NOPSEMA
Australia's offshore energy regulator

GUIDANCE NOTE

Hazard identification

Document No: N-04300-GN01070107 A98726

Date: 24/06/2020

Core concepts

- The aims of a robust hazard identification process are to ensure that the operator and members of the workforce know about existing hazards which could lead to major accident events (MAEs) at their facility and that new hazards are recognised before they are introduced.
- Once hazards have been identified, the operator of a facility will be able to take action to properly manage them.
- It is important to choose a hazard identification technique, or techniques, which provide an adequate depth of analysis.
- Hazard identification should provide sufficient knowledge, awareness and understanding of the hazards that could lead to a MAE to be able to prevent and mitigate undesirable outcomes.
- During hazard identification, operators may wish to incorporate identification of all health and safety related hazards as the safety management system (SMS) must provide for all hazards and risks, not just risks of MAEs.
- Hazard identification provides a basis for identifying, evaluating, defining and justifying the selection (and rejection) of control measures for reducing risk.
- The full range of hazard and event types should be considered and the outputs of the hazard identification process fully documented.
- Identified hazards should not be ignored or discounted simply because control measures are, or will be, in place.
- The hazard identification process should consider all operating modes of the facility, and all activities that are expected to occur. It should also consider human and system issues as well as engineering issues.
- The hazard identification process should recognise that combinations of failures can occur, even though these may appear highly unlikely. Whilst it is important to be systematic, it is also necessary to think laterally.
- The hazard identification process should be ongoing and dynamic. It should not just be carried out during development of the safety case, but also in a range of defined circumstances, such as when there is a facility modification, after any major accident event or dangerous occurrence, if a control measure deficiency is identified, and at defined intervals.

Table of Contents

Core concepts 1
Table of Contents 2
Abbreviations/Acronyms 3
Key definitions for this Guidance Note 4
1. Introduction 5
1.1. Intent and purpose of this guidance note 5
1.2. The risk management process applied in the safety case 6
1.3. Formal Safety Assessment 7
1.4. Involving the workforce 10
2. Hazard identification 10
Reg 2.5(3)(c) The safety case for the facility must also contain a detailed description of the safety management system that *[provides evidence that the Safety Management System];* provides for the continual and systematic identification of hazards to health and safety of persons at or near the facility 11
2.1. The aims and outcomes of hazard identification 11
2.2. Features of successful Hazard Identification Processes 11
3. Planning and preparation for Hazard Identification 12
3.1. General approach 12
3.2. Scope 14
3.3. Selecting the Hazard Identification Technique 14
3.4. Selecting the Hazard Identification team 16
3.4.1. Workforce involvement in Hazard Identification 16
3.5. Scheduling 17
3.6. Documentation and linkages 18
4. The Hazard Identification process 18
4.1. Information for Hazard Identification 18
4.2. Providing an adequate depth of analysis 20
4.3. General considerations of Hazard Identification 21
4.4. Lateral thinking and realism in Hazard Identfication 22
4.5. Rejecting hazards from consideration 23
5. Identifying Major Accident Events 24
Formal safety assessment 24
Reg 2.5(2)(a) The safety case for the facility must also contain a detailed description of the formal safety assessment for the facility, being an assessment, or series of assessments, conducted by the operator that identifies all hazards having the potential to cause a major accident event 24
6. Other considerations 26
6.1. Review and revision of Hazard Identification 26
6.2. Quality Assurance 26
7. Success factors for Hazard Identification 26
7.1. Practical factors for success of Hazard Identification 26
7.2. Potential pitfalls in Hazard Identification 27
8. References, acknowledgements and notes 28
Appendix A: Benefits and disadvantages of Hazard Identification (HAZID) techniques 29

Abbreviations/Acronyms

ALARP	As low as reasonably practicable
EER	Evacuation, Escape and Rescue Analysis
FD	Facility Description
FMEA	Failure Mode Effects Analysis
FMECA	Failure Mode Effects and Criticality Analysis
FSA	Formal Safety Assessment
HAZID	Hazard Identification study
HAZOP	Hazard and Operability study
HSR	Health and Safety Representative
JHA	Job Hazard Analysis
JSA	Job Safety Analysis
LEL	Lower Explosive Limit
LOPA	Layers of Protection Analysis
MAE	Major accident event
MoC	Management of Change
NOPSEMA	National Offshore Petroleum Safety and Environmental Management Authority
OHS	Occupational health and safety
OPGGS(S) Regulations	Offshore Petroleum and Greenhouse Gas Storage (Safety) Regulations 2009
QRA	Quantitative Risk Analysis
SDS	Safety Data Sheets
SMS	Safety Management System

Key definitions for this Guidance Note

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

ALARP	This term refers to reducing risk to a level that is As Low As Reasonably Practicable. In practice, this means that the operator has to show through reasoned and supported arguments that there are no other practicable options that could reasonably be adopted to reduce risks further.
Control Measure	A Control Measure is any system, procedure, process, device or other means of eliminating, preventing, reducing or mitigating the risk of major accident events arising at or near a facility. Control measures are the means by which risk to health and safety from events is eliminated or minimised. Controls can take many forms, including physical equipment, process control systems, management processes, operating or maintenance procedures, emergency response plans, and key personnel and their actions.
Formal Safety Assessment	A formal safety assessment in the context of the OPGGS(S) Regulations, is an assessment or series of assessments that identifies all hazards having the potential to cause a major accident event, is a detailed and systematic assessment of the risk associated with each of those hazards, including the likelihood and consequences of each potential major accident event; and identifies the technical and other control measures that are necessary to reduce that risk to a level that is as low as reasonably practicable [OPGGS(S) subregulation 2.5(2)]
Hazard	A Hazard is defined as a situation with the potential for causing harm to human health or safety.
Hazard Identification	Hazard Identification is the process of identifying potential hazards. In the context of the OPGGS(S) regulations, hazard identification involves identifying all hazards having the potential to cause a major accident event [OPGGS(S) subregulation 2.5(2)(a)], and the continual and systematic identification of hazards to health and safety of persons at or near the facility[OPGGS(S) subregulation 2.5(3)(c)].
Major Accident Event	A Major Accident Event is an event connected with a facility, including a natural event, having the potential to cause multiple fatalities of persons at or near the facility [OPGGS(S) Regulation 1.5].
Performance Standard	Performance standard means a standard, established by the operator, of the performance required of a system, item of equipment, person or procedure which is used as a basis for managing the risk of a major accident event [OPGGS(S) Regulation 1.5].
Risk Assessment	Risk assessment is the process of estimating the likelihood of an occurrence of specific consequences (undesirable events) of a given severity.
Workforce	Members of the workforce includes members of the workforce who are: (a) identifiable before the safety case is developed; and (b) working, or likely to be working, on the relevant facility. [OPGGS(S) subregulation 2.11(3)]

1. Introduction

1.1. Intent and purpose of this guidance note

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

This guidance note, "Hazard Identification", forms part of a suite of guidance notes which are designed to help operators through the process of conducting a formal safety assessment in support of the evidence that risks are reduced to a level that is ALARP. These guidance notes include:

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

Section 1 of the guidance note gives an overview of the Formal Safety Assessment process, and then the balance of the guidance note discusses hazard identification aspects in particular.

The purpose of hazard identification is to help all stakeholders understand the hazards and potential major accident events (MAEs) that could occur at or near a facility and develop an awareness of the possible causes and contributing factors. The aim of this guidance note is to provide guidance on the approaches and methodologies that an operator could use to systematically and comprehensively identify hazards, and to communicate the findings effectively.

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

Figure 1 below illustrates the scope of the NOPSEMA safety case guidance notes overall, and their interrelated nature. This guidance note on hazard identification should be read in conjunction with the other relevant guidance notes; the full set is available on the NOPSEMA website along with guidance on other legislative requirements such as operator nomination, validation, and notifying and reporting accidents and dangerous occurrences.

Guidance notes indicate what is explicitly required by the regulations, discuss good practice and suggest possible approaches. An explicit regulatory requirement is indicated by the word **must**, while other cases are indicated by the words **should**, **may**, etc. NOPSEMA acknowledges that what is good practice and what approaches are valid and viable will vary according to the nature of different offshore facilities and their hazards. Whilst this guidance note puts forward a selection of the possible approaches that operators may choose to explore in addressing the risk assessment requirements of the OPGGS(S) regulations, the selection is not exhaustive and operators may choose to use other techniques not covered by this guidance note.

This guidance note is not a substitute for detailed advice on the regulations or the Acts under which the regulations have been made.

Figure 1 – Safety Case Guidance Note Map

1.2. The risk management process applied in the safety case

The Australian/New Zealand Standard on Risk Management AS/NZS ISO 31000:2009 provides a generic framework for establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk. ISO 17776 also provides guidance in relation to tools and techniques for hazard identification and risk assessment for offshore petroleum production facilities. The requirements under the OPGGS(S) Regulations reflect the current thinking on risk management and hence call for application of the key elements of risk management. These are outlined in subregulation 1.4(2) "objects" summarised below.

OPGGS(S) Regulation – Objects	
Reg 1.4(2)	An object of these Regulations is to ensure that safety cases for offshore petroleum facilities make provision for the following matters in relation to the health and safety of persons at or near the facilities: (a) the identification of hazards, and assessment of risks; (b) the implementation of measures to eliminate the hazards, or otherwise control the risks; (c) a comprehensive and integrated system for management of the hazards and risks; (d) monitoring, audit, review and continuous improvement.

1.3. Formal Safety Assessment

OPGGS(S) Regulation – Formal Safety Assessment Requirement	
Reg 2.5(2)	The safety case for the facility must also contain a detailed description of the formal safety assessment for the facility, being an assessment, or series of assessments, conducted by the operator that: (a) identifies all hazards having the potential to cause a major accident event; and (b) is a detailed and systematic assessment of the risk associated with each of those hazards, including the likelihood and consequences of each potential major accident event; and (c) identifies the technical and other control measures that are necessary to reduce that risk to a level that is as low as reasonably practicable.
Note	*A formal safety assessment relates only to major accident events*

The Formal Safety Assessment is focused on Major Accident Events (MAEs). Providing a well-considered, detailed description of a suitable and sufficient formal safety assessment within the safety case will enable operators to provide evidence of:

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

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

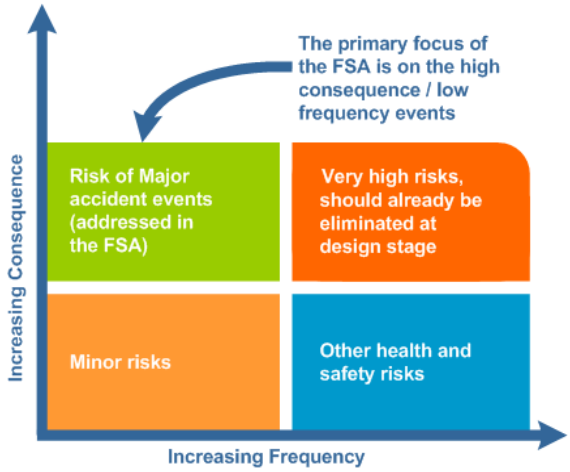

Figure 2 – Formal Safety Assessment to focus on MAEs

For the purposes of a safety case submission, the hazard identification and risk assessment described in the formal safety assessment need only relate to major accident events. It should be noted however, that the

detailed description of the safety management system in the safety case must provide for all hazards and risks to persons at the facility, not just risks of major accident events. Therefore, operators may wish to consider broadening the scope of their hazard identification and risk assessment studies to address non-MAE related hazards, e.g. noise, exposure to exhaust fumes, etc.

Further guidance is available in the NOPSEMA guidance note:

"Safety Management Systems (SMS)"

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

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

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

Further guidance is available in the NOPSEMA guidance note:

"Risk assessment"

Further guidance is available in the NOPSEMA guidance note:

"Control measures and performance standards"

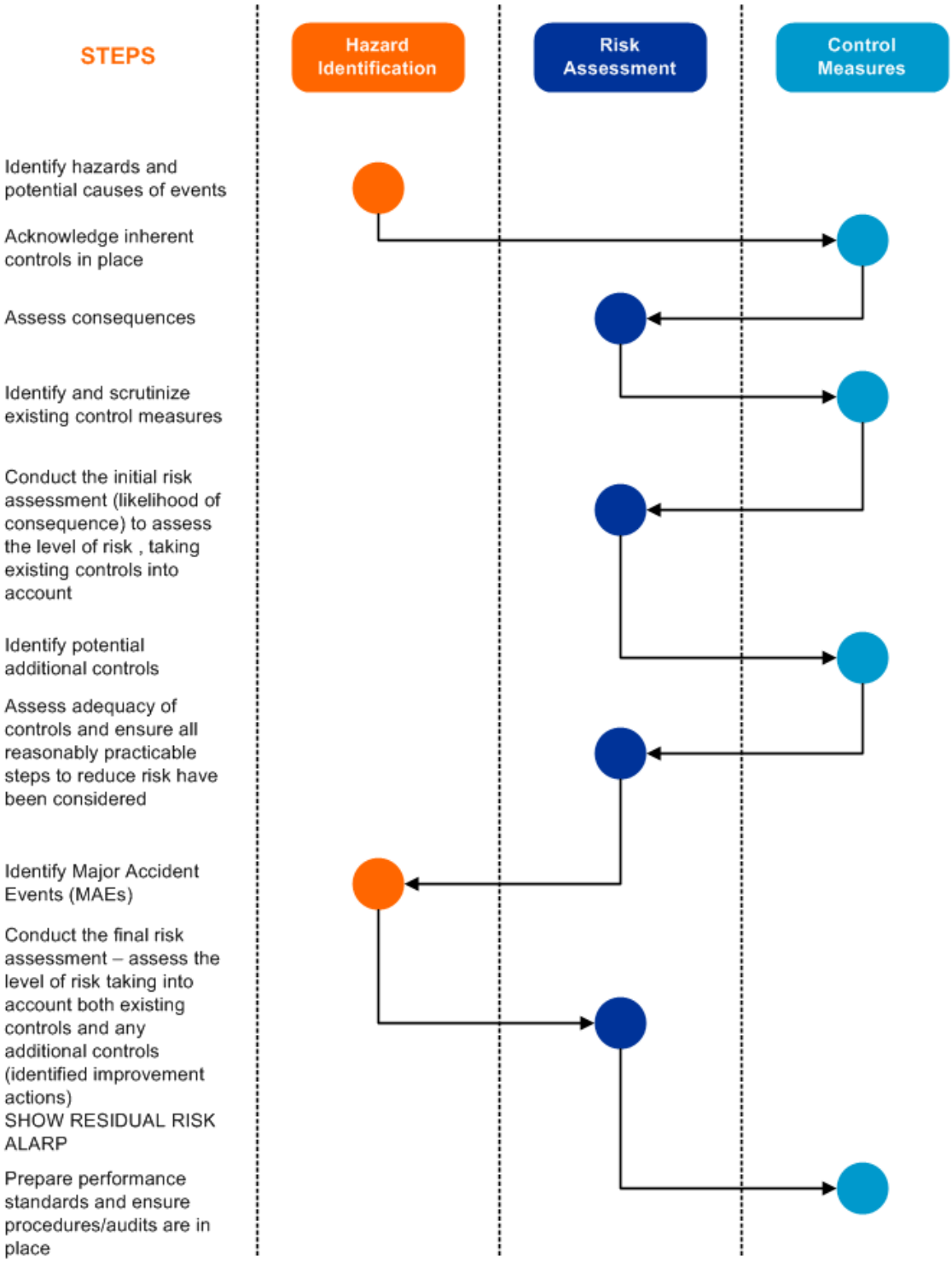

Figure 3 – The FSA Process

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

1.4. Involving the workforce

OPGGS(S) Regulation – Involvement of members of the workforce

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

(a) in the development or revision of the safety case for the facility, there has been effective consultation with, and participation of, members of the workforce; and

(b) the safety case provides adequately for effective consultation with, and the effective participation of, the members of the workforce, so that they are able to arrive at informed opinions about the risks and hazards to which they may be exposed on the facility.

(2) A demonstration for paragraph (1) (a) must be supported by adequate documentation.

(3) In subregulation (1):

members of the workforce includes members of the workforce who are:

(a) identifiable before the safety case is developed; and

(b) working, or likely to be working, on the relevant facility.

Formal safety assessment is the process of debating, analysing, creating and sharing views, information and knowledge on the risk of major accident events and the means to prevent or mitigate them. It must include the active participation of people at the 'coal face' who influence safe operation, and hence hazard identification and risk assessment roles should be defined for members of the workforce. Formal safety assessment should not be limited to desktop theoretical studies. It can include any activity the operator employs to understand the facility and its risks. For example, an FSA could incorporate information from incident investigations, discussions during safety meetings regarding hazards and ways of controlling them, condition monitoring programs, analysis of process behaviour, evaluation of trends or deviations from critical operating parameters, procedure reviews, etc.

The knowledge generated by the formal safety assessment should be captured, managed and disseminated to ensure it remains up to date and is used in the design, operation and maintenance of the facility. The management of knowledge generated through hazard identification and risk assessment will also greatly assist the efficient development of a safety case for the facility. For example, these processes will assist in handling assumptions, actions arising, etc. through the safety case development process.

It is not possible to involve everyone in the hazard identification and risk assessment processes; therefore, it is important that regular feedback is provided to the rest of the workforce. This feedback should take the form of communicating the hazards that are present, the risks associated with those hazards, the controls in place and any recommendations arising. The workforce should also be provided with an opportunity to review and comment on the risk assessment output. This is important both as a quality control activity and as part of the mandatory workforce consultation and participation required by the OPGGS(S) regulations. It also fosters a feeling of ownership among personnel not directly involved in the risk assessment process.

Further guidance is available in the NOPSEMA guidance note:

"Involving the workforce"

2. Hazard identification

OPGGS(S) Regulation – Hazard Identification Requirement

Reg 2.5(3)(c)	The safety case for the facility must also contain a detailed description of the safety management system that *[provides evidence that the Safety Management System];* provides for the continual and systematic identification of hazards to health and safety of persons at or near the facility

2.1. The aims and outcomes of hazard identification

The outcomes of the hazard identification process are to:

- identify all hazards to the health and safety of people at or near the facility;
- identify the associated events and outcomes and rank them based on risks;
- show clear links between hazards, causes and the potential events;
- identify hazards can lead to major accident events;
- provide the 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 health and safety of people at or near the facility, and in particular those which may lead to major accident events, together with any assumptions; and
- provide a basis for identifying, evaluating, defining and justifying the selection (and rejection) of control measures for eliminating or reducing risk.

2.2. Features of successful Hazard Identification Processes

The following factors lead to successful hazard identification:

- The hazard identification process should be appropriate and relevant to the facility;
- The hazard identification team should take a fresh view of any existing knowledge, and should not automatically assume that no new knowledge is required;
- Appropriate members of the workforce are actively involved and regular and ongoing consultation occurs;
- Assumptions and uncertainties are explicitly identified and recorded for later analysis;
- All methods, results, assumptions and data are fully documented; and
- The documented identification of hazards is regularly maintained (e.g. updates from alerts and incidents) and used as a live document.

Outcomes from hazard identification should be used to plan for management of health and safety and should be provided to people who require it in order to work safely. Knowledge of hazards and their implications is necessary for the next steps of the safety case development process, including risk assessment and evaluation of control measures.

3. Planning and preparation for Hazard Identification

3.1. General approach

Hazard identification is usually a qualitative brainstorming process undertaken by a group of skilled and experienced people with knowledge of the particular facility, project and/or activities being undertaken. Most hazard identification techniques involve a team approach, since few individuals have expertise on all hazards, and group interactions are more likely to stimulate consideration of hazards that even well-informed individuals might overlook. Those who will be exposed to the hazards while on an offshore facility can make a valuable contribution to the hazard identification process. Operating staff are likely to have ideas on potential accidents based on their own experience. It follows that hazard identification is usually an element of the safety case development process which lends itself to workforce involvement.

Hazards are diverse, and many different methods are available for hazard identification. While some methods have become standard for particular applications (e.g. FMEA for ballast system failures), it is not necessary or desirable for the regulator to specify which approach should be adopted in particular cases.

The methodology should be chosen by the operator to meet the objectives as efficiently as possible given the available information and expertise. It may be a standard technique, following an established protocol, a modification of one, or a combination of several.

ISO 17776 provides guidance on tools and techniques for hazard identification for offshore petroleum production facilities.

Figure 4 shows some possible steps in hazard identification as an example.

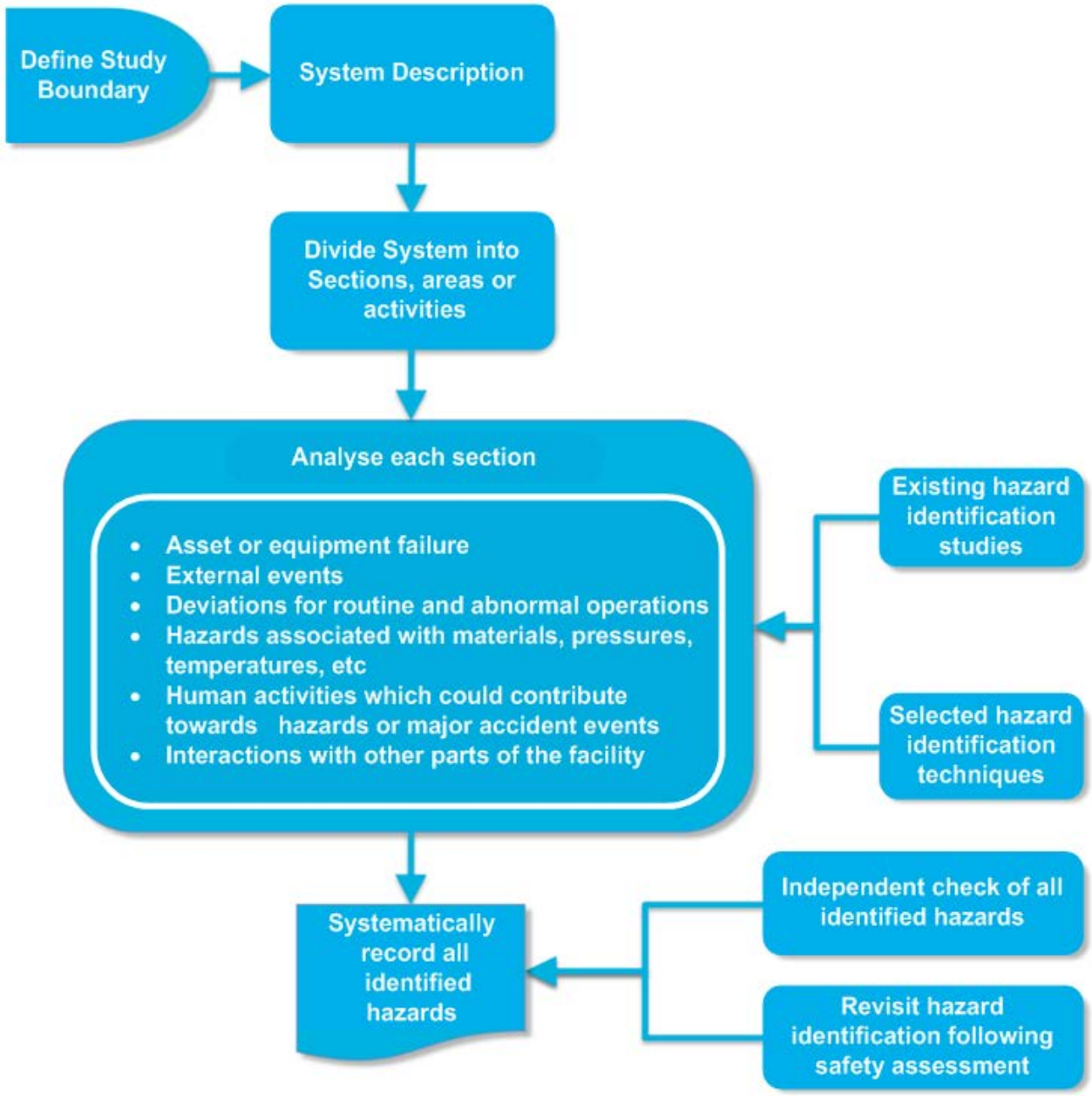

Figure 4 – Hazard Identification Steps

3.2. Scope

In determining the scope of the hazard identification process, the operator should consider where to set the boundaries for each study. It is important to define and record any assumptions relevant to the facility or activities and then ensure that the hazard identification process operates within the defined envelope. It may assist to divide the facility into manageable sections, areas or activities for the hazard identification process. Note however, if the overall scope of hazard identification is split into discrete sections or studies, the interfaces at the boundaries between the various studies will need to be specifically covered as well. Care must be taken when deciding to exclude any area or operation, and reasons recorded for the purposes of demonstrating in the safety case that such decisions were appropriate.

3.3. Selecting the Hazard Identification Technique

The hazard identification technique(s) chosen should be appropriate to the facility and to the activities being conducted at the facility; therefore in selecting a hazard identification process, operators may wish to consider:

- the size and complexity of the facility;
- the duration and complexity of the activities or phase being considered;
- the nature of the activities and processes associated with the facility; and
- pilot studies / safety cases from similar facilities.

The hazard identification process sets the foundation for the remainder of the safety case development process. All hazards are identified during this phase so they can be assessed and safely managed. Therefore the technique selected should:

- be systematic and structured;
- foster creative and lateral thinking about possible hazards that have not previously been experienced;
- be appropriate for the facility and its phase of development or level of maturity;
- consider which approach will extract the maximum quantity of useful information; and
- should be appropriate for the people involved.

There are many techniques, or combinations of techniques that an operator may choose to apply. Some of the more common hazard identification techniques are listed below:

- Incident Data (having company and/or external incident data at hand can assist in validating the opinions/experience of the team)
- Checklist Analysis
- Brainstorming
- What-if (or Structured What-If Checklist Technique – SWIFT)
- Guideword Analysis
- Hazard and Operability Study (HAZOP)
- Failure Modes and Effects Analysis (FMEA)
- Task Analysis

- Event Tree
- Fault Tree

A summary of the techniques, along with guidance on their use, applicability, benefits and disadvantages is presented in Appendix A. Table 1 below summarises some of the issues that should be considered in selecting a hazard identification technique.

Table 1 – Hazard Identification Technique Selection Issues

Issue	Check
Depending on what phase in the lifecycle the facility is in	• At a concept development phase it may be appropriate to use a coarse HAZOP or HAZID technique. • During detailed design more detailed techniques may be required to provide a greater understanding of operational concerns. • For construction, installation, commissioning and start-up the focus on procedures and task analysis may be of benefit. If this is conducted early enough it can influence the design measures incorporated to minimise the risk during various phases of the project as well as for on-going maintenance activities. • For the on-going 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, safety alerts, etc.)
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 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 (e.g. task analysis, procedural HAZOP etc.). • 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 and Event Tree Analysis may be beneficial.

A simple structured brainstorming technique (e.g. guideword based analysis) will satisfactorily identify the majority of hazards for many facilities. However, an operator may need to apply a combination of different hazard identification techniques to ensure that the full range of factors is properly considered.

For example, a review of incident data is useful to check that known hazards have not been missed. An operator should take into account the operating history of their facility, and similar facilities within their organisation and/or industry. However, for the overall hazard identification process, the operator should not rely solely on historical data.

A recorded incident is just one example out of a vast range of potential incidents (most of which may never occur). The challenge for operators is to identify and control all the potential incidents that may occur, not just prevent repetitions.

Operators will also need to decide when it is appropriate to use a more detailed technique. Situations where more detailed techniques may be required include:

- where there is uncertainty as to the underlying causes of a particular incident;
- where the complexity of a particular hazard is high;
- where a more detailed breakdown of the hazardous event is required in order to adequately assess the likelihood during the risk assessment phase; and
- where the facility is of a new type or novel application for the operator, a more detailed technique may provide greater insight

In cases where it is not clear what method may be successful, a 'pilot' study on a selected area of the facility may be beneficial. Operators should include a check on the appropriateness of the hazard identification technique(s) as part of their quality assurance (see Section 6.2).

3.4. Selecting the Hazard Identification team

The amount of work required to demonstrate a case for safety requires a large commitment in terms of both onshore management and facility personnel at all stages, including hazard identification. When carrying out hazard identification it is recommended that the following aspects are considered:

- providing the right mix of expertise and involving all relevant designated workgroups – hazards not evident to individual workgroups may be identified through interaction between work groups;
- involving manufacturers, contractors and suppliers as necessary;
- where relevant, include personnel with a thorough knowledge of the facility and its history;
- including people with sufficient technical expertise in areas relevant to the facility, such as process plant knowledge, or maintenance procedures; and
- the inclusion of designers allows the capturing of design intent

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

3.4.1. Workforce involvement in Hazard Identification

The operator should endeavour to develop a role for members of the workforce in the hazard identification process. The role should allow them to contribute and gain knowledge in relation to hazard identification, and in recognising where a hazard could contribute to causing a major accident event. The operator should also be particularly vigilant in ensuring that contributions from the workforce are considered on the basis of technical / working knowledge and not on the seniority of the contributor.

It is recommended that the workforce is 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; and
- assisting in providing feedback of workshop outcomes to the rest of the workforce.

For a proposed new facility where the 'makeup' of the workforce has not yet been fully established, operators may wish to consider whether members of the workforce from their other similar facilities should be invited to participate.

It is not usually possible to involve all members of the workforce in hazard identification workshops; however it is important to provide feedback to those not directly involved. This feedback should be in the form of both training on the hazards that are present and the controls that are in place. It should also provide an opportunity for the workforce to review and comment on the hazard identification output i.e. an opportunity to raise additional concerns if it is considered that the hazard identification process is not complete or the assumptions that have been made as part of the process are incorrect. This is an important quality control activity.

Sufficient time needs to be allocated to the hazard identification phase of safety case development. This is true for new safety cases and revisions to existing safety cases. The operator should allow for time to:

- verify information to be used in the workshop(s);
- undertake the workshops themselves; and
- perform independent checks.

Although independent checks are not strictly required, it is a generally prudent to carry them out as part of a sound quality assurance process.

3.5. Scheduling

It is important to allow sufficient time to complete the full scope of the hazard identification at a depth which is appropriate to the chosen technique(s).

When scheduling workshops an operator will need to consider:

- the availability of key personnel and workforce involvement;
- cross - shift involvement;
- the need to maintain safe manning levels if taking people off-line to attend workshops;
- the need to maintain mental alertness with adequate breaks to avoid fatigue; and
- the need for continuity and consistency.

Once the workshops have been completed, it is important that the operator conducts a review on the information gathered. Workshop participants should be encouraged to provide feedback in the weeks following these workshops, as they might see things at a later time which were not included during the workshops.

There should also be an allowance for some contingency in the schedule for additional hazard identification activity that may arise from other steps within the formal safety assessment process.

3.6. Documentation and linkages

The hazard identification documentation forms the basis for the later steps of safety case development. The outcomes from hazard identification should clearly and logically link with the risk assessment and control measure steps.

Time spent upfront by the operator in planning how to link the various aspects of the safety case will be time well spent.

The main requirements are that the hazard identification documentation:

- clearly shows linkages between hazardous events, hazards, underlying causes and control measures where appropriate. A numbering system for hazards and controls to allow easy identification of safety case findings and tracking of linkages (ISO 17776 has a useful numbering system that people may consider using);
- contains sufficient information to support the later steps of safety case development. This allows an operator to describe the basis for a decision at a later time; don't rely on the memory of those present during the hazard identification as personnel and recollections can change;
- is maintainable; The records of hazard identification can directly accommodate the process of revisiting and updating the knowledge of hazards, including assumptions, uncertainties, debated issues, gaps in knowledge, details of hazards, incidents, control measures, learning's from accidents and dangerous occurrences, etc.; and
- is managed under a document control system.

For larger facilities it is likely that an electronic system for recording identified hazards will be easier for ongoing maintenance of the records.

4. The Hazard Identification process

4.1. Information for Hazard Identification

An operator should base the hazard identification process 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 (e.g. MSDS), etc. Prior to conducting the hazard identification, the operator should collect all relevant information, compile it and then check it for accuracy.

The hazard identification may be supported by past risk assessments and historical incident data. The operator should refer to previous hazard studies, if they are relevant, along with the issues discussed in this guidance note. However, it is important to ensure that for any existing studies:

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

While previous studies can be quite helpful, it cannot be assumed that they are always correct. For example, the absence of identified hazards in previous risk studies should not automatically be taken as an

indication that there are no hazards to be identified. It may simply be that the previous hazard identification process was inadequate, hazards were inappropriately screened (e.g. not considered further based on incorrect assumptions), and/or there have been changes to the facility since the risk study.

It is useful to have a record of the operator's and/or the Industry's past accidents and dangerous occurrences (near misses) at the hazard identification workshop. Past accidents or dangerous occurrences, either at the operator's facility or at similar facilities, provide a clear indication of what has gone wrong in the past, and could go wrong again. This information is best used as a quality check at the workshop to avoid missing potential hazards and major accident event scenarios. It should be noted that some operators actively track incidents both internally and externally and therefore are able to have this information as a direct input into the hazard identification process.

For an existing facility, the operator should review their own facility operating history and conditions (e.g. corrosion, breakdowns and maintenance) for potential hazards, bearing in mind however that historical incidents are unlikely to represent the full range of potential incidents. The operator should therefore use incident data to supplement more systematic hazard identification techniques. Figure 5 shows some useful sources of hazard identification input.

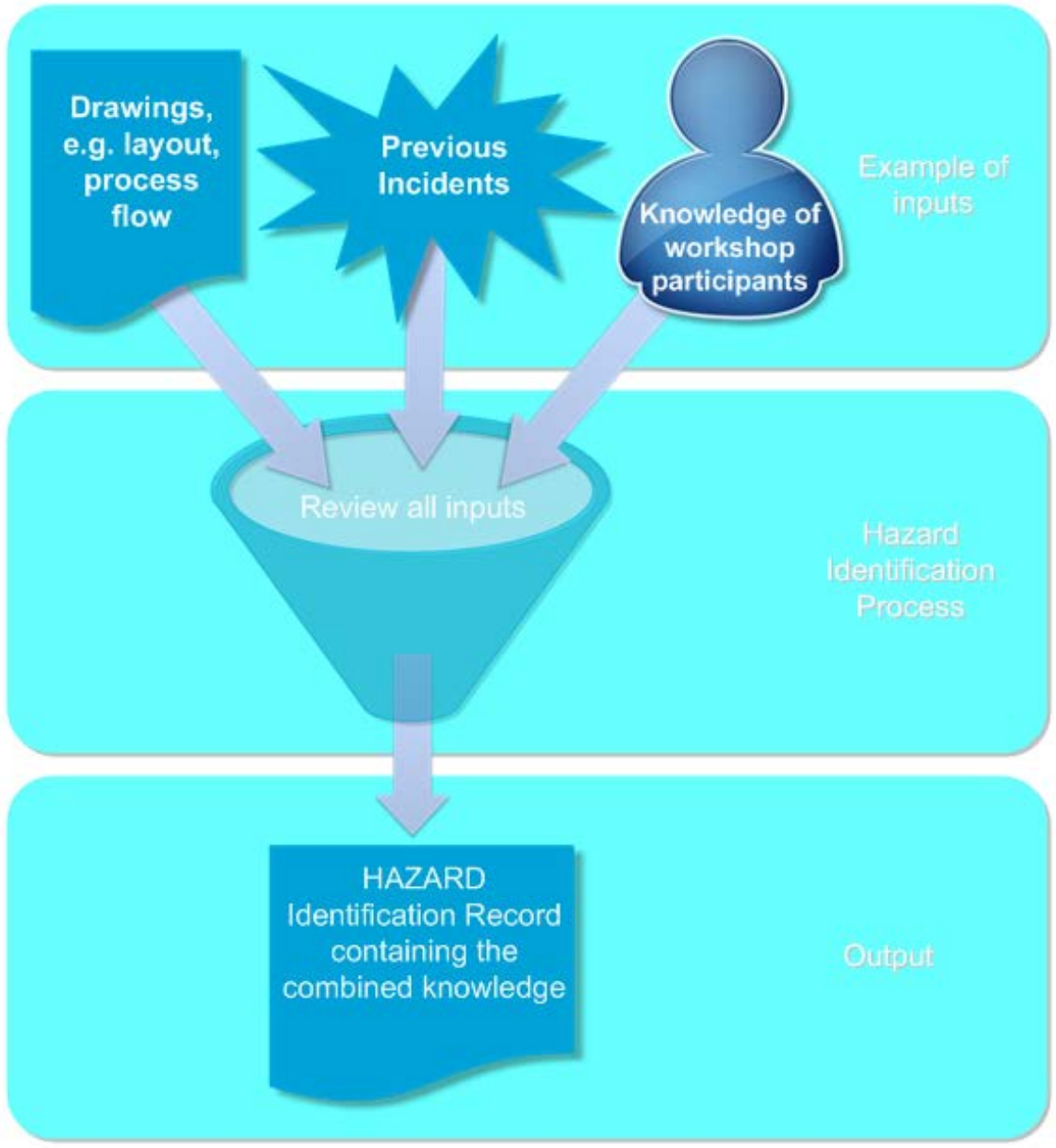

Figure 5 – Sources of Hazard Identification Input and Knowledge Flow

4.2. Providing an adequate depth of analysis

The hazard identification process should provide sufficient detail for an operator to fully understand the nature of each hazard and to identify the controls necessary for the management of each hazard.

As with incident investigation, where it is important to get to the root cause of the incident, it is very important to get to the most basic/root causes (or hazards) leading to an undesirable event or major accident event. The hazard identification should also detail when, where and why the hazard is present, where this aids the understanding of the hazard. If adequate detail is provided during hazard identification, it helps in the assessment of the relevant control measures as part of the remainder of the Formal Safety Assessment process.

4.3. General considerations of Hazard Identification

Ensuring hazard identification is comprehensive, accurate and complete is extremely important for the later steps of safety case development. As depicted in Figure 4 above, it may assist to divide the facility into manageable sections for the hazard identification process. For each section the operator should ask themselves a range of questions, including:

- Can the process or activity deviate from the design intent or 'safe operating envelope'?
- What activities are conducted and how could they go wrong?
- What hazards are present continuously or only occasionally?
- What abnormal or infrequent activities can be conducted, and how could they go wrong?
- What equipment within the section could fail or be impacted by internal or external hazardous events?
- What are the possible events/consequences?
- What could happen in this section to create additional hazards, e.g. SIMOPs, etc.?
- Could this section of the facility interact with other sections (e.g. 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. Examples include:

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

The identification of controls can occur during the hazard identification, separately or during other stages of the formal safety assessment process. If an operator chooses to record control measures during the hazard identification then they should document the hazard identification in such a way that it is clear which control measure(s) control a specific cause or consequence. This is important for two reasons:

- it assists third parties to understand that all identified hazards have controls; and
- when combined with performance indicators and other relevant information, it helps to demonstrate adequacy of hazard and major accident event risk reduction measures.

It is generally helpful to display the linkage between incidents, hazards and controls diagrammatically, e.g. using a bowtie or an event/fault tree diagram.

Operators can also consider upfront if it is possible to group certain types of hazards, especially if they are to occur facility-wide, or on every bowtie diagram (e.g. natural hazards, power loss, etc.). This can reduce the level of effort required as these hazards can 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 (e.g. equipment particularly vulnerable to loss of power).

4.4. Lateral thinking and realism in Hazard Identfication

It is important to employ realism and lateral thinking in hazard identification. The operator must not only identify 'obvious' hazardous events, but also look for potentially complex events, for example, those consisting of a sequence of failures or a set of concurrent problems. Figure 6 shows how a combination of active and latent failures in risk control barriers can allow a hazardous event to progress to an accident.

It is therefore important that the hazard identification team:

- challenge assumptions and existing norms of design and operation to test whether they may contain weaknesses;
- think beyond their immediate experiences;
- explore the effect of failure of management systems, controls and procedures; and
- considers how relatively minor problems may grow into major accident events because of other problems that arise to compound the seriousness.

In relation to the 'Swiss Cheese' model it should be kept in mind that there may be a variety of outcomes with a range of consequences, depending on which barriers function and which ones 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 still may result in toxic effects depending on the nature of the gas release.

It should be noted that both companies and individuals can exhibit 'corporate blindness' when identifying or reporting hazards. For example, it is often assumed that the systems and procedures in place only ever function as intended.

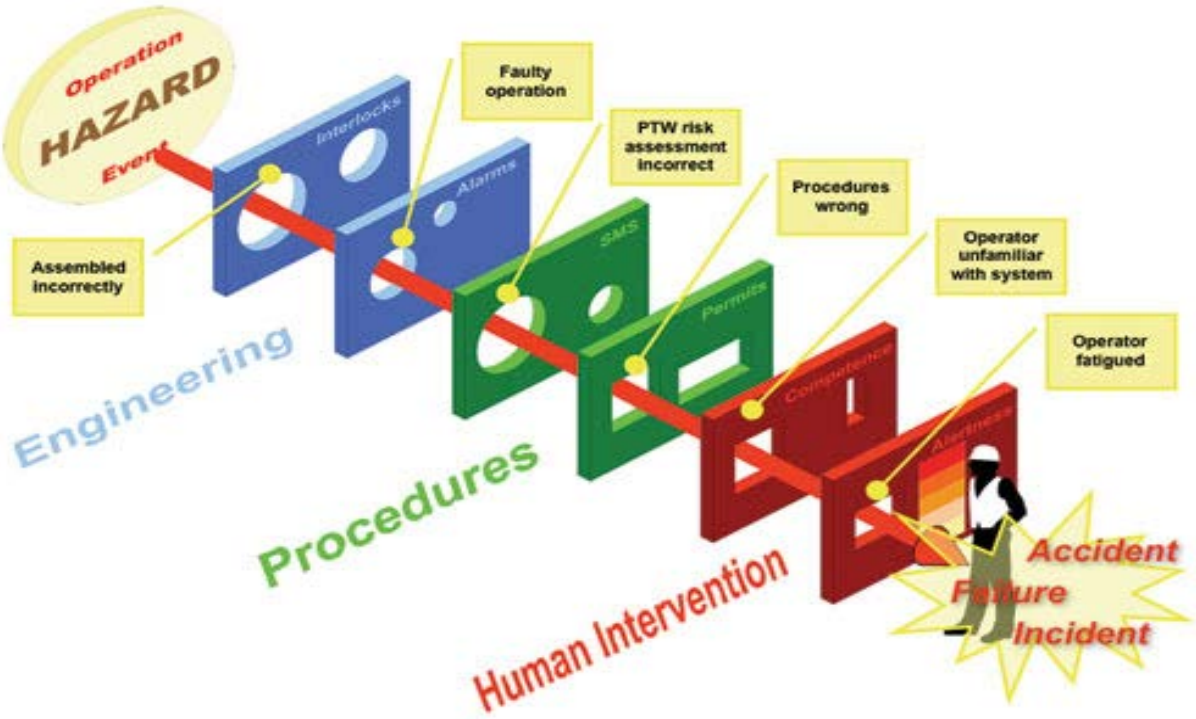

Figure 6 – 'Swiss Cheese' Model

Some other points operators need to consider include:

- worst case events and not only those events used for the design basis of the facility. The worst case will depend on a large number of factors such as extreme process conditions, the potential failure of isolation systems, the proximity and layout of vessels, presence of personnel, etc.;
- how relatively minor problems may grow into major accident events because of other problems that arise to compound the seriousness;
- the full range of factors that can result in a hazard with the potential for a major accident event. This includes the technology used, human error, the systems in place, the type of task, the operating mode and external factors;
- hazards relating to the construction, installation and commissioning phases for new facilities; and
- any changes / modifications intended at the time of submitting the safety case. This includes any changes to current conditions, such as facility modifications, increased or reduced throughput, increased or reduced manning levels, material or equipment changes.

4.5. Rejecting hazards from consideration

Operators should not eliminate hazards from further consideration simply because they have a very low likelihood. For example, when identifying hazards that could lead to the major accident event of an 'engine room fire' (on a vessel), the fact that a range of control measures may be put in place to minimise the risk of an engine room fire does not mean that this is no longer a major accident event (MAE) – it may simply mean that adequate controls have been put in place.

It is unlikely that NOPSEMA will accept a safety case where a MAE has been ignored, especially where related incidents have been experienced elsewhere in industry.

Operators may be tempted to exclude events because they are perceived to be extremely unlikely or of low consequence. The assessment of low likelihood can often result from an assumption that the existing controls are highly effective. This type of exclusion is undesirable for the following reasons:

- the control (that was thought to eliminate the risk) may not be as robust as first thought; for example, controls can deteriorate over time and the effectiveness of 'new' controls is often unproven – the effectiveness of technical controls should be regularly tested, including the final element, where practicable;
- controls may not be adequately managed if their importance is not recognised;
- the initial assessment may not be based on adequate grounds, and further detailed assessment may indicate that the risk is higher due to site-specific considerations; and
- knowledge of all potential events is essential for emergency planning.

5. Identifying Major Accident Events

OPGGS(S) Regulation – Hazard Identification Requirements	
Formal safety assessment	
Reg 2.5(2)(a)	The safety case for the facility must also contain a detailed description of the formal safety assessment for the facility, being an assessment, or series of assessments, conducted by the operator that identifies all hazards having the potential to cause a major accident event

As per the definition given in OPGGS(S) regulation 1.5, a major accident event is an event connected with a facility, including a natural event, having the potential to cause multiple fatalities of persons at or near the facility. Thus MAEs by definition are consequence based. Identifying major accident events is the backbone of the formal safety assessment. Each hazard which may lead to a MAE should be transparently assessed as part of the formal safety assessment process.

Major accident events usually occur as a result of a combination of factors. In some cases the facility operators had never considered these combinations of factors, or had dismissed them as 'non-credible'. Care needs to be taken during the formal safety assessment that combinations of events that could lead to high consequence incidents are not dismissed as 'double contingency' or 'double jeopardy' events.

All identified hazards should be subject to a "screening" process to determine if they can result in a MAE. A preliminary risk assessment may see relatively simple techniques used initially to assess the risk of identified major accident events, e.g. a qualitative or semi-quantitative approach. The results of the preliminary risk assessment should provide guidance towards the types of detailed studies required. Once this has been done, the areas of high risk or uncertainty may be subjected to more detailed and specific assessment to better understand the mechanisms by which a major accident event could occur. In particular, where there is insufficient knowledge of causes, likelihoods, etc. in key areas, consideration should be given to using more detailed studies to reduce this uncertainty. At the hazard identification stage, prior to conducting an in-depth risk analysis, it may not be clear if a hazard can lead to a MAE. Therefore it is prudent to include the hazard in the formal safety assessment process rather than eliminate it at this stage. If a decision is taken to eliminate a hazard from further consideration, operators should document the decision so that the thinking behind the decision is clear to others.

Figure 7 shows a hazard identification process where the hazards are screened and then separated according to whether or not they can lead to events where multiple fatalities could occur. Those hazards which can lead to MAEs must be considered in the formal safety assessment, whereas those hazards that cannot result in a MAE but are a hazard to health and/or safety must be covered by the operator's safety management system. The SMS should address both MAEs and non-MAEs through procedural systems designed to reduce risks to a level that is ALARP.

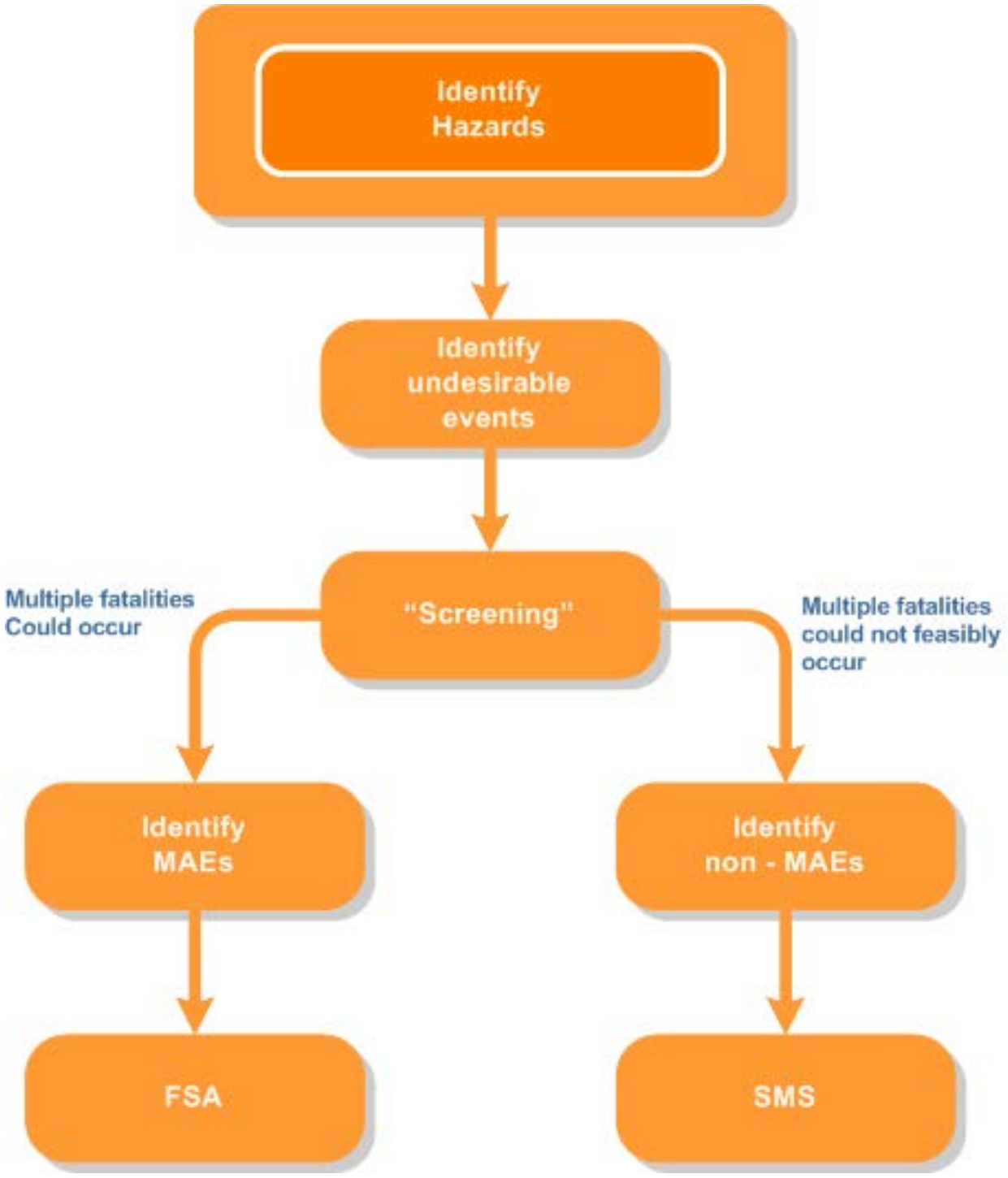

Figure 7 – 'Screening for MAEs

6. Other considerations

6.1. Review and revision of Hazard Identification

It is the operator's ongoing responsibility to identify hazards which may lead to an undesirable event before conditions arise where these hazards may lead to an incident. Therefore hazard identification must be a dynamic process, which stays ahead of any changes in the facility that could erode the safe operating envelope or introduce new hazards. Hazard identification should also be an integral part of the 'Management of Change' process and operations management systems so that the hazard identification process will be implemented before changes are made.

The hazard identification process should be ongoing and dynamic. It should not just be carried out during development of the safety case, but also in a range of defined circumstances, such as when there is a facility modification, after any major accident event or dangerous occurrence, if a control measure deficiency is identified, and at defined intervals.

6.2. Quality Assurance

During, and at the completion of, the hazard identification phase it is important that operators have a quality assurance process in place. Key activities and checks that operators should undertake to ensure quality in the hazard identification process are described below. These checks will also assist to ensure that operators have identified all major accident events and all hazards which could cause major accident events. Quality assurance may be based on inputs and process and/or outputs. It is generally prudent to utilize both. Inputs and process for hazard identification include:

- the qualifications, training, experience and facility knowledge of the team performing the task;
- the involvement of health and safety representatives and members of the workforce, including a reasonable opportunity for other members of the workforce, who are not directly involved, to provide input;
- the methods of hazard identification used and their suitability;
- the project documentation available, its comprehensiveness and accuracy; and
- the time available for the task.

Quality assurance of the hazard identification requires documentation both of the hazard identification system and of the hazard identification activities conducted. It should leave an audit trail which can be followed if necessary.

7. Success factors for Hazard Identification

7.1. Practical factors for success of Hazard Identification

Some of the practical factors for success of hazard identification include:

- Appropriate members of the workforce have been actively involved in the hazard identification process and others have been given the opportunity to provide input.
- The operator has conducted early planning on how to link the various aspects of the safety case to provide information to the FSA process in a timely manner.

- The hazard identification processes chosen are appropriate to the facility and the operator is able to justify why particular hazard identification processes have been chosen.
- Any hazard identification technique selected is systematic and structured, fosters creative thinking about possible hazards that have not previously been experienced, and has included consideration of which approach will extract the maximum quantity of useful information.
- The operator has considered the scope of hazard identification studies in relation to not only MAE related hazards but also general health and safety hazards.
- The operator has based the hazard identification process on a comprehensive and accurate description of the facility, including all necessary drawings, process information, existing conditions, modifications, procedures and work instructions, hazardous materials information, etc.
- The operator has not screened out hazards simply because they have a very low likelihood.
- The hazard identification process has included involvement and/or input from designers, manufacturers, contractors and suppliers, where appropriate.
- Assumptions and uncertainties are explicitly identified and recorded so that these can be verified or analysed later.
- The hazard identification has produced sufficient documented records which list at least all potential major accident events and hazards along with the underlying causes, control measures and any assumptions.
- The hazard identification documentation has recorded properly worded "SMART" actions (specific, measurable, attainable realistic, timely) that can be managed and closed out in an auditable manner.
- The operator can justify why certain control measures have been adopted while others have been rejected.
- Once the hazard identification workshop(s) have been completed, the operator conducts a review on the information gathered.

7.2. Potential pitfalls in Hazard Identification

Potential pitfalls in the hazard identification process that should be avoided include:

- Becoming complacent. It is important that all involved in hazard identification remain ever vigilant and wary about hazards they are exposed to. Just because an incident has not happened in the past does not mean that it can't happen in the future.
- Being too generic in identification of hazards and potential major accident events. For example, to record "corrosion" as a potential cause of loss of containment may not be sufficiently specific; it may be necessary to record where specifically the corrosion can occur, under what circumstances, and at what rate.
- Limiting the hazard identification to the immediate cause of potential major accident events, without determining the fundamental underlying cause. For the above example, the immediate cause may be corrosion, but the underlying cause might be use of incorrect materials of construction, change of operating conditions, or a failure to conduct routine inspections.

- Attempting to conduct the risk assessment and assessment of control measures during the hazard identification. Except for very simple facilities, it is almost certainly better to separate hazard identification from the subsequent stages; this helps ensure a systematic hazard identification process.
- Carrying out the hazard identification with incomplete or inaccurate facility description information.
- Proceeding with the study without first having developed, agreed and planned the approach, and the method of recording. In cases where it is not clear what method may be successful, a "pilot" study on a selected area of the facility may be beneficial.
- Being comprehensive and systematic with respect to plant areas and equipment, which are easily identified, without being comprehensive and systematic with respect to the activities, operations and possible different states of each part of the facility.
- Failing to record important information discussed during the hazard identification, e.g. assumptions, uncertainties or debated issues, gaps in knowledge, details of hazards, incidents or control measures, etc.
- Allowing the hazard identification workshops to be dominated by individual persons, or groups within the organisation, excluding input from others.
- Where hazard identification activities are conducted across several sessions, failing to:
    - review or close gaps from previous session findings;
    - remind participants of the scope and objectives; or
    - introduce new participants to the process, ground rules, etc.

8. References, acknowledgements and notes

Offshore Petroleum and Greenhouse Gas Storage Act 2006

Offshore Petroleum and Greenhouse Gas Storage (Safety) Regulations 2009

AS/NZS (2009) Australian/New Zealand Standard "Risk Management" (AS/NZS ISO 31000:2009)

International Standard ISO 17776 "Petroleum and natural gas industries – Offshore production installations – Guidelines on tools and techniques for hazard identification and risk assessment."

Lees (2005) Loss Prevention in the Process Industries, *Hazard Identification Assessment and Control*, 3rd Edition.

HSE (2001) Marine Risk Assessment, Offshore Technology Report 2001/03.

HSE (2000) Review of Hazard Identification Techniques

NOPSEMA would like to acknowledge Worksafe Victoria for their assistance in the preparation of this guidance documentation. For more information regarding this guidance note, contact the National Offshore Petroleum Safety and Environmental Management Authority (NOPSEMA):

Telephone: +61 (0)8 6188-8700, or

E-mail: safetycaseguidance@nopsema.gov.au

Appendix A: Benefits and disadvantages of Hazard Identification (HAZID) techniques

Technique	Summary
HAZOP	A Hazard and Operability (HAZOP) Study is a highly structured technique that delivers a detailed understanding of the possible 'deviations from design intent' to identify hazards and operability concerns. The primary focus of this technique for the offshore petroleum industry is on hydrocarbon process and associated systems. HAZOP is less suitable for identification of hazardous scenarios associated with mechanical integrity failures and external events such as vessel collisions or dropped objects. HAZOP seeks to identify causes and consequences from a deviation whereas the FSA is seeking the causes for major accident events. The information is present but may require manipulation to create a useable input to the FSA. Also, since HAZOP analysis uses a 'section by section' approach, it may not identify hazards associated with the interactions between different nodes.
Checklists	These can be an effective way of capturing and passing on the experience of others, and therefore are a valuable hazard identification tool. However, checklists should only be used as a final check that nothing has been neglected or missed by other studies. They should not be used as the sole tool in a hazard identification process, since they may not cover all types of hazard, particularly facility-specific hazards, and they do not encourage lateral thinking. These can be used effectively to demonstrate compliance with an engineering standard.
Historical records of incidents	Actual accidents and dangerous occurrences that have occurred provide valuable information to consider as part of hazard identification as they can provide insight on root causes and contributing factors. Operators should consider their own facility(s) and industry history. There are a number of publicly accessible databases that contain summaries of accidents and near misses that have occurred in hazardous processes around the world. However, major accident events are rare and the range of incidents that has actually occurred may not address the entire range of possible incidents.
What-if	This is a technique using a set of pre-prepared and customised 'What-if' questions on potential deviations and upsets at the facility. For example: • What if a shut-down valve fails to close? • What if the 'high high' level alarm fails to automatically trigger a stop in process flow? The questions are often based on the experience of others and hence this technique has some of the same limitations as a checklist approach. The rigour of this approach can be improved by increasing the structure of the 'What-if' analysis. An advantage of this approach over HAZOP is that hazards associated with interactions between sections of the process plant may be more readily identified. However, in general this tool delivers results that are less detailed than HAZOP.

Task Analysis	This technique was developed specifically to identify hazards associated with human factors, procedural errors and the 'man-machine interface'. The technique can be applied to working environments such as control rooms, or to specific jobs such as start-up of shutdown processes. Types of hazard identified may include procedure failures, human resources issues, hazardous human errors and incorrect responses to alarms. The assessment can be time consuming and therefore is generally only used when areas of a facility have a low 'fault-tolerance', or where human error could easily take a process, activity or facility out of its safe operating envelope.
FMECA and FMEA	Failure Modes, Effects and Criticality Analysis (FMECA) and Failure Modes and Effects Analysis (FMEA) are highly structured techniques. They are most often applied to a complex item of mechanical or electrical equipment, which contains a number of sub-systems and components. The overall system is broken down into a set of related sub-systems, and each of these as a set of smaller sub-systems, and so on down to component level. Failures of individual systems, sub-systems and components are then systematically analysed to identify potential causes (which stem from failures at the next lower-level system), and to determine their possible effects (which are potential causes of failure in the next higher-level system). The technique is most often used to analyse the level of safety achievable by safety critical mechanical or electrical plant items such as firewater pumps, gas detection devices or trip systems.
Brainstorming	Typically a relatively unstructured group process, brainstorming can be effective at identifying obscure hazards of a type that may be overlooked by the more systematic methods. It can be used to complement other techniques, but should not be used as a replacement as hazards are likely to be missed.
Guide word based techniques	This is basically a structured brainstorming technique. The hazard identification is split into sections which may be areas, processes or activities and then guidewords are raised to prompt creative thinking. This technique is different from a checklist approach. Rather than focus on a specific list of desired design or operating features, guidewords are more general and focus on hazard categories. For example: overpressure, corrosion, leak etc.; or more general categories such as fire, explosion, gas release, external events, etc. Guidewords are intended to prompt creative thought about the underlying causes for each hazard category. Thus guidewords provide focus while not limiting the options in the same way as a checklist. The technique is good at identifying major accident event hazards but is not as detailed as techniques such as a HAZOP. Other techniques may need to be applied at the detailed design phase of a project. This technique provides the greatest advantage where similar hazards exist across a facility and the guidewords are based at a level that provides specific focus (i.e. overpressure).

Fault Tree and Event Tree Analysis	Fault Trees describe an incident (e.g. loss of containment) in terms of the combinations of underlying failures that can cause them (such as a control system upset combined with failure of alarm, shutdown and relief systems). Event trees describe the possible outcomes of a hazardous event, in terms of the failure or success of reduction and mitigation measures such as isolation and fire-fighting systems. Fault-tree and event-tree analysis is time-consuming, and it may not be practicable to use these methods for more than a small number of incidents. Structuring a large complex facility around a fault tree approach is not considered practicable. The technique can also suffer from the disadvantage that incidents are the starting point, and thus need to be identified first, before working backwards to hazards. For complex facilities, if this were the only technique used for hazard identification, some incidents or scenarios could be inadvertently screened out of consideration before the studies begin. Nevertheless, the technique is useful for detailed identification of hazards related to highly critical or high consequence incidents. The methods also have the advantage that they include control measures in a transparent way, can be reformatted into the "bowtie" concept and are amenable to quantification as part of a risk assessment e.g. QRA.