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

Petroleum safety and major hazard facility – guide

Hazard identification

February 2020

Disclaimer

Creative commons

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.

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 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 for effective hazard identification required under Western Australian legislation administered by the Department.

For the purpose of this Guide, the term “safety case” will be used to cover all of the safety documents referred to in the respective 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” (MAEs). Reference within this Guide is made to MAE which will encompass the term “major incident”.

The Dangerous Goods Safety (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 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

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 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. These include:

- AS ISO 31000 *Risk management – Guidelines*
- IEC ISO 31010 *Risk management – Risk assessment techniques*
- ISO 17776 *Petroleum and natural gas industries – Offshore production installations – Major Accident Hazard Management during design of new installations*
- AS/NZS 2885.6 *Pipelines – Gas and liquid petroleum – Part 6: Pipeline safety management*
- AS IEC 61882 *Hazard and operability studies (HAZOP studies) – Application guide*
- 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 hazard identification, risk assessments and risk management needs to be conducted effectively within their organisations.

1.4 Aims and outcomes of hazard identification

The aims and outcomes of the hazard identification processes are to:

- identify all hazards to the safety and health of all people at or near a facility
- identify all hazards from dangerous goods to people, property and environment
- identify the associated events and outcomes and rank these based on risk
- show clear links between hazards, causes and the potential events
- identify hazards that can lead to major accident events
- provide the licensee or operator and the workforce with sufficient knowledge, awareness and understanding of the hazards to be able to prevent and deal with accidents and dangerous occurrences
- provide a systematic record of all identified hazards which may affect safety and health of all people and property or the environment at or near the facility, and in particular those which may lead to major accident events, together with assumptions
- provide a basis for identifying, evaluating, defining and justifying the selection (or rejection) of control measures for eliminating or reducing risk.

1.5 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.

- *Risk assessment and management including operational risk assessment*
- *Major accident events, control measures and performance standards*
- *ALARP demonstration*

These three guides together with this document are a suite of 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.

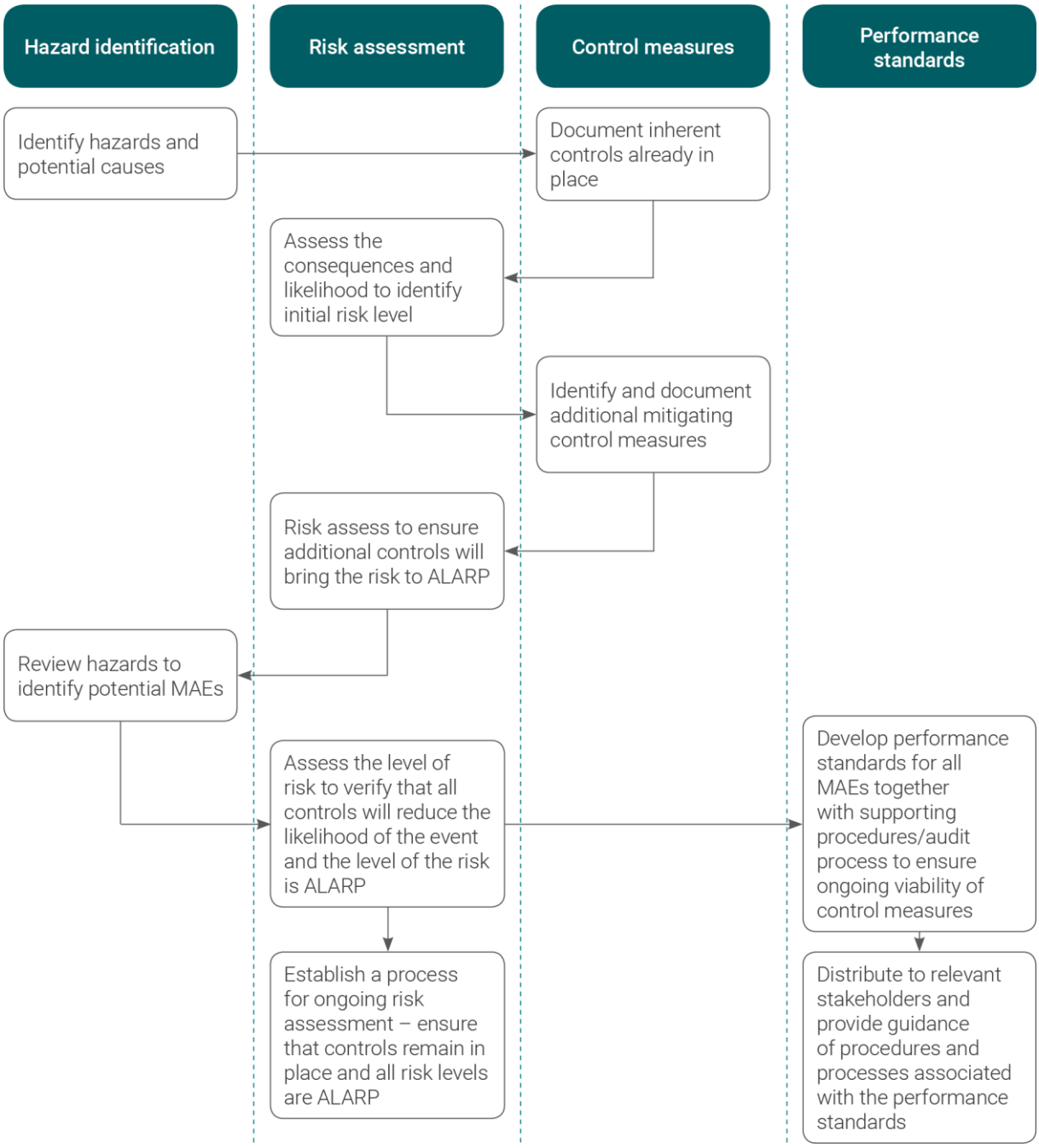

Figure 1 Formal safety assessment process

2 Hazard identification planning and preparation

Detailed planning and preparation for hazard identification is critical to the successful outcome of the process. Apart from the collation and provision of all the information required to support the hazard identification process, schedule the workshop to:

- ensure key subject matter (SME) experts and workforce representation will be available
- allow sufficient time for participants to review and consider all aspects of the hazards identified including relevant historical incidents on similar facilities both locally and internationally
- include regular breaks to avoid fatigue
- ensure safe manning levels are maintained at the facility.

Regardless of the methodology to be adopted for a hazard identification study, this will generally be conducted using a brainstorming process undertaken by a group of skilled and experienced people with knowledge of the particular facility, project or activities to be undertaken.

While the main aim of the formal safety assessment is the identification and control of MAEs or serious harm incidents (depending on the relevant legislation) it is important that all known hazards which may affect the safety and health of personnel at or near the facility, as well as property and environment if related to a major hazard facility, are identified, assessed and documented.

2.1 Successful hazard identification processes

A successful hazard identification may include:

- hazard identification processes relevant and appropriate for the facility
- hazard identification teams should take a fresh view of any existing knowledge and should not assume that no new knowledge is available
- appropriate members of the workforce are actively involved in the hazard identification process and there are regular and ongoing consultation sessions with the workforce
- any assumptions and uncertainties are explicitly identified and recorded for later analysis
- full documentation of all methods, results, assumptions and data
- documented identification of hazards is regularly reviewed and maintained from alerts and incidents and used as a live document.

Hazard identification outcomes should be used to plan for management of safety and health and should be provided to the workforce.

Hazard identification outcomes should be used to plan for management of harm to all people, property and environment arising from dangerous goods.

Knowledge of hazards and their implications is necessary for the next steps of risk assessment and evaluation of control measures.

Figure 2 shows the various steps in the hazard identification process.

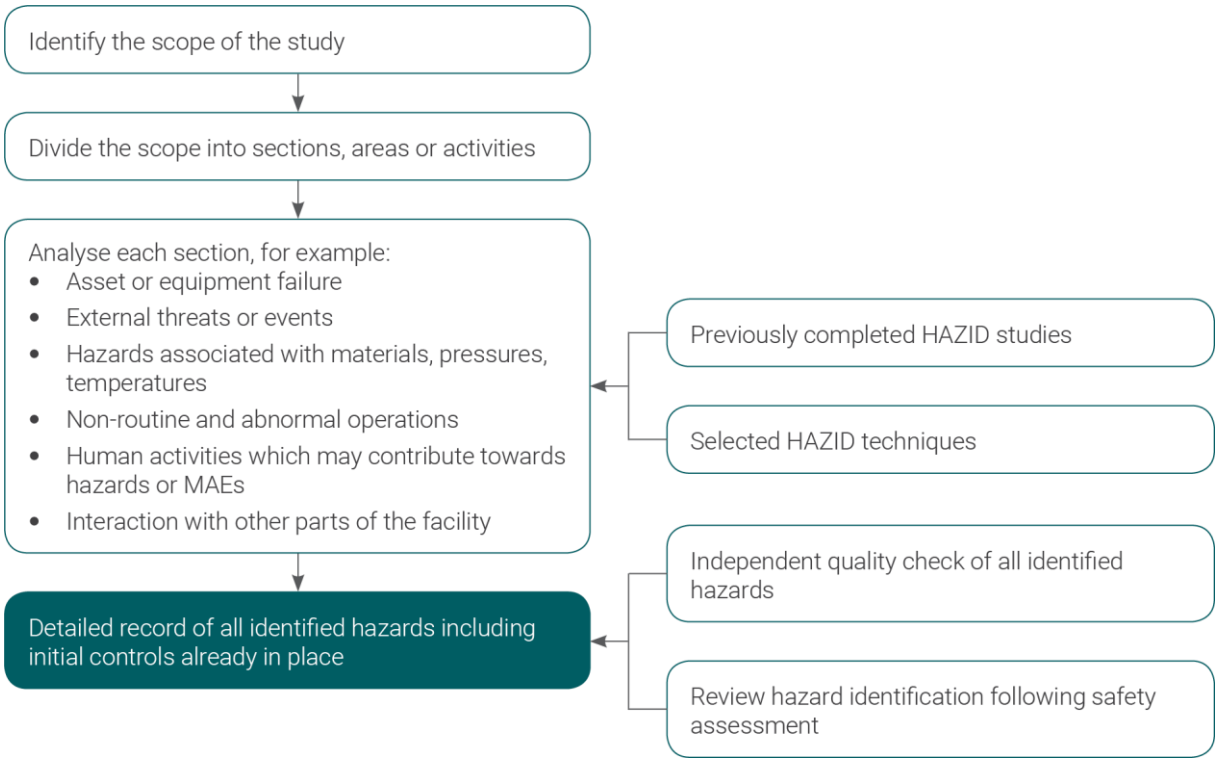

Figure 2 Hazard identification process

2.2 Hazard identification techniques

There are a number of techniques and methodologies, or combinations of appropriate techniques and methodologies that can be used for the identification of hazards on a facility. Some common techniques are:

- incident data – review of past incident and accidents that have occurred on the facility or known to have occurred elsewhere can be useful in identifying hazards
- brainstorming
- guideword analysis
- what-if – using a set of pre-prepared and customised what-if questions on potential deviations and upsets at the facility
- facility operational experience
- hazard and operability study (HAZOP)
- safety management studies – identifies threats to onshore pipelines or pipeline systems and associated surface facilities (AS 2885.6)
- failure modes and effects analysis (FMEA)
- task analysis
- event tree
- fault tree.

Some issues to consider when selecting a hazard identification technique are listed in Table 1.

Table 1 Hazard identification technique selection issues

Issue	Check
Depending on the lifecycle phase of the facility	• At a concept development phase it may be appropriate to use a HAZOP or HAZID technique • During detailed design, more detailed techniques may be required to provide a greater understanding of operational concerns • For onshore pipelines and associated aboveground facilities, a safety management study in accordance with AS 2885.6 to identify all threats to the pipelines • For construction, installation, commissioning and start-up, a focus on procedures and task analysis may be beneficial • For ongoing routine operations phase, the technique will be influenced by factors such as the level of knowledge of hazards, the history of risk assessments and the extent of change that has occurred • Accident and dangerous occurrences that have occurred at the facility or at other similar facilities (e.g. lessons learned and safety alerts) • Dangerous goods incidents relating to people, property and environment that have occurred at the facility or at other similar facilities (e.g. lessons learned and safety alerts).
Complexity and size	The complexity and size of a facility includes the number of activities or systems, the number of pieces of equipment, the type of process and the range of potential outcomes. Some techniques can get bogged down when they analyse complex problems. For example, event tree and fault tree analyses can become overly time consuming and difficult to structure effectively. However, simple techniques may not provide sufficient focus to reach consensus or confidence in the identification of hazards.
Type of process or activity	• Where activities are procedural or human error is dominant then task analysis may be appropriate • Where knowledge of the failure modes of equipment is critical (e.g. control equipment) then FMEA may be appropriate • Where the facility is readily shown on a piping and instrumentation diagram or process and instrument diagram, then HAZOP may be used • Where multiple failures need to combine to cause an accident or multiple outcomes are possible, then fault tree or event tree analysis may be beneficial.

The methodology chosen will depend on the type, size and complexity of the facility and the activities to be conducted during operations.

Hazard identification is key to the development and review of the safety case, and all hazards must be identified so they can be assessed and appropriately managed for ongoing safety at the facility.

The selected technique should:

- be systematic and structured
- encourage lateral thinking about possible hazards that have not previously been identified and considered
- be appropriate for the facility and its phase of development or level of maturity
- provide for the maximum amount of information to be extracted during the process.

2.3 Input information for hazard identification

Once the scope of the hazard identification process is defined, the input information needs to be collated and reviewed prior to the workshop.

The hazard identification process should be based on a comprehensive and accurate description of the facility, including:

- all necessary diagrams
- process information
- existing conditions
- modifications
- procedures and work instructions
- hazardous materials information (safety data sheet).

This input information can be drawn from a number of areas including:

- site drawings including process flows, layouts, pipeline and instrumentation diagrams (P&IDs)
- detailed description of the equipment to be installed on the facility and its mode of operation; any new equipment (i.e. not previously installed on similar facilities) should be clearly identified as it may require additional analysis
- any previously documented workshops conducted for the facility under review or similar facilities which may also be relevant to the scheduled study
- details of any incidents or accidents reported either on the facility under review or similar facilities.

Conduct a quality check once the information has been gathered and prior to commencement of the workshop to ensure:

- all information is accurate and relevant to the proposed hazard identification study
- that no critical information is missing which may restrict the required depth of analysis being completed by the workshop attendees.

The hazard identification study may be supported by past risk assessments, historical incident data and previous hazard identification studies. Ensure any existing studies used:

- are understood by the hazard identification team participants
- are still relevant for the current operating conditions and condition of the facility
- were conducted to an acceptable standard
- addressed any gaps identified in the studies.

Previous studies may be helpful but should not be assumed to be correct. The absence of identified hazards in previous risk studies may not indicate there are no hazards to be identified. The previous hazard identification process may have been inadequate, with hazards inappropriately screened (not considered further based on incorrect assumptions) or there have been changes to the facility.

2.4 Hazard identification team

When selecting the attendees, 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 workshop 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.

2.5 Workforce involvement in hazard identification

Workforce involvement should be integral to the hazard identification process. In the event that a proposed hazard identification process relates to a new facility where the workforce is not in place, consideration should be given to inviting members of the workforce from a similar facility to participate.

It is important to ensure that contributions from the workforce are considered on the basis of technical and working knowledge and not on the seniority of the contributor. Workshops should not be dominated by individual persons or groups within the organisation excluding input from others.

Those members of the workforce invited to attend the hazard identification process should be involved in:

- development of the hazard identification process
- forming the team and workshop scheduling
- relevant workshops
- reviewing the workshop results
- implementation of any actions arising from the process
- assisting in feedback of the workshop outcomes to the rest of the workforce.

Further details are included in the *Involvement of members of the workforce* guide.

2.6 Inclusion of all hazards identified

In order to provide a comprehensive report of the hazard identification process conducted it is important to include all identified hazards regardless of whether they are considered to have a very low impact on the safety of the facility.

Licensees and operators should not eliminate hazards with a very low likelihood as these may become MAEs after further analysis. See Section 3 for further clarification.

2.7 Depth of analysis

The hazard identification process should provide sufficient details for a licensee or operator to understand the nature of each hazard and to identify the controls necessary for the management of that hazard.

It is important to get to the root causes (or hazards) leading to an undesirable event or MAE. The hazard identification should detail when, where and why the hazard is present. This helps in the assessment of the relevant control measures.

2.8 General considerations of hazard identification

An effective hazard identification is comprehensive and accurate. It may assist the process to divide the facility into sections.

Licensees and operators should review each section and ask:

- Can the process or activity deviate from the design intent or ‘safe operating procedure’?
- What activities are conducted and how could they go wrong?
- What hazards are present continuously or only occasionally?
- What equipment within the section could fail or be impacted by internal or external hazardous events?
- What abnormal or infrequent activities could be conducted and how could they go wrong?

- What are the possible events or consequences?
- What could happen in the section under review to create additional hazards, for example SIMOPs?
- Could the section of the facility interact with other sections (for example adjacent equipment, an upstream or downstream process or something sharing a service) in such a way as to cause an incident or lead to escalation?
- Could additional hazards result from the introduction of control measures?

The analysis should consider the interaction between these influencing factors such as:

- a safety system may be by-passed in start-up mode
- workers may not be adequately trained for start-up due to its infrequent occurrence.

Licensees and operators may also consider the possibility of grouping types of hazards if they could occur facility-wide, for example natural hazards and power loss. These hazards can then be considered generically and not for each part of the facility, unless special circumstances apply to a part of the facility and it needs to be considered individually (for example equipment vulnerable to loss of power).

2.8.1 Identification of controls

If the decision is made to identify and record control measures during the hazard identification process, then this should make clear which control measures apply to a specific cause or consequence. This assists third parties to understand that all identified hazards have controls. When combined with performance indicators and other relevant information, it helps to demonstrate adequacy of hazard and MAE risk reduction measures.

It may be helpful to chart the links between incidents, hazards and controls using either a bowtie or an event or fault tree diagram.

2.8.2 Realism and lateral thinking in hazard identification

Look for potentially complex events when conducting hazard identification studies. Figure 3 shows how a combination of active and latent failures in risk control barriers progress from a hazardous event to an accident.

The hazard identification team should:

- challenge assumptions and existing norms of design and operation
- think beyond their immediate experiences
- explore the effect of failure of management systems, controls and procedures
- consider how relatively minor problems may grow into MAEs because of other problems compounding the seriousness of the event.

The Swiss cheese model in Figure 3 demonstrates that there may be a variety of outcomes with a range of consequences depending on which barriers function and which do not. For example, if adequate technical barriers are put in place to prevent the ignition of a gas release, then the event may not result in fire or explosion but may still result in toxic effects depending on the nature of the gas release.

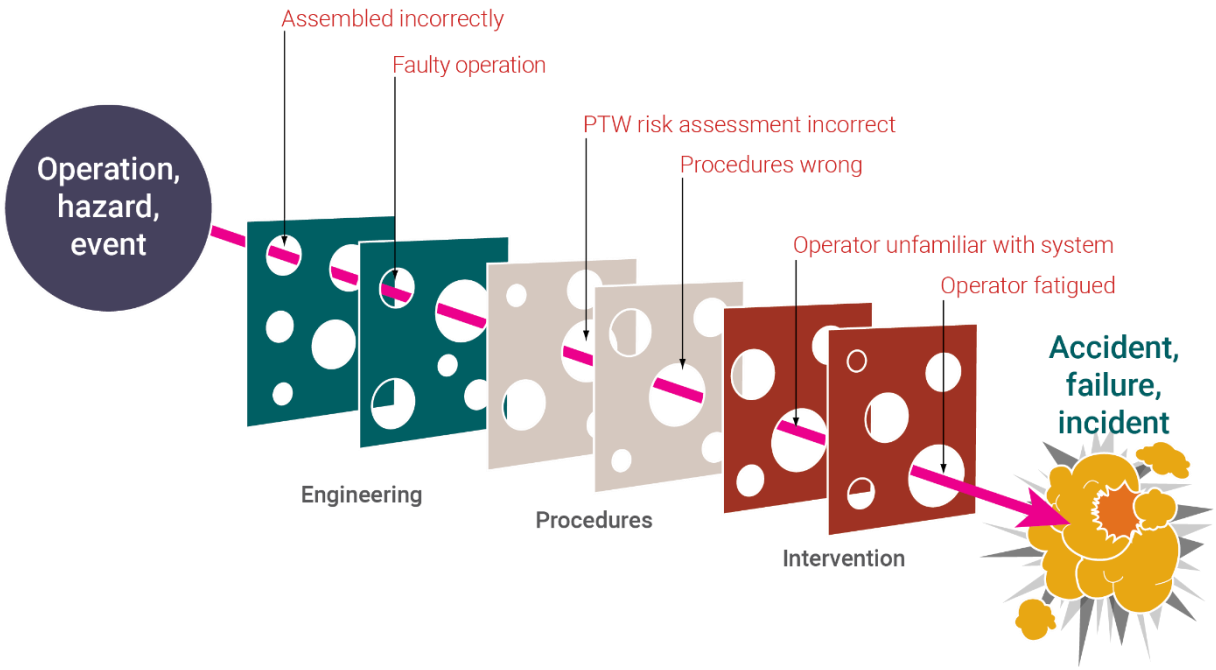

Figure 3 Swiss cheese model

2.9 Documenting the hazard identification outcomes

It is important that the results of hazard identification are clearly documented, including any underlying causes and control measures already identified. This process forms the basis for the later steps of safety case development including ongoing risk assessment and identification of further mitigating controls that will reduce the risks arising from the hazard to ALARP.

All reports and documentation generated from hazard identification and risk assessment should be managed within a document control system with version control.

2.10 Review and monitoring of hazards

Upon the completion of the hazard identification process, the findings should be circulated to the workshop attendees for review and comment. This will serve as a quality check that all relevant information has been captured and included in the documentation.

Once finalised, the outcomes of the hazard identification workshop should be conveyed to the rest of the workforce by the attendees.

Licensees and operators should ensure that there is a process or procedure in place for the ongoing review and monitoring of identified hazards to ensure controls remain in place and the levels of risk associated with each identified hazard are maintained at ALARP.

Hazard identification is a dynamic process which should precede any changes in a facility that could affect the safe operating environment or introduce new hazards.

3 Major accident events

A major accident event (MAE) is an event connected with a facility or pipeline operation, including a natural event, having the potential to cause multiple fatalities of persons at or near the facility.

Therefore by definition MAEs are consequence based.

Identification of MAEs is a key area of the formal safety assessment of a safety case and each hazard that may lead to an MAE must be assessed as part of the formal safety assessment process.

All hazards should be subject to a screening process to determine if they can result in an MAE. Figure 4 shows a process where hazards are screened and separated according to whether or not they could lead to events where multiple fatalities could occur. Those hazards which can lead to MAEs must be considered in the formal safety assessment, whereas hazards that cannot result in an MAE but are a hazard to safety and health must be covered by the operator's safety management system (SMS). The SMS should address both MAEs and non-MAEs through procedural systems designed to reduce risks to a level that is ALARP.

Further details on the management of identified MAEs and the control measures and performance standards associated with those MAEs are in *Major accident events, control measures and performance standards* guide.

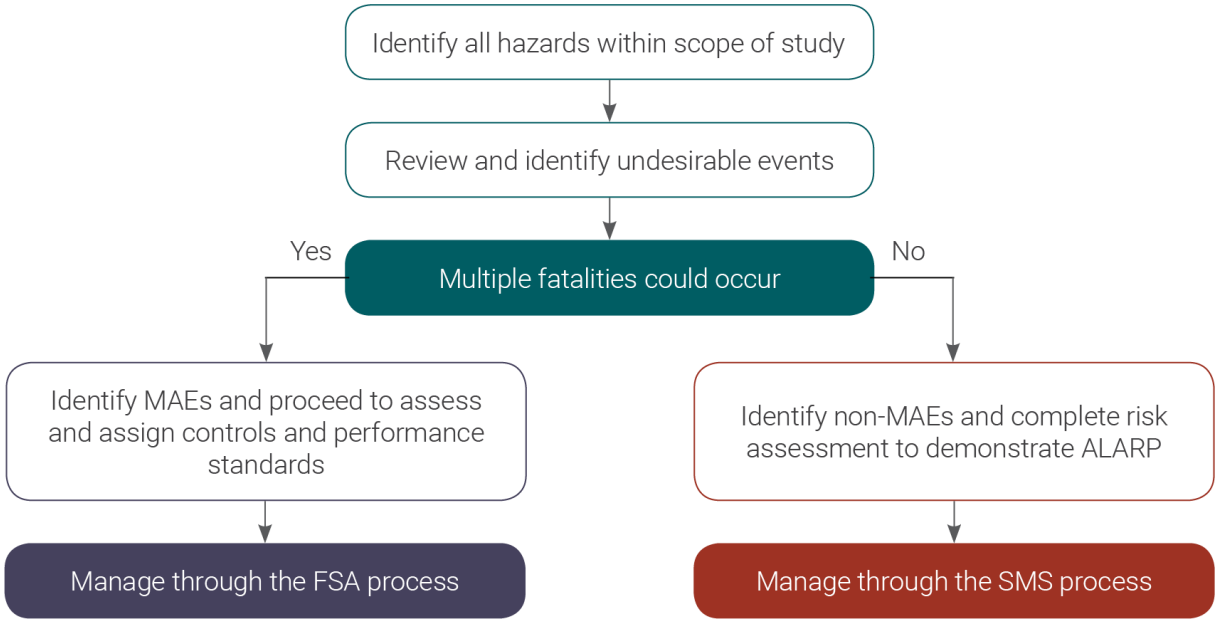

Figure 4 Screening of hazards for MAEs

4 Success factors for hazard identification

Hazard identification should include:

- appropriate members of the workforce (i.e. experienced, skilled and includes members of the workforce potentially exposed to the risks) actively involved in the process and others that have been given the opportunity to provide input
- processes appropriate to the facility and that the operator is able to explain the process selection
- systematic and structured techniques which foster creative thinking about possible hazards not previously identified
- the scope of hazard identification and that studies include MAE related hazards and general safety and health hazards
- hazards with a very low likelihood
- a process based on a comprehensive and accurate description of the facility, including all necessary drawings, process information, existing conditions, modifications, procedures and work instructions and hazardous materials information
- involvement and input from designers, manufacturers, contractors and suppliers where appropriate
- any assumptions and uncertainties thave been explicitly identified and recorded so that these can be verified or analysed later
- documented records which list at least all potential MAEs and hazards together with the underlying causes and control measures
- specific, measurable, attainable, realistic and timely (SMART) actions managed and closed out in an auditable manner
- an explanation why certain control measures have been adopted and others have been rejected included in the ALARP demonstration process
- the operator conducting a review of the information gathered once the hazard identification workshops have been completed.

5 Potential issues in hazard identification

Potential issues to avoid in the hazard identification process include:

- becoming complacent; it is important that all involved in hazard identification remain vigilant and wary about the hazards they are exposed to
- being too generic in identification of hazards and potential MAEs; for example, recording corrosion as a potential cause of loss of containment may not be sufficiently specific, it may be necessary to record where the corrosion can occur, under what circumstances, and at what rate
- limiting the hazard identification to the immediate cause of potential MAEs without determining the fundamental underlying cause; for example, the underlying cause of corrosion might be use of incorrect materials of construction, change of operating conditions, or a failure to conduct routine inspections
- carrying out the hazard identification with incomplete or inaccurate facility description information
- allowing the workshops to be dominated by individual persons or groups within the organisation
- assuming systems and procedures only function as intended
- failing to:
  - review or close gaps from previous session findings
  - remind participants of the scope and objectives
  - introduce new participants to the team without first explaining the process and assumptions.

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:

- NOPSEMA suite of guidance notes
- AS/NZS ISO 31009 *Risk management – Principles and guidelines*
- ISO 17776 *Petroleum and natural gas industries – Offshore production installations – Guidelines on tools and techniques for hazard identification and risk assessment*
- AS2885 *Pipelines – Gas and liquid petroleum – suite of standards*
- AS IEC 61882:2017 *Hazard and operability studies (HAZOP studies) – Application guide*

Appendix 3 Glossary

ALARP. As low as reasonably practicable. Also includes the term “so far as reasonable practicable (SFARP) for the purpose of this Guide.

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.

FMEA. Failure modes and effects analysis.

FSA. Formal safety assessment.

HAZID. Hazard identification study.

HAZOP. Hazard operability study.

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 document referred to as an MAE.

P&ID. Pipeline and instrumentation diagram.

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.

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.

SIMOPS. Simultaneous operations.

SME. Subject matter expert.

SMS. Safety management system.

Appendix 4 Further information

Other guidance:

- *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*
- *Involvement of members of the workforce*
- *Major accident events, control measures and performance standards*
- *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*