processes)
- administrative controls (includes procedures, work practices, training and education)
- personal protective equipment.

The control hierarchy is applied during each risk assessment and should be revisited as part of SCE identification and selection.

To identify whether a control measure is an SCE requires an understanding of the relationship of the control to the hazards, hazardous events and event consequence it is controlling against and also its relationship to other controls, systems and processes.

A bowtie analysis provides a basic approach to achieve this by graphically representing MAEs and their associated hazards, hazardous events, event consequences and control measures as shown in Figure 3.

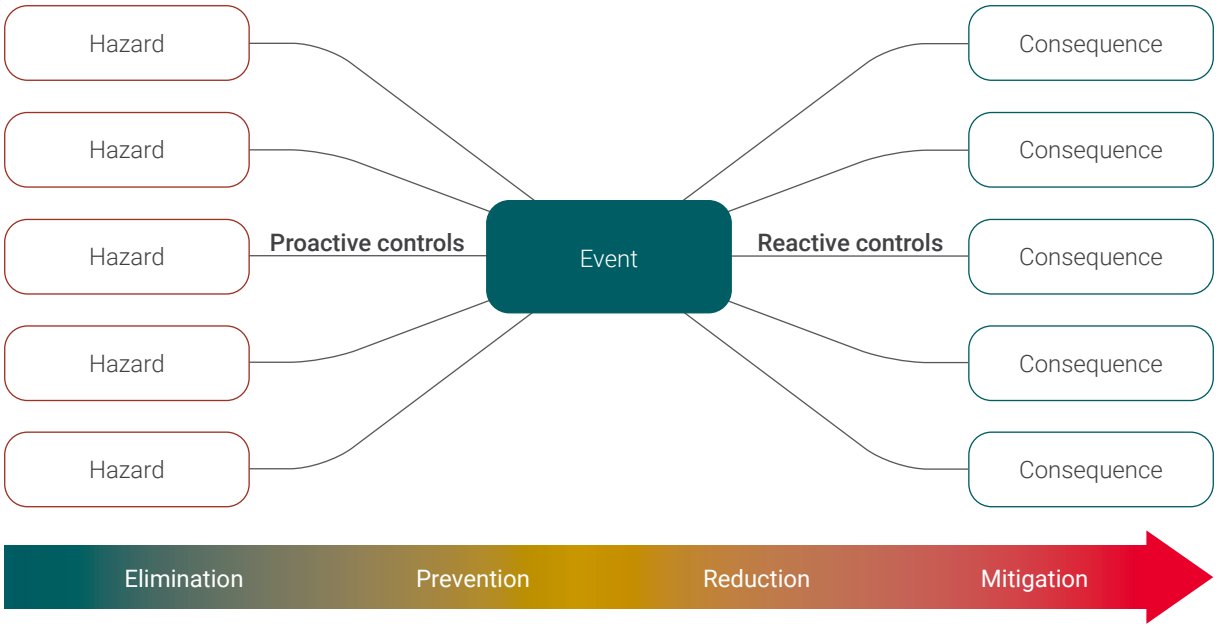

Figure 3 Schematic representation of a bowtie diagram

The type of controls relate to whether they act on the hazard, the hazardous event or the event consequence(s) and whether they are technical controls (i.e. physical characteristics of the facility) or procedural and administrative controls (i.e. rely on workers' action/intervention).

A selection of technical and procedural or administrative controls are necessary to ensure effective risk management as demonstrated in the layers of protection diagram presented in Figure 4 Layers of protection.

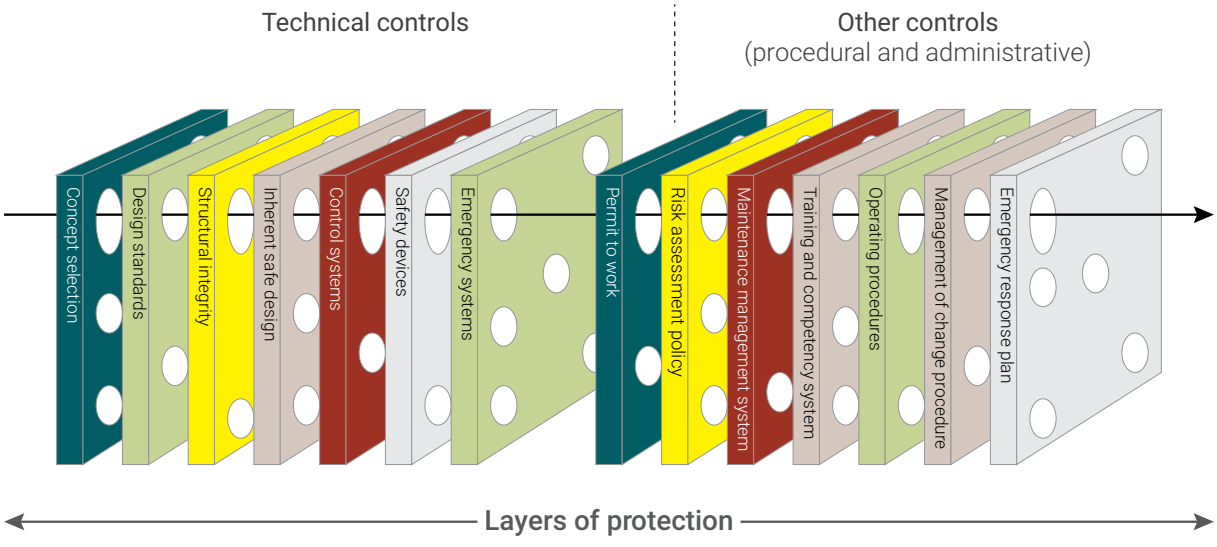

Figure 4 Layers of protection

Figure 4 shows that different control types can act as distinct, independent barriers that can prevent or limit the likelihood or consequence of an MAE. The holes in each barrier recognise that any barrier can be subject to failure. For this reason, having a variety of different barriers provides security against the failure of one or more barriers.

To confirm whether a particular control measure should be classified as safety critical, it is necessary to apply a reasoned check when conducting the bowtie analysis. A sample approach is presented in Figure 5.

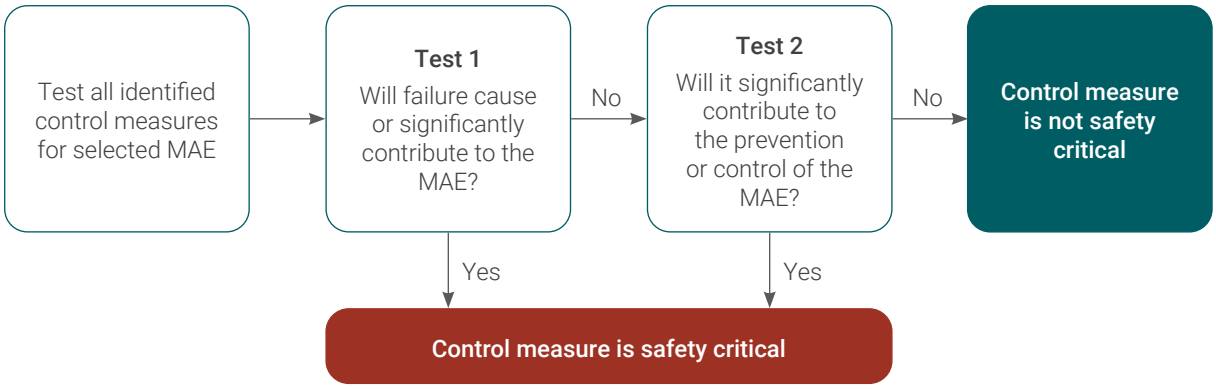

Figure 5 Basic decision criteria for SCE selection

Confirmed SCEs require further consideration to determine whether specific sub-elements exist whose performance can significantly contribute to SCE failure or MAE risk mitigation. The same logic as presented in Figure 5 can be used for this purpose. If consensus cannot be reached in determining safety criticality of a particular control, the flowchart in Figure 6 can be used.

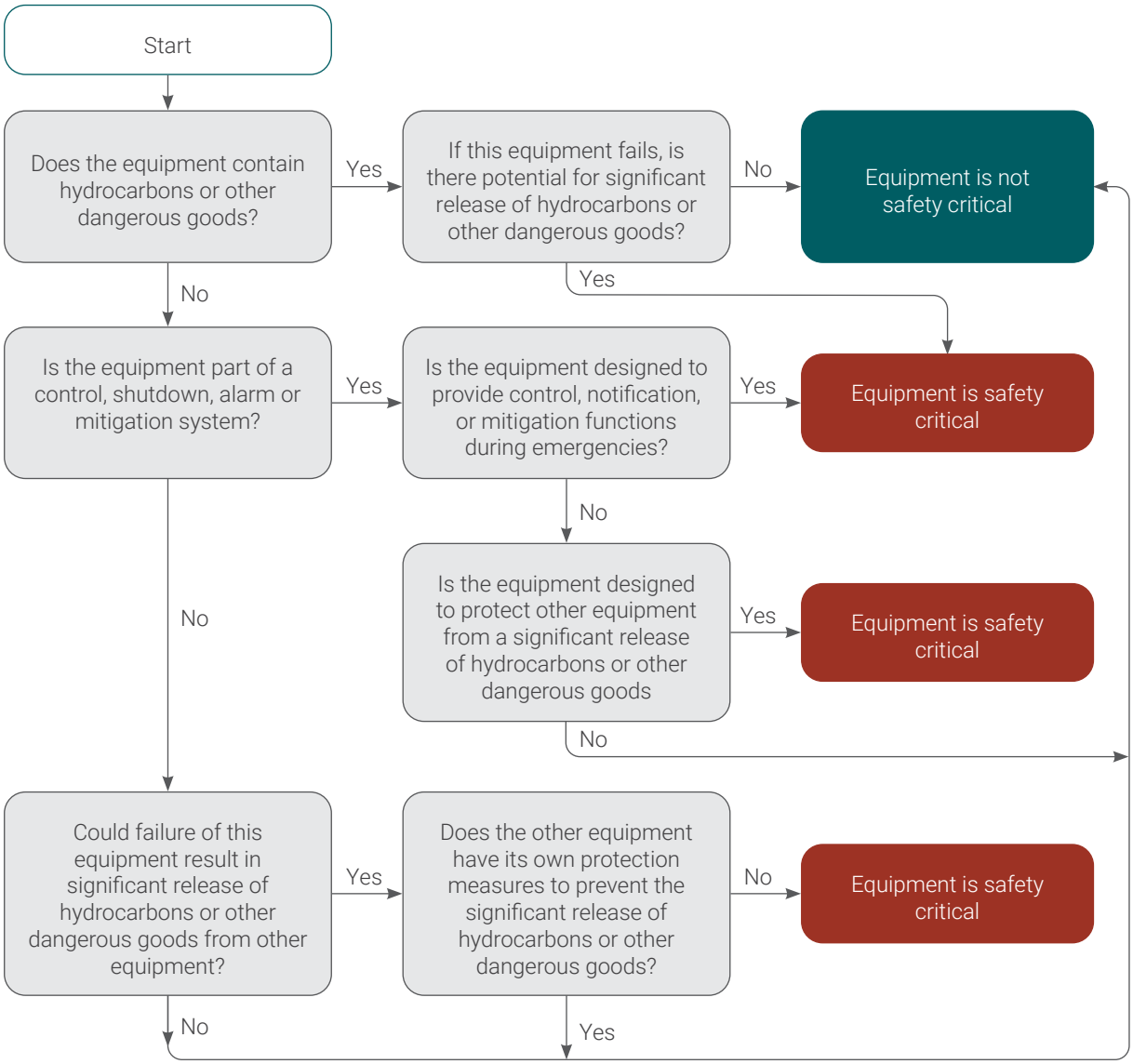

Figure 6 Detailed SCE identification process

SCE identification provides a superficial classification of MAE control measures by classifying these as either safety critical or not safety critical. Further analysis is required to understand the importance of each SCE and whether its effectiveness reflects its importance.

The importance of each SCE can be established by considering if it:

- provides control over multiple MAEs
- prevents hazardous events from the most likely hazards
- protects against the most severe consequence events
- is supported by alternative/back-up control measures that offer control over the same hazards or consequences.

The effectiveness can be determined by understanding if the SCE is:

- vulnerable to events that it is designed to protect against
- susceptible to failure modes common to other SCEs
- dependent on other controls, processes and systems
- sensitive to operational circumstances.

This will allow the performance requirements of the SCE to be determined by:

- functionality
- reliability
- availability
- survivability
- interdependency.

These parameters form the basis for SCE performance standards, which are described in Section 5.

The majority of information required for SCE analysis should be available from basis of design and design philosophy documentation, manufacturer specifications, operating procedures and formal safety assessment studies, which may include:

- hazard identification workshops (scheduled or as required)
- hazard and operability (HAZOP) studies
- control HAZOP studies (CHAZOP)
- AS 2885.6 *Pipeline safety management* (safety management studies)
- safety integrity level assessments (SIL)
- layers of protection analysis (LOPA)
- failure mode and effect (and criticality) analysis (FMEA)
- fire and explosion risk assessment (FERA)
- evacuation, escape and rescue analysis (EERA)
- quantitative risk assessment (QRA).

The level of SCE analysis should reflect the anticipated level of risk reduction that the control contributes over one or more MAEs based on the outcomes of the formal safety assessment studies and bowtie analysis.

4 Performance standards

WHS PAGEO Regulations r. 32(4)
Content of safety cases – Safety management system

4.1 Overview

Performance standards are the parameters against which SCEs can be assessed to ensure they are reducing the risk of an MAE so far as is reasonably practicable.

Performance standards provide a benchmark for measuring, monitoring and testing effectiveness of an SCE, and identify the need for corrective action based on deviations from these benchmarks or performance trends.

4.2 Performance standard content

Performance standards are required for those features of an SCE critical in ensuring control over MAEs. A sample template for a performance standard is included at Appendix 3 of this Guide.

Generally, the following content is required for each performance standard, although this may vary depending on the type of SCE. The content requirements listed in Table 2 should be reflected in a performance standard template.

Table 2 Performance standard template fields

Template fields	Field content description
Title, code, owner, revision, revision date, next revision due	Identify the details of relevant facility, performance standard reference number, owner of the document, revision number, date and date of next revision of the particular performance standard.
Scope	A brief summary of the SCE system and its boundaries, together with a listing of the SCE components within the system boundary. Also identifies scope exclusions, typically as components within the system boundaries that are covered by other performance standards (provide reference to these), or components that are not considered to contribute to the stated objective.
Objective	A brief overview of the overall objective, intention of the SCE which should be aligned to its risk function (prevention, detection, control or mitigation) with respect to the associated MAEs.
MAEs	Identifies the MAEs that the control measure is related to in terms of prevention, detection, control, mitigation or recovery from the event.
Functionality	Defines what the SCE is required to do and how it is required to perform in order to achieve the necessary risk reduction.
SCE component	Specifies the SCE component against which the performance criteria relates.
Key requirement	The specific function required to be performed by the SCE component in the context of mitigating the risk of the associated MAEs.
Performance criteria	The required performance that the SCE component must achieve to confirm that it is effectively performing its function.

Template fields	Field content description
Performance criteria reference	The reference(s) providing the basis for selection of the performance criteria. This shall be in the form [X] where "X" denotes the reference number corresponding to the relevant number in the references table.
Assurance	The activities in place to confirm that the performance criteria are being achieved (e.g. inspection, maintenance, monitoring, testing, exercises and drills).
Assurance reference	The reference(s) that confirm the implementation of assurance measures. Include document title and document number. This shall be in the form [X] where "X" denotes the reference number corresponding to the relevant number in the references table.
Availability/reliability	When must the SCE be available and how reliable must it be to perform its intended function.
SCE component	The component against which the performance criteria is specified.
Availability	Availability is related to the expected probability that an SCE will function as required "on demand" at any point of time and is expressed in units of probability. It is often expressed in terms of probability of failure on demand, or PFD. For example, if there were a 10 per cent chance that an SCE would fail when needed, the probability of failure on demand would be: PFD = 10% = 0.1 and the availability would be: Availability = (100% - PFD) = (100% - 10%) = 90% = 0.9 Availability usually refers to an SCE that sits in the background until required ("on demand"), such as a pressure safety valve.
Availability reference	The reference(s) providing the basis for selection of the availability performance criteria. This shall be in the form [X] where "X" denotes the reference number corresponding (with active link) to the relevant number in the References table.
Reliability	Reliability is related to the expected probability that an SCE will function as required for a specified period of time. It is expressed in units of frequency. It is usually expressed as failure rate. For example, if a pressure piping system is estimated to fail once every 10 years or 0.1 times per year, the failure rate would be: $Failure\ rate = \frac{failures}{time} = \frac{0.1\ failures}{1\ year} = 0.1/year$ Reliability is also expressed as mean time between failures (MTBF), which is the inverse of failure rate: $MTBF = \frac{time}{failures} = \frac{1\ year}{0.1\ failures}\ 10\ year\ (per\ failure)$ Reliability usually refers to an SCE that is in continuous use, such as the integrity of a pressure piping system.
Reliability reference	The reference(s) providing the basis for selection of the reliability performance criteria. This shall be in the form [X] where "X" denotes the reference number corresponding to the relevant number in the References table.
Assurance	The activities in place to confirm the availability and reliability performance criteria are being achieved (e.g. inspection, maintenance, monitoring, testing, exercises and drills).

Template fields	Field content description
Assurance reference	The reference(s) that confirm the implementation of assurance measures. This shall be in the form [X] where "X" denotes the reference number corresponding to the relevant number in the References table.
Survivability	Will the SCE function for as long as required in an emergency event?
Event	The event that the equipment or system must be capable of functioning during and/or after as applicable.
Performance criteria	The criteria that must be maintained to ensure that the equipment or system can continue to function during and/or after the specified event.
Performance criteria reference	The reference(s) providing the basis for selection of the performance criteria. This shall be in the form [X] where "X" denotes the reference number corresponding to the relevant number in the References table.
Assurance	The activities in place to confirm that the performance criteria are being achieved (e.g. inspection, maintenance, monitoring, testing, exercises and drills).
Assurance reference	The reference(s) that confirm the implementation of assurance measures. This shall be in the form [X] where "X" denotes the reference number corresponding to the relevant number in the References table.
Interdependencies	To what extent is the SCE reliant on other systems in order for it to be able to perform its intended function?
Key component	Specifies the SCE or its components against which the interactions are being specified.
Interacting SCE	Specifies any SCEs that interact directly with the specified SCE or its components and may impact their ability to achieve the stated performance criteria.
Input / output	Identifies whether the specified SCE or its components are influenced by (input) or influence (output) the interacting SCE.
Explanation	Provides an overview of the type of interaction that occurs and how this may impact the ability of the SCE or its components from achieving the stated performance criteria, or the interacting SCE from achieving its own performance criteria.
Reference	The reference(s) that provide further detail on the interaction between the specified SCE or its components and the interacting SCE. This shall be in the form [X] where "X" denotes the reference number corresponding to the relevant number in the References table.
References	Identifies any reference cited within the performance standard document in the form [X], where "X" is the actively linked reference number. The reference table shall include the reference identifier (e.g. document number or system ID) and title (e.g. document title or system name).
Holds	Any issues that remain un resolved during the development of the performance standard should be listed in the holds section with reference to the associated "Responsible Party". Each Hold shall be numbered and referenced in the document in the form "[Hold #]".
Revision history	A summary of the revision history of the individual performance standard document including a description and comment indicating the reason for revision.
Approvals	Review and approval shall be undertaken by the performance standard custodian and relevant members of management for example: • performance standard custodian • engineering authority • asset manager.

4.3 Performance standards criteria

Each performance standard must state the key requirements (indicators) that the SCE has to achieve in order to perform as intended in relation to its functionality, availability, reliability, survivability and inter-dependencies.

Performance criteria can be identified and developed from a number of sources, including:

- industry codes and standards
- company policies, philosophies and standards
- company risk acceptance criteria
- design philosophy
- engineering determinations
- vendor specifications
- qualitative risk assessment
- quantitative risk assessment
- maintenance and repair strategies
- historical maintenance records
- legislation
- regulatory directions
- industry best practice
- lessons learnt from incidents
- workers performance and improvement strategies.

It is important that performance standards based on industry codes and standards include the key requirements that the control will be measured against during its life and not simply list the codes and standards that apply.

In development of performance criteria, use the expertise of those competent in the particular phase to which the performance standards relate. For example:

Operational performance standards – Discipline engineers and technical workers involved either in the facility design or involved with its operation together with input and review from facility operators and maintenance workers.

Parameters set in the performance standard must be SMART:

S **Specific** – performance standards should be well defined and not open to wide interpretation.

M **Measurable** – whenever possible, performance standards should be based on quantitative measures such as direct counts, percentages, and ratios.

A **Appropriate** – the performance standard should be in alignment with the overall goal of the control measure.

R **Realistic** – performance standards should be achievable (but may be challenging) and attainable using resources available.

T **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.

5 Performance standards development

5.1 Overview

It is important that the process for development and management of performance standards is systematic, robust and auditable, commencing at engineering design and continuing through to the end of facility life.

The following sections detail the approach required for development of performance standards. Appendix 3 provides a sample performance standard template to assist operators.

Published performance standard documents are subject to strict control and all approval entities nominated in the performance standard must approve any proposed changes to the document prior to those changes being published.

It should be noted that this document deals specifically with development of operational performance standards. Performance standards for non-operational phases should follow the same process as that described for operational performance standards.

5.2 Operational performance standards

Operational performance standards are typically developed using the finalised design basis memorandum as a reference, once it is certain that the design will not change.

The performance standards must capture the performance criteria that demonstrate ongoing operational capability and support the facility's safe operation and can only be developed once the:

- design is finalised
- operational phase risk assessments, as part of the formal safety assessment process, have been completed and SCEs have been established for the identified MAEs
- the facility safety management systems for the operational phase are reasonably well defined, including the establishment of operating and maintenance procedures and administrative systems
- operational workers, performance standard custodian(s) and engineers are available to provide guidance on the content of the performance standards.

Operational performance standards should be developed by:

1. Confirming the SCEs as an output of the formal safety assessment process and as described in Sections 3.2 and 3.4 of this Guide.
2. Establishing performance standard groupings, usually linked to the identified SCEs at the top level.
3. Establishing the basis for operational performance criteria by review of relevant source information in consultation with relevant stakeholders (typically operations and maintenance workers and those responsible for implementation of the safety management system).
4. Developing performance criteria and assurance requirements based on review outcomes, again with stakeholder consultation, and document in the performance standard template using one document per performance standard grouping. Performance criteria will be specified within each document at the relevant element, system, or sub-system level. Ensure that the content meets the SMART requirements and has clear linkages to the facility safety management system and maintenance management system.
5. Distributing the draft operational performance standards for review and comment by the relevant stakeholders and then update to incorporate any valid comments.
6. Consulting with stakeholders, to review the draft operational performance standards and gain consensus or highlight amendments prior to publishing the document.
7. Publishing the operational performance standards document(s).
8. Adding and referencing the operational performance standards in the facility safety case.

This process for developing performance standards is a recommendation and may vary depending on the SCE and the basis of the performance criteria.

6 Performance standards assurance

Performance standard assurance measures are checks to confirm that each safety critical element (SCE) is achieving the necessary level of performance as defined within the performance standard.

Performance standard assurance can be achieved via a number of different approaches, which ultimately depend on the individual SCE and the risk it is mitigating, together with the established practices within the safety management system. Assurance activities for a given SCE may include one or more of:

- **Comparison with codes and standards** – assurance aligns with the requirements set out in recognised national or international codes, standards and guidelines.
- **Verification and quality assurance and quality control** – internal activities that require the checking or testing of plant and equipment to ensure it has been manufactured to specification, installed correctly and is fit for its function and use.
- **Validation** – an activity undertaken by an independent, competent party (usually third party) to ensure that the design, construction and installation of safety critical hardware, firmware and software (including instrumentation, process layout and process control systems) of the facility incorporate appropriate measures that will protect the health and safety of persons at the facility.
- **Audit** – auditing implementation of the safety management system ensures that the strategies, procedures, work instructions, maintenance strategies and other aspects of the safety management system are in place and effective.
- **Performance data analysis** – evaluating safety-related performance data as evidence of adequate 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.
- **Technical analysis** – evaluating control measures in technical terms; assess strengths and weaknesses, e.g. effectiveness, functionality, availability, reliability, compatibility, survivability, correspondence of SCEs to hazards and risks, appropriateness of performance standards.
- **Monitoring and inspections** – carry out monitoring and inspections of SCEs and their surrounds to confirm the condition.
- **Engineering judgement** – provide considered judgements as to the suitability of SCEs, through the input of a cross-section of skilled and experienced stakeholders, e.g. key members of the workforce, senior management and independent observers.
- **Practical and function testing** – demonstrate that the SCE functions effectively e.g. using major incident simulations, management system tests, equipment breakdown and recovery tests.

The timing and frequency of assurance activities should reflect:

- the risk of SCE performance deviating from the performance criteria
- the risk associated with SCE performance deviation
- the time and resources involved to return an SCE to its required performance following a deviation
- SCE reliability and availability requirements
- codes and standards
- regulatory requirements
- maintenance strategies.

The safety management system provides the means to implement assurance activities.

All assurance activities should be clearly referenced to the appropriate document(s) and system(s) that provide for the assurance activity, and the referenced document or system describes a process for recording the undertaking of, and findings associated with, the assurance activity.

If operational performance criteria use the maintenance management system for assurance, the performance standards should reference the relevant maintenance management system regime. If performance criteria specify a preventative maintenance requirement, ensure that the maintenance management system contains the corresponding maintenance regime. This regime can then be referenced within the performance standard. In this scenario, the assurance task would be to audit the maintenance management system records to confirm that the particular regime for the preventative maintenance activity exists and that it has been carried out.

Integration of performance standards and their assurance activities into the safety management system, as illustrated in Figure 7, provides an auditable approach to demonstrating the management of risks associated with MAEs.

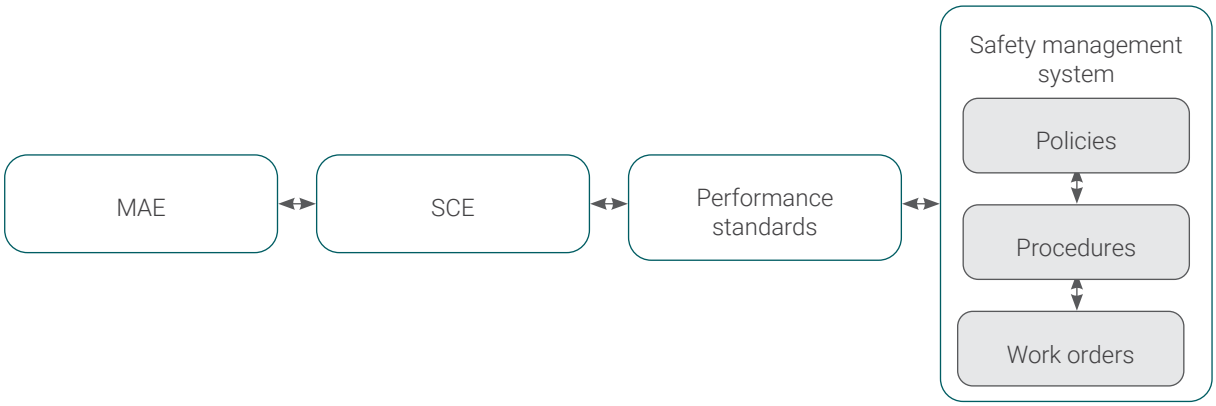

Figure 7 Performance standards integration into SMS

Where audit activities have identified that performance criteria are not being achieved, this will be recorded as a non-compliance on the audit report and appropriate actions generated. The timeliness and type of action to rectify the performance deviation is commensurate with the level of risk aligned with the non-compliance and the action will be tracked through to effective closure. Further information in relation to managing performance deviations and contingency planning is provided in Section 7.

7 Performance standards lifecycle management

It is essential that performance standards remain relevant and effective for the life of the facility. This will provide assurance that the risks associated with SCEs are being managed to a level that is minimised SFAIRP. The summarised performance standard lifecycle is depicted in Figure 8.

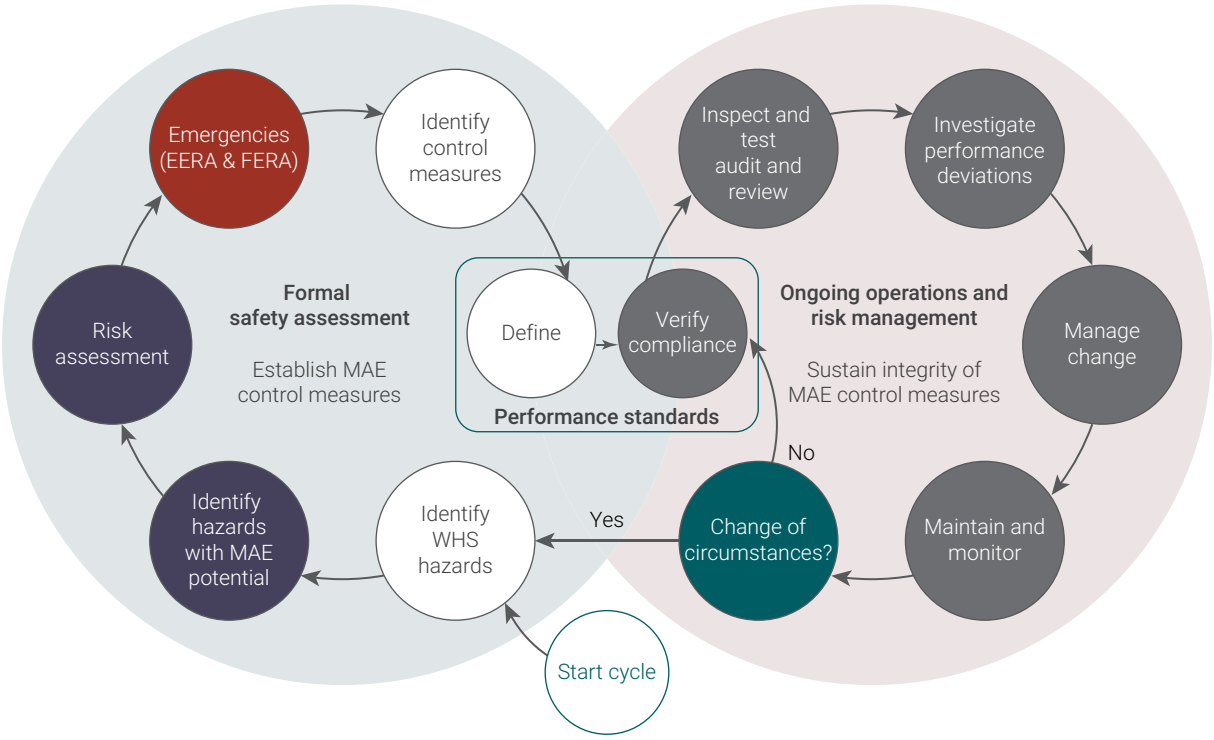

Figure 8 Performance standard lifecycle

Once SCEs and their performance standards are established and the assurance processes described in Section 6 are initiated, this provides the capability to measure the effectiveness of the SCE by comparing actual performance against the performance criteria.

To ensure the continued appropriateness of performance standards, they should be reviewed, for example:

- initially every two years to verify conformance with the assurances specified
- in conjunction with the five yearly AS 2885.6 safety management study requirements for the facility covered by the performance standards
- when a trigger for revision of the in force safety case occurs (or comparable regulatory requirement)
- when changes to the basis by which the performance standards have been developed happen (e.g. changes to codes and standards)
- any other change in circumstances that may change the facility risk profile with respect to MAEs, for example operational risk reviews, incident investigations.

Where there is a change in plant or equipment, procedures, or administrative structure, management of change should be initiated, including a trigger for review of how the facility risk profile is affected by the change. This process can identify new or changed MAEs or SCEs that may subsequently require the revision of existing, or development of new, performance standards.

For more information, refer to the *Guide: Management of change*.

Performance criteria and assurance requirements may be refined over time to reflect the increasing understanding of facility operability and maintainability, improvements in performance capability, or changes in risk acceptance criteria. Such changes to performance criteria may arise from:

- outcomes from maintenance programs that establish performance histories for each SCE, resulting in improved maintenance strategies (e.g. increased ratio of preventative maintenance activities)
- outcomes from other assurance activities, prompting management of actions which result in improved effectiveness of SCE performance or adjustment of assurance tasks
- outcomes from incident and near miss investigations, targeting improvements in the management of specific hazards and newly identified failure modes
- changes in policies or risk acceptance criteria, to a more stringent base, resulting in a review of previously accepted levels of risk.

Integration of performance standards within the safety management system, ensures the audit, review and improvement cycle is applied which is inherent to the safety management system. Effective implementation ensures SCEs remain fit-for-purpose, and the facility risk profile (as it relates to MAEs) remains minimised SFAIRP.

8 Common weaknesses

8.1 Control measures

Common weaknesses associated with control measures include:

- considering a single control measure rather than a range of independent control measures
- concentrating effort on mitigation measures for fire and explosion risks rather than consideration of measures higher up the hierarchy of controls
- assuming that industry codes and standards are suitable by default, without justification of their application in the specific situation
- not directly linking to clearly established performance standards for control measures
- missing as-built information.

8.2 Performance standards

Common weaknesses associated with performance standards include:

- failing to define performance parameters to facilitate the design of assurance tasks and supporting verification
- failing to provide information on interdependencies
- failing to cross reference to the source information
- failing to provide direction or link to what actions or processes should be followed if the performance standard is not met
- failing to conduct ongoing review of performance standards
- failing to address degradation and lifecycle asset management issues using control measure performance standards
- for offshore facilities, using marine standard classification provisions for shipping to mobile offshore drilling units and platform applications without conducting reviews of the suitability of those standards.

Appendix 1 Glossary

The following terms are defined for the purposes of this Guide.

Key terms	Meaning
CHAZOP	Control hazard operability study
Competent person	A person who has acquired through training, qualification or experience the knowledge and skills to carry out the task. The definition of 'competent person' in the Work Health and Safety (General) Regulations prescribes specific requirements for some types of work such as diving.
DSMS	Diving safety management system
EERA	Evacuation, escape and rescue analysis
Facility	**Geothermal energy facility** – a place at which geothermal energy operations are carried out and includes any fixture, fitting, plant or structure at the place **Petroleum facility** – a place at which petroleum operations are carried out and includes any fixture, fitting, plant or structure at the place **Mobile facility** – includes an onshore drilling rig The term facility has been adopted throughout this document to cover offshore and onshore facilities and pipelines including aboveground structures associated with onshore pipelines.
FERA	Fire and explosion risk assessment
FSA	Formal safety assessment
Geothermal energy operation	Means an operation to: • explore for geothermal energy resources • drill for geothermal energy resources • recover geothermal energy • or is any other kind of operation that is prescribed by the regulations to be a geothermal energy operation for the purpose of this definition and carry on of such operations and the execution of such works as are necessary for that purpose.
HAZAN	Hazard analysis
HAZID	Hazard identification study
HAZOP	Hazard and operability study
LOPA	Layers of protection analysis
MAE	Major accident events – an event connected with a facility, including a natural event, having the potential to cause multiple fatalities of persons engaged at or in the vicinity of the facility
MoC	Management of change

Key terms	Meaning
MTBF	Mean time between failures
Operator	A person who has, or will have, the day-to-day management and control of operations at a facility and is registered as the operator of the facility under r.22(3).
ORA	Operational risk assessment
Performance standard	A standard established by the operator defining the performance required for a safety critical element typically defining the functionality, availability, reliability, survivability and interdependency of the safety critical element.
Person conducting a business or undertaking (PCBU)	A PCBU is an umbrella concept capturing all types of working arrangements or relationships. A PCBU includes a company, unincorporated body or association and sole trader or self-employed person. Individuals who are in a partnership that is conducting a business will individually and collectively be a PCBU. A reference to a PCBU includes reference to the operator of a facility.
Petroleum operation	Means an activity that is carried out in an area in respect of which a petroleum title is in force, or that is carried out in an adjacent area, for the purpose of any of the following: • exploring for petroleum • drilling or servicing a well for petroleum • extracting or recovering petroleum • injecting petroleum into a natural underground reservoir • processing petroleum • handling or storing petroleum • the piped conveyance or offloading of petroleum.
PFD	Probability of failure on demand
QRA	Quantitative risk assessment
Regulator	The WorkSafe Commissioner is the regulator under the *Work Health and Safety Act 2020*.
Safety case	In this document covers all safety management systems, plans and other safety related documents referred to in WHS Act and WHS PAGEO regulations
Safety critical element (SCE)	Any item of equipment, system, process, procedure or other control measure the failure of which can contribute to an MAE.
SFAIRP	So far as is reasonably practicable
SME	Subject matter expert
SMS	Safety management system
WHS Act	*Work Health and Safety Act 2020*
WHS PAGEO Regulations	Work Health and Safety (Petroleum and Geothermal Energy Operations) Regulations 2022
Worker	Any person who carries out work for a person conducting a business or undertaking, including work as an employee, contractor or subcontractor (or their employee), self-employed person, outworker, apprentice or trainee, work experience student, employee of a labour hire company placed with a 'host employer' or a volunteer

Appendix 2 Further information

Petroleum safety guidance

Interpretive guidelines

- *Development and submission of a diving safety management system*
- *Development and submission of a safety case*
- *Development and submission of an onshore facility safety case – drilling operations*

Guides

- *Audits, review and continual improvement*
- *Bridging documents and simultaneous operations (SIMOPS)*
- *Dangerous goods and hazardous chemicals in petroleum, pipeline and geothermal energy operations*
- *Decommissioning and management of ageing assets*
- *Demonstration of risk reduction so far as is reasonably practicable (SFAIRP)*
- *Diving start-up notices*
- *Emergency response planning*
- *Facility design case*
- *Hazard identification*
- *Health and safety leading and lagging performance indicators*
- *Human factors fundamentals for petroleum and major hazard facility operators*
- *Human factors self-assessment guide and tool for safety management systems at petroleum and major hazard facility operations*
- *Identification of major accident events, control measures and performance standards*
- *Inspections – Land-based drilling rigs*
- *Involvement of workers*
- *Management of change*
- *Nomination of an operator*
- *Records management including document control*
- *Risk assessment and management including operational risk assessment*
- *Validation requirements*

Australian and international standards

- AS 2885 Pipelines – *Gas and liquid petroleum - suite of standards*
- AS IEC 61511 *Functional safety – Safety instrumented systems for the process industry sector*
- AS IEC 61882 *Hazard and operability studies (HAZOP studies) – Application guide*
- AS/NZS ISO 31000 *Risk management – Principles and guidelines*
- IEC ISO 31010 *Risk management – Risk assessment techniques*
- ISO 17776 *Petroleum and natural gas industries – Offshore production installations – Guidelines on tools and techniques for hazard identification and risk assessment*

Codes of practice

- *How to manage work health and safety risks*
- *Mentally healthy workplaces for fly-in fly-out workers in the construction and resources sector*
- *Psychosocial hazards in the workplace*
- *Workplace behaviour*

Other resources

WorkSafe WA

- *Discriminatory, coercive and misleading conduct – Interpretive guideline*
- *How to determine what is reasonably practicable to meet a health and safety duty – Interpretive guideline*
- *Incident notification – interpretive guideline*
- *The health and safety duty of an officer – Interpretive guideline*
- *The meaning of 'person conducting a business or undertaking' (PCBU) – Interpretive guideline*

Other agencies

- Centre for Chemical Process Safety (CCPS), Guideline for initiating events and independent protection layers in layer of protection analysis
- National Offshore Petroleum Safety and Environmental Management Authority's (NOPSEMA), Hazard identification guidance note
- National Offshore Petroleum Safety and Environmental Management Authority's (NOPSEMA), Risk assessment guidance note

Appendix 3 Sample performance standard template

The performance standard template is available from WorkSafe's website.

Safety critical element (SCE) performance standard – template

Title	*Performance standard title*					**Code**	*Unique performance standard identifier*
Owner	*Performance standard owner*	**Revision**	*Revision*	**Revision date**	*Date of this revision*	**Next revision due**	*Date for next revision*
Scope	**Inclusions:**						
	A brief summary of the performance standard scope by stating the SCE system boundaries and listing the SCE components within the system boundaries						
	Exclusions:						
	If applicable						
Objective	*A brief overview of the overall objective/intention of the SCE. This should be aligned to the SCE's risk function (prevention, detection, control or mitigation) with respect to the associated MAEs*						
MAEs	*List the MAEs against which the SCE functions to mitigate risk*						

Functionality					
SCE component	**Key requirement**	**Performance Criteria**	**Reference**	**Assurance**	**Reference**
	The specific function required to be performed by the SCE component in the context of mitigating the risk of the associated MAEs		*Reference providing basis for performance criteria*	*The activities in place to confirm the performance criteria are being achieved (e.g. inspection, maintenance, monitoring, testing, exercises and drills)*	*Reference confirming implementation of assurance measures*

Availability or reliability						
SCE component	**Availability**	**Reference**	**Reliability**	**Reference**	**Assurance**	**Reference**
The SCE component against which the performance criteria is being specified	*Availability is related to the expected probability that an SCE will function as required "on demand" at any point of time. It is often expressed in terms of "probability of failure on demand" (PFD) and refers to an SCE that sits in the background until required ("on demand"), such as a pressure safety valve. For further details on the calculation of this requirement refer to Section 4.2 of the Major accident events, control measures and performance standards guide.*	*Reference providing basis for availability criteria*	*Reliability is related to the expected probability that an SCE will function as required for a specified period of time. It is usually expressed as a "failure rate". Reliability usually refers to an SCE that is in continuous use, such as the integrity of a pressure piping system. For further details on the calculation of this requirement refer to Section 4.2 of the Major accident events, control measures and performance standard guide.*	*Reference providing reliability performance criteria*	*The activities in place to confirm the performance criteria are being achieved (e.g. inspection, maintenance, monitoring, testing, exercises and drills)*	*Reference confirming implementation of assurance measures*

Survivability				
Event	**Performance criteria**	**Reference**	**Assurance**	**Reference**
The event that the equipment/system must be capable of functioning during/after as applicable	*The criteria that must be maintained to ensure that the equipment/system can continue to function during/after the specified event*	*Reference providing basis for performance criteria*	*The activities in place to confirm the performance criteria are being achieved (e.g. inspection, maintenance, monitoring, testing, exercises and drills)*	*Reference confirming implementation of assurance measures*

Inter-dependencies				
SCE component	**Interacting SCE**	**Input / output**	**Explanation**	**Reference**
The SCE components against which the interactions are being specified	*Identify any SCEs that interact directly with the specified SCE or its components and may impact their ability to achieve the stated performance criteria*	*Identify whether the specified SCE or its components are influenced by (input) or influence(output) the interacting SCE*	*An overview of the type of interaction that occurs and how this may impact the ability of the SCE or its components to achieve the performance criteria*	*Reference providing additional detail of the interaction*

References		
Reference	**ID / Document No.**	**Title**
Reference number in the format [X]	*ID or document number for the reference system or document*	*Title of the system or document that corresponds to the stated ID or document number. All references made in the performance standard should be in the form [X], linked to the corresponding reference [X] in this table.*

Holds		
Hold No.	**Description**	**Responsible party**
Hold number	*Description of the holds*	*Name and/or title of person responsible for resolving the hold*

Revision history		
Revision	**Revision trigger**	**Revision details**
Record of each revision number	*Select revision trigger (i.e. periodic revision, performance standard scope change, performance criteria change, other change)*	*Highlight the key changes made to the performance standard document for the stated revision (inclusive of MoC and reference MoC number*

Approvals			
Title	**Name**	**Signature**	**Date**
Position title	*Current position incumbent*		
Position title	*Current position incumbent*		
Position title	*Current position incumbent*		

GOVERNMENT OF WESTERN AUSTRALIA

Department of **Energy, Mines, Industry Regulation and Safety**

WorkSafe Group

Department of Energy, Mines,
Industry Regulation and Safety
303 Sevenoaks Street
CANNINGTON WA 6107

Telephone: 1300 307 877
NRS: 13 36 77
Email: Safety@dmirs.wa.gov.au
Website: www.dmirs.wa.gov.au

WS Jan24_1287