Government of **Western Australia**
Department of **Mines, Industry Regulation and Safety**

# Petroleum safety and major hazard facility – guide

## Major accident events, control measures and performance standards

**February 2020**

## Disclaimer

The information contained in this publication is provided in good faith and believed to be reliable and accurate at the time of publication. However, the information is provided on the basis that the reader will be solely responsible for assessing the information and its veracity and usefulness.

The State shall in no way be liable, in negligence or howsoever, for any loss sustained or incurred by anyone relying on the information, even if such information is or turns out to be wrong, incomplete, out-of-date or misleading.

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).

## Creative commons

The State of Western Australia supports and encourages the dissemination and exchange of its information. The copyright in this publication is licensed under a Creative Commons Attribution 4.0 International (CC BY) licence.

Under this licence, with the exception of the Government of Western Australia Coat of Arms, the Department's logo, any material protected by a trade mark or licence and where otherwise noted, you are free, without having to seek our permission, to use this publication in accordance with the licence terms.

We also request that you observe and retain any copyright or related notices that may accompany this material as part of the attribution. This is also a requirement of the Creative Commons Licences.

For more information on this licence, visit creativecommons.org/licenses/by/4.0/legalcode

## Contact

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:

Safety Regulation Group – Regulatory Support

Department of Mines, Industry Regulation and Safety

100 Plain Street

EAST PERTH WA 6004

Telephone: +61 8 9358 8001

NRS: 13 36 77

Email: SafetyComms@dmirs.wa.gov.au

## Guides

A guide is an explanatory document that provides more information on the requirements of legislation, details good practice and may explain means of compliance with standards prescribed in the legislation. The government, unions or employer groups may issue guidance material.

Compliance with guides is not mandatory. However, guides could have legal standing if it were demonstrated that the guide is the industry norm.

This Guide has an operations focus and is set out in the context of risk assessment and legislative requirements of all responsible persons. Consequently, each operation needs to understand its limitations and skills base.

The Guide is based on current experience and is not claimed to be complete.

## Who should use this Guide?

You should use this Guide if you are responsible for hazard identification and risk management including the management of risks to a level that is as low as reasonably practicable (ALARP) and identification of major accident event (MAE) control measures and development of performance standards.

# Contents

# 1 Introduction

This document has been developed to provide assistance and guidance to licensees and operators to meet the Western Australian Petroleum safety and major hazard facility legislation administered by the Department of Mines, Industry Regulation and Safety (the Department).

The relevant legislation covered by this Guide is listed in Appendix 1.

## 1.1 Scope and objective of this Guide

This Guide has been developed to provide licensees and operators with assistance in adhering to the requirement to identify effective control measures for hazards that have the potential to cause MAEs and the development of performance standards.

For the purpose of this Guide the term “safety case” will be used to cover all of the safety documents required under the different regulations.

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

Under the Dangerous Goods Safety (Major Hazard Facility) Regulations 2007, reference is made to a “major incident” whereas petroleum legislation refers to “major accident events”. Reference within this Guide is made to MAE which will encompass the term “major incident”.

The Dangerous Goods (Major Hazard Facility) Regulations 2007 refers to “harm to people, property and the environment” (which includes the general public) whereas petroleum legislation refers to “occupational safety and health of all people”. Where specific reference is made to both the petroleum safety and major hazard facility (MHF) regulations, both descriptions will be included, otherwise for generic references, the term “safety and health” will encompass the additional requirements of property and environment in this Guide.

The objective is to provide clarity to both industry and Department personnel on areas of the legislation which may be ambiguous or open to interpretation.

The following appendices are included:

Appendix 1 Legislative provisions

Appendix 2 References and acknowledgements

Appendix 3 Glossary of terms

Appendix 4 Further information

Appendix 5 Sample performance standard template

## 1.2 Definitions and abbreviations

Definitions and abbreviations are included in Appendix 3 Glossary of terms.

## 1.3 Use of standards and approved codes of practice

There are a number of standards and approved codes of practice that can provide guidance and assistance to licensees and operators for completion of their hazard identification and subsequently risk assessments and then ongoing risk management. Examples are:

- AS/NZS ISO 31000 *Risk management – Guidelines*
- ISO 17776 *Petroleum and natural gas Industries – Offshore production installations – Major accident hazard management during design of new installations*
- AS/NZS 2885.6 *Petroleum – Gas and liquid petroleum – Part 6: Pipeline safety management*
- AS IEC 61882 *Hazard and operability studies (HAZOP studies) – Application guide*
- CCPS *Guideline for initiating events and independent layers of protection analysis*

- AS IEC 61511 *Functional safety – Safety instrumented systems for the process industry sector*

Approved codes of practice for dangerous goods – information is located on the Department website.

Licensees and operators should reference the current versions of these publications to support the requirements of the safety case and how identification of control measures and development of performance standards needs to be conducted effectively within their organisations.

## 1.4 Linked guides

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

- *Hazard identification*
- *Risk assessment and management including operational risk assessment*
- *ALARP demonstration*

These guides and this document 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 licensees and operators to identify and manage the hazards and risks within their organisations and also meet the requirements of the relevant regulations.

## 1.5 Identifying hazards and potential causes

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 place and the need for further control measures to be identified and assessed.

*Hazard identification* and *Risk assessment and management including operational risk assessment* guides provide further details on this requirement.

## Formal safety assessment process

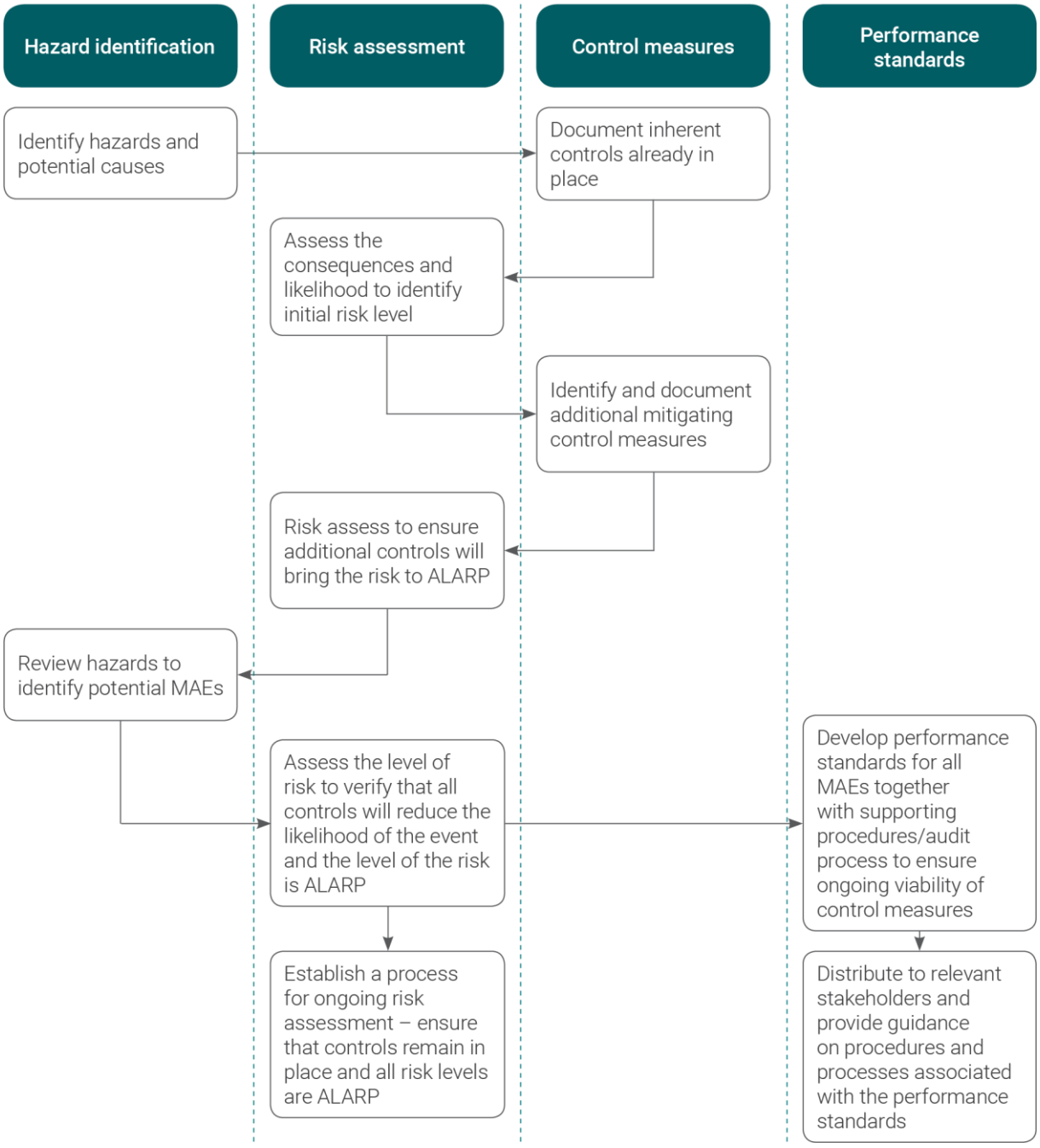


*Figure 1 Formal safety assessment process*

# 2 Control measure assessment

Control measures are applied to activities on a facility that eliminate, prevent, reduce or mitigate the risk to health and safety associated with potential MAEs or other hazardous events. These are the means by which a licensee or 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 Selecting the assessment team and scheduling workshops

Include representatives who are managers, supervisors, operators, maintenance personnel and relevant technicians when scheduling and preparing for workshops to carry out control measure identification, selection and assessment. The hazard identification and risk assessment reports already conducted on the facility must be available for the control measure assessment.

It may also be helpful to engage a risk facilitator, or bring in technical expertise in a specific area.

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 personnel 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 personnel from one facility to review the assessments completed in relation to another similar facility.

## 2.2 Workforce involvement

Members of the workforce involved in the hazard identification and risk assessment workshops leading up to the identification and application of control measures should be included in this phase of the process of risk management.

As well as including the subject matter experts, other members of the workforce 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.

Those members of the workforce 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 personnel 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.

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

An MAE is defined as an event connected with a facility (including a natural event) with the potential to cause multiple fatalities of people at or near the facility. In the case of a major hazard facility (MHF) a major incident means an incident involving or affecting a Schedule 1 substance that causes serious harm to people, property or the environment.

Events that result in catastrophic consequences are generally 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 occupational health and safety.

Identifying the 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 licensee's or 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 reduce risks to a level that is ALARP. Figure 2 depicts the screening process for MAE and non-MAE control measures.

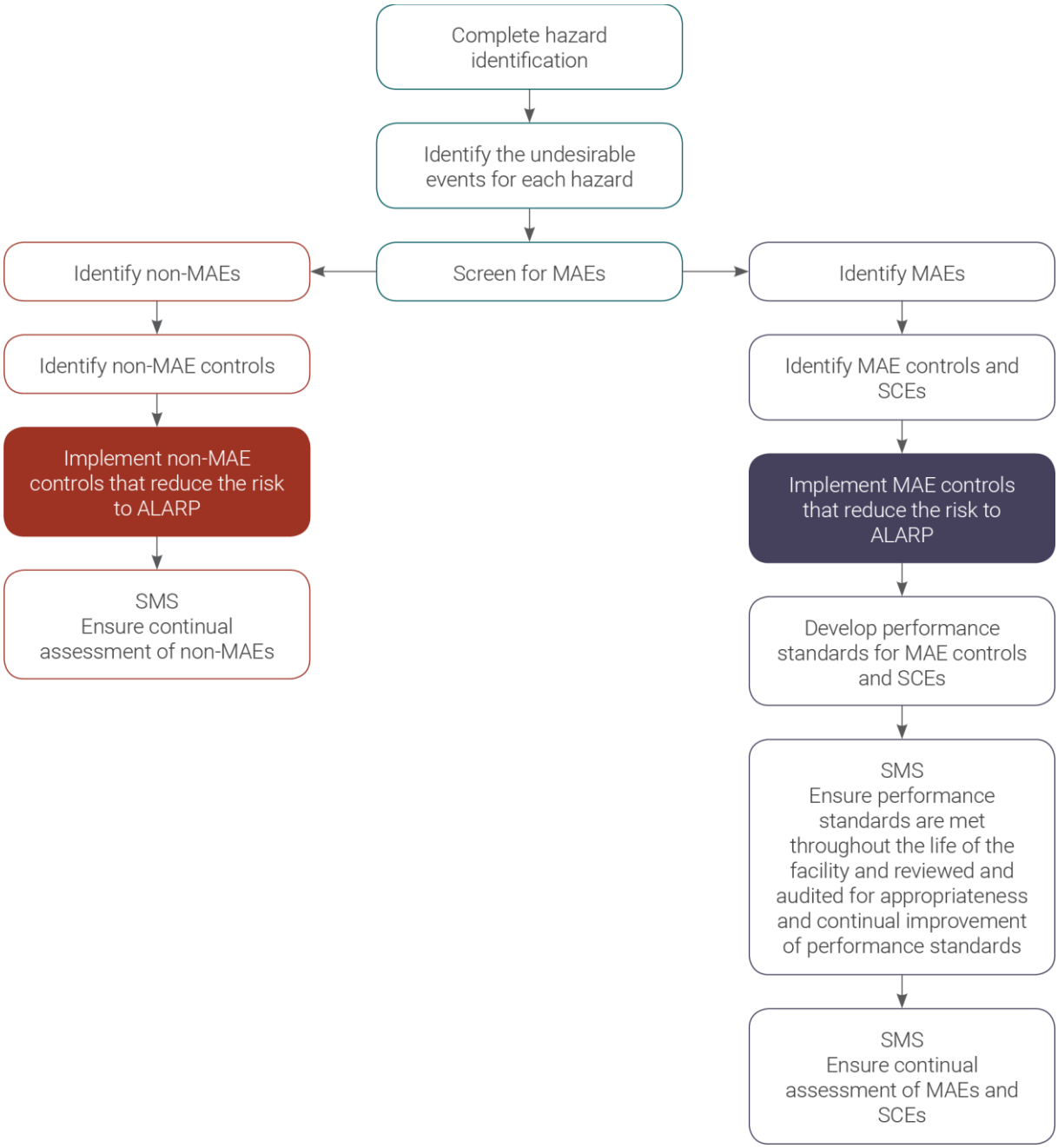


*Figure 2  MAE and non-MAE control measures*

## 2.4 Aims and outcomes of control measure assessment

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

- provide operations 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 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.

# 3 Identifying and selecting control measures

## 3.1 Identifying control measures

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

## 3.2 Safety critical elements

Safety critical elements (SCEs) are defined as those physical control measures the failure of which could lead to, or purpose is, to prevent or limit the consequences of 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 reduced to a level that is as low as reasonably practicable (ALARP)
- 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 SCE 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. Establish performance requirements 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**<br>Typically are groups of systems on a facility which are used to achieve the same general outcome | Emergency shutdown |
| **Safety critical system**<br>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**<br>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**<br>Component of a critical sub-system where the failure of the component will lead to failure of the critical sub-system | Actuated isolation valves |

| Category | Example |
|---|---|
| **Safety critical tag item**<br>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 to ALARP.

Good practice requires application of the hierarchy of controls when determining the most effective risk mitigation. Applying a 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 is structured in accordance with priorities (highest to lowest):

- 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 2.

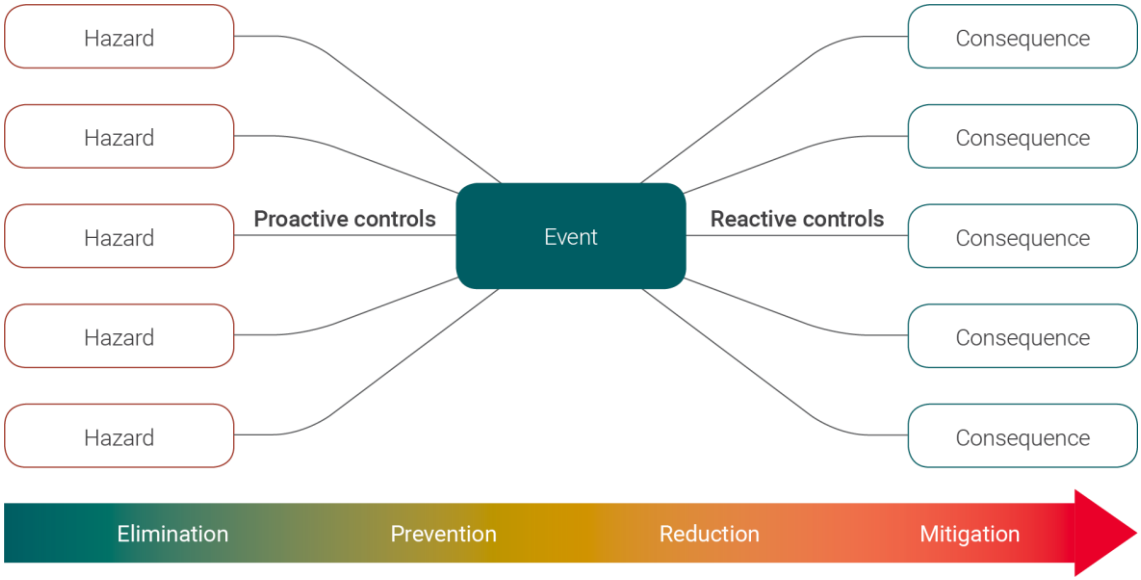


*Figure 2 Schematic representation of a bowtie diagram*

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 personnel 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.

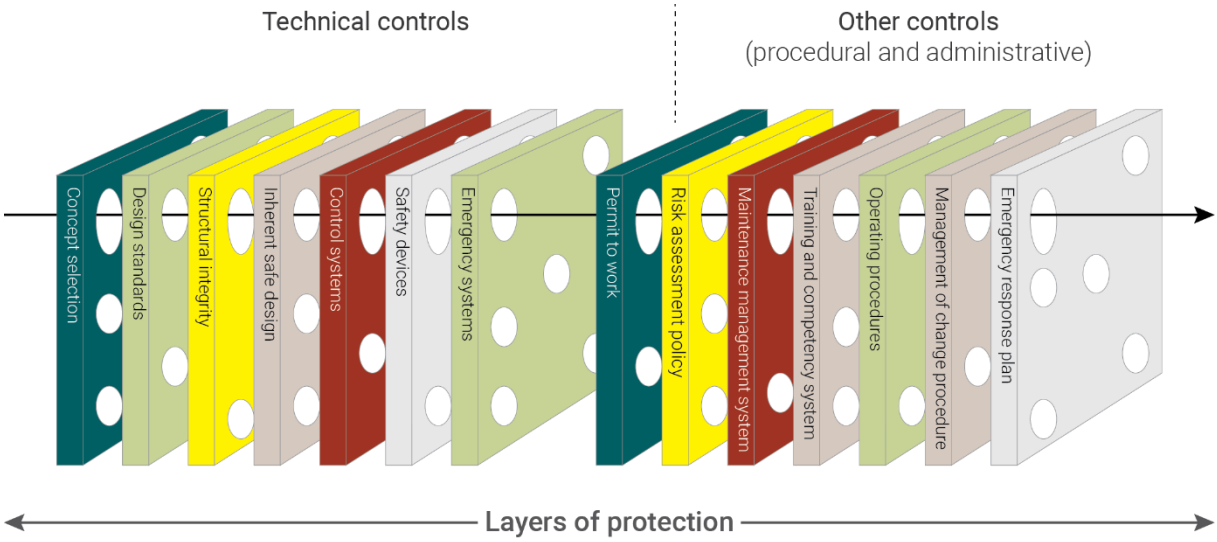


*Figure 4 Layers of protection*

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.

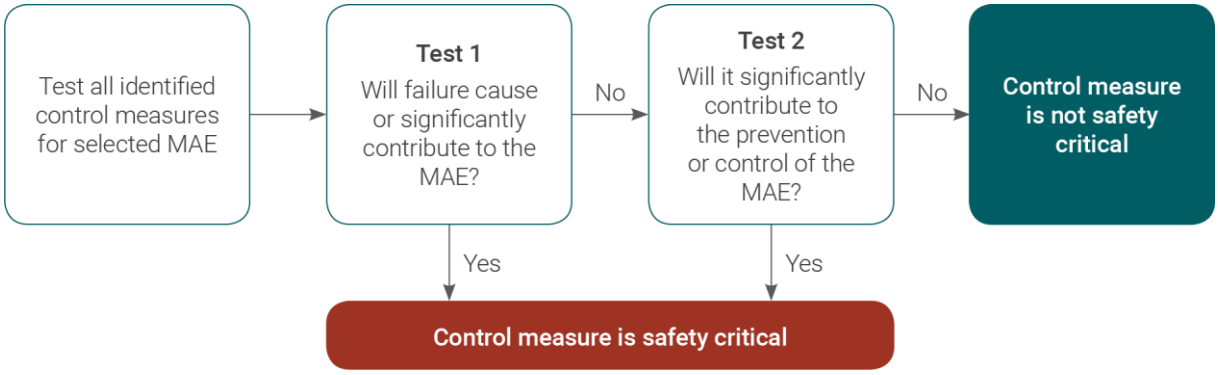


*Figure 5 Basic decision criteria for SCE selection*

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.

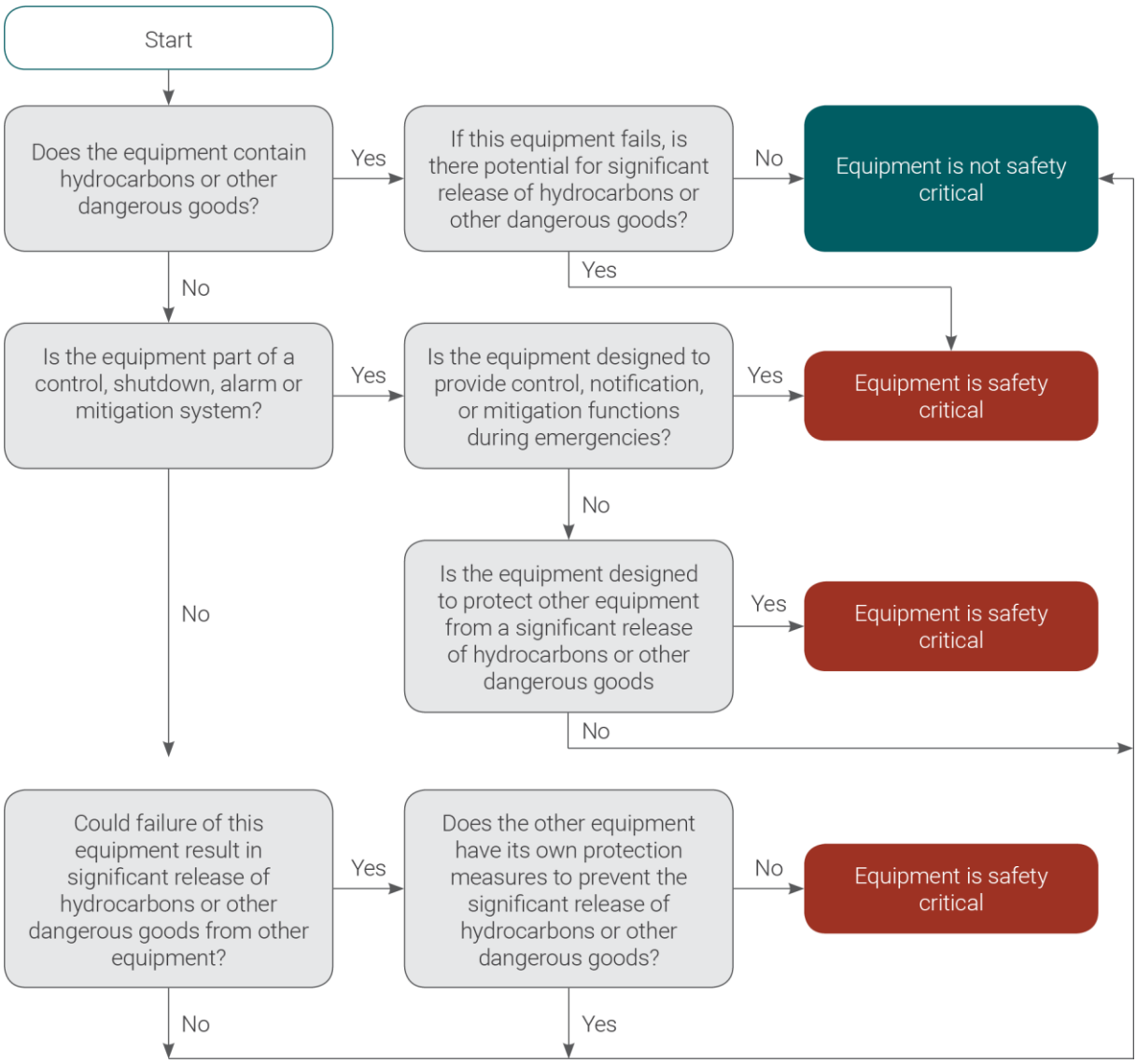


*Figure 6 Detailed SCE identification process*

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 bulk 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 safety management studies
- safety integrity level assessments
- layers of protection analysis (LOPA)
- failure mode and effect (and criticality) analysis
- fire and explosion risk assessment (FERA)
- emergency systems survivability 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

## 4.1 Overview

Performance standards are the parameters against which SCEs can be assessed to ensure they are reducing the risk of an MAE to a level that is ALARP.

Performance standards provide a benchmark for measuring, monitoring and testing an SCE's effectiveness 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.

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. |
| 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. |

| Template fields | Field content description |
|---|---|
| **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:<br>$$PFD = 10\% = 0.1$$<br>and the availability would be:<br>$$Availability = (100\% - PFD) = (100\% - 10\%) = 90\% = 0.9$$<br>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:<br>$$Failure\ rate = \frac{failures}{time} = \frac{0.1\ failures}{1\ year} = 0.1/year$$<br>Reliability is also expressed as *mean time between failures* (MTBF), which is the inverse of *failure rate*:<br>$$MTBF = \frac{time}{failures} = \frac{1\ \text{year}}{0.1\ \text{failures}} = 10\ year\ (per\ failure)$$<br>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). |
| 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. |

| Template fields | Field content description |
|---|---|
| **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 unresolved 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:<br>• performance standard custodian<br>• engineering authority<br>• 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 (in no particular order):

- 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
- personnel 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 personnel involved either in the facility design or involved with its operation together with input and review from facility operators and maintenance personnel.

Parameters set in the performance standard must be specific, measurable, appropriate, realistic and timely (SMART).

- **Specific** – performance standards should be 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.

# 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 which shall be presented in the approved performance standard template developed by the operator.

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 personnel, 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 Section 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 personnel and those responsible for implementation of 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. Convening a stakeholder workshop 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 only 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 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, etc.
- **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 using major incident simulations, management system tests, equipment breakdown and recovery tests, etc.

The timing and frequency of assurance tasks 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.

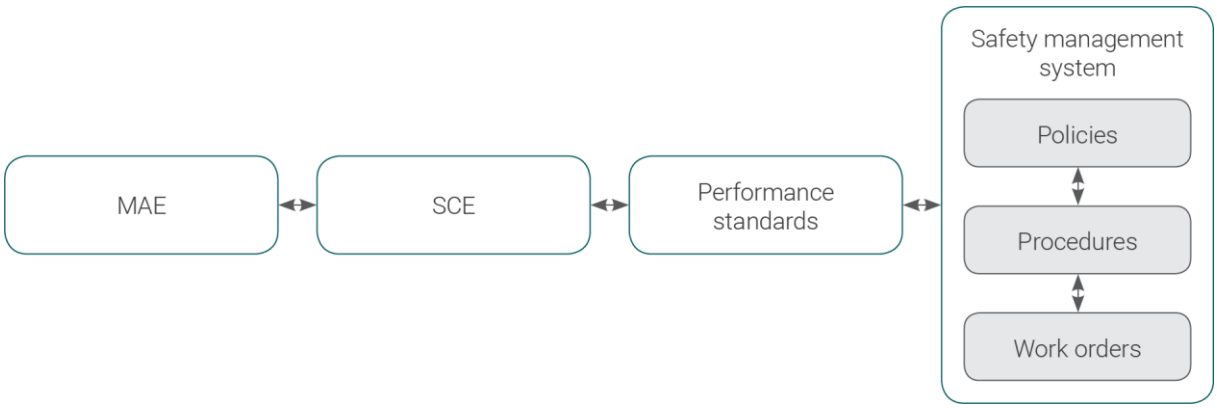


*Figure 7  Performance standards integration into SMS*

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 0.

# 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 ALARP. The summarised performance standard lifecycle is depicted in Figure 8.

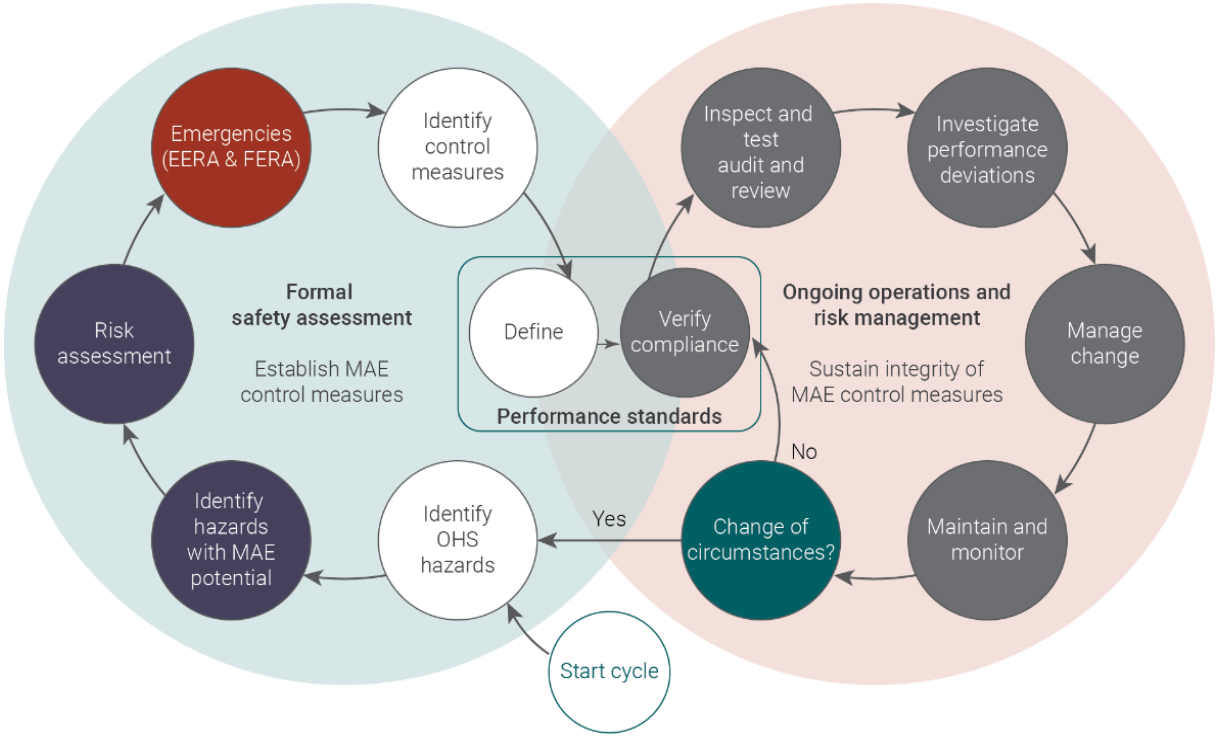


*Figure 8 Performance standard lifecycle*

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 regime deliverable)
- 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 may identify new or changed MAEs or SCEs that may subsequently require the revision of existing, or development of new, performance standards. This is covered in more detail in the *Management of change* guide.

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 (for example 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 ALARP.

# 8 Common weaknesses

## 8.1 Control measures

Common weaknesses associated with control measures include:

- a single control measure has been considered rather than a range of independent control measures
- concentrating effort on mitigation measures for the 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.

## 8.2 Performance standards

Common weaknesses associated with performance standards include:

- performance standards have no defined performance parameters to facilitate the design of assurance tasks and supporting verification
- performance standards have 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
- failure 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 Legislative provisions

**Petroleum (Submerged Lands) (Management of Safety of Offshore Facilities) Regulations 2007**

r. 16 Facility description, formal safety assessment and safety management system

**Petroleum (Submerged Lands) (Pipelines) Regulations 2007**

r. 29 Description of pipeline management system

**Petroleum (Submerged Lands) (Diving Safety) Regulations 2007**

r. 7 Contents of DSMS

**Petroleum and Geothermal Energy Resources (Management of Safety) Regulations 2010**

r. 10 Principal provisions of safety management systems

r. 11 Risk assessment for major accident events

r. 12 Ongoing management of safety

**Petroleum Pipelines (Management of Safety of Pipeline Operations) Regulations 2010**

r. 10 Pipeline operation description, formal safety assessment and safety management system

**Dangerous Goods Safety (Major Hazard Facilities) Regulations 2007**

r. 23 Risk assessment, operator of major hazard facility to prepare

r. 27 Safety report, approval of by Chief Officer

# Appendix 2 References and acknowledgements

Development of this Guide has used:

- reference to the NOPSEMA suite of guidance notes
- 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*
- AS IEC 61511 *Functional safety – Safety instrumented systems for the process industry sector*
- AS 2885 *Pipelines – Gas and liquid petroleum* – suite of standards

# Appendix 3 Glossary

**ALARP**. As low as reasonably practicable.

**CHAZOP**. Control hazard operability study.

**Facility**. The term facility has been adopted throughout this document to cover offshore and onshore facilities and pipelines including aboveground structures associated with onshore pipelines and major hazard facilities.

**EERA**. Evacuation, escape and rescue analysis.

**FERA**. Fire and explosion risk assessment.

**FSA**. Formal safety assessment.

**HAZID**. Hazard identification study.

**HAZOP**. Hazard operability study.

**LOPA**. Layers of protection analysis.

**MAE**. Major accident event – an event connected with a facility, including a natural event, having the potential to cause multiple fatalities of persons at or near the facility (or as defined within the relevant legislation pertaining to a facility).

**Major incident**. An incident involving or affecting a Schedule 1 substance (Dangerous Goods Safety (Major Hazard Facilities) Regulations 2007) that causes serious harm to people, property or the environment. For the purposes of this Guide, referred to as an MAE.

**MHF**. Major Hazard facility.

**MTBF**. Mean time between failures.

**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 interdependencies of the safety critical element.

**PFD**. Probability of failure on demand.

**Safety case**. In this document covers all safety management systems, plans and other safety related documents referred to in WA legislation.

**Safety critical element**. Any item of equipment, system, process, procedure or other control measure the failure of which can contribute to an MAE.

**SCADA**. Supervisory control and data acquisition.

**Serious harm**. Significant incident associated with substances listed in Schedule 1 of Dangerous Goods legislation.

**SME**. Subject matter expert.

**SPAE**. Significant pipeline accident event – an event that:

a) is connected (whether immediately or after delay) with work carried out on, or in relation to, a pipeline

b) causes, or creates a significant risk of causing, human death (for example, because of hydrocarbon releases).

# Appendix 4 Further information

Other guides available:

- *ALARP demonstration*
- *Audits, review and continual improvement*
- *Bridging documents and simultaneous operations (SIMOPS)*
- *Dangerous goods safety guide – Risk assessment for dangerous goods*
- *Dangerous Goods Safety (Storage and Handling of Non-explosives) Regulations 2007 – guide*
- *Diving safety management system*
- *Emergency planning*
- *Hazard identification*
- *Involvement of members of the workforce*
- *Management of change*
- *Offshore facility safety case*
- *Pipeline management plan*
- *Pipeline operation safety case*
- *Records management including document control*
- *Reporting of accidents, incidents and dangerous occurrences*
- *Reporting dangerous goods incidents – guideline (6th edition)*
- *Risk assessment and management including operational risk assessment*
- *Safety management system*

# Appendix 5 Sample performance standard template

The performance standard template is available from the Department's website.

*Insert company logo*

## 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 sated 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* | | |