INDUSTRY SCIENCE RESOURCES

Guidelines for the Preparation and Submission of Facility Safety Cases

2nd Edition

Department of industry, Science and Resources
Petroleum and Electricity Division

Canberra

2000

ISBN 0 642 72091 6
ISR 1999/113

Cover photo courtesy of Mobil Exploration and Producing Pty Ltd.

Disclaimer

Those using the guidelines should be aware that any representation, statement, opinion or advice expressed or implied in these documents are made in good faith, but on the basis that the Commonwealth Government, the State and Northern Territory Governments, and their employees are not liable (whether by reason of negligence , lack of care or otherwise) to any person for any damage or loss whatsoever which has occurred or may occur in relation to that person taking or not taking (as the case may be) action in respect of any representation, statement, opinion or advice referred to in these documents.

Inquires to:

National Oil and Gas Safety Advisory Committee
C/- Department of Industry, Science and Resources
Petroleum and Electricity Division
GPO Box 9839
Canberra ACT 2601

(Draft) Forward

(Letter to be inserted)

Facility Safety Case Guidelines Introduction

Introduction

Aim

To describe the

- ***legislative framework for establishing the Australian offshore petroleum safety case regime***
- ***safety case concept and its application to facilities under the* Petroleum (Submerged Lands) Act 1967 *and associated legislation.***
- ***structure and purpose of the* Guidelines for the Preparation and Submission of Facility Safety Cases (the Guidelines).**

Scope

The non-mandatory provisions in these guidelines underpin the objective-based Petroleum (Submerged Lands) (Management of Safety on Offshore Facilities) Regulations 1996 by proposing a model to assist operators to prepare and submit facility safety cases.

The second edition of the Guidelines have been developed specifically for facilities (including Floating Production Storage and Offloading Vessels). Separate guidelines have been developed for mobile offshore drilling units (MODUs) and are available from the Department of Industry, Science and Resources.

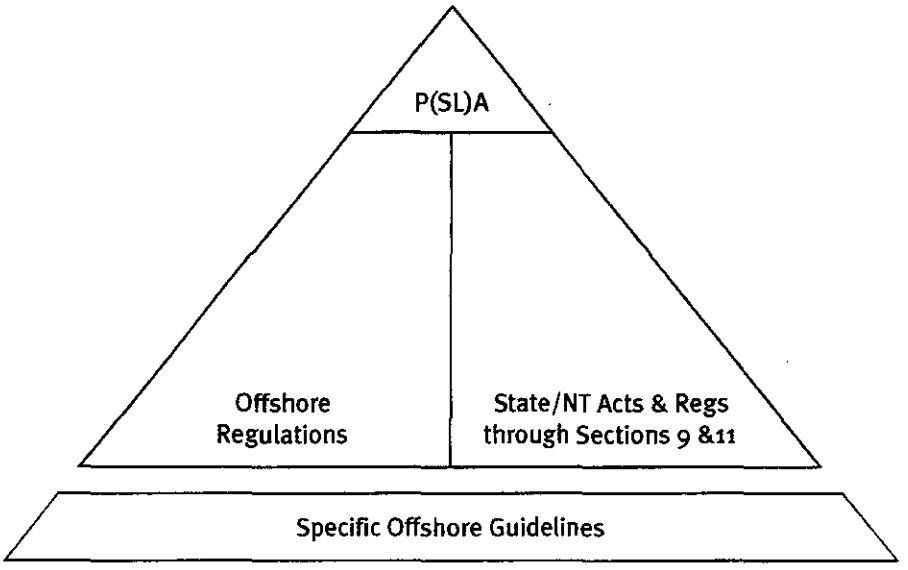
The Regulatory Framework

Since 1967, Australia's offshore petroleum industry has been regulated by broadly consistent Commonwealth, State and Territory legislation. The States/Northern Territory have jurisdiction over onshore petroleum operations including petroleum within coastal waters.

Petroleum operations in Australia, beyond 3 nautical miles from the territorial sea baseline, are subject to the Commonwealth *Petroleum (Submerged Lands) Act 1967* (PSLA)

- the key subordinate and related legislation which impacts on offshore health and safety is the Petroleum (Submerged Lands) (Management of Safety on Offshore Facilities) Regulations 1996 and the State and Northern Territory occupational health and safety Acts and Regulations which are applied through Section 9 of the PSLA
- other State and Territory laws are applied to the offshore areas via Section 11 of the PSLA.

Figure 1: *Legislative framework Commonwealth waters*



The PSLA established two administrative decision-making bodies for the offshore petroleum industry – a Joint Authority and a Designated Authority in respect of each adjacent area (defined areas adjacent to each State and the Northern Territory). For the Territory of Ashmore and Cartier islands there is no Joint Authority and the Commonwealth performs the equivalent functions of Joint and Designated Authorities.

Joint Authorities comprising the Commonwealth Minister responsible for resources and the equivalent State / Northern Territory Minister were established as the principal decision making bodies to administer the Commonwealth offshore petroleum legislation of each State and the Northern Territory (for example: the Commonwealth Minister for Industry Science and Resources and the Western Australian Minister for Mines constitutes the Joint Authority for the Western Australian adjacent areas).

- the Joint Authorities grant titles to explorers and developers, and determine the conditions that apply to these titles, thus providing a legitimate basis for companies' offshore petroleum activities. These titles are:
  - exploration permits
  - retention leases
  - production licences, and
  - pipeline licences.
- a Designated Authority (DA) (relevant State/NT ministers and their departments), handles the day-to-day administrative matters relating to petroleum activities in the area adjacent to each State/Northern Territory. These responsibilities include offshore safety.

- title holders under the PSLA are responsible for all petroleum related activities (including safety) in the permit/licence area
- the designated representative of the title holder is the operator.

Australian Offshore Petroleum Safety Case Regime

Petroleum (Submerged Lands) (Management of Safety on Offshore Facilities) Regulations 1996, require operators to submit safety cases for all facilities operating or proposed to be operating in Commonwealth waters.

What is a Safety Case?

A safety case is a detailed document, that outlines the types of safety studies undertaken and the results obtained together with management arrangements in place, to ensure the continued safety of the facility and personnel on it. The preparation and submission of a safety case constitutes a key strategy in the drive for improved safety in the offshore oil and gas industry.

A safety case, prepared in consultation with employees and their representatives, must be a true reflection of the state of safety arrangements for the existing or proposed facility. It must demonstrate to the satisfaction of the DA, by its contents and supporting material, that the operator knows what technical and human activities occur, how they are to be managed and how safety will be managed in the event of an emergency. It must also identify methods to be used for monitoring and reviewing all activities in connection with the facility, with a view to the continual improvement of the safety arrangements of the facility.

Once a safety case has been accepted, the DA continually reviews the safety performance of the operator, through on-site audits, inspections and statistical analysis of incidents, to determine whether the applicable standards and arrangements are being followed.

Objective of a Safety Case

The objective is to demonstrate via a written description that an operator of a facility has a safety management system that is capable of systematically and continually identifying hazards, assessing them and eliminating or minimising, in so far as is reasonably practicable the risks to employees at the facility. The safety management system must be effective over the life of the facility.

Once accepted by the DA, the facility safety case constitutes the basis of a co-regulatory regime and becomes the set of recognised legal requirements with which the operator must comply.

The Facility Safety Case and Secondary Pipelines

Details on secondary lines (for example: gathering lines, gas lift lines or fuel lines) should be included in the facility safety case. Secondary line safety case documentation should be submitted as per the acceptance process required under the *Petroleum (Submerged Lands)(Management of Safety on Offshore Facilities) Regulations 1996* and include, or refer to, documentation equivalent to that which would be required for a Pipeline Management Plan as if the line required approval under the Pipeline Regulations, either as a discrete part, or identifiable in parts, of the Safety Case documentation. However the level of detail required in the documentation, as for licensed pipelines, should reflect the nature of hazards relating to the particular secondary line and should be agreed between the proponent and the Director. Also, the supplied or referenced documentation may be submitted for a number of secondary lines and licensed pipelines. The purpose of this requirement is to ensure all secondary lines and pipelines are managed, and assessed by the regulator, commensurate to the hazards involved, regardless of whether they are secondary lines or licensed pipelines. Also an aim is to avoid unnecessary documentation and regulatory costs and to this end cross-referencing of relevant documents is encouraged

- for further assistance refer to *Attachment 5* of the *Offshore Petroleum Guideline for the Grant of a Pipeline Licence.*

Review Mechanism

The National Oil and Gas Safety Advisory Committee (NOGSAC) was established as a mechanism to ensure continual improvement in the Australian offshore petroleum safety case regime.

NOGSAC comprises representatives from industry, its employees and State / Northern Territory and Commonwealth Governments. Committee members are appointed by the Minister for Industry, Science and Resources and the Committee Chair reports directly to the Minister. The functions of the committee include:

- to inquire into, and to report to the Minister on, matters affecting health and safety in the offshore petroleum industry
- to inquire into, and to report to the Minister on, matters referred to it by the Minister in relation to health and safety in the offshore petroleum industry
- to develop, and to submit to the Minister, recommendations, guidelines and plans for measures consistent with achieving a healthy and safe environment in the offshore petroleum industry
- to consult and co-operate with other persons and organisations in matters affecting health and safety in the offshore petroleum industry; and
- such other functions as are conferred upon the committee by the Minister.

NOGSAC through its Commonwealth secretariat and tripartite working group is responsible for the development of this edition of the *Guidelines for the Preparation and Submission of Facility Safety Cases.*

Structure of Safety Case Guidelines

The Guidelines are structured as a series of prompts under each of the system elements to provide assistance to operators in the preparation and submission of facility safety cases.

Prompts are also provided to check for system linkages - that is, the way the operator ensures that, where changes occur in work systems, other work systems register the change and adjust accordingly.

Guidance notes have been provided which further elaborate on prompts and are marked in superscript example[xx]. These notes are not meant to be interpreted as requirements but should be consulted for clarification.

Submission Requirements – Safety Case

The operator is not required to give information to the DA (as part of the safety case submission process) if, at any relevant time, the information has been given in compliance with any other provision of the PSLA or the regulations (for example: Petroleum (Submerged Lands) (Management of Environment) Regulations 1999.

Technical Guidelines

To further reinforce petroleum safety, the peak upstream industry body, the Australian Petroleum Production and Exploration Association (APPEA) has taken the lead in the development of a suite of technical industry guidelines for the Australian petroleum industry. These non-mandatory guidelines are designed as examples of good industry practice and cover such specialised areas as Fire and Explosion Management, Lifting Equipment, Permit to Work, Well Abandonment, Helicopter Operations and Incident Data Base Guidelines etc.

The APPEA Incident Database Guidelines provide a minimal standard for incident reporting under the PSLA. In addition, operators should consult with their relevant DA to ensure that there are no additional reporting requirements in that jurisdiction.

These guidelines are available directly from APPEA.

NOTE:

The Guidelines for the Preparation and Submission of Facility Safety Cases detail a model for structuring a safety case- this is a suggested model only. The key issue in the operator's development of a safety case is that all the elements identified in this document are adequately addressed

- operators should (where appropriate) cross reference the submitted safety case to these guidelines.

Contents

Preparation and Submission of Facility Safety Case Guidelines

Chapter 1

Contents

Introduction

Aim

***To provide assistance to operators, employees and their representatives in the preparation and submission of a facility safety case in accordance with the requirements of the Commonwealth* Petroleum (Submerged Lands) (Management of Safety on Offshore Facilities) Regulations 1996.**

Scope

To provide the basic information required to prepare facility safety case submissions as they apply to design, construction, installation, drilling, operation, modification, decommissioning, abandonment and associated activities covered by exploration permits, retention leases or production licences of offshore petroleum facilities.

1.1 Preparation of a Facility Safety Case

The facility safety case should contain information about the facility, set out in three sections:

- Facilities Description (FD)
- Safety Management System (SMS); and
- Formal Safety Assessment (FSA).

Facility Description

The facility description should contain sufficient information to verify that the design and operating philosophy is consistent with the safety management system and the assumptions and outputs of the formal safety assessment.

The facility description section should contain, as a minimum, a description of the:

- facility, its purpose and its operation;
- interaction between the facility and its surroundings; and
- interrelationship between the facility and other facilities and industries.

The facility description should reflect the outputs of the formal safety assessment and the safety management system.

Safety Management System

The safety management system should detail how hazards are identified and how risk is continually and systematically assessed and either eliminated or controlled. The safety management system should demonstrate that:

- risk management objectives and action plans are in place, and are systematically pursued;
- accountabilities and responsibilities are clearly defined and appropriate levels of supervision exist;
- management, employees and contractors understand the hazards at a particular facility and their role in identifying and controlling them;
- work processes and facilities have been designed to reduce risks to as low as reasonably practicable;
- effective communication processes exist;
- safety critical activities are identified and managed appropriately;

- provides assurance that risks are managed when change occurs in facilities, personnel, information, or work methods;
- suitable arrangements exist for responding to any emergency situation;
- people are competent and actively involved in safety management;
- validation and measurement processes exist to confirm that objectives and performance standards are met; and
- system effectiveness needs are periodically assessed to ensure continuing improvement occurs
- effective incident and near miss investigation and reporting systems exist

Where appropriate, the Safety Management System should:

- comply with the requirements of the International Safety Management Code (ISM) as required by the Commonwealth Navigation Act
- reflect the principles of ISO 14000 series and Australian Standard 4804; and
- demonstrate that all necessary linkages between system elements (for example: change management and risk assessment) are identified.

Formal Safety Assessment

The Formal Safety Assessment should:

- detail the risk acceptance criteria and performance standards;
- describe the nature, likelihood, consequence and escalation potential of major accident events that may occur at the facility; and
- detail the means to prevent occurrence of these events, or to minimise their consequences should they occur.

Discussion of the operator's risk acceptance criteria should include the rationale for the selection and references used.

Details of the risk assessment studies conducted into potential major accident events should cover the identification, assessment, and control measures implemented during each phase of the facility's life. Facility formal safety assessment studies should include but not be limited to:

- drilling
- design
- construction within the production licence area;

- installation;
- commissioning;
- operation;
- major change;
- decommissioning
- abandonment

Formal Safety Assessment studies should include but not be limited to:

- hydrocarbon releases
- fire and explosion
- toxic release
- dropped objects
- extreme environmental conditions
- well control
- aviation incidents;
- marine incidents; and
- loss of structural integrity

Fomal Safety Assessment studies should jointly demonstrate that the physical integrity of:

- the temporary refuge
- escape, evacuation, and rescue
- emergency control systems

are maintained in so far as is reasonably practicable in the case of a major accident event and all necessary steps have been taken to ensure the safety of employees in the event of an emergency and during transit to a place of safety.

Both qualitative and quantitative methods of analysis can be applied to the assessment of risk. *It is recommended that early consultation with the DA should occur before selecting the appropriate method of analysis.*

Where appropriate, the results of the formal safety assessment studies should be translated into risk reduction plans. Risk reduction plans should follow the ALARP principle.

Linkages between elements of the Safety Case

The operator should demonstrate the linkages that exist between the three sections of the safety case ie. facility description, safety management system and the formal safety assessment.

Use of external parties in the preparation of safety cases

While the operator may use external resources to assist in the preparation of the safety case, it should work closely with the external party in all facets of its preparation. It should be noted that under the Commonwealth *Petroleum (Submerged Lands) Act 1967* legal responsibility for the content and execution of the facility safety case resides with the title holder (represented by the operator) and this responsibility cannot be abrogated or devolved.

To demonstrate management's ownership, responsibility for, and commitment to, the principles of the facility safety case, the document should be approved and signed by appropriate senior management prior to submission to the DA.

Employee participation and involvement

Employee representatives from the field-based workforce, or in the absence of such a workforce, a relevant organisation whose members might make up that workforce, should be involved in the preparation of the facility safety case.

This involvement comprises two key elements

- consultation
- participation.

Consultation

Effective consultation between employees and employers should be achieved through adhering to the consultative mechanisms established under existing State / Territory and Commonwealth Occupational Health and Safety (OH&S) legislation as it applies at the facility.

For example, consultation should occur on:

- any changes to the facility and its operations which may impact on the health and safety of employees
- preparation of, and/or major modification to, the safety case, including hazard identification, risk assessment, risk control; and
- the investigation of incidents, the findings of incident investigation, and any resulting modifications which may affect the integrity of the facility.

In the absence of a workforce, consultation should occur between the operator and the relevant employee organisation (where practical and appropriate) whose members might make up such a workforce and the DA.

Participation

The participation of employees and their representatives should be consistent with their knowledge and skills. Employee participation should lead to a common understanding of the facility hazards and a common commitment to their control. For example, hazard identification sessions and ALARP workshops should have representation from field based personnel.

Both consultation and participation should provide for involvement of employee representatives in the decision-making process related to safety of the facility.

1.2 Submission of a Safety Case

Companies intending to operate a facility, or utilise the services of a contractor to perform activities associated with a facility are required to submit, and have a safety case (or parts of a case) accepted by the DA before they are granted legal Consents or Licences to:

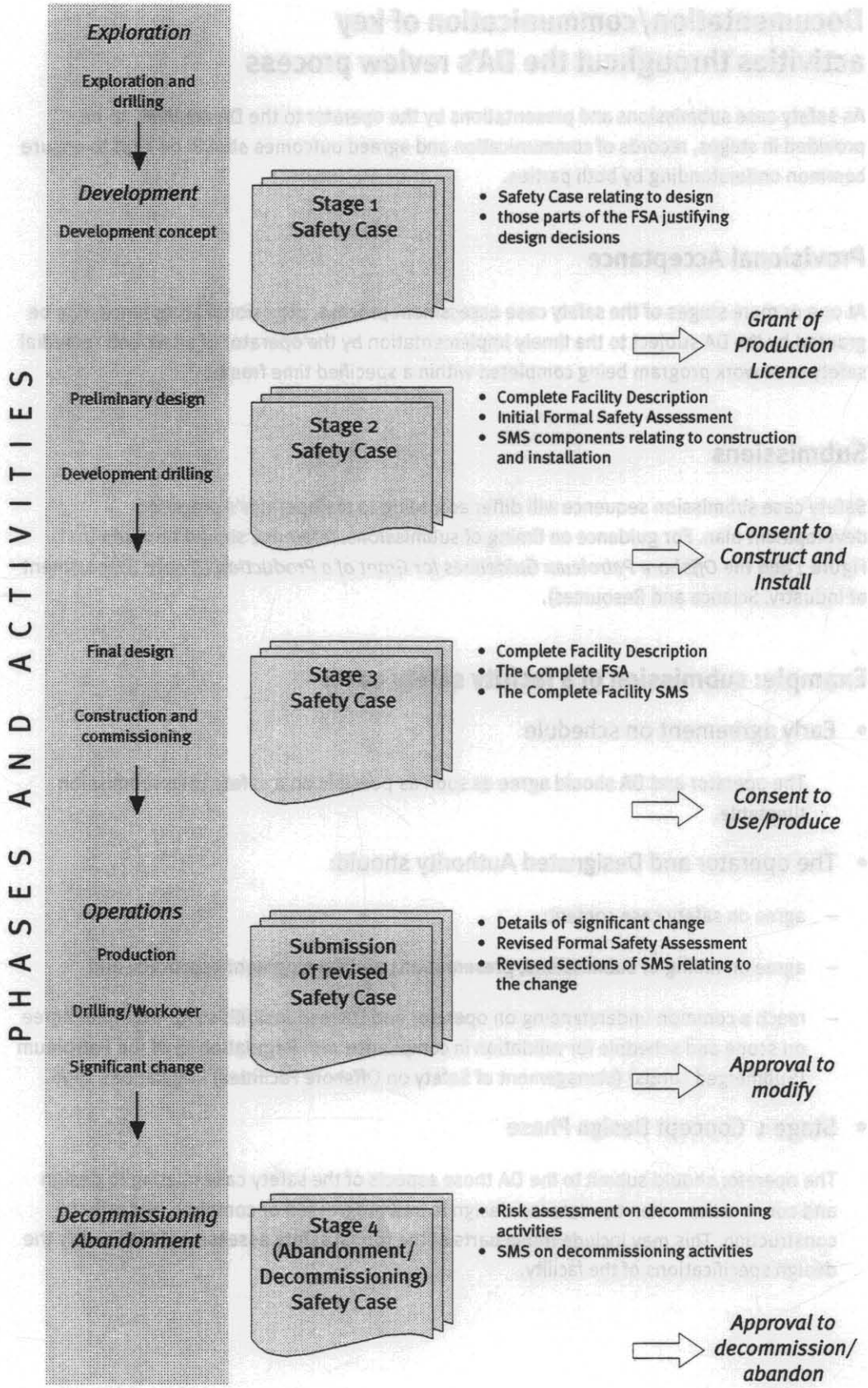
- construct and install
- use
- drill
- abandon / removal

Submission of the facility safety cases should be in accordance with the requirements of the *Petroleum (Submerged Lands) Act 1967* and the Petroleum (Submerged Lands) (Management of Safety on Offshore Facilities) Regulations 1996.

As the safety of personnel on a facility is determined from the earliest stages of design, the Petroleum (Submerged Lands) (Management of Safety on Offshore Facilities) Regulations 1996 require operators to submit to the DA documented safety case components which demonstrate that the selection of the development concept has taken into account safety considerations.

Consequently safety case submission may occur over time with different sections being submitted progressively, corresponding to the facility's stage of development. Therefore, the submission process should be flexible with the operator in conjunction with the DA establishing a submission timetable at the earliest opportunity. Figure 1 graphically illustrates the submission process, detailing key:

- phases of the facility safety case life cycle
- approvals under the *Petroleum(Submerged Lands) Act 1967*; and
- safety case submission requirements.


PHASES AND ACTIVITIES
Exploration
Exploration and drilling
Development
Development concept
Preliminary design
Development drilling
Final design
Construction and commissioning
Operations
Production
Drilling/Workover
Significant change
Decommissioning
Abandonment
Stage 1 Safety Case
• Safety Case relating to design
• those parts of the FSA justifying design decisions
Grant of Production Licence
Stage 2 Safety Case
• Complete Facility Description
• Initial Formal Safety Assessment
• SMS components relating to construction and installation
Consent to Construct and Install
Stage 3 Safety Case
• Complete Facility Description
• The Complete FSA
• The Complete Facility SMS
Consent to Use/Produce
Submission of revised Safety Case
• Details of significant change
• Revised Formal Safety Assessment
• Revised sections of SMS relating to the change
Approval to modify
Stage 4 (Abandonment/ Decommissioning) Safety Case
• Risk assessment on decommissioning activities
• SMS on decommissioning activities
Approval to decommission/ abandon

Documentation/communication of key activities throughout the DA's review process

As safety case submissions and presentations by the operator to the DA are likely to be provided in stages, records of communication and agreed outcomes should be kept to ensure common understanding by both parties.

Provisional Acceptance

At one or more stages of the safety case assessment process, provisional acceptance may be granted by the DA subject to the timely implementation by the operator of an agreed remedial safety case work program being completed within a specified time frame.

Submissions

Safety case submission sequence will differ according to the operator's proposed development plan. For guidance on timing of submissions, reference should be made to Figure 1 and the *Offshore Petroleum Guidelines for Grant of a Production Licence* (Department of Industry, Science and Resources).

Example: submission of a facility safety case:

- **Early agreement on schedule**

  The operator and DA should agree as soon as possible on a safety case submission timetable.

- **The operator and Designated Authority should:**

  - agree on safety case content;
  - agree on timing of submissions, presentations and development approvals; and
  - reach a common understanding on operator and DA responsibilities for example: agree on scope and schedule for validation in compliance with Regulation 13 of the Petroleum (Submerged Lands) (Management of Safety on Offshore Facilities) Regulations 1996.

- **Stage 1 Concept Design Phase**

  The operator should submit to the DA those aspects of the safety case relating to design and construction when the detailed design is well progressed or complete, but prior to construction. This may include those parts of the formal safety assessment that justify the design specifications of the facility.

The objectives of Stage 1 are to:

- confirm that there are no major design deficiencies which would in due course prevent the DA from approving the commencement of production;
- confirm that there are no major deficiencies in the project execution plan; and
- demonstrate that the process followed to determine the selected design is consistent with the ALARP principle.

• Stage 2 Construction, Installation and Commissioning

The operator should submit:

- a complete facility description and provide any certificates of independent validation as agreed with the designated authority;
- initial formal safety assessment;
- relevant elements of the corporate safety management system (where distinctly separate from the facility safety management system and including those systems that control construction) to demonstrate that the operator maintains control during the design and construction phases; and
- other elements that have a bearing on activities being undertaken during the next phase of the design.

A description of the company's safety management system at **Stage 2** may include the arrangements in place for:

- establishing, reviewing and monitoring safety policies and objectives
- ensuring responsibilities for safety assurance during the design, procurement, construction and commissioning phases
- ensuring hazard and risks are identified and managed during the design, construction and commissioning phases
- ensuring competency of employees and third parties involved in design, procurement, construction and commissioning
- ensuring adequate management of change during the design, construction and installation process
- controlling the procurement process to assure the integrity of the final facility and its operations
- controlling the activities of contractors and third parties involved with the design, construction and commissioning process;
- ensuring non conformances and incidents are investigated and corrective actions are applied; and
- audit, review and continually improvement arrangements.

Other submitted documents could include:

- design specification;
- construction specification; and
- application for Consent to Construct and Install.

- **Stage 3 - Operations**

The objective of the stage 3 safety case submission is to ensure that there are no major deficiencies that would prevent the DA from in due course accepting the safety case and approving production.

Prior to the commencement of operations the operator should submit

- components of the final facility description relating to
  - final design(as built);
  - safety critical equipment performance standards;
  - certificate of Construction Validation, and other test validations as agreed with the Designated Authority covering operations
- the complete safety management system
- the complete formal safety assessment, including details of any additional risk studies.

NB: The facility safety management system should be complimentary to the corporate safety management system (if one has previously been submitted).-

Other submitted documents may include:

- commissioning specification; and
- application for Consent to Use.

- **Stage 4 – Abandonment**

Prior to abandonment the operator should submit to the DA those aspects of the safety case relating to the abandonment of the facility, including a risk assessment and safety management system on decommissioning activities

Other submitted documents may include:

- Application for Consent to Abandon.

1.3 Revision of an Accepted Safety Case

It is the responsibility of the operator to define and the DA to accept the threshold criteria to resubmit a safety case following the implementation or proposed implementation of a series of minor changes.

The documentation contained in the facility safety case should be kept up to date to reflect major change to the facility as should all supporting documentation. Apart from the obvious operational need for updating, it will be necessary to keep a record of all changes for inspection by the DA safety case auditors.

Where proposed modifications to the installation, its plant or systems have the potential to significantly alter the previously accepted level of risk, the change will be considered major. The operator should than seek DA agreement for the revision of the safety case before implementing changes under the Petroleum (Submerged Lands) (Management of Safety on Offshore Facilities) Regulations 1996.

Examples of major changes that may result in revision of the facility safety case include:

- changes in the ranking of risk contributors
- major modifications to the structure, plant or equipment that have an impact on safety, for example: the addition or removal of modules, major engineering changes, replacement of existing detection or protection systems or upgrading of structural arrangements
- introduction of any new or simultaneous operations, such as drilling, diving or major maintenance activities, which fall outside the accepted safety case
- substantial changes to the operating parameters. These could include debottle-necking projects, start up satellite operations, subsea completions or reservoir changes causing operations to be performed outside the original design parameters
- changes in ownership or operator
- significant changes resulting from a serious incident
- introduction of changes in technology for example: a significant change of materials used to replace an existing system, introduction of new software for control purposes, or the use of automated systems to enhance or replace manual control
- significant changes to the facility's organisational structure that have an impact on the facility safety management system for example: a change from company employees to contractors or vice versa, changes in management's span of control, or the introduction of multi-skill concepts
- significant changes to working or on-shift arrangements on the facility such as duty cycles, shift times, staffing levels and other employee-related changes that may have safety implications at the facility; and

- a regulatory change.

Notwithstanding the above, the operator will be required to submit an updated safety case

- every five years or at other such intervals as specified in the Commonwealth *Petroleum (Submerged Lands) Act 1967; and/or*
- if requested by the Designated Authority.

The operator should also monitor the cumulative impact of minor changes on facility safety. This monitoring may take the form of audits (internal, external or regulator) or may result from periodic reviews of risk as an aspect of the continuous improvement life cycle of the facility safety case.

A safety case must be revised and re-submitted if there is likely to be a significant change in risk levels resulting from a series of minor changes to the facility structure, plant, equipment, operating procedures or other elements of the facility's systems.

1.4 Definitions

Definitions and terms used in this document may vary from those adopted by individual operators or in other standards. When a drilling contractor / operator uses different terms, the operator should clearly define the terms used in the particular safety case.

As Low As Reasonably Practicable (ALARP)	A level of *risk* that is not intolerable, and can not be reduced further without the expenditure of costs that are grossly disproportionate to the benefit gained
Application to construct and install	As defined under the Commonwealth Petroleum (Submerged Lands) (Management of Safety on Offshore Facilities) Regulations 1996.
Assessors	Personnel reviewing and auditing safety cases under the Commonwealth Petroleum *(Submerged Lands) (Management of Safety on Offshore Facilities) Regulations 1996*
Audit	A critical examination of all or part of a total operating system with reference to safety.
Control measures	Actions to eliminate or reduce the chance of an event occurring or to reduce the effect of the hazard event if it does occur.
Contractors	See Employees.
Drilling Contractor	Operator of an Offshore Drilling Unit.
Corporate Safety management System	Those elements of the operator's wider safety management system that control risk but are not necessarily facility-specific. Where there is more than one facility, corporate safety management system elements are common across all facilities.
Dangerous goods	As defined under State/Territory legislation.
Directions	Refers to Directions issued under Section 101 of the Commonwealth *Petroleum (Submerged Lands) Act 1967 and* the Schedule of Specific Requirements as to Offshore Petroleum Exploration and Production in waters under Commonwealth jurisdiction 1997.
Design Validation Philosophy	Arrangements and basis for validating aspects of the facility design.
Employee	In relation to a facility, includes any individual on the facility in the course of his or her duties (for example: an official or officer, or a company director) or in a self-employed capacity (for example: as a contractor). For the purposes of this document the *Petroleum (Submerged Lands) Act 1967* definition of employee has been extended to include:

- visiting personnel, inspectors, various officials and other government personnel.

Employee representative — An employee member of a health and safety committee where established in the workplace, or person elected to represent a group of employees on health and safety matters.

Escape — Movement from the place of work to the temporary refuge

Evacuation — Movement from the temporary refuge off the facility (orderly evacuation). Movement from anywhere off the facility (disorderly evacuation).

Event — Significant change in normal state (whether process or hazard management).

Facility — A 'platform' as defined in the Directions/ Regulations, viz: a construction platform, a fixed platform, a service platform.

For the purposes of these guidelines, a facility also includes all other associated production and ancillary equipment in the relevant area associated with the 'platform'. For example, a subsea completion is considered to be a facility. But does not include a drilling platform.

For convenience, the definitions of the various types of 'platform' included under the legislation are provided below:

'Construction platform' means a ship, barge or other vessel or floating structure from which construction or installation operations for, or in conjunction with, the exploration for or recovery of petroleum are or are to be carried out.

'Fixed platform' means a structure (including a floating structure) that is:

- fixed or connected to the seabed from which operations for the recovery of petroleum are or are to be carried out; or
- fixed or connected to the seabed otherwise than only by a part of the structure lowered to the seabed for the purpose of supporting the structure, from which petroleum exploration operations or operations for the recovery of petroleum are or will be carried out, and that is not or will not to be capable of being readily moved from one position to another as such a structure.

'Service platform' means a ship, barge or other vessel, or floating or fixed structure, that in connection with petroleum exploration operations or operations for the recovery of petroleum, provides a base from or on which services such as diving, firefighting, accommodation, processing or storage are controlled, mounted or performed.

Facility Safety Management System	Those elements of the operator's safety management system that directly contribute to the management of a facility's safety. Facility safety management system elements support, and are an adjunct to, corporate safety management system elements.
Floating, Production, Storage and Off-load facility	see facility
Formal Safety Assessment (FSA)	A formal investigation of the nature, likelihood and impact of potential major accident events and the means to prevent or minimise their occurrence or consequences to as low as is reasonably practicable. Within the context of the safety case the term 'formal safety assessment' may also refer to the reporting of facility-specific studies conducted by the operator that provide reasoned arguments and judgments about the findings of the formal investigation.
Good oilfield practice	As defined in the Commonwealth *Petroleum (Submerged Lands) Act 1967*: All those things that are generally accepted as good and safe in the carrying on of exploration for petroleum, or in operations for the recovery of petroleum, as the case may be.
Hazard	A physical situation which may result in harm, including death or injury to people or damage to property.
Hazardous goods	As defined under State/Territory legislation.
Hazard identification	Identification of the nature of all hazards at the facility.
Hazard register	A document or process detailing hazards associated with all aspects of operating the facility. The hazard register may be ranked according to severity and/or probability and should indicate the control measures in place to manage them.
Hazard/risk control	Risk reduction actions that are undertaken by the operator in response to the need to reduce risk to as low as is reasonably practicable.
Incident (near miss)	Any unplanned event where control is lost and/or there is or could be an impairment to either employees or the facility.
Individual risk	The frequency at which an individual may be expected to sustain a given level of harm from the realisation of specific events (usually per annum - IRPA).
Major accident event (MAE)	Any event connected with work activities that could cause multiple fatalities arising from hydrocarbon releases, or other events whether immediate or delayed.

	Examples of events that may be considered include: • fire or explosion, or release of a hazardous substance; • major damage to the structure of the facility or equipment affixed thereto, or loss in the stability of the structure; • any event which significantly impairs options for escape to the temporary refuge (TR), the integrity of the TR itself, or escape from the TR to a place of safety; • helicopter or vessel collision with installation; and • failure of a life support system for diving operations.
Major emergency	An event with the potential to escalate to become a MAE.
'Mobile Drilling Unit'	A ship, barge or other vessel or floating structure including a structure any part of which may be lowered to the seabed for the purpose of supporting the structure, that carries or includes equipment for drilling, or carrying out other operations on, a well from the vessel or structure.
MODU safety case	The combination of a vessel safety case and bridging document detailing site specific information and linkages between drilling contractor and operator safety management systems. Or a safety case equal in coverage to the vessel safety case and bridging document and developed for a specific campaign.
Monitoring	A line management function of checking for acceptable performance as tasks are completed.
Operator	As defined in the Commonwealth *Petroleum (Submerged Lands) Act 1967*, which states '... the representative of the titleholder responsible for the overall management and control of the operations for the exploration or exploitation of petroleum reserves for which the title is held'.
Performance Standards	Standards established by the operator that indicate who is responsible for carrying out an activity, what has to be done, when an activity has to be performed and what outcomes are to be expected.
Personal risk	See Individual Risk.
Personnel/Persons	See Employee.
Person in charge (PIC)	The person who has responsibility for the safe operation of a facility

Place of safety	A place where an employee's physical and emotional wellbeing can be assured. The location of a place of safety for any individual during an emergency will depend on a number of factors, including: • physical and emotional condition (considering effects of injury and trauma); • location of facilities where the employee's individual needs can be met (for example: another nearby facility which can provide first aid treatment for a mild injury, a hospital for a seriously injured employee). The place of safety will be specified in the emergency response plan (ERP) as part of the safety case. Generally, a lifeboat or an evacuation helicopter would not be considered a place of safety. A supply boat or nearby platform could be considered a place of safety, depending on the physical and emotional condition of the employee.
Potential Loss of Life (PLL)	The estimated number of fatalities per year on a site, evaluated by taking account of the number of persons exposed to the risk and the magnitude of the *Individual Risk*.
Production licence application	As required by the Commonwealth *Petroleum (Submerged Lands) Act 1967*.
Probability	The likelihood of a specific event occurring within a specific time frame.
Proposed development concept	A conceptual description of a development envisaged by the operator. The proposed development concept is the first submission in the process of seeking DA approval of a new development.
Petroleum (Submerged Lands) Act 1967	Refers to the Commonwealth *Petroleum Submerged Lands) Act 1967* and subservient legislation.
Rescue	Retrieval of people from the water or lifecraft/life boats to a place of safety.
Review	Evaluation of how well the operators safety management system achieves its goals specified in the OH & S policies. A review check on issues such as whether audits have demonstrated compliance, whether the system remains appropriate given advances in techniques and technology.

Risk	The likelihood of a specified undesired event occurring within a specific period or in specified circumstances. It may be either a frequency (the number of specified events occurring in unit time) or a probability (the probability of a specified event following a prior event), depending on the circumstances or product of both.
Risk acceptance criteria/ acceptance standards	Qualitative and quantitative criteria/standards selected by the operator / drilling contractor which reflect contemporary societal values, what is reasonably practicable, and good oilfield practice.
Risk management	The ongoing management process of identifying hazards, evaluating the consequences and probabilities of these hazards, and then reducing the risk levels to as low as reasonably practicable.
Risk reduction plan	A plan to implement the risk reduction strategies identified in the formal safety assessment. The time frame to complete and the priorities should be provided.
Safety case	The presentation of a justification for the safety of an installation.
Safe haven	See temporary refuge.
Safety Management System (SMS)	A comprehensive integrated system for managing safety at a facility which sets out: – the safety objectives; – the systems and performance standards by which these are to be achieved; – the performance indicators which are to be met; and – the means by which adherence to these standards are to be maintained, verified and continually improved
Severity	The level of impairment associated with the realisation of a hazard.
Staff	See Employee.
Temporary refuge (TR)	An open and/or closed area on the facility where employees can muster without undue risk or serious harm, and from which, if necessary, safe and full evacuation can be effected. Equipment is provided within the TR for emergency communications, monitoring and control of the emergency as is necessary to ensure the safety of employees.
Validation	Evidence (test reports, certificates, etc) that equipment and/or systems are fit for purpose.

1.5 Abbreviations

ALARP	as low as reasonably practicable
AS	Australian Standards
DA	designated authority
EBD	emergency blow-down
ERP	emergency response plan
ERT	emergency response team
ESD	emergency shut-down
FD	facility description
FMEA	failure mode effects analysis
FPSO	floating production, storage and off-loading facility
FSA	formal safety assessment
FSO	floating storage and off-loading facility
HAZIDS	hazard identification session
HAZOP	hazard and operability study
HS	health system
HUET	helicopter underwater escape training
IRPA	individual risk per annum
IS	information system
ISM	international safety management code
JSA	job safety analysis
MAE	major accident event
MODU	mobile offshore drilling unit
MSDS	material safety data sheet
NORM	naturally occurring radioactive material
OH & S	occupational health and safety
PEP	project execution plan
PIC	person-in-command
PLL	potential loss of life
PPE	personal protective equipment
PSLA	*Petroleum (Submerged Lands) Act 1967*
PSV	pressure safety valve
QRA	quantitative risk assessment
SIMOPS	simultaneous operations
SMS	safety management system
SSIV	sub-sea isolation valve
TEMPSC	totally enclosed motor propelled survival craft
TEMPSEC	temporary security
TR	temporary refuge

1.6 References

Several categories of useful references are provided. It should be noted that reference material is constantly changing, and that the information provided here is not exhaustive and while accurate at the time of publication is subject to change.

The categories are:

- Lead Government Agencies
- Australian Standards and Codes of Practice
- International

Lead Government Agencies (Internet address list)

- Commonwealth Department of Industry Science and Resources - http://www.isr.gov.au
- Northern Territory Department of Mines and Energy - http://www.dme.nt.gov.au
- Western Australian Department of Minerals and Energy - http://www.dme.wa.gov.au
- Victorian Department Natural Resources and Environment - http://www.nre.vic.gov.au
- South Australia Department of Mines – www.mines.sa.gov.au/petrol
- Queensland Department of Mines & Energy – http://www.dme.qld.gov.au
- Australian Maritime Safety Authority - http://www.amsa.gov.au

National Standards and Codes of Practice (Internet address list)

- Standards Australia – http://www.standards.com /
- Australian Institute of Petroleum - http://www.aip.com.au
- Australian Petroleum Production and Exploration Association http://www.appea.com.au

International

- International Maritime Organisation - http://www.imo.org/imo
- Oil industry International Exploration and Production Forum http://www.eandpforum.co.uk
- Health and Safety Executive (United Kingdom) http://www.open.gov.uk/hse/
- United Kingdom Offshore Operators Association (UKOOA) http://www.ukooa.co.uk/
- American Petroleum Institute http://www.api.org

Facility Safety Case Guidelines Facility Description

Chapter 2

Contents

Introduction

Aim

To provide guidance in the preparation of the facility description (FD) component of a safety case.

Scope

This checklist should be used as a guide to preparing the FD of a safety case.

The FD of the safety case should include information under the six detailed headings :

- general description
- structure of facility and layout
- primary functions
- hazardous substances quantities
- safety features and systems
- drawing set

Detailed checklists under these headings provide guidance in the development of the FD.

The FD section should contain sufficient information about the facility to validate that the design and operating philosophy is consistent with the safety management system and the assumptions and outputs of the formal safety assessment.

The FD section should detail all linkages to the safety management System and formal safety assessment sections. For example the FD may contain a description of the escape routes, the design basis of which may have been a direct outcome of the evacuation studies conducted as part of the formal safety assessment.

2.1 General Description of Facility

Aim

To provide an overview of the facility, highlighting key assumptions and operational phases of the development.

Scope

The overview should include the following:

- facility overview
  - operator or permit/licence number
  - structure
  - geographical location
  - water depth
- development bases and phases
- key design performance standards
- design validation philosophy
- metocean conditions (should include the adopted design values)
  - limiting sea state conditions and return periods
  - wind
  - seawater and air temperature
- geotechnical
  - foundation strength
  - geotechnical data
  - anchoring
  - seabed conditions
- structural integrity and corrosion management philosophy
- use of novel technology or materials
- interaction with shipping
- standards and design and construction specifics
- staffing philosophy and arrangements.

Cross-references to data sources, figures etc. should be provided.

2.2 Structure or Vessel Layout

Aim

To describe the structure or vessel, its unique features (if any), equipment layout for all decks, operational parameters and interaction with existing offshore/onshore facilities.

Scope

This section should include a description of at least the following (where applicable):

- Structure Layout:
  - platform orientation
  - elevation/plan views
  - hazardous area classification
  - equipment
  - design codes used for the structure
  - structural details, including modelling of structure and loadings
  - accommodation
  - well bays
  - riser(s)
  - wells and sub-sea system
  - helipad
  - cranes
- Vessel layout (include the following where applicable for Floating Production Storage and Offloading Vessels):
  - mooring release facility
  - riser release facility
  - mooring patterns

The safety-related aspects of the layout and orientation of the facility should be detailed, for example: segregation of process equipment from living quarters, influence of prevailing winds on distribution of heat and smoke throughout the facility, influence of prevailing seas on location of escape craft, location of helideck etc.

- interaction with other facilities:
  - physical connections including product offloading facility and pipelines
  - support from existing facilities (aircraft, supply boats)
  - allowance for impact by vessels
- interaction with expected facilities (where applicable).

2.3 Primary Functions

Aim

To describe the functions and systems of the facility at the various stages of its life, detailing key processes, wellhead, process and utility systems, pipeline systems, drilling, workover and wireline systems, and marine and helicopter operations.

Scope

This section should include a description of the following referencing performance and design standards where applicable.

- process systems:
  - process description (overview)
  - process control features
  - safety control systems for use during emergencies for example: controls at the temporary refuge or emergency assembly area
- pipeline and riser systems:
  - platform and sub-sea installation
  - location, separation, protection
  - riser connect/disconnect system (Floating Processing, Storage and Off-load Facility (FPSO) and Floating Storage, Off-load Facility (FSO)
- wells and sub-sea systems:
  - wellheads and christmas trees
  - sub-sea flowlines, umbilicals and associated equipment
  - shutdown and control system
  - downhole equipment
  - well design and construction
- utility systems:
  - power generation and distribution (including supply and safety critical equipment)
  - standby power systems (including starting systems)
  - emergency lighting
  - communications (voice and data)
  - instrument air system
  - hydraulic control system
  - potable water
  - drains and sumps
  - navigation lighting

  - chemical injection
  - inert gas systems
  - heating, ventilation and airconditioning

- drilling systems:
  - drilling capability and rig features
  - integration with platform systems
  - assumed rig and its load on platform

- workover and wireline systems:
  - extent and type of activity planned
  - integration with platform systems
  - assumed rig and its load on platform

- marine functions/systems:
  - supply/service vessels
  - standby vessels
  - diving operations
  - ballast and stability systems (FPSO/FSO)
  - integrity of off-take tankers
  - mooring systems/ jacking systems
  - station keeping system
  - cargo and offload system

- aircraft operations:
  - onshore base
  - capability of aircraft
  - route taken to/from facility
  - helicopter refuelling
  - helideck

2.4 Hazardous Substances and Inventories

Aim

To summarise all hazardous substances and hydrocarbon inventories stored and/or handled on the facility.

Scope

The hazardous inventories section should cover at least the following (where applicable):

- reservoir fluids
- pipelines fluids
- process fluids
- stored fuels and compressed gases
- product crude oil cargo
- process fluids
- stored liquids and solids
- radioactive materials for example: NORM's
- other substances

The range of sizes of isolated inventories in the event of a platform shutdown shall be given. Material safety data sheets should be referenced in the safety management system section of the safety case.

2.5 Safety Features and Systems

Aim

To describe the facility design safety philosophy, features and systems.

Scope

The description of the safety features and systems should contain the design philosophy which should include:

- when and how safety features and systems are activated in an emergency, and where from – manual, auto-electric, air etc
- their required performance criteria in an emergency
- safety system performance standards.

Note: It is possible that some systems may fail in extreme events, and the formal safety section must show that the probability is acceptable.

The safety features and systems and their performance standards to be described should, as a minimum include:

- detection systems
  - visual monitoring system (if applicable)
  - fire and gas detection/alarm system
  - toxic detection
    - heat detection
    - smoke detection
- drilling
  - blowout detection and prevention systems
  - well control systems
- platform shutdown system(s)[1]:
  - total platform shutdown
  - subsurface shutdown
  - surface shutdown
  - process shutdown system

including shutdown of connected facilities and arrangements for control of emergency shutdown valves (ESD valves) and sub-sea isolation valve (SSIVs) (where applicable).

- fire and blast protection — passive [2]

- fire protection — active [3]
  - fire pumps
  - deluge system
  - sprinkler system
  - hose reels, monitors and extinguishers
  - inert systems
  - other support services
- relief and blowdown[4]
  - instrumentation systems
  - pressure safety valves (PSVs)
  - flare, vents and drains [5]
- heating, ventilating, air conditioning system[6]
- emergency power, communications and lighting
- escape routes and temporary refuge[7]
- evacuation and rescue [8]
  - equipment
  - location
  - types
  - capacities
- Ship movement monitoring.

Guidance Note: 1

Provide the logic of the shutdown, reliability of the signal to the end device such as a switch, valve etc.

Guidance Note: 2

Provide details on the blast rating and heat resistance over time.

Guidance Note: 3

Reference or provide details of the reliability of the pump start, water rates, protection, location of pump enclosure and response times for the active fire protection systems.

Guidance Note: 4

Reference or detail the blowdown system's:

- reliability
- response time
- blowdown duration
- emergency blowdown criteria
- heat flux / radiation levels on the platform during blowdown

Guidance Note: 5

Reference or provide details on the capacity, segregation philosophy and locations of drains and vents to handle emergency flows.

Guidance Note: 6

Detail the system for

- pressurisation in electrical or mechanical enclosed areas
- gas and/or smoke detection in electrical and mechanical enclosed areas protection from smoke and gas ingress

Guidance Note: 7

Reference or provide the performance standards for the temporary refuge and escape and evacuation routes.

Guidance Note: 8

Reference or provide performance standards for the dependability of the evacuation and rescue arrangements for example: availability of helicopters or standby boats.

2. 6 Drawing Set

Aim

To detail key process equipment layout, process flow, safety equipment, escape routes and protective system drawings.

Scope

A typical drawing set could include (where applicable):

- development location map
- deck plot plans
- major equipment/facilities layout (including sub-sea)
- process and instrumentation diagrams
- safety critical electrical, hydraulic and pneumatic systems
- fire and blast protection
- location of emergency shut-down valves
- fire and safety equipment
- escape routes/emergency assembly area/temporary refuge
- fire and gas systems
- flare, vent and drain system
- structural layout (including riser(s) location)
- quarters layout
- mooring layout
- hazardous area classification drawings
- riser and associated pipelines
- seabed plan view showing fixed hazards (if appropriate)
- heating ventilation and air conditioning system (HVAC) (intakes and vents).
- fire and gas cause and effect matrices
- process schematic
- emergency shut-down logic.

Facility Safety Case Guideline Safety Management System

Chapter 3

Contents

Introduction

Aim

To provide guidance in the preparation of the safety management system (SMS) of the facility safety case.

Scope

The description of the SMS should demonstrate that risk associated with the facility is managed for continuous improvement throughout its life cycle. This process is shown in Figure 3.1

Structure of Guidelines

Key elements of the SMS are identified and an aim is specified for each.

Sub-elements are grouped broadly under the key elements.

Evidence of implementation of key elements and sub-elements is demonstrated by responding to prompt questions under the sub-elements.

Several of the sub-elements detail compliance standards which provide a test of implementation.

Additional information is provided in guidance notes referenced in superscript (for example:[1]).

Special Requirements

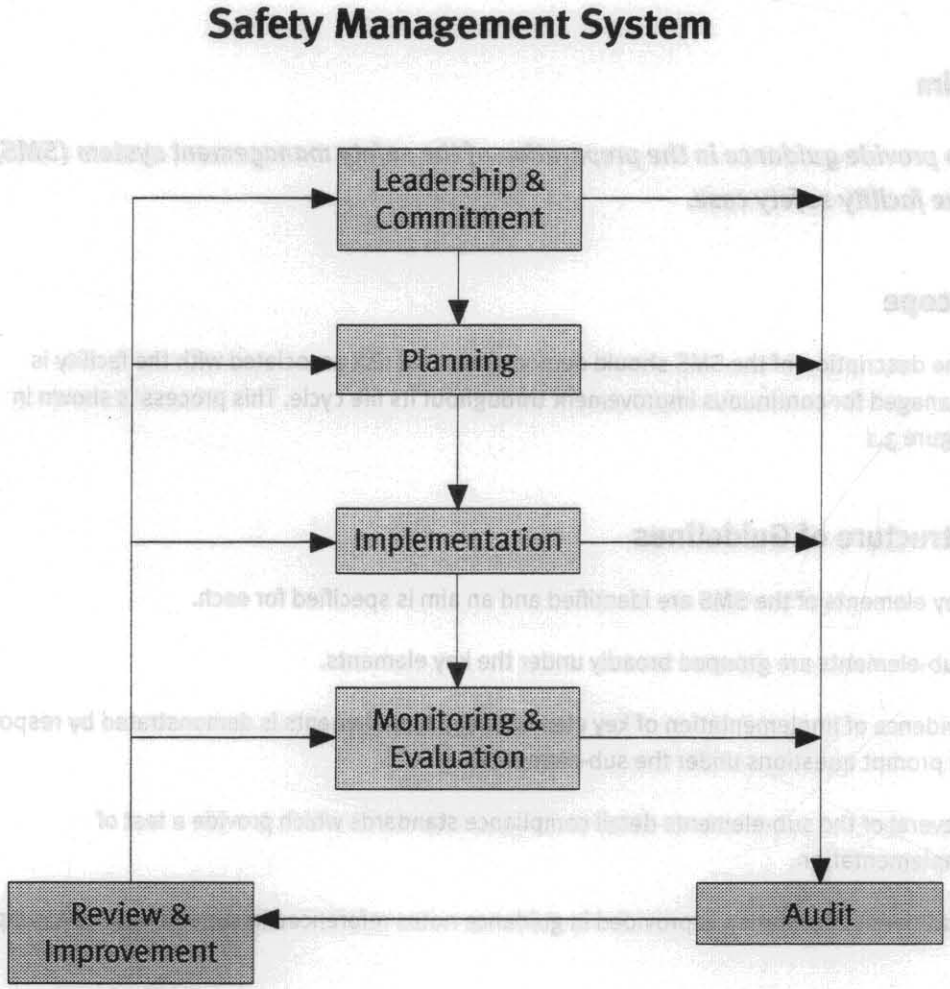
The safety case submission process does not require operators to submit safety management system procedures to the DA. However, it requires that a clear description of the arrangements and reference to site procedures and other supporting evidence be provided.

Not-with-standing the DA may at any time request operators safety management system procedures.

Verification

Details provided in the description of the SMS will be verified by the DA during site verification audits.

Figure 3.1 *SMS Process*



3.1 Key Element

Leadership and Commitment

Aim

The operator should demonstrate commitment to achieving a high standard of health and safety in the organisation through the development of effective health and safety policies supported by appropriate organisational structures, positive behaviour of individual managers and the promotion of a cooperative effort at each level in the organisation.

3.1.1 Policy and Leadership

Standard

The operator's health and safety policy should be supported by a high level commitment to effective risk and safety management consistent with and at least equal to other business aims.

Policy

The operator should demonstrate:

- there is a documented health and safety policy[9] authorised by the accountable chief executive that clearly states strategic health and safety objectives and a commitment to improving health and safety performance. The policy should:
  - reflect a commitment to safety at least equal to other business aims
  - establish a commitment to reduce health and safety risk to as low as is reasonably practicable
  - establish compliance with relevant legislation as a minimum requirement
  - include a commitment to develop and maintain appropriate systems and arrangements for the management of safety
  - include a commitment to continual improvement
- policy intent is communicated to employees and interested parties[10]
- arrangements are in place for the periodic review of the policy to ensure its relevance and appropriateness to the organisation's activities.

Leadership

The operator should demonstrate:

- appropriate senior managers take direct responsibility for coordinating the implementation and maintenance of the health and safety policy
- there are mechanisms by which senior managers are held accountable for achievement of the health and safety outcomes established in the policy
- there are mechanisms that promote the active involvement of all employees in achieving policy objectives

Guidance Note: 9

In addition to a general health and safety policy the operator may have a number of specific policies. For instance:

- Corporate or facility specific policies, employment policies, training policies, health policies, rehabilitation policies, etc.

Guidance Note: 10

Interested parties likely to be associated with the facility include:

- trades-people, caterers
- Support staff
- contractors
- visitors including management and guests.

3.1.2 Organisation and Responsibility

Standard

The operator should develop an effective organisational structure (roles and responsibilities) for implementation and maintenance of the health and safety policy.

Responsibilities

The operator should demonstrate :

- there is an appropriate structure for the management of safety
- broad safety responsibilities consistent with authority levels are defined for each level in the organisation and for specified support personnel [11]
- specific responsibilities are allocated for the management of safety critical activities[12]
- employees are informed of their health and safety related roles, responsibilities, accountabilities and authorities
- employee understanding of, and adherence to, roles, responsibilities, accountabilities and authorities are verified; and
- roles, responsibilities and accountabilities are regularly reviewed and maintained.

Staffing

The operator should demonstrate:

- sufficient personnel with appropriate skills are available to safely operate the facility during normal and emergency situations
- hours of work and shift patterns reflect health and safety considerations.

Supervision

The operator should demonstrate:

- levels of supervision at a facility are commensurate with the level of risk associated with the tasks being performed; and
- personnel and third parties entering and leaving the site are controlled.

Guidance Note: 11

General responsibilities should be consistent with the general duty of care requirements and reflect the intent of the operator's health and safety policy. Responsibilities should also reflect accountabilities of line management in the implementation and maintenance of the management system and the control of hazards and risk.

Typical examples of supporting documentation that may be sited in the Safety Case include:

- company organisation chart showing the reporting relationships between the corporate/company organisation and the facility
- documented roles and responsibilities for each organisational unit / level having safety management or support responsibility
- reporting roles and responsibilities between facility management and contractor organisations
- roles and responsibilities for contractor organisational units
- safety management plans showing roles and responsibilities allocated to specific individuals.

Guidance Note: 12

Specific responsibilities for controlling key safety activities such as maintenance, inspection testing and combined operations, etc should be allocated to key individuals or supervisors.

Specific responsibilities may be recorded in job descriptions, specific contracts, procedural manuals or other documents.

3.1.3 Employee Involvement and Communication

Standard

The operator should develop and maintain effective participation and consultative mechanisms that promote active communication and involvement of all personnel in the management of safety, the control of workplace hazards and risk and the development of the safety case.

Consultation

The operator should demonstrate:

- formal health and safety consultative mechanisms are in place within the organisation and at the facility
- safety representatives and or safety committees are elected or established in accordance with the relevant health and safety legislation applying to the operation [13]
  - health and safety and or committee representatives are trained and competent to perform their duties in accordance with occupational health and safety legislative requirements
  - sufficient resources are provided to employee safety representatives or committee members involved in safety related functions.

Participation

The operator should demonstrate:

- mechanisms exist for involving personnel in:
  - the development and implementation of health and safety policies and procedures
  - the identification and management of hazards and risk; and
  - the preparation of the safety case[14]
- clearly defined issue resolution processes are in place and these are known by all concerned parties.

Communication

The operator should demonstrate:

- formal and informal methods of communication are used to inform employees of health and safety issues[15].

- formal methods of communication are used to advise personnel of their health and safety related roles, responsibilities, accountabilities and authorities

Guidance Note 13

General health and safety legislation in most jurisdictions provides for the formal election of safety representatives or the election of safety committee members or both.

While legislation in each jurisdiction differs, the elected health and safety representative and or the committee should be involved and consulted on:

- the management of health and safety
- changes proposed to the plant facility or operations
- initiatives for improving health and safety including plans, objectives and targets and any other issue relevant to health and safety at the facility.

In addition employee health and safety representatives or committee members should be provided with an opportunity to inform employees in their work area of the actions and progress on specific OHS issues and to receive information, suggestions or inquiries from employees for resolution with senior management.

Guidance Note: 14

In the case of a new facility, it is recognised that facility employees may not be available at the time of SMS preparation. In this case attempts should be made to gain some employee representation by other means, (for example: from other areas of the organisation or appropriate employee representative bodies) to achieve a similar broad range of experience from different disciplines.

Guidance Note: 15

Examples of methods to communicate safety issues include:

- health and safety meetings
- e–mail correspondence
- safety alerts and bulletins
- safety representatives
- generally accessible relevant company databases
- external professional organisations

Types of information that may be communicated include:

- health and safety performance reporting
- results of health & safety audits and reviews
- reporting of incidents and system failures
- reporting on hazards identification
- reporting on preventative and corrective action

3.1.4 Resources

Standard

The operator should ensure sufficient resources to develop, implement and maintain the SMS.

The operator should demonstrate:

- sufficient resources (financial, human, including specialist advisers) are available to implement the health and safety policy and maintain and improve the SMS[16].

Guidance Note 16:

The operator should allocate sufficient resources: financial, human and time to develop, implement and maintain the SMS.

Where necessary, specialist advisers (either in-house or external) should be sourced to assist with development, implementation or maintenance of the system.

Specialist advisers can include (but are not limited to)

- medical practitioners
- risk engineers
- occupation health and safety advisers
- occupational hygienists
- inspection and testing specialists
- ergonomists
- human factor specialists etc.

A budget for development and implementation of the SMS should be prepared consistent with the programs or projects being undertaken.

Specific health and safety related programs and issues requiring allocation of resources may originate from:

- different phases of operation
- incident/hazard reports
- various initiatives such as safety campaigns
- training programs
- personal protective equipment
- emergency response
- safety audits
- safety case development and review
- changes to regulations etc.

3.2 Key Element

Planning

Aim

The operator should demonstrate a systematic approach to the management of facility hazards and risk through the identification and assessment of hazards and risk, the establishment of objectives, plans and performance standards, and the development of adequate documentation.

3.2.1 Hazard Identification and Risk Management

Standard

The operator should have procedures in place for the systematic review of health and safety hazards and risk over the life cycle of the facility.

(Note: While this section deals with the management of all hazards and risk, those that may result in major accident events, are more comprehensively dealt with in Chapter 4 of these Guidelines – formal safety assessment).

Hazard Identification and Risk Management

The operator should demonstrate:

- policies, standards and procedures are in place for the systematic identification, assessment and control of hazards and risk associated with the design, construction, commissioning, operation and abandonment of the facility. The demonstration should establish the:
  - company's risk acceptance criteria and basis for selection[17]
  - scope, methods and timings for undertaking periodic formal and informal task level identification of hazards and assessment of risk to health and safety associated with the production system and technology, working environment and work activities at each lifecycle stage [18]
  - hierarchy of risk reduction measures used for the control of risk [19]
  - methods used to ensure that risk levels are systematically reduced to ALARP
  - methods of ensuring appropriate and competent personnel (including facility employees, where appropriate) are involved in the identification of hazards and selection of risk reduction measures
  - methods used to document, review and keep current information obtained during the formal hazard identification and assessment process and the selected control measures
  - methods for ensuring risk reduction measures are implemented and maintained for ongoing control
  - method used to review the overall effectiveness of the risk management system [20]
  - general approach used for hazard identification and risk management
  - measures of risk reduction used.

Communication

The operator should demonstrate arrangements for:

- informing employees of the risk management system and their role in identifying and controlling hazards and risk at the facility
- communicating to employees of day to day changes in the existing and newly identified hazards on the facility
- communicating to employees of day to day changes in the status of control measures at a facility.

Specific Requirements

The operator should specifically demonstrate:

- initiating events and possible escalation factors are considered in the risk assessment for identified hazards
- physical and human factor hazards and risk associated with safety critical tasks (including commissioning, start-up, shut-down and maintenance tasks) are identified and assessed
- how results are used in establishing organisational and facility objectives.

Guidance Note: 17

Risk acceptance criteria may include:

- qualitative and/or quantitative organisational or facility objectives
- regulatory requirements
- prevailing codes of practice and industry standards

Guidance Note: 18.

Documented procedures should establish:

- the processes, facilities or systems to be assessed at each lifecycle phase: for example:
  - areas of the facility, including engine room, process areas, auxiliary machine space
  - systems, including hydrocarbons processing and storage, diesel fuel, compressed air
  - activities and tasks including diving, lifting, vessel entry, maintenance, operations etc
  - environment, including heat, noise, hazardous substances.
- the types of formal hazard identification and risk assessment tools (quantitative or qualitative or both) to be used (HAZOP, HAZID, JSA)
- specific risk criteria associated with the identification, analysis and management of hazards being considered
- when the assessments should be carried out

Quantitative and qualitative risk assessments may be appropriate at the new development or project level where it is likely that major hazards will be encountered. Further information on this type of analysis is provided in Chapter 4 of these guidelines.

Guidance Note: 19

The following hierarchy of risk reduction measures should be used in the order of preference as listed:

- elimination
- substitution
- control
- mitigation
- recovery

(engineering, procedures, training or PPE)

Guidance Note: 20

Events that may prompt a review of hazards information include:

- a planned major change by the operator
- a major incident (for the operator or in the industry generally)
- industry experience
- a scheduled regular risk review.

3.2.2 Objectives, Plans and Performance Standards

Standard

The operator should establish, maintain and monitor measurable and achievable health and safety objectives, plans and performance standards consistent with the company's health and safety policy.

Objectives and Targets

The operator should demonstrate:

- measurable and achievable health and safety objectives are routinely developed, documented and implemented for relevant function and levels within the organisation and for the facilities
- achievements against objectives are routinely reviewed

Health and Safety Management Plans and Performance Standards

The operator should demonstrate:

- plans and performance standards are routinely established for attaining objectives and targets [21]
- plan implementation is monitored and performance against standards is appraised
- management is held accountable for meeting health and safety performance standards
- plans are updated to reflect changes in performance standards, or outcomes of appraisals of the systems effectiveness

Communication

The operator should demonstrate:

- safety objectives, plans and performance standards and the subsequent level of achievement are communicated to all employees and interested parties.

Guidance Note: 21

There should be a balance of:

- leading indicators, for example: percentage close-out of audit actions, training schedule completion etc
- lagging indicators, for example: lost time injury frequency, total recordable case frequency etc.

3.2.3 Sources of Information (Legislative and other Standards)

Standard

The operator should develop, implement and maintain procedures for the identification, collection, review and dissemination of information and standards relevant to the safe design and operation of the facility.

The operator should demonstrate:

- procedures and arrangements are in place for the routine identification, collection, update and effective communication of information relevant to health and safety. Information should include but is not limited to:
  - –legislation and associated amendments
  - –relevant industry standards (AS, API etc)
  - –relevant equipment/product information
  - –safety bulletins issued by Regulators and industry bodies
  - –relevant codes of practice
  - –incident and hazard data
  - –safety alerts.

3.2.4 Management System Documentation

Standard

The operator should develop and maintain an accessible documented SMS integrated with other management systems.

The operator should demonstrate:

- manuals, procedures, plans, and drawings exist in either hard copy or electronic form for the management of health and safety and control of risk at a facility. The demonstration should detail :

  –the structure of manuals and documents used to manage safety at the facility

  –arrangements for ensuring documents are current and readily accessible to employees

  –how the documentation encourages the understanding and use of the SMS.

3.3 Key Element

Implementation

Aim

The operator should demonstrate that hazards associated with facilities and work activities are controlled and arrangements are in place for responding to emergencies.

3.3.1 Design, Construction and Commissioning

Standard

The operator should demonstrate that hazards and risk associated with the design, construction and commissioning of the facility and its plant, equipment and systems are eliminated, or reduced to as low as reasonably practicable.

Design Planning

The operator should demonstrate:

- the incorporation of results from risk assessment studies as an interactive element of the design process (for both process hazards and workplace hazards)
- responsibility for design of facilities and work systems and activities is clearly defined
- personnel involved in design are competent
- methods of co-ordination exist that ensure design information is communicated between project and operational groups
- hazards are identified and risk is assessed, eliminated or controlled at each stage of the design
- design changes are reviewed as part of the overall risk management process

Design Input

The operator should demonstrate:

- design specifications for all major project work refer to appropriate technical standards, safe design criteria, safety performance standards, regulatory requirements, good oil-field practice and the operator's safety objectives
- task and facility design specifications reflect human factor considerations[22].

Design Output

The operator should demonstrate:

- documented drawings, reports, calculations and analyses meet the design specification brief
- ergonomics are considered in design[23]
- hazards and risk associated with construction, commissioning and operation are identified and assessed

- operations and maintenance procedures and purchasing specifications include safety performance standards.

Design Review

The operator should demonstrate:

- formal design reviews are conducted at each stage of the design
- personnel from relevant functional groups are involved in the review
- modifications to the design are initiated and controlled.

Design Validation

The operator should demonstrate:

- key hardware and systems design aspects are validated by independent and competent persons or bodies [24]
- validation of the design against the design specification and safety performance standards occurs at key design phases and at commissioning.

Construction

The operator should demonstrate:

- construction hazards and risks are identified and plans and procedures are established to control them
- verification of the final construction against the design specification takes place.

Commissioning

The operator should demonstrate:

- procedures for ensuring safe commissioning are established, implemented and maintained[25].

Guidance Note: 22

Human Factor issues:

Task design –

- the design of the task
- the capacity for - overwork, underwork, boredom
- the effects of scheduling of work - stress, control of fatigue
- ergonomic requirements
- decision making requirements
- communication requirements
- availability of work standards
- information requirements
- instructions – training requirements
- warning sign requirements

Personal Factors

- skill levels
- physical attributes of personnel operating plant or conducting tasks
- experience of employees
- employee knowledge
- fitness for work

Tools, Materials and Technology

- design, control systems
- access and design of tools
- integrity and suitability of materials.

Guidance Note: 23

Ergonomic considerations associated with design can include:

Lay-out of and use of controls and displays

- control should reflect the equipment functions,
- control should be accessible, easy to distinguish and arranged to promote ease of use
- displays and controls should be arranged to encourage good working postures and allow movement and variation
- control systems should be designed to accommodate operator intervention in computer controlled processes
- displays should provide essential information about fault and emergency states and indicates priority where possible.
- displays should be visible and easily intelligible from all relevant working positions.

General plant design

- automatic safety devices should be provided where a rapid response and/or where complex information handling is required
- automatic devices or help from other personnel should be available for periods of overload on individuals
- plant, equipment and facilities should be designed to allow access and egress for normal maintenance operations and during emergencies
- lifting equipment

Guidance Note: 24

The Petroleum (Submerged Lands) (Management of Safety on Offshore Facilities) Regulations 1996 (the Regulations) requires independent validation of design, construction and installation for:

- proposed facilities.
- significant changes to existing facilities.

Refer to clause 13 of the Regulations

Guidance Note: 25

Start up and commissioning procedures should address:

- operations hookup
- emergency response
- review of software alarms/trips and tests
- maintenance
- personnel training issues
- project phase handover to operations personnel
- extra manning or supervision requirements
- start-up isolations/defeats.

3.3.2 Management of Change

Standard

The operator should ensure changes and modifications are reviewed for hazards and risk prior to implementation and information on change requirements are communicated to all relevant employees and stakeholders.

Engineering

The operator should demonstrate:

- arrangements in place for controlling modifications to plant, equipment and materials used at a facility[26]. The demonstration should detail how:
  - change requests are initiated, processed and authorised
  - change requests are prioritised and safety and risk implications are assessed
  - the cumulative impact of minor changes is assessed and actioned
  - those affected by change are consulted prior to implementation
  - changes are communicated to interested parties.

Organisation and Work systems

The operator should demonstrate:

- Arrangements are in place for controlling permanent and temporary organisational, and work activity modifications and changes and this is communicated to relevant employees[27]. The demonstration should indicate how:
  - change requests are initiated, processed and authorised
  - change requests are prioritised and safety and risk implications are assessed
  - the cumulative impact of minor changes is assessed and actioned
  - those affected by change are consulted prior to implementation.

Documents

The operator should demonstrate:

- procedures are established, implemented and maintained for the control of all relevant safety and risk management documents, plans, drawings and data. The demonstration should indicate:

  - how current versions of documents and data are authorised, distributed and made available to appropriate personnel. If electronic documents are used, detail measures established to make these documents available during power outages
  - responsibility for and how documents are periodically reviewed and updated when changes occur
  - arrangements in place for the withdrawal of obsolete documents and arrangements that ensure superseded documents and data are not unintentionally used.
- documents and data are maintained and are in a format suited to the requirements of users.

Guidance Note: 26

A management of change system will ensure that changes will be analysed, evaluated and communicated to employees prior to implementation. Changes should be supported by document control systems. Features of such a system normally include:

For engineering and process changes

- evaluation of hazards, resources needed and the effect on operational conditions, construction, decommissioning requirements, maintenance requirements
- assessment of risk levels
- review of change requirements in other systems (for example: changes in inspection and test frequencies)
- communication of intended changes to affected groups
- training requirements.

Guidance Note: 27

Health and safety implications should be assessed when there are organisational or work activity changes for example:

- change of company ownership
- change of organisational structures and reporting relationships
- changes in staffing numbers (or staffing philosophy, down sizing, upsizing or outsourcing)
- job or task redesign
- changes in duty allocations.

3.3.3 Purchasing and Control of Materials and Services

Standard

The operator should develop and maintain appropriate arrangements for the control of purchased services and materials to ensure additional hazards are minimised.

Services

The operator should demonstrate:

- tender specifications are established that incorporate health and safety requirements for all major contracts[28]
- procedures for the selection of contractors incorporate a review of safety requirements in accordance with the tender specification
- arrangements are in place for the review and integration of the operator and contractor safety management systems prior to commencement of activities. The demonstration should detail:
  - mechanisms to involve contractors in hazard identification and risk assessment
  - arrangements for communicating safety related issues between the operator and contractors
  - how responsibilities for emergency response are assessed and allocated between contractors and the operator and revised organisation descriptions and roles and responsibilities are determined and communicated
  - arrangements in place for assuring contractor competence[29].
- procedures and arrangements for monitoring the performance of contractors during and on completion of the contract or assigned work. The demonstration should establish the arrangements for:
  - supervision, monitoring and auditing of the contractor's performance during operation
  - verifying and accepting the work undertaken against the tender specification on completion of the contract.

Materials and Equipment

The operator should demonstrate:

- purchase specifications and/or purchase orders incorporate health and safety requirements[30]

- employees are consulted prior to the purchase of materials and equipment with potential health and safety implications
- procedures are in place for the inspection and verification of materials supplied against the purchase specification
- arrangements are in place for the review of operating procedures and practices when purchases have health and safety risk implications [31]
- personnel are informed of health and safety implications associated with purchases
- personnel are aware of their responsibilities with respect to hazard identification and risk management during the process of materials and equipment specification and purchasing.

Guidance Note: 28

Contractor selection criteria should consider the capacity of the tenderers to comply with the tender specifications, legislative compliance, health safety and environment (HSE) performance. The contractors HSE management system could include:

- objectives
- plans
- records
- training

Guidance Note: 29

Contractors should be verified as competent in all activities critical to managing the risk associated with their assigned tasks. As a minimum, induction training should be provided in:

- emergency response
- permit to work.

Guidance Note: 30

Purchase specifications should include compliance with relevant technical, design, operational and legislative standards: for example:

- Australian Standards, Australian Petroleum Institute (API) codes and recommended practice, for example: emission standards (noise etc),
- legislative standard's requirements for manufacturers risk assessment, validation certificates for example: *Industrial Chemicals (Notification and Assessment) Act*

Purchase specifications should also require the provision of information and data associated with the safe operation, handling and use for example: Material Safety Data Sheets (MSDS)

- operational and maintenance procedures and manuals.

Guidance Note: 31

All purchased items, equipment and material should be assessed to determine the need for changes in operating, maintenance and safety management practices and procedures, for example: training, provision of additional risk control measures, communication etc.

3.3.4 Safe Operational Procedures

Standard

The operator should develop and use operational procedures that effectively manage risk arising from operations.

The operator should demonstrate:

- operating and maintenance procedures exist for all key work activities and tasks[32]. The demonstration should detail:
  - safety critical procedures established as a result of risk assessment studies
  - procedures and arrangements for conveying information between shifts on matters such as maintenance in progress, plant out of service, process abnormalities etc[33]
- arrangements in place for obtaining feedback on and reviewing the adequacy of operational procedures. The demonstration should indicate employees responsible for task execution are involved in this review.

The operator should demonstrate that standard operational procedures are in place for both routine and non-routine work activities. The demonstration should establish that safe operational procedures are:

- appropriate, established, implemented and maintained
- understood, current and accessible

Standard operational procedures should include, but not be limited to:

Permit to work

Setting out procedures for[36]:

- authorisation and issuing of permits
- distribution and display of permits
- isolation procedures
- hazard identification and risk management
- simultaneous operations
- change in operating status
- close-out of permits
- etc

Simultaneous and Non Routine Activities

Setting out procedures for:

- the control of safety critical, simultaneous and non-routine activities
- restrictions on activities when all or part of key safety systems are unavailable

Maintenance operations

Setting out procedures for:

- operation of main engines, generators, auxiliary equipment and utilities.
- planned maintenance activities
- breakdown and emergency maintenance activities, etc.

Safe Work

Setting out procedures for:

- working at heights
- working over the side
- confined space entry
- pressure testing, etc.

Well Management

Setting out procedures for:

- well design
- well operations
- well control
- well suspension
- well abandonment

Guidance note: 32

Safe operational procedures should be developed to control or prevent risks occurring during all phases of the facility's life: design, construction, commissioning, operation (including modification phases if any) and abandonment.

Procedures referred to in this section relate to work activities including those that adequately control hazards during normal operations (including routine and non-routine operations and maintenance) and planned change (including those that arise from construction, and changes to structures, plant, substances, other procedures, personnel, or information). Other sections of this manual deal with additional procedures for controlling emergencies, design and construction.

Operational procedures should deal with risks identified during the FSA and comply with regulatory requirements. The procedures should also be consistent with the operator's control philosophy.

A list of reference documentation should be provided to allow the assessor to trace appropriate procedures.

Guidance Note: 33

For example, employees need to be made aware of:

- the shutdown of a fire pump
- the temporary removal of a lifeboat
- the failure of part of the public address system on the facility
- inhibition of the detection or shutdown systems.

Guidance Note: 34

The operator's summary of the facility's work permit system and isolation procedures should contain references to the following:

- types of work permits in use
- type of work for which a permit is required
- methods of hazard recognition and control
- personal safety of those carrying out the work
- safety of other employees
- overall safety and integrity of the facility
- locking, tagging and isolation procedures
- limits on number of active permits
- responsibility for issue and cancellation of permits
- shift handover procedures relating to permits
- intermediate inspections (including gas testing)
- post-completion inspections
- procedures for suspension or cancellation of work
- concurrent operations
- period of permit validity, duration of work
- close-out and sign off of permits.

3.3.5 Materials Handling and Storage

Standard

The operator should have in place a safe system for handling and storing of materials.

Material Handling

The operator should demonstrate that procedures are in place to ensure

- safe movement of materials and personnel[35]
- manual handling activities are carried out safely[36]
- activities involving cranes, hoists, winches and other lifting appliances are carried out safely[37]
- lifting gear such as slings and shackles are used in a safe manner[38]
- lifting equipment such as containers, pallets, racks and work baskets are used in a safe manner
- risk associated with the handling of hazardous materials are controlled[39]

Material Storage

The operator should demonstrate that procedures are in place to ensure:

- storage areas for materials are located in appropriate areas, and are fit for purpose
- hazardous materials are properly stored given due regard to the nature of the hazards and need for segregation.[40]

Guidance Box 35

Procedures for movement of materials and personnel should include, where applicable:

- supply vessels
- helicopter operations
- lifting operations
- manual handling
- communications
- certification and control for lifting gear
- personnel baskets
- vessel transfer limitations
- isolation/depressurisation of hydrocarbon lines if lifting over them

References should be made to any dropped object and impact studies and associated procedural and hardware controls.

Guidance Note: 36

Procedures should be in place to minimise the risk of manual handling injuries, particularly back injuries. Means to reduce the risk should include:

The use of mechanical lifting aids, such as:

- cranes
  - winches
  - hoists
  - fork lifts
  - wheeled trolleys
- training in safe lifting and carrying techniques

Guidance Note: 37

Procedures should be in place for the safe operation of lifting devices. These should include:

- ensuring lifting appliances meet appropriate standards and codes
- installation requirements for items such as padeyes and monorails
- inspection, testing and maintenance requirements
- operator training.

Guidance Note: 38

Procedures should be in place for the appropriate supply and usage of lifting gear such as slings and shackles. These should include:

- certification and marking requirements
- inspection, maintenance and testing requirements
- lifting gear register
- training and qualifications of persons who inspect and use lifting gear.

Guidance Note: 39

Procedures should be developed, authorised, implemented and maintained for the labelling, handling, storage and disposal of hazardous materials. These procedures should reference any standards, registers or manifests required by relevant legislation or international standards or codes.

Prior to shipping offshore, health and safety information on the relevant material should be obtained by the operator, for example:

- MSDSs and signage for all chemicals and other materials onsite
- storage, labelling and handling requirements for any hazardous or toxic substance
- disposal of any materials, for example: oils, hydraulic fluids, or other petrochemical products that may impact upon the environment on or off site
- the methods used to inform employees of storage, handling and disposal methods .

Guidance Note: 40

Procedures should be in place for the safe handling, storage and disposal of any materials requiring special precautions as defined by MSDSs. In addition, segregation of materials during transport, storage or usage may be required, for example:

- storage of flammable materials in specially designated areas away from sources of heat or ignition
- segregation of oxidising materials from flammable materials
- segregation of poisons from foodstuffs.

3.3.6 Maintenance

Standard

The operator should have an effective system of maintenance to ensure the safe operation of the facility

Maintenance Planning

The operator should demonstrate:

- standards and procedures are in place for maintaining plant, equipment and facilities. The demonstration should:
  - indicate how safety critical items are determined
  - detail what maintenance procedures are validated
  - establish the operator's maintenance philosophy
  - detail responsibilities for authorising, conducting and supervising maintenance activities
  - indicate how routine maintenance frequencies are determined [41]
  - indicate how maintenance items are prioritised
  - indicate how maintenance of safety critical equipment is scheduled and controlled

Maintenance Implementation

The operator should demonstrate:

- inspections, maintenance, repair and plant alteration records are established and maintained
- procedures are in place for the review of hazards and risk associated with maintenance activities and tasks prior to undertaking these activities
- plant and equipment requiring registration with external authorities is identified and procedures ensure that registration is maintained
- procedures are in place for the periodic review of action against maintenance schedules to verify critical plant maintenance is being undertaken and equipment is safe before being returned to service
- procedures are established for the reporting, isolation and withdrawal of unsafe plant and equipment from service

- procedures are in place for the periodic review and improvement of maintenance procedures.

The operator should detail how maintenance employees are involved in the review of procedures and planning schedules.

Guidance Note: 41

Maintenance schedules should:

- reflect the assumptions and outcomes of the FSA studies and
- be consistent with relevant codes and standards and manufacturer's recommendations.

3.3.7 Employee Selection, Competency & Training

Standard

The operator should ensure ongoing competence of personnel.

Employee Selection

The operator should demonstrate:

- procedures exist for the specification, selection and placement of competent personnel[42], detailing how competence and personal attributes relating to safety are identified and used in the selection of personnel:
  - establishing the method for reviewing job and position specifications
  - indicating how minimum skills, experience and qualifications of prospective employees are assessed and verified.
- the mechanism for communicating roles and responsibilities to employees.

Competency and Training

The operator should demonstrate:

- adequate resources are allocated to training
- health and safety training needs are periodically assessed in conjunction with employees
- training and development specific to health and safety occurs[43]
- training in relevant work and safety critical procedures is provided to new, transferring and existing employees
- visitors, casual and new employees are inducted
- competence of employees is assessed on appointment and periodically reviewed
- training courses, programs, and modules are assessed, maintained and current
- training records are maintained and reviewed (to capture refresher training requirements)
- training programs effectiveness are reviewed (including verification of employees competence) and modified or updated where necessary

Guidance Note: 42

Typically, job specifications may be detailed in position descriptions, job descriptions and employee contracts.

Position descriptions or job specifications should identify minimum skills, qualifications and experience requirements including health, physical and psychological capacities for the tasks to be undertaken.

Guidance Note: 43

Training programs should be established for each level in the organisation. Training could include:

- *safety management system*
- *legal requirements*
- *human factors*
- *hazard identification and control*

Job Training

- operational procedures
- emergency response
- health and safety responsibilities
- training in areas specified in legislation
- training in the use of PPE, hazardous substances handling etc

Induction Training

- emergency response
- health and safety responsibilities
- incident / hazard reporting
- permit to work
- hazard identification and control.

3.3.8 Workplace Environment

Standard

The operator should demonstrate facilities and processes are in place to ensure and promote a safe work environment.

The operator should address (as a minimum):

- atmospheric contamination
- housekeeping
- lighting and ventilation[44]
- noise and vibration [45]
- sign posting
- personal protective equipment[46]
- temperature extremes[47]
- hygiene[48]
- radiation
- working hours
- basic amenities[51]

Guidance Note: 44

Lighting and Ventilation

- lighting and ventilation levels should be assessed and periodically reviewed to ensure they are adequate with regard to the location and nature of the work being done.

Guidance Note: 45

Noise and Vibration

- procedures should be in place for the identification, assessment and control of noise and vibration risks associated with the design, selection and operation of plant and equipment
- noise levels should be reassessed when changes occur
- design and purchase specifications establish noise levels consistent with legislative requirements

Guidance Note: 46

Personal Protective Equipment

Personal protective equipment (PPE) needs should be assessed and procedures in place for the selection, issue, training, and use of the PPE.

Guidance Note: 47

Temperature control

Facilities and procedures should be in place to ensure that:

- as far as is practicable, heating and cooling is provided to enable employees to work in a comfortable environment; and
- employees are protected from extremes of heat and cold.

Guidance Note: 48

Hygiene

Procedures should be in place for the transport, storage and preparation of food.

Guidance Note: 49

Work Place Facilities

Facilities and amenities must conform to legislative requirements, standards and codes of practice for items such as:

- drinking water
- sufficient workspace
- surfaces and floors
- change rooms, toilets and showers
- cabins and other accommodation space.

3.3.9 First Aid and Emergency Response

Standard

The operator should implement effective first aid and emergency response arrangements.

First Aid

The operator should demonstrate:

- first aid requirements and facilities are identified and assessed. The demonstration should:
  - identify the types of incidents that may occur on or in the area of the facility
  - indicate the inventories of first aid equipment and facilities
  - detail the need for numbers, classifications and competence of trained first aid personnel
  - detail the types of training provided to personnel
  - detail the management of first aid coverage at remote sites (if applicable)
  - detail the arrangements for 24-hour cover for first aid.
- procedures are established for maintenance of first aid facilities. The demonstration should indicate the:
  - arrangements for ensuring the security of prescription medications
  - arrangements for maintaining the first aid inventory
  - availability of additional medical advice.

Emergency Response

The operator should demonstrate:

- all potential emergencies (including those listed in the FSA) are identified and procedures and facilities exist for mitigating their effects[50]. The demonstration should indicate:
  - the offshore command structure to manage the emergency response on the facility
  - the onshore command structure to co-ordinate and support the emergency response on the facility
  - the roles and responsibilities of all key employees associated with the execution of the emergency response plan

  - how all parties, including external agencies, are informed of their role in executing emergency response actions for example: onshore office, police, maritime agencies and other emergency services
  - how conflicting demands are managed where services and equipment of one contractor are shared by a number of operators, for example: helicopters for pre-cyclone evacuation, emergency and rescue equipment
  - the procedures for issuing and maintenance of safety equipment, emergency equipment and specialised tools
  - the procedures in place for search, rescue and recovery operations
  - the availability of sufficient numbers of competent emergency trained response team personnel at all times
  - the procedures for accounting for all personnel on board in an emergency
- a schedule of regular emergency drills and exercises are conducted for each emergency scenario.
- procedures are established to assist employees who are exposed to critical incidents at work.
- all personnel are competent to perform their roles during an emergency. The operator should
  - indicate how the emergency command ability of the person-in-command of the facility is assessed prior to appointment
  - establish the training provided and the methods of assessing competence for all key personnel.
- procedures are established for communicating emergency response arrangements to employees
- emergency communication procedures are established
- emergency equipment is fit for purpose, available at appropriate locations and accessible[51]. The demonstration should indicate contingencies in the event of damage/loss or unavailability of equipment, for example: life boats
- emergency equipment, exit signs and alarm systems are inspected, tested and maintained at regular intervals
- the effectiveness of the emergency response system is periodically assessed, reviewed and improved.

Guidance Note: 50

The operator should have plans and procedures in place for all identified emergency scenarios that could reasonably be expected to occur during each operational phase.

Identified scenarios should cover at a minimum those identified in the formal safety assessment studies for example:

- hydrocarbon release resulting in fire/explosion
- oil spill
- serious injury or death
- helicopter incidents
- loss of well control
- ship collision
- adverse weather
- loss of ballast control, stability and station keeping
- subsea hydrocarbon releases, for example: pipelines or flowlines
- diving emergencies
- terrorist activities
- events requiring evacuation of the facility
- confined space emergencies
- person overboard
- toxic release

The emergency response plan should reflect the combined operator and contractor procedures and be discussed and agreed with all relevant parties. Emergency response procedures should:

- have clear contents and directions for use
- contain up to date names and contact numbers for key personnel and organisations
- clearly show the chain of command and lines of communication to be put in place during an emergency
- define the responsibilities of essential personnel and outline the basic procedures for responding to emergencies
- ensure all relevant personnel and organisations are kept informed of the plan and
- any updates.

The plan should also contain or reference a program of emergency drills and exercises which:

- involves all relevant facility and support personnel as well as outside agencies
- is closely aligned with emergency scenarios relevant to those identified in the FSA
- includes a review on completion of the exercises and allowance for updates if necessary.

Guidance Note: 51

In the event of unavailability or insufficient TEMPSC either personnel should be transported from the facility or production ceased and made safe.

3.4 Key Element

Monitoring and Evaluation

Aim

The operator should demonstrate that facility, plant, process, work system and management arrangements are measured, monitored and, evaluated and, where deficiencies are identified, corrective actions are implemented.

3.4.1 Inspection, Testing and Monitoring

Standard

The operator should have effective systems of inspection, testing and monitoring to ensure technical integrity of the facility.

The operator should demonstrate:

- appropriate condition monitoring programs exist
- regular inspections of workplace and facilities are carried out
- informal hazard inspections take place
- inspection and tests of safety critical risk control and mitigation devices are regularly conducted[52]. The demonstration should indicate how:
  - inspection and test frequencies are determined
  - completion of test schedules is verified
- procedures exist for the safe execution of inspection and test activities
  - inspection processes should seek input from personnel required to undertake the tasks being inspected
- inspection, test and monitoring equipment is maintained, stored and calibrated to an appropriate standard
- inspection reports contain recommendations for the prioritisation and implementation of corrective actions
- responsibility for implementing corrective actions arising from inspection reports is assigned to specified personnel
- arrangements exist for verifying that corrective actions have been completed
- corrective actions arising from inspections are evaluated to determine their effectiveness
- workplace environmental monitoring is conducted (where appropriate) and records of the results are maintained
- inspection and testing results are periodically reviewed and used in assessment of the work priorities of the facility.

Guidance Note 52

Facilities typically subject to inspection test activities include:

- electrical and control loop integrity
- emergency power
- lifting and rigging equipment
- navigation and communications equipment
- emergency response equipment
- pressurised equipment – PSVs etc
- facility integrity (for example: corrosion)

The frequency of routine inspections should match:

- the specifications cited in the assumption outcomes of the formal safety assessment studies and the assessment of the general risk
- regulatory requirements
- good oil field practice (for example: vibrations and corrosion checks)
- manufacturer's recommendations
- appropriate Australian (or international) standards or codes of practice.

3.4.2 Health Monitoring System

Standard:

The operator should monitor and evaluate the effects of the work environment on the health of employees.

The operator should demonstrate:

- employee health monitoring requirements are identified and procedures exist for conducting monitoring [53]
- where required by legislation, the health of employees exposed to specified hazards is monitored and recorded
- employee health monitoring records are periodically reviewed and programs are established to reduce health risk
- pre-employment assessments are carried out on employees

Rehabilitation

The operator should demonstrate procedures exist for rehabilitation and supervised return to work for employees injured or suffering ill health.

Guidance Note: 53

A program of employee health monitoring may consist of:

- pre-employment medicals
- ongoing medicals, for example: pre SOLAS training
- lifestyle assessments
- specific monitoring and analysis for identified hazards, for example: noise and hearing loss, hazardous substances and exposure effects.

3.4.3 Incident/Hazard Investigating and Reporting

Standard

The operator has an effective system of reporting and investigating hazards and incidents and establishes measures to prevent recurrence.

The operator should demonstrate:

- procedures exist for reporting and investigating hazards and incidents and implementing corrective actions. The operator should:
  - indicate how the level of investigations is determined
  - specify the reporting requirements
  - indicate the roles and responsibilities of employees, supervisors, health and safety representatives and visitors for reporting and investigating incidents
  - indicate who is involved in the investigation of different categories of incident or accident
  - indicate how the investigative information is used
  - indicate how the quality of the investigation is reviewed
  - indicate how the close-out of corrective actions is monitored
  - indicate how regulatory reporting requirements are satisfied
  - indicate the methods of informing employees of significant incidents and corrective actions
- employees, supervisors, health and safety representatives and managers involved in incident and hazard investigation and reporting are trained and competent.

3.4.4 Health and Safety Information and Reports

Standard

The operator should maintain a system for the analysis, dissemination, storage/archiving and retrieval of information relevant to health and safety.

Managing Health and Safety Information

The operator should demonstrate:

- procedures are in place for the collection, maintenance, and confidential retention of employee health and safety records
- documents and data relevant to health and safety are collected, disseminated, filed and retained[54]. The demonstration should indicate:
  - the types of documents and data collected
  - how health and safety documents are used.

Analysis and Reporting of Health and Safety Performance Data

The operator should demonstrate:

- procedures exist for the collection and analysis of health and safety performance data. The operator should describe the lead and lag indicators used for measuring health and safety performance [55]
- regular reports on health and safety performance are produced and disseminated to relevant personnel.

Guidance Note: 54

Documents, reports and data collected by the operator can include:

- safety alerts
- hazard and Incident reports
- log books
- audit close-out reports
- inspection maintenance records
- hazards registers or similar
- statistical information
- training records
- calibration results
- Non Destructive Testing (NDT) reports
- measures of injury or loss potential

Where appropriate, analysis of the data should take place and reports should be developed that provide personnel with indicators of the effectiveness of the health and safety programs and initiatives.

Reports and data should be retained for periods consistent with local legislation

Guidance Note: 55

The procedures should specify the method of collecting and analysing incident data to provide information on the:

- location and nature of incidents
- frequency and severity of incidents
- effectiveness of hazard and risk controls

This information should be provided to employees and to management to allow trends to be identified and performance to be monitored.

3.5 Key Element

Auditing and Review

Aim

The operator should demonstrate the system for managing health and safety risk is implemented, effective and continually improving.

3.5.1 SMS Audit

Standard

The operator should periodically verify the operation of the safety management arrangements.

The operator should demonstrate

- an audit program and procedures are established, implemented and maintained to verify that health and safety management arrangements are being operated to specified performance standards[56]. The demonstration should indicate:
  - the schedule of internal and independent audits
  - the methodology for conducting audits, including: audit scope and objectives, criteria for selection of audit teams and leaders and reporting requirements
  - how relevant employees are involved in the audit process
- procedures exist for the reporting of audit results and the implementation of corrective actions. The demonstration should indicate how:
  - corrective actions and findings are recorded and prioritised
  - affected employees are made aware of audit results and corrective actions
  - corrective actions are reviewed for appropriateness prior to implementation
  - follow-up action is monitored for timely close-out.

Guidance Note: 56

The operator's audit system should evaluate whether safety procedures and management arrangements are:

- documented
- implemented
- used as intended by the organisation
- effective.

3.5.2 Review and Improvement

Standard

The operator should regularly review the safety management system to assure the arrangements adopted are effective in meeting the operator's policies and objectives.

The operator should demonstrate

- accountable senior management periodically review the effectiveness of the safety management system. The demonstration should indicate:
  - when reviews take place and who is involved
  - the sources of information used to determine if the system is adequate and policy is complied with and objectives are being met [57]
  - how the operator makes use of the review
  - how outcomes are communicated to employees
  - what continuous improvement plans exist

Guidance Note:. 57

Information that may be used in a management review include:

- changes to legislation
- changes in business objectives and expectations
- changes in business/operational activities
- changes in technology
- changes in the organisations structure and personnel
- employee feedback
- results of audits and associated actions
- results of accident and incident investigations
- sampling of work practices
- sampling of safety perception/safety 'climate' (for example: surveys)
- performance against objectives and targets
- review of community expectations

Information and benchmark data from other organisations and industries may also be used if appropriate.

Safety Case Guidance Formal Saftey Assessment Facility

Chapter 4

Contents

Introduction

Aim

To provide guidance in the preparation of the Formal Safety Assessment (FSA) component of the facility safety case.

Scope

The guidelines detail six key elements that should form the basis of the facility methodology:

- process (technique)
- hazard identification
- hazard and risk assessment studies
- assessment of results
- hazard and risk reduction measures
- apply ALARP principles (assessment of tolerability and fitness for purpose)

These steps are shown in Figure 4.1: FSA schematic.

Structure of Guidelines

An **aim** is specified for each element.

Prompts are grouped under the following categories as a guide to matters that would generally be expected to be included within the FSA:

- methodology
- assumptions and data
- outcome and results.

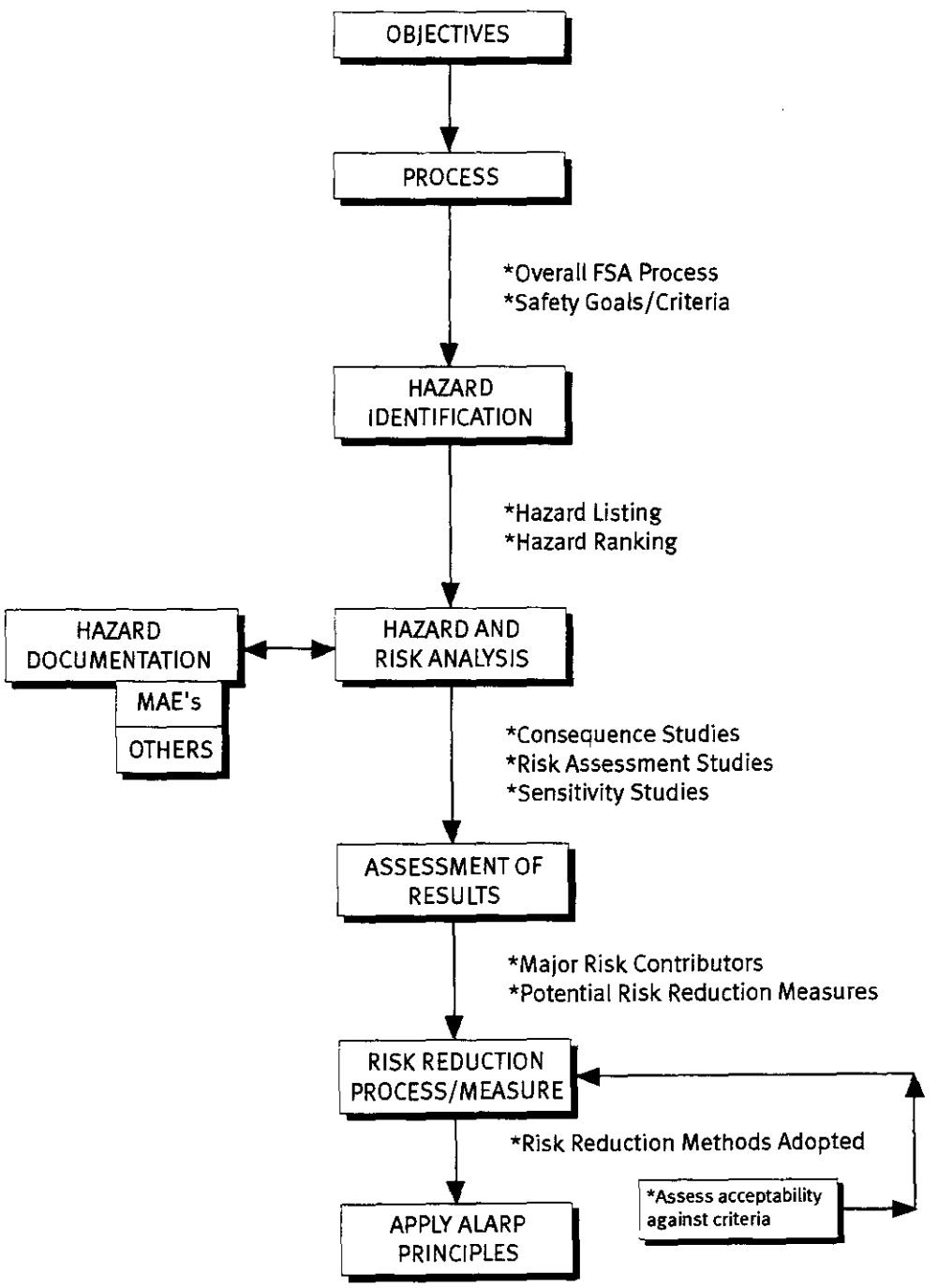
Employee Participation in FSA Studies

There should be a demonstration that there has been appropriate field based employee (or their representatives) involvement in the FSA process to maximise opportunities to identify and control hazards.

Formal Safety Assessment Studies

The relative effort expended between safety management system development/implementation and FSA studies varies between facilities. The balance of effort should be discussed with the DA.

Figure 4.1: *Formal Safety Assessment (FSA) Schematic*



4.1 Formal Safety Assessment Process

Aim

To reduce major accident event risk to as low as reasonably practicable (ALARP). Including, but not limited to a demonstration that:

- ***the exposure of employees on the facility to hazards has been minimised, firstly through elimination of hazards; and secondly through control of remaining hazards***
- ***the integrity of the temporary refuge, protection and detection systems, escape routes, evacuation/embarkation points and lifeboats/liferafts is maintained and steps have been taken to ensure the safety of persons in the temporary refuge, in the escape routes and at the embarkation points until such time as all employees have reached a place of safety or left the facility, whichever is first.***
- ***there are adequate facilities within the temporary refuge to expedite safe escape and evacuation of employees during a major accident event.***

Methodology

The operator should demonstrate that:

- the FSA process starts at the concept selection phase and feeds into the conceptual design stage. The following should be addressed:
  - hazard identification
  - hazard and risk analysis
  - assessment of results; and
  - risk reduction measures [58]
- initial FSA results feed into and influences facility design[59] and construction stages and all drawings/documents are referenced in document control registers
- safety considerations are part of the facility selection process
- appropriate and competent people are involved in the FSA process[60]
- appropriate quality assurance procedures are adopted in the development of the FSA.

Assumptions

The operator should demonstrate that assumptions made in the FSA are based on appropriate data, which:

- track change
- are referenced
- detail geographic limitations
- are reasonable
- are justified for example: by comparison with external data and/or references
- are reviewed by appropriate personnel, and
- highlight modifications.

Outcomes and Results

The operator should demonstrate that the:

- FSA process includes all assessments necessary for a comprehensive safety analysis for the defined activities
- risk goals and acceptance criteria are adequate and justifiable.

Guidance Note: 58

The FSA process typically includes the following elements:

Hazard Identification

This step involves the identification of hazards at the facility. The hazards are typically categorised into major groups such as hydrocarbon and non-hydrocarbon and sub groups of loss of containment, fire, explosion, dropped objects, structural failure, ship collision, loss of stability, etc. A hazard register or similar document is then developed for all identified hazards.

The next step involves ranking identified hazards by their consequence and determining if they fall inside the definition of a major accident event. (See the definition of a major accident event in section 1.4). Hazards identified as potential major accident events are then carried forward to the assessment phase of the analysis.

The ranking process may rely solely on qualitative (judgmental assessment), or may include a degree of preliminary quantitative assessment (including an assessment of relative likelihood).

Guidance Note: 58 (cont)

Hazard and Risk Analysis

Following identification of hazards and major accident events, analysis should then concentrate on the likelihood and the impact or consequences of the hazards relating to major accident events. These major accident event studies may be carried out using qualitative or quantitative techniques, or a combination of both.

These studies should typically address the following area:

- fire and explosion hazards
- vulnerability of critical emergency systems
- impact on escape, evacuation and rescue
- temporary refuge integrity
- the impact of smoke and toxic gases
- other impacts for example: storm, transportation, towing
- loss of stability
- startup
- simultaneous operations
- shutdown hazards

The operator should provide a description of the assumptions made during the hazard ranking process and during the more detailed assessment of major accident events. These assumptions may draw on the operator's procedures described in the safety management system and facility description parts of the safety case.

Assessment of results

The results of hazard and risk assessment studies should be used to identify and rank the major risk contributors. The results may be expressed in terms of consequence, personnel risk basis or a combination of both. Sensitivity studies should be carried out to assess the benefits of various risk reduction options, and/or when a change in the input assumptions markedly affects the results.

Risk Reduction Measures

This step develops hazard and risk reduction measures to reduce overall risk from major accident events to as low as reasonably practicable. References to the safety management system and facility description sections of the safety case should be made where appropriate.

Apply ALARP Principles (assess tolerability and fitness for purpose)

This final step ensures that risk levels are as low as reasonably practicable (ALARP). This is often demonstrated by adopting risk reduction measures until their benefit is exceeded by their cost. This is usually done by cost benefit analysis (CBA)

The residual risk levels (after risk reduction measures are allowed for) needs to be checked against the organisation's risk acceptance criteria. Consideration should also be made of societal risk aversion to low frequency, high consequence events

Guidance Note 59

New facilities may achieve lower residual risk levels than existing facilities. Existing facilities can be constrained by the higher costs of retro-fitting equipment, or upgrading, compared to making a design change to a new facility.

New facilities can also take advantage of technological advances in equipment and facilities and enhanced knowledge and understanding of key risk drivers.

Design of facilities, still at the conceptual stage, can incorporate principles such as inherently safer design.

Incorporating these approaches can lead to a positive trend of reducing levels of residual risk associated with new facilities.

Guidance Note: 60

Design engineers require training in the principles of the safety case philosophy and risk based design and on their responsibilities and accountabilities in the process ie attendance at HAZIDS, ALARP workshops, HAZOPS etc. Specialist risk assessment and safety management expertise will be required and safety management expertise will be required in support of this process.

4.2 Hazard Identification

Aim

To demonstrate that the operator has systematically identified hazards (both hydrocarbon and non-hydrocarbon) associated with the facility and that the selection of major accident events is reasonable and justifiable.

Methodology

The operator should demonstrate:

- steps taken in the hazard identification process
- adequate resourcing of the hazard identification process
- comprehensive hazard identification documentation
- how the hazard identification approach meets the performance standards of the facility safety management system
- the mechanism and extent of employee involvement in the hazard identification process.

Assumptions and Data

The operator should demonstrate

- hazard identification processes and techniques used[61]
- hazards have been identified on both a compartment and systems basis
- appropriateness of the criteria used for selecting major accident events from the ranked hazard list
- sources of information including its relevance, validity and currency used in identifying hazards.

Outcome and Results

The operator should demonstrate:

- a hazard register[62] or similar document is available which describes:
  - identified hazards and their causes
  - risk level
  - major accident events
  - control/mitigation and recovery measures
  - links to the safety management system.

- steps undertaken to ensure that the hazards and major accident events listed in the hazard register are comprehensive enough for the facility type.
- the system for maintenance of the hazard register
- how identified corrective actions are documented for example: remedial action list
- mechanisms in place to ensure remedial actions are assessed and closed-out.

Guidance Note: 61

Hazard identification can be based on:

- safety reviews
- task based reviews
- industry experience
- operations experience
- audits
- employee involvement
- incident/hazard investigations/reports
- ALARP workshops

In addition, there are several well-recognised hazard identification techniques:

- hazard and operability study (HAZOP)
- 'what if?' analysis
- checklist
- failure mode and effects analysis (FMEA)
- human factor analysis

Guidance Note: 62

When assessing the hazards registers and the major accident events, cross reference should be made to:

- the safety management system to ensure that assumptions concerning safety management and the input assumptions for the FSA are consistent; and
- the facility description to ensure the hazards register is consistent with the operations and function of the facility.

Hazard categories identified could include:

- hydrocarbon/flammable hazards, for example: gas release
- toxic substances release for example: H_2S
- non-hydrocarbon type hazards, for example: dropped objects, helicopter incident
- external hazards, for example: ship collision.

4.3 Hazard and Risk Assessment Studies

Aim

To determine the consequences of identified major accident events and the likelihood with which these events may occur with respect to the safety of employees.

Methodology

The operator should demonstrate:

- the systematic approach employed for the analysis of major accident events[63]
- that the type and extent of FSA studies undertaken are commensurate with the type of facility and the major accident events that have been identified[64]
- the relationship between all the studies which have been completed detailing linkages
  - between the studies to ensure an appropriate use of common data
  - to the operator's safety management system
- the use and choice of analytical tools[65].

Assumptions and Data

The operator should demonstrate:

- the assumptions for physical/climatic data including the geographic limits for the data. The basis for the selection of data (including its relevance and currency) should be identified and justified[66]

Outcome

The operator should demonstrate:

- the likelihood and consequences of all identified major accident events
- the mechanism for evaluating major accident events including:
  - integrity of the temporary refuge
  - availability of escape routes
  - integrity of safe evacuation and rescue systems
  - escalation potential.

- that integrity assessments are consistent with the physical features of the facility described in the facility description[67]. Document control systems should ensure that:
  - assessment teams have the latest design information
  - a given assessment can be traced back to a specific facility description.
- that sensitivity analyses have been conducted to determine the adequacy of critical input assumptions[68]
  - sensitivity analyses have improved the quality of the results
  - sufficient critical variables have been tested for their sensitivity
- assessments have been undertaken by competent analysts
- where assessments are not conducted inhouse, the mechanism which ensured there will be sufficient knowledge of the assessment tools to manage the on-going maintenance of risk assessment
- the mechanism to verify software model results
- that adequate provision has been made to protect employees from the consequences of major accident events involving:
  - riser(s); and
  - pipeline(s)
- that identified hazards and the major accident events are reasonably in line with findings from industry hazard identification for similar facilities in similar settings.

Guidance Note: 63

Acceptable methods for analysis of hazards include qualitative comparisons and the use of quantitative analysis. The analysis methodologies should develop step by step descriptions detailing how the:

- energy or toxic capacity of each identified hazard can be realised (with particular emphasis on hazards linked to major accident events)
- emergency systems needed to protect employees from serious injury or death may be impaired, and how the employees on or escaping from the facility may be affected.

Guidance Note: 64

Studies undertaken should include an analysis of major accident events. Typically, these studies should assess (where applicable):

- extreme climate events such as storms, tsunamis and earthquakes
- hydrocarbon releases frequency/size/duration, explosions, smoke and fires, including jet fires
- external events for example: ship collision
- toxic release exposures
- dropped objects
- loss of structural integrity.

For hydrocarbon/flammable events, where applicable, the following aspects of the event and its consequences could be analysed:

- release frequency / size / duration
- directional nature of event
- ignition probability (immediate and delayed)
- flame effects - emissivity, surface extent, width and length, and the radiation levels at various distances from the flame surface
- smoke generation
- blast effects
- toxicity
- congestion on the facility (for example: process area, - blast pressure generation)
- nature of boundaries separating areas of the facility (for example: fire/blast walls, & deck type – grating or plate)
- other employee impairment mechanisms
- population distribution to cover other operating conditions, simultaneous operations and campaign maintenance.

The studies should also include an analysis of the ability of critical control and safety equipment to continue functioning under the conditions identified in the analysis of major accident events. The analysis should demonstrate that a series of logical scenarios has been developed to determine which critical safety systems will be required for the preservation of life during any major accident event.

An analysis of the functionality of the escape, evacuation and rescue routes, and facilities should be completed. For a new facility this may be conducted using a simulation; for established facilities a simulation or a scenario-based approach may be followed.

The analysis should show the probable location of employees at the start of any incident and justify those locations. The analysis should show for each of the scenarios or for the whole of the simulation, both the assessed and probabilistically analysed fractional fatalities. These may be split into immediate, delayed or evacuation and rescue. The possible impairments to the facility, equipment or escape route which may cause loss of life should be described, so that alternatives can be evaluated as part of the process of minimising risk.

Guidance Note: 64 (cont)

The hazard and risk assessment studies should consider the vulnerability and endurance under major accident event conditions of the following, as a minimum:

- temporary refuge boundaries and its impairment (whether outside or inside)
- emergency shutdown systems
- fire water deluge system, including the fire pump system
- emergency communication systems
- emergency power systems
- escape, evacuation and rescue system
- life saving equipment.

Guidance Note: 65

Typical tools which are used include proprietary software products and spreadsheet-based software. New software is regularly released and therefore it is inappropriate to define what software should be used. However, the use by the operator of new or untested software, or unprotected spreadsheets / models, should be evaluated. The assessment of new software should either be an audit of the results obtained using a known and accepted software package, or by review of the software assumptions, and appropriateness of application and the software developer's quality control system. Also important is the application of principles by the person using the package with respect to checking input data to models, especially with spreadsheets

Guidance Note: 66

Typical examples of justification of data selection include:

- Australian experience
- overseas experience
- logical argument.

When a number of information sources provide different data on the same subject, such as the range of release frequencies quoted in different databases, the operator should provide information which shows why the selected data are the most appropriate for the application. Sensitivity studies should be considered over the credible range of frequencies.

The operator should adopt a system of checking the work of analysts to ensure the appropriate choice and application of data, and the validity of output.

Guidance Note: 67

At any stage in the analysis a given study should be able to be traced back to a defined facility description. The design will be ever changing: this requires good document control to ensure that the safety case team have the latest documents.

Guidance Note: 68

Sensitivity analyses are usually used as part of a quantitative risk assessment (QRA) to test the effect of the input assumptions on the QRA results and thus qualify confidence in the numerical results.

If, for example: varying an input assumption by an order of magnitude has little impact on the results, then usually the input assumption need not be subject to further scrutiny.

If, on the other hand, an order of magnitude variation in the input assumption has a similar effect on the results of a particular event, then the validity of the results is highly dependent on the validity of that input assumption. In this case, the quality of the input assumption should be re-considered. If there is high confidence in the value selected, then no further scrutiny would normally be required. If, however, there is low confidence in the input assumptions, there should be a demonstration as to how the lack of certainty has been dealt with as part of assessing and presenting the results of the analysis.

4.4 Assessment of Results

Aim

To demonstrate that the operator has properly assessed the results of the hazard and risk assessment studies and has identified major risk contributors.

Methodology

The operator should demonstrate:

- how analysis results have been used
- the review mechanism for the analysis results[69]
- the impact of the analysis results on operator confidence.

Assumptions and Data

The operator should demonstrate:

- what assumptions, if any, have been made in assessing the results.

Outcomes

The operator should demonstrate

- the mechanism for identifying major risk contributors [70]
  - qualitatively – for example: risk matrix
  - quantitatively – including potential loss of life (PLL), individual risk per nnum (IRPA) [71].
- The mechanism for communicating the results of the hazard and risk assessment studies, identification of major risk contributors, and potential risk reduction measures to employees.

Guidance Note: 71

The analysis should:

- address uncertainties in the key assumptions
- ensure adequate sensitivity analyses are conducted to ensure confidence in the results
- identify the major risk contributors
- identify and justify risk reduction measures which have been considered and those which were rejected
- demonstrate that risk is as low as reasonably practicable
- consider societal risk aversion for credible events with very high consequences.

Guidance Box: 72

Demonstrate a clear understanding of the major risk contributors:

- are there several events contributing equally to risk or is the risk dominated by a single (or few) scenarios?

Demonstrate a clear understanding of the reasons why each identified event is a major risk contributor for example:

- high frequency of serious consequences
- occurs in the immediate area of the Temporary Refuge
- occurs during evacuation, escape and rescue.

Any escalation mechanism contributing significantly to risk should be identified. Examples of escalation mechanisms include:

- vessel or structural failure due to fire impingement; and
- explosion damage causing the incident to escalate or a safety system to become inoperative.

Guidance Box: 73

The quantified risk assessment should be reviewed with the knowledge that QRA is not an exact analytical tool. Despite advances in techniques and input data quality in recent years it remains, principally, a comparative tool.

The results from QRA are highly dependent on the quality of the input assumptions and the integrity of the modelling of the sequence of events that follows an initiating occurrence.

QRA does aid risk assessment and control measures evaluation, however it should not be used in isolation; but rather in conjunction with other types of qualitative and engineering assessments.

Reliance on the use of QRA in absolute terms should generally be avoided. QRA can be used with more confidence when comparing the risk reduction benefits of two or more alternatives.

4.5 Risk Reduction Measures and Application of ALARP

Aim

To demonstrate that appropriate risk control measures have been adopted to reduce risk to personnel to as low as reasonably practicable.

Methodology

The operator should demonstrate

- the criteria for selection of risk reduction measures[72]
- adequate employee consultation in the selection of risk control measures
- the range of risk control measures considered

Assumptions and Data

The operator should demonstrate

- the assumptions (if any), in selecting the risk reduction measures.

Outcome

The operator should demonstrate

- risk control measures for major accident events (where appropriate) are identified [73].
- that appropriate risk reduction measures have been adopted for each major accident event until risk has been reduced to as low as reasonably practicable[74]
- the application of a hierarchy of risk reduction measures, for example: elimination, prevention, control, mitigation and recovery
  - the implementation plan and time frame for the introduction of selected risk reduction measures
- how control measures are linked and referenced to the safety management system and facility description[75].

Guidance Note: 72

The process for determination of risk control measures should be detailed. The risk control measures will aim to do one of the following:

- remove the hazard
- decrease the initiating event frequency
- decrease the consequences of the initiating event by, for example:
  - inventory reduction by introduction of emergency shut-down valves may reduce the consequence of release
- decrease the potential for escalation; or
- increase the probability of successful escape, evacuation and rescue.

The operator should ensure that risk reduction measures have been considered for all major risk contributors and that the measures considered include either hardware changes or safety management system solutions, or both.

Risk reduction measures are specific to a facility. Measures which might be considered include provision of a pipeline subsea isolation valve (SSIV), inherently safer design, elimination, substitution and simplification, and decreasing the vulnerability of: emergency systems, temporary refuge, control room and communications centre during major accident events.

Increased benefit can come from early adoption of risk reduction measures. Incorporating the measures early in design can often remove the hazard altogether and lead to inherently safer design.

Guidance Note: 73

Measures for the elimination, control, or mitigation of hazards, are shown below. However, prior to consideration of prevention measures, the minimisation of hazards through measures such as inventory reduction, reduction of complexity, should also be considered.

Elimination

Designing out the hazard should be the first priority. If designing out is not possible, consideration should be given to the following risk reduction measures.

Prevention Measures

Sequences of events that may result in major accident events occurring should have already been identified and discussed. To ensure the safe operation of the facility, measures should be considered to prevent the initiation of each of these sequences.

The discussion concerning the measures should take the form of a structured, qualitative argument which should take into account relevant employee input.

Guidance Note: 73 (cont)

The discussion should also include consideration of the management system as applied to the following typical list

- Design procedures
- Quality assurance
- Inspection
- Maintenance

Control Measures

It may not be possible to prevent the initiation of all the sequences of events that could lead to a major accident event. In cases where preventive measures are not possible, risk reduction measures should be considered to prevent or reduce propagation. These measures act to intervene at some point in the sequence of events, in an attempt to control and contain the developing situation before a major accident event occurs.

Risk reduction measures could include:

- ventilation
- fire and gas detection/protection
- emergency shutdown systems - manual or automatic
- pressure relief systems
- depressurisation/blowdown/venting
- liquid dumping
- ignition control
- subsea isolation valves (SSIVs)

Mitigation Measures

It may not always be possible to intervene in the sequence of events to avoid the major accident event starting. In such cases measures should be taken to mitigate and minimise the consequences of the major accident event. Such measures will have effect only after the major accident event has started.

Such measures could include:

- alarm system
- public address/communications system
- fire protection - active and passive
- temporary refuge
- having people separate from the process area
- escape and evacuation
- procedures
- protective personal equipment (PPE).

Guidance Note: 73 (cont)

Recovery Measures

Dealing with a major accident event includes returning to normal operations. Return to normal operations can be hazardous. Plans which address return to normal operations could include:

- recovery measures
- making the facility safe
- repair, testing and recommissioning

Remedial Measures

During the FSA studies, the results may show that some hazards will not have been adequately managed. In such cases, further risk assessment may need to be carried out to investigate what remedial work is required.

Remedial work may take the form of engineering modifications, changes to procedures or to system controls.

It is possible that engineering modifications are not reasonably practicable (for example: elimination, intensification, alleviation, substitution and simplification). In such cases, more reliance may have to be placed upon procedural or system controls. These controls should provide equivalent levels of risk reduction compared to engineering modifications. The level of residual risk needs to be linked to the operator's risk acceptance criteria, and the safety management system for its management.

Guidance Box: 74

The operator should show that the risk to employees is as low as reasonably practicable by describing risk reduction measures and showing that the cost associated with adopting further control measures is disproportionate to the accrued benefits.

The assessment of the benefit of each risk reduction may take into account:

- risk from the implementation of the measure
- the risk in installing and maintaining the measure (particularly relevant for sub-sea measures)
- the reduction in other forms of risk, such as environmental, asset, business interruption and reputation that follow as a consequence of the risk reduction measure.

The effectiveness of risk reduction measures may be determined individually and in groups. It is possible that risk reduction measures may not be independent, for example:

- introduction of emergency shut down valves to reduce inventory available for release; and
- passive fire protection to surrounding members

may each be practicable measures, but carrying out both may not be reasonably practicable.

Guidance Box: 74 (cont)

Cost alone should not be the sole criteria for adopting (or not adopting) risk reduction measures. Results of qualitative processes such as the ALARP workshop (including regulator participation where possible) should also be taken into consideration.

Operators should demonstrate that the employees carrying out activities have been adequately consulted as to their safety implications.

Guidance Box: 75

The equipment, systems and procedures which help eliminate, detect or control identified hazards should be included in this review. Many should be covered in the safety management system or facility description for example:

- fire and gas detection systems, heating, ventilation air conditioning (HVAC) and maintenance system(s)
- emergency shutdown system
- fire protection system (active and passive)
- PSV and pressure vessel inspection system
- corrosion monitoring
- crane safety system
- work management and maintenance system
- maintenance of escape craft and escape routes.

The nominated testing and maintenance frequencies and required performance standards for these various systems should assure the performance and reliability assumed in the FSA (for example: regular testing of firewater pump systems).

The operator should demonstrate that the employees carrying out these activities have been adequately consulted as to their safety implications

Appendix – Acknowledgments

The Department of Industry, Science and Resources would like to thank the following people for their efforts in developing these guidelines.

Participants in the National Oil and Gas Safety Advisory Committee safety case review sub-group

Mr Murray West
Safety Case Engineer
Offshore Operations
Woodside Energy Ltd

Mr Chris Deluca
Risk Engineer
Department Minerals and Energy
Western Australia

Mr Glenn Jordan
Consultant
SysTec P/L
Victoria

Mr Dan Ahern
Occupational Health and safety Officer
Atwood Oceanics Australia P/L
Western Australia

Mr Eddie Knott
AMWU
Transfield Worley

Mr Gunther Gahleitner
Employee Rep

Ms Lucy Gentile
Petroleum Safety Engineer
Department of Mines and Energy
Northern Territory

Mr Geoff Donnes
Safety and Audit Co-ordinator
BHP Petroleum

Mr Colin Turner
State Counsellor
CEPU

Mr David Ffrench
Safety Health & Environment Manager (Former)
Esso Australia