Identification and management of environmental barriers
FOREWORD
DNV GL recommended practices contain sound engineering practice and guidance.

© DNV GL AS August 2015

Any comments may be sent by e-mail to rules@dnvgl.com
CHANGES – CURRENT

General
This is a new document.
CONTENTS

CHANGES – CURRENT .................................................................................................. 3

Sec.1  General ............................................................................................................ 5
  1.1  Introduction ................................................................................................. 5
  1.2  Objectives .................................................................................................... 5
  1.3  Scope ............................................................................................................. 6
  1.4  Application ................................................................................................... 7
  1.5  Structure of this recommended practice ................................................... 8
  1.6  Definitions and abbreviations ..................................................................... 8
  1.7  References ................................................................................................... 11

Sec.2  Methodology .................................................................................................... 13
  2.1  Stage 1 - establish context ......................................................................... 14
  2.2  Stage 2 - hazard identification ................................................................... 19
  2.3  Stage 3 - risk analysis and evaluation ...................................................... 20
  2.4  Stage 4 - risk management and identification of critical elements .......... 22
  2.5  Stage 5 - performance standards for SECEs and ECEs ......................... 27
  2.6  Stage 6 - design and operate .................................................................... 28
  2.7  Stage 7 - SECEs and ECEs assurance and verification ......................... 29

Sec.3  Documentation and update process ............................................................. 32
  3.1  Process documentation .............................................................................. 32
  3.2  Review and updating .................................................................................. 34

App. A  Examples of SECEs and ECEs ................................................................. 35
App. B  DNV GL guidance on defining a ‘barrier’ ............................................. 36
App. C  Example: MA (MEI potential) bow-tie diagram .................................... 39
App. D  Example: MPI bow-tie diagram ............................................................... 40
SECTION 1 GENERAL

1.1 Introduction

The US Chemical Safety and Hazard Investigation Board inquiry of the explosion and fire at the Macondo well which occurred in 2010 in the Gulf of Mexico highlighted "on the day of the April 20 tragedy, no effective safeguards were in place to eliminate or minimize the consequences of a process safety incident. The safeguards (or barriers) intended to prevent such a disaster were not properly constructed, tested, or maintained, or they had been removed. The management systems intended to ensure the required functionality, availability, and reliability of these safety critical barriers were inadequate. Ultimately, the barriers meant to prevent, mitigate, or control a blowout failed on the day of the accident." /1/

Following the Macondo accident, the European Commission (EC) undertook a review of safety and environmental risk management for offshore oil and gas operations in the European Union (EU). In 2013, the EC published the EU Directive 2013/30/EU on safety of offshore oil and gas operations (hereafter referred to as the EU offshore safety directive) /2/ which came into force in all relevant EU countries on the 19th July 2015. The objective of this Directive is to reduce as far as possible the occurrence of major accidents (MA) from offshore oil and gas operations and to limit their consequences. Operators of offshore installations are required to demonstrate that "all the major hazards have been identified, their likelihood and consequences assessed, including any environmental, meteorological and seabed limitations on safe operations and that their control measures including associated safety and environmental critical elements are suitable so as to reduce the risk of a major accident to an acceptable level"./2/

To date, whilst there is considerable experience within the offshore oil and gas industry of managing risks to people (i.e. safety risks) through the identification, definition and management of Safety Critical Elements (SCEs) there is no common approach for the management of the environmental risks using critical elements.

To assist industry, DNV GL has developed this recommended practice (RP) to describe the DNV GL recommended approach for the identification and management of major releases to the environment and their associated risks through the use of critical elements.

The EU Offshore Safety Directive requires only that a major environmental incident (MEI) be identified and controlled where it may result from a MA that has the potential to cause significant harm to people. It is also possible that a MEI could occur that does not have the potential to cause significant harm to people; DNV GL considers it good practice to also identify and manage these incidents even though they are not required by the scope of the EU Offshore Safety Directive. For clarity, this RP hereafter uses the following terms to help the reader to distinguish between the legislative requirements of the EU offshore safety directive and what DNV GL considers to be good practice:

— A major environmental incident (MEI) is preceded by a MA that has the potential to cause significant harm to people. For MEI, critical elements are termed safety and environmental critical elements (SECEs).
— A major pollution incident (MPI) is a MEI without a preceding MA. For MPI, critical elements are termed Environmental Critical Elements (ECEs).

The approach being recommended in this RP is the same for both MEI and MPI. The approach builds on and aligns with the existing approach used within the management of MA safety risk and is applicable to support compliance with the EU Offshore Safety Directive as well as in support of effective environmental risk management worldwide.

1.2 Objectives

The objectives of this RP are to:

1) Provide guidelines and good practice for identification of potential MEIs and MPIs on or in connection with offshore oil and gas installation operations, and the management of the associated environmental risks through the use of critical elements to prevent MEIs and MPIs from occurring and reduce the consequences should one occur.
2) Provide guidelines to assist offshore oil and gas installation operators to comply with the EU offshore safety directive in relation to MEIs.
1.3 Scope

With respect to harm to people and the environment, a MA is an incident that results in a level of damage to people and the environment that meets defined MA criteria. The MA criteria may vary around the world. The EU offshore safety directive defines a MA as:

a) an incident involving an explosion, fire, loss of well control, or release of oil, gas or dangerous substances involving, or with a significant potential to cause, fatalities or serious personal injury
b) an incident leading to serious damage to the installation or connected infrastructure involving, or with a significant potential to cause, fatalities or serious personal injury
c) any other incident leading to fatalities or serious injury to five or more persons who are on the offshore installation where the source of danger occurs or who are engaged in an offshore oil and gas operation in connection with the installation or connected infrastructure
d) any MEI resulting from incidents referred to in points (a), (b) and (c).

Criteria (a), (b) and (c) relate to harm to people and (d), which is conditional on (a), (b) or (c) being met, relates to harm to the environment. The EU offshore safety directive therefore places a duty on offshore operators to manage MEI risks only when the incidents have the potential to result from a MA that has significant potential to cause fatalities or serious personal injury.

In most situations, environmental incidents on or in connection with an offshore installation will have the potential to cause significant harm to people and will therefore be covered by the EU offshore safety directive. There may be situations for a major release to the environment to occur without the potential to cause harm to people (e.g. a large chemical spill to sea, or a large leak from the diesel transfer system or crude discharge system, or a large incident occurring outside the 500 m safety zone such as a large subsea pipeline leak). Such incidents (termed MPIs in this RP) would be outside the requirements of the EU offshore safety directive. DNV GL considers that it is good practice that the risks from both MEIs and MPIs are effectively managed.

This RP covers the identification and the use of critical elements in the management of environmental risk for both:

— MEIs that meet the EU offshore safety directive MA criteria (which are termed SECEs in the RP).
— MPIs which have potential for major environmental damage, but no potential for significant harm to people (which are termed ECEs in the RP).

This RP does not address the risk management of small polluting events or the breach of discharge limits in environmental permits.

Note: Organisations operating offshore installations will have a health, safety and environment (HS&E) risk management system and this RP assumes that the reader has a basic understanding of risk management principles. As such, this RP does not attempt to describe these, but focuses on the specific RP objectives. If the reader wishes to better understand the principles of risk management, DNV GL recommends International Organisation for Standardisation ISO 31000 Risk Management – Principles and Guidelines and ISO 17776 Petroleum and natural gas industries – Offshore production installations – Guidelines on tools and techniques for hazard identification and risk assessment which describes the framework for risk management and the systematic risk management process.

The scope of this RP is illustrated in Figure 1-1.
1.4 Application

Use and users of this RP

This RP applies to all existing and future offshore units, meaning any fixed or floating offshore installation or structure engaged in gas or oil exploration or production activities, loading or unloading of oil including drilling rigs, oil platforms, floating production, storage and offloading units (FPSOs), floating storage and offloading units (FSOs), subsea equipment, wells and associated pipelines.

The EU offshore safety directive is mandatory throughout Europe, and the methodology presented within this RP can be used to help meet the requirements of this Directive as transposed by each Member State through their national law.

This RP has been developed to be applicable also in non-European waters, and can be applied as good practice to control major environmental risks either in combination with safety risk management or where there is no major risk to people.

Anticipated users of this document include:

— offshore oil and gas exploration and production operators and their contractors
— regulators
— independent verification bodies/persons.

Alternative methods, the principle of equivalence

This document describes a practice recommended by DNV GL. This should not inhibit use of other alternative approaches meeting the overall objectives of the RP. Alternatives to detailed recommendations in this RP are acceptable when the approaches taken result in MEI and MPI risk management that is at least equivalent to that recommended in this RP. This also applies to requirements formulated in the verbal form “shall”.

Regulatory requirements

Regulatory requirements are, in the context of this RP, defined as requirements from legislative instruments relevant to offshore oil and gas activities, such as:

— internationally binding conventions/directives
— federal/national acts
— federal/national/state/province/local regulations
— terms and conditions of licenses and permits.

Regulatory requirements represent the minimum requirements to be complied with. Recommendations from this RP may be stricter or additional to regulatory requirements. In the case of contradiction or conflict between regulatory requirements and recommendations in this RP, regulatory requirements shall prevail.
Integration with safety risk management

The oil and gas industry has considerable experience in the management of MA safety risks through the use of SCEs, and can be referenced in the Assurance & Verification Practitioner’s Guide, *Managing Risks to prevent and minimise the impact of Major Accidents* [5]. This has resulted in well-established methodologies and routines for activities related to SCE management, including SCE identification, Performance Standard development, SCE maintenance, training, processes for safe operation, performance assurance and 3rd party verification activities.

It is recommended that the management of MEI and MPI should use, or at least align with, the approach used within risk management of MAs that have the potential to cause significant harm to people. This RP encourages companies to adapt and utilize existing practices with respect to using SCEs, expanded to cover MEI and MPIs with updated or new critical elements. Managing environmental risk through the use of critical elements should not be considered as an “add-on”, instead it should be considered as an opportunity to enhance the effectiveness of managing risks associated with operation of an offshore installation.

1.5 Structure of this recommended practice

Sec.2 describes the methodology for the identification of MEI and MPIs and the management of the environmental risks through relevant critical elements (SECEs and ECEs). This includes:

- establishing a context for the study
- the identification of MEI and MPI
- risk analysis and evaluation of MEI and MPI
- risk management and identification of SECEs and ECEs
- development of Performance Standards for the SECEs and ECEs
- assurance of SECEs and ECEs and independent verification of SECEs.

Sec.3 recommends how to document the process and reflect changes.

1.6 Definitions and abbreviations

Table 1-1 Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Barrier</td>
<td>Physical and/or non-physical means planned to prevent, control, and/or mitigate undesired incidents, events or accidents. Synonymous with Control or Safeguard</td>
<td>Commonly accepted definition by Skelt (2006) [6] See Appendix B DNV GL Guidance on Defining a ‘Barrier’</td>
</tr>
<tr>
<td>Bow-tie diagram</td>
<td>A diagram method for showing barriers that represents a risk management program guarding a major hazard from all its causes and potential consequences. It takes the visual form of a bow-tie as there are multiple causes and consequences, but all pass through a central top event. Barriers on the left side of the Top Event are known as preventive barriers and on the right are side as mitigation barriers.</td>
<td>The definition is specific to this RP. See Appendix B: DNV GL Guidance on Defining a ‘Barrier’</td>
</tr>
<tr>
<td>Environmentally critical elements (ECEs)</td>
<td>Means parts of an installation, including computer programs; (a) the purpose of which is to prevent or limit the effect of an MPI, or (b) the failure of which could cause or contribute substantially to an MPI.</td>
<td>The definition is specific to this RP.</td>
</tr>
</tbody>
</table>
Environmental damage means;
(a) damage to protected species and natural habitats, which is any damage that has significant adverse effects on reaching or maintaining the favourable conservation status of such habitats or species. The significance of such effects is to be assessed with reference to the baseline condition, taking account of the criteria set out in Annex I of this Directive;
(b) water damage, which is any damage that significantly adversely affects the ecological, chemical and/or quantitative status and/or ecological potential, as defined in Directive 2000/60/EC, of the waters concerned, with the exception of adverse effects where Article 4(7) of that Directive applies;
(c) land damage, which is any land contamination that creates a significant risk of human health being adversely affected as a result of the direct or indirect introduction, in, on or under land, of substances, preparations, organisms or micro-organisms”.

Environmental resource means natural resources, plants, or animals. This might include habitats or sensitive subgroups such as endangered plant and animal species.

Hazard means a source of potential harm.

Hazardous event means an accident or incident which occurs when a hazard is realized.

Major accident means, in relation to an installation or connected infrastructure:
(a) an event involving an explosion, fire, loss of well control or the release of oil, gas or dangerous substances causing, or with a significant potential to cause, fatalities or serious personal injury;
(b) an incident leading to serious damage to the installation or connected infrastructure involving, or with a significant potential to cause, fatalities or serious personal injury;
(c) any other incident leading to fatalities or serious injury to five or more persons who are on the offshore installation where the source of danger occurs or who are engaged in an offshore oil and gas operation in connection with the installation or connected infrastructure; or
(d) Any MEI resulting from incidents referred to in points (a), (b) and (c).

Major environmental incident (MEI) means an incident which results, or is likely to result, in significant adverse effects on the environment in accordance with Directive 2004/35/EC of the European Parliament and of the Council of 21 April 2004 on environmental liability with regard to the prevention and remedying of environmental damage.

Major pollution incident (MPI) means an incident which results, or is likely to result, in significant adverse effects on the environment in accordance with Directive 2004/35/EC of the European Parliament and of the Council of 21 April 2004 on environmental liability with regard to the prevention and remedying of environmental damage.

Performance standard means a statement, which can be expressed in qualitative or quantitative terms, of the performance required of a system, item of equipment, person or procedure, and which is used as the basis for managing the hazard – for example, planning, measuring, control or audit - through the lifecycle of the installation.

Recovery time means the time from an environmental incident occurs until the biological features have recovered to 99% of pre-spill state or to a new stable state taking into consideration natural ecological variations.

Risk management means coordinated activities to direct and control an organization with regard to risk.
Risk treatment

Process to modify risk, which can involve:
— avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk
— taking or increasing risk in order to pursue an opportunity
— removing the risk source
— changing the likelihood
— changing the consequences
— sharing the risk with another party or parties (including contracts and risk financing)
— retaining the risk by informed decision.

Risk treatments that deal with negative consequences are sometimes referred to as “risk mitigation”, “risk elimination”, “risk prevention” and “risk reduction”.

Safety critical elements

Means parts of an installation and such of its plant, (including computer programmes), or any part thereof-
(a) a purpose of which is to prevent or limit the effect of a major accident, or
(b) the failure of which could cause or contribute substantially to a major accident.

In the UK, all SCEs will become SECEs as per the Offshore Installations (Offshore Safety Directive) (Safety Case etc.) Regulations. This is the transposed requirements to be compliant with the EU Offshore Safety Directive from 19th July 2015.

Safety and environmental critical elements (SECEs)

Means parts of an installation, including computer programs;
(a) the purpose of which is to prevent or limit the effect of an MEI, or
(b) the failure of which could cause or contribute substantially to an MEI.

The definition is specific to this RP, derived from the definition for SCE’s

Table 1-1 Definitions (Continued)

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk treatment</td>
<td>Process to modify risk, which can involve:</td>
<td>ISO 31000</td>
</tr>
<tr>
<td></td>
<td>— avoiding the risk by deciding not to start or continue with the activity</td>
<td></td>
</tr>
<tr>
<td></td>
<td>that gives rise to the risk</td>
<td></td>
</tr>
<tr>
<td></td>
<td>— taking or increasing risk in order to pursue an opportunity</td>
<td></td>
</tr>
<tr>
<td></td>
<td>— removing the risk source</td>
<td></td>
</tr>
<tr>
<td></td>
<td>— changing the likelihood</td>
<td></td>
</tr>
<tr>
<td></td>
<td>— changing the consequences</td>
<td></td>
</tr>
<tr>
<td></td>
<td>— sharing the risk with another party or parties (including contracts</td>
<td></td>
</tr>
<tr>
<td></td>
<td>and risk financing)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>— retaining the risk by informed decision.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Risk treatments that deal with negative consequences are sometimes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>referred to as “risk mitigation”, “risk elimination”, “risk prevention”</td>
<td></td>
</tr>
<tr>
<td></td>
<td>and “risk reduction”.</td>
<td></td>
</tr>
<tr>
<td>Safety critical elements</td>
<td>Means parts of an installation and such of its plant, (including computer</td>
<td>Definition from the Offshore Installations (Safety Case) Regulations 2005, UK S.I. 2005/3117, 2005.</td>
</tr>
<tr>
<td></td>
<td>programmes), or any part thereof-(a) a purpose of which is to prevent</td>
<td></td>
</tr>
<tr>
<td></td>
<td>or limit the effect of a major accident, or (b) the failure of which</td>
<td></td>
</tr>
<tr>
<td></td>
<td>could cause or contribute substantially to a major accident.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In the UK, all SCEs will become SECEs as per the Offshore Installations</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Offshore Safety Directive) (Safety Case etc.) Regulations. This is the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>transposed requirements to be compliant with the EU Offshore Safety</td>
<td></td>
</tr>
<tr>
<td>Safety and environmental</td>
<td>Means parts of an installation, including computer programs; (a) the</td>
<td>The definition is specific to this RP, derived from the definition for</td>
</tr>
<tr>
<td>critical elements (SECEs)</td>
<td>purpose of which is to prevent or limit the effect of an MEI, or (b)</td>
<td>SCE’s</td>
</tr>
<tr>
<td></td>
<td>the failure of which could cause or contribute substantially to an MEI</td>
<td></td>
</tr>
</tbody>
</table>

Table 1-2 Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALARP</td>
<td>as low as reasonably practicable</td>
</tr>
<tr>
<td>BAP</td>
<td>UK Biodiversity Action Plan</td>
</tr>
<tr>
<td>CDOIF</td>
<td>Chemical and Downstream Oil Industries Forum</td>
</tr>
<tr>
<td>COMAH</td>
<td>control of major accident hazards</td>
</tr>
<tr>
<td>EC</td>
<td>European Commission</td>
</tr>
<tr>
<td>ECEs</td>
<td>environmental critical elements</td>
</tr>
<tr>
<td>EIA</td>
<td>environmental impact assessment</td>
</tr>
<tr>
<td>ENVID</td>
<td>environmental hazard identification</td>
</tr>
<tr>
<td>ERA</td>
<td>environmental risk analysis</td>
</tr>
<tr>
<td>ESA</td>
<td>environmentally sensitive area</td>
</tr>
<tr>
<td>FEED</td>
<td>front-end engineering and design</td>
</tr>
<tr>
<td>FPSO</td>
<td>floating production, storage and offloading unit</td>
</tr>
<tr>
<td>FSO</td>
<td>floating storage and offloading unit</td>
</tr>
<tr>
<td>HAZID</td>
<td>hazard identification</td>
</tr>
<tr>
<td>HS&amp;E</td>
<td>health, safety and environment</td>
</tr>
<tr>
<td>IOGP</td>
<td>International Association of Oil &amp; Gas Producers</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organisation for Standardization</td>
</tr>
<tr>
<td>KPI</td>
<td>key performance indicator</td>
</tr>
<tr>
<td>MA</td>
<td>major accident</td>
</tr>
<tr>
<td>MATTE</td>
<td>major accident to the environment</td>
</tr>
<tr>
<td>MEI</td>
<td>major environmental incident</td>
</tr>
<tr>
<td>MNR</td>
<td>Marine Nature Reserve</td>
</tr>
<tr>
<td>MOC</td>
<td>management of change</td>
</tr>
</tbody>
</table>
Verbal forms

For verification of compliance with this RP, the following definitions of the verbal forms, shall, should and may are applied:

Table 1-3 Verbal forms

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>shall</td>
<td>verbal form used to indicate requirements strictly to be followed in order to conform to this document</td>
</tr>
<tr>
<td>should</td>
<td>verbal form used to indicate that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required</td>
</tr>
<tr>
<td>may</td>
<td>verbal form used to indicate course of action permissible within the limits of the document</td>
</tr>
</tbody>
</table>

1.7 References


SECTION 2 METHODOLOGY

The methodology recommended for the effective management of MEI and MPIs is shown in a process diagram in Figure 2-1. The diagram shows the process for compliance with the EU offshore safety directive where only MEIs which have a potential to cause a major risk to people need to be considered, as well as the additional activities to manage any MPIs.

The recommended process, which aligns with existing safety risk management practice, consists of the following key stages:

Stage 1. Establish context for MEI and MPI risk management
Stage 2. Hazard identification, including identification of MEI and MPIs
Stage 3. Risk analysis and evaluation (consequence and likelihood analysis)
Stage 4. Risk management and identification of critical elements
Stage 5. Development of performance standards for critical elements
Stage 6. Lifecycle management of critical elements
Stage 7. Assurance and verification of critical element performance

Each of these stages is discussed separately in the following sub-sections.
2.1 Stage 1 - establish context

Main objectives

The main objective of Stage 1 is to define the guiding parameters for the risk management process including objectives, boundaries, methods, responsibilities, deliveries and execution, and to set the scope and criteria for the process. The context may include both parameters related to the internal context (anything within the organization that may influence the process) and the external context (anything outside the organization that may influence the process).
For environmental risk management key requirements in setting the context are to:

- define the criteria for what constitutes a MEI and MPI which is an essential input to the hazard identification exercise where all potential releases will be identified and evaluated, and
- prepare for the hazard identification by establishing inventory of hazardous materials and overview of local environment, and
- set the environmental risk acceptance/tolerability criteria that will be used in risk evaluation.

**Recommended method**

*Defining the criteria for what constitutes an MEI and MPI*

For European waters, the EU Offshore Safety Directive states that a “major environmental incident means an incident which results, or is likely to result, in significant adverse effects on the environment in accordance with Directive 2004/35/EC of the European Parliament and of the Council of 21 April 2004 on environmental liability with regard to the prevention and remediying of environmental damage.”

According to Directive 2004/35/EC /7/ environmental damage means a measurable adverse change and damage to;

- protected species and natural habitats, affecting significantly the favourable conservation status of such habitats or species, or;
- water, which is any damage that significantly adversely affects the ecological, chemical and/or quantitative status and/or ecological potential of the water, or;
- land, which is any land contamination that creates a significant risk of human health being adversely affected.

Protected species and natural habitats shall refer to species and natural habitats protected under the 1992 Habitats Directive¹ /8/ and the 1979 Wild Birds Directive² /9/. Additional species and habitats that are specified in national regulations shall also be considered.

According to Annex 1 of Directive 2004/35/EC the significance of adverse effects can be determined by reference to the individuals/habitat size affected, the rarity of species/habitat impacted, or the species/habitat capacity to recover/propagate/regenerate. Damage with a proven effect on human health shall always be classified as significant damage. Negative variations that are smaller than natural variations or damage to species or habitats that will recover without intervention within a short time are not classified as significant.

Currently there is no clear definition of the level of significant adverse effects that correspond to MEI, and there is no good practice established in this field for offshore exploration and production. But, the criteria for what constitutes a MEI shall be developed in line with Directive 2004/35/EC, local HSE regulations and company requirements and practices. The criteria should be developed to be compatible with the environmental risk acceptance/tolerability criteria of the operator. The criteria for what constitutes MPI should be the same as for defining MEI.

Lacking good practice in offshore exploration and production, good practice in other industries may provide guidance. The Seveso III Directive /10/ which is the basis for the Control of Major Accident Hazards (COMAH) regulations in the UK /11/ also refers to Directive 2004/35/EC for evaluation of environmental damage. The 2015 COMAH Regulations aim to prevent and mitigate major environmental incidents that can result in a major accident to the environment (MATTE) /11/. Good practice for setting criteria for what constitutes MATTEs by receptor type, has been documented in the Chemical and Downstream Oil Industries Forum (CDOIF) guideline *Environmental Risk Tolerability for COMAH Establishments*, Appendix 4 – MATTE tolerability tables /12/. The criteria by receptor type are combined with criteria for recovery time to identify MATTEs. The criteria for what constitutes MATTEs could be used as the basis for establishing criteria for what constitutes a MEI and MPI (see Table 2-1).

¹ Covers all local species listed in Annex II and IV, and habitats listed in Annex I. Also covers breeding sites or resting places of the species needing strict protection as listed in Annex IV.

² Covers all local species mentioned in Annex I and their habitats; migratory species (breeding, moulting, wintering areas and staging posts along their migration routes) with special focus on wetlands.
Environmental damage or consequence can also be assessed only based on evaluation of the recovery time of environmental receptors. In this case it is recommended to focus on protected species and natural habitats as defined in Directive 2004/35/EC/[7], but include criteria for their presence and importance in the exposed area (see example below).

An example of the interpretation of the severity of the environmental incidents and the corresponding environmental consequences in recovery time for protected species and habitats is shown in the table below. MEI and MPI are expected to represent a severity 3 or 4 incident. This would mean that the criteria for what constitutes a MEI and MPI are an incident that can lead to environmental damage with recovery time of 1-3 years or more.

<table>
<thead>
<tr>
<th>Environmental Incident</th>
<th>Corresponding Damages (Recovery Time)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity 1</td>
<td>&lt; 1 month</td>
</tr>
<tr>
<td>Severity 2</td>
<td>1 month - 1 year</td>
</tr>
<tr>
<td>Severity 3</td>
<td>1-3 years</td>
</tr>
<tr>
<td>Severity 4</td>
<td>3-10 years</td>
</tr>
<tr>
<td>Severity 5</td>
<td>&gt; 10 years</td>
</tr>
</tbody>
</table>

When evaluating the recovery time of protected species or habitats the following criteria for their presence and importance could apply:

- have a significant presence in the exposed area, and
- be sensitive to the relevant hazardous substance, and
- be important to local human populations, or
- have a national or international interest, or
- have ecological importance.

Such criteria can avoid focus on solitary animals, fringe populations or habitats with no ecological importance.
Table 2-1 Examples of severity/harm criteria for what constitutes a major accident to the environment for COMAH establishments /12/. The criteria are used together with criteria for recovery time of the receptor type

<table>
<thead>
<tr>
<th>Receptor Type</th>
<th>Severity of Harm (1)</th>
<th>Severity Level</th>
<th>Comments (2)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Significant</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>While this level of</td>
<td>2</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>harm might be</td>
<td>3</td>
<td>NNR, SSSI, MNR, MPA</td>
</tr>
<tr>
<td></td>
<td>considered to be</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td></td>
<td>not considered a</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MATTE.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Severe</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DETR Criteria – the</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>lowest level of harm</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>that might be</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>considered MATTE.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Major</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>&gt;50% of site area,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>associated linear</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>feature or</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>population</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Catastrophic</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>&gt;50% of site area,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>associated linear</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>feature or</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>population</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Receptors include:

- Designated Land/ Water Sites (Nationally important): <0.5ha or <10% of site area, associated linear feature or population.
- Designated Land/ Water Sites (Internationally important): <0.5ha or <5% (<5% LF/Pop) of site area or 5-25% of associated linear feature or population.
- Scarce Marine Habitat: <2ha or <10% of habitat.
- Marine: <2ha littoral or sub-littoral zone, <100ha of open sea benthic community, <100 dead sea birds (<500 gulls), <5 dead/significantly impaired sea mammals.
- Fresh and estuarine water habitats: Impact below that of Severity level 2.

1) Littoral: pertaining to the shore of a lake, sea, or ocean; Sub-littoral zone: from the low water line to the edge of the continental shelf Benthic community: is made up of organisms that live in and on the bottom of the ocean floor.

Establish inventory of hazardous materials and overview of local environment

As a part of establishing the context for the management of MEI and MPI, an inventory of materials that are hazardous to the environment should be developed for the activity or operations that are being assessed.

In addition a good understanding of the local environmental receptors and their distribution and sensitivity should be established. This information will in most cases be documented in the Environmental Impact Assessment (EIA) that should be available for the activity1).

1) In the UK, oil pollution emergency plans (OPEPs) (that have been developed according to the 2015 DECC Guidance Notes for Preparing Oil Pollution Emergency Plans) shall include an inventory of oil, and the information which is necessary to establish a good overview of the local environmental resources and their distribution and sensitivity. This may be another source of information.

The inventory of materials and the overview of local environmental receptors is a prerequisite for the identification of MEI and MPI during hazard identification in Stage 2. It follows that the potential environmental consequences of a spill or release can vary depending on:
— the characteristics and toxicity of the substance being released
— the type and sensitivity of environmental receptors
— the distance from the location of the spill / incident to the environmental receptor(s)
— the degradation or dispersion of harmful substance in the environment
— the prevailing ocean currents, and the metrological and climatic conditions.

The location of the environmental incident may be just as critical as the release itself, because if a substance is accidentally released near to shore or in a MPA, the extent of environmental consequences may be significantly greater than if the same substance is accidentally released 150km offshore in a non-sensitive marine environment (not withstanding that there will be an environmental consequence in the latter example as well).

**Setting environmental risk acceptance/tolerability criteria**

The organization should define criteria to be used to evaluate the significance of environmental risk. The criteria can be imposed by, or derived from, legal and regulatory requirements. Environmental risk criteria need to be consistent with the organisation’s risk management policy and other risk criteria.

When defining environmental risk criteria, factors to be considered should include the following:

— the nature and types of causes and consequences that can occur and how they will be measured
— the criteria for what constitutes a MEI and MPI
— how likelihood will be defined
— the timeframe(s) of the likelihood and/or consequence(s)
— how the level of risk is to be determined
— the views of stakeholders
— the level at which risk becomes acceptable or tolerable
— whether combinations of multiple risks should be taken into account and, if so, how and which combinations should be considered.

The risk criteria should as far as possible:

— be suitable for evaluation of the facility, activity or operations in question
— be suitable for comparison with the results of the assessment to be performed
— be suitable for decisions regarding risk reducing measures
— be suitable for communication
— be unambiguous in their formulation (such that they do not require extensive interpretation or adaptation for a specific application)
— not favour any particular concept solution explicitly nor implicitly through the way in which risk is expressed.

Environmental risk acceptance/tolerability criteria can be quantitative or qualitative. The criteria can be defined for facilities, specific activities or larger operations. More than one type of risk acceptance criteria can be established to be able to cover several analytical endpoints.

Environmental risk acceptance/tolerability criteria should include likelihood of exposure (combination of likelihood of release and likelihood of exposure of the environmental receptor) that results in defined environmental consequences. Environmental consequences should be defined based on the same type of consequences that are used for evaluating MEI and MPI, for example, consequences for species or habitats, degree of exposure of areas of a certain environmental sensitivity, and recovery time.

**Main results**

The main output from stage 1 will be a defined clear basis and terms of reference for managing environmental risks, including criteria for what constitutes a MEI and MPI, and acceptance/tolerability criteria for evaluating the environmental risk. In addition stage 1 provides for the hazard identification process and the identification of MEI and MPIs through establishing an inventory of materials that are hazardous to the environment, and establishing a good understanding of the local environmental receptors and their sensitivity.
2.2 Stage 2 - hazard identification

Main objectives

The main objectives of Stage 2 are:

— identify hazards with the potential to create an MEI and MPI
— identify characteristics of MEIs and MPIs (e.g. spill volume, fluid type)
— identify risk management measures.

Recommended method

The hazard identification process and procedures should be documented and consistent with ISO 31000 on Risk Management.

Identifying environmental hazards may be carried out in isolation in the form of an Environmental Hazard Identification (ENVID) workshop or in conjunction with the safety hazard identification (HAZID) workshop. A combined HAZID and ENVID workshop is recommended as it allows integration of safety and environmental risk management discussion which is a beneficial approach in most instances.

People with appropriate background and knowledge should be involved in hazard identification. For identification of MEI and MPIs this will include people with environmental competence, and an overview of the local environmental receptors and their sensitivity. Expert judgment is essential to the identification of hazards, however for novel systems or new environments, care should be taken in directly applying past experience.

Typically the HAZID-ENVID examines the installation methodically and systematically using guidewords, checklists and question-sets to ensure a suitably robust process is undertaken. All events or combination of events deemed credible with the potential to lead to a MA shall to be identified.

Environmental hazardous events to be identified may include, but are not limited to:

— spills/releases due to well leak or blowout
— spills/releases from ruptured or leaking flow-lines, pipelines, risers and/or subsea process equipment
— loss of containment, for example, spills from storage facilities or offloading/transfer
— spills/releases due to ship collision or collapse of the installation
— spills/releases from topside processing systems or utilities
— spills/releases during bunkering or fuelling operations.

For the identified events, the characteristics should be identified. These include the magnitude (e.g. the volume of a spill, release rate and duration), and the properties (e.g. contents of spill, toxicity etc.).

For the identified events the planned or existing risk management measures should also be identified. Potential additional measures may be identified. Identification of the measures should include all the physical (e.g. shields, isolation, separation, protective devices, etc.) and non-physical (e.g. procedures, alarm systems, training, drills, etc.) measures to prevent, detect, control and mitigate a hazardous event. Measures identified during Stage 2 Hazard Identification will be further analysed in Stage 4 Risk Management.

All hazards where it is reasonably foreseeable for an MEI and MPI to occur need to be included in Stage 3 Risk Analysis. Some examples of hazards that may cause potential MEI and MPI are shown in Table 2-2.
Main results

The main output from Stage 2 Hazard Identification will be a register of all reasonably foreseeable hazardous events including associated characteristics and risk management measures that meet the defined criteria for MA, including MEIs and MPIs. For strict compliance with the EU Offshore Safety Directive there is no need to include MPIs in the register. However, it is recommended to include MPI in order that the risk from such events can be managed effectively through the processes used for MA events.

2.3 Stage 3 - risk analysis and evaluation

Main objectives

The main objectives of Stage 3 are:

— examine the consequences and likelihoods of the potential MEI and MPI identified in Stage 2
— compare the results of MEI and MPI risk analysis with operator risk acceptance/tolerability criteria to determine whether the risk level is tolerable (i.e. below defined acceptable levels).

Recommended method

The risk analysis and evaluation process and procedures should be documented and consistent with ISO 31000 on Risk Management /3/. According to ISO 31000 the risk analysis and evaluation stage involves developing an understanding of the risk, provides an input to decisions on whether risks need to be reduced, and the most appropriate risk reduction strategies and methods. Existing risk reducing measures and their effectiveness and efficiency should also be taken into account.

The risk analysis can be qualitative, semi-quantitative or quantitative, or a combination of these, depending on the circumstances.

Consequence analysis

The environmental consequence analysis for hydrocarbon releases should be performed in line with the International Association of Oil & Gas Producers (IOGP) 2013 Guideline on oil spill risk assessment and response planning for offshore installations /13/. Examples of both qualitative and quantitative analysis are given in the appendix of the IOGP guideline.

For releases of harmful substances to the environment other than hydrocarbons (e.g. chemical spills), the main principles of risk analysis in the IOGP guideline should be applied.

Analysis of environmental consequences should, as a minimum, be based on the sensitivity of the environmental receptors, the toxicity and characteristics of the hazardous substance, and the potential exposure to the hazardous substance. The consequences can be determined by modelling or by extrapolation from experimental studies, historical events or other available data for the relevant hazardous substances.

---

Table 2-2 Example of activities, related potential events and their likely categorisation into potential MEI, MPI or less significant incident ¹

<table>
<thead>
<tr>
<th>Activity</th>
<th>Event</th>
<th>Potential MEI, MPI or less significant incident*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drilling/Well operations</td>
<td>Blowout</td>
<td>MEI</td>
</tr>
<tr>
<td>Import of well stream fluids</td>
<td>Large leak from riser</td>
<td>MEI</td>
</tr>
<tr>
<td>Export of pressurised oil</td>
<td>Large leak from oil export riser subsea</td>
<td>MPI</td>
</tr>
<tr>
<td>Transfer and storage of diesel or methanol</td>
<td>Large leak from diesel or methanol storage tanks</td>
<td>MEI</td>
</tr>
<tr>
<td></td>
<td>Large spill of diesel or methanol into sea during bunkering</td>
<td>MPI</td>
</tr>
<tr>
<td>Use of hydraulic oil</td>
<td>Large leak from hydraulic hose</td>
<td>MPI</td>
</tr>
<tr>
<td>Use of cleaning agent</td>
<td>Minor spill of cleaning agent</td>
<td>Less significant incident</td>
</tr>
</tbody>
</table>

¹ The potential environmental consequences of an environmental hazard can vary depending on the type and sensitivity of environmental resources, the distance from the location of the spill / incident to the environmental resource(s), and the behavior of pollutants in the environment. Thus the same incident could be deemed major at one location but not at another.

* The MEIs, MPIs and less significant incidents presented above are examples and may vary from installation to installation.
The analysis of environmental consequences shall include evaluations against the criteria for what constitutes a MEI and MPI (see [2.1]).

The consequence analysis could include dispersion, or fate and trajectory modelling of the released substance. The modelling output should reflect local metrological and oceanographic data (e.g. currents and wind), and climatic conditions to provide input to the location specific environmental consequences.

According to Directive 2004/35/EC environmental damage means a measurable adverse change and damage to protected species or habitats, water or land, as described and further defined in [2.1]. Thus, to evaluate the environmental consequences of MEI and MPI, the spatial and temporal distribution of the relevant local environmental receptors must be mapped within the exposed area, and their sensitivity to the spilled substance evaluated. EIA and monitoring data can provide valuable input to the detailed mapping and sensitivity evaluation of resources.

Impact indicators should be selected to perform the consequence analysis. This means that a limited number of receptors are selected among the environmental receptors, and used to categorise or quantify the consequences. The impact indicators should be selected based on the sensitivity evaluation and other pre-defined criteria for this purpose.

**Likelihood analysis**

Likelihood may be quantitative (e.g. an accidental release of 100 m3 of diesel to the marine environment during bunkering operations is likely to happen once every ‘X’ years) or qualitative (e.g. by replacing numbers with words such as frequent, unlikely, rare).

Likelihood may be assigned either during the HAZID-ENVID (if the appropriate expertise is present) or thereafter. The likelihood of MEI and MPI may have been determined in existing safety studies for the same activity or operations. If this is the case, this information should be used and built on. Experience from relevant historical events may be applied in the likelihood analysis. In particular, failure and accident data may be applied to establish the likelihood of hazardous events. It should be ensured that the data is representative for the events being analysed.

Thus, the likelihood of MEI and MPI can be based on:

- expert judgment, or
- information available in safety studies, for example the Quantitative Risk Assessment (QRA), or
- information available from recognized databases and models.

Recognized sources of data should be used wherever possible. When no data are available, or where the data are uncertain, assumptions may be applied. In this case, conservative values should be applied (i.e. leading to higher level of risk), or the uncertainty should be reflected in the results of the risk analysis.

Whichever method is used to analyse the likelihood of hazardous events, the outcome should be an ascribed likelihood value or likelihood category which can be used in the risk analysis. The likelihood of the environmental consequences should reflect the combined likelihood for the environmental hazardous event and the likelihood of exposure of the environmental receptors given a release or incident.

**Risk evaluation**

Risk evaluation within the risk assessment process involves comparing the level of risk found during the analysis process with the risk criteria established when the context was defined. Based on this comparison, the risk acceptance/tolerability can be evaluated and the need for risk reduction can be considered.

As a minimum the risk of each hazardous event should be presented in a risk matrix, and the risk results should be presented so that the results can be easily compared with the environmental risk acceptance/tolerability criteria.

In some circumstances, the risk evaluation can lead to a decision to undertake further analysis (e.g. refinement of input data and more detailed environmental consequence analysis). The risk evaluation can also lead to a decision not to reduce the risk in any way other than maintaining existing risk reducing measures.
Main results

The main results of Stage 3 are the environmental risk picture of the activity or operation, showing the likelihood and environmental consequences of MEIs and MPIs, and the risk level compared with the risk acceptance/tolerability criteria. This should provide an understanding of the magnitude, profile and drivers for environmental risks.

The risk analysis should also allow for a good understanding of the effect of existing risk reducing measures, and for the development of the most appropriate risk reduction strategies and methods.

2.4 Stage 4 - risk management and identification of critical elements

Main objectives

The main objectives of Stage 4 are to:

— Manage MEI and MPI risks through the application of relevant good practice and the implementation of additional risk management to a level that is tolerable for the operator and regulator, and As Low As Reasonably Practicable (ALARP).

— Identify all critical elements (i.e. identify SECEs and ECEs of the risk management measures that are required to function to effectively manage the MEI and MPI risks).

Recommended method

Risk management strategies

When deciding the strategy to be adopted to manage the major risks the following should be recognised:

— that prevention is better than protection

— that risk management measures are rarely perfect

— multiple risk management measures are usually better than only a few

— passive systems are more reliable than active ones which, in turn, are more reliable than those dependent on human operational intervention, with systems dependent on vigilance of an external party being least reliable of all

— the potential for extreme events.

A systematic approach of risk management at source should be applied to each MEI and MPI. This should adopt a hierarchical approach to risk management as follows (in priority order):

1) eliminate the hazard
2) substitute the hazard for a less hazardous one
3) minimise the likelihood by eliminating some causes and reducing the probability of others (Prevention)
4) minimise the severity of the hazards and their potential to cause harm or escalate (Control)
5) minimise the exposure of recipients and critical plant to the effects of any initiating events (Mitigation and Emergency Response).

Relevant industry good practice for managing risks should form the basis of risk management. "Good practice" is defined within industry reference sources such as codes, standards, RP's and industry guidance documents that the relevant regulator has judged and recognised as satisfying the law, when applied in an appropriate manner.

Where there is relevant, recognised good practice, it is recommended that it is followed and if not, that a robust demonstration is made that the practice proposed to be used is at least as effective in managing the risk. Where there is no relevant good practice, good practice should be followed as far as it can be, and then consideration given to whether there is more that can be done to reduce the risk.

A progressive approach to risk management should be adopted, giving attention first to those measures which have greatest effect in risk reduction for least effort. The effectiveness of risk management measures can be evaluated qualitatively by expert judgement or through re-analysing and evaluation of the risk as
detailed in Stage 3. Successive evaluations of risk reducing measures are undertaken until a point is reached where all the risk acceptance criteria have been satisfied and no further risk reduction is reasonable to implement when considered against the benefit likely to be achieved.

ALARP Concept

It is recommended that the concept of reducing and maintaining risk to a level that is tolerable and ALARP is used. The ALARP process provides a robust, systematic and auditable process to manage risks down to, and maintain them at, an acceptable level. Fundamental features of the ALARP process are presented in Table 2-3 with the process illustrated in Figure 2-2.

Table 2-3  Fundamental features of the ALARP process

<table>
<thead>
<tr>
<th>Feature</th>
<th>RP Stage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk tolerability and acceptance criteria are set by the organisation (e.g. offshore installation operator) based on regulatory, company and society requirements.</td>
<td>1</td>
</tr>
<tr>
<td>Criteria to assess whether it is reasonable (in terms of cost, time, effort, resources, etc.) to implement practicable (i.e. physically possible) risk reduction are set by the organisation.</td>
<td>1</td>
</tr>
<tr>
<td>All reasonably foreseeable hazards are identified and adequately assessed to understand the risk profile and risk drivers.</td>
<td>2 and 3</td>
</tr>
<tr>
<td>Checking that all relevant good practice has been followed or implemented appropriately to establish the basis for risk management.</td>
<td>4</td>
</tr>
<tr>
<td>If hazard risks cannot be reduced to meet the tolerability criteria then the operation or activity that creates or significantly contributes to the intolerable risk level will not be permitted.</td>
<td>4</td>
</tr>
<tr>
<td>Even when the risks are considered tolerable there is a requirement to continue to look for additional, practicable, risk reduction and to adopt it if it is not unreasonable to do so (i.e. adopt risk reduction unless it can be demonstrated that the sacrifice - cost, time and effort - of implementing it is grossly disproportionate to the risk reduction that it delivers).</td>
<td>4</td>
</tr>
<tr>
<td>Critical risk management measures both physical and procedural that are key to the effective management of hazard risk are identified and an acceptable minimum level of performance for each element defined in a Performance Standard.</td>
<td>4 and 5</td>
</tr>
<tr>
<td>The critical risk management measures are designed, commissioned and maintained to deliver the specified level of performance.</td>
<td>6</td>
</tr>
<tr>
<td>Inspection, testing and other assurance and verification processes are undertaken to ensure that the critical risk management measures are working as intended to meet their defined Performance Standard.</td>
<td>7</td>
</tr>
<tr>
<td>There is a periodic cycle of review to ensure hazards, risks and risk management remain well understood, that changes in relevant good practice are acted upon, and that the risks are maintained at a demonstrable ALARP level throughout the lifecycle of the operation or installation.</td>
<td>-</td>
</tr>
</tbody>
</table>
Figure 2-2 Risk management ALARP process

For hazards that pose both safety and environment risks, an integrated risk management approach should be taken to ensure that the influence on the risks from risk management can be fully understood.

Measures that aim to eliminate or prevent a hazardous event from occurring will have a combined benefit of reducing both the safety and environmental risks. There will be a stronger justification for implementing such measures when both the safety and environmental benefits are combined. Measures that contribute to reducing risks after the initiation of an event may result in a risk reduction for both safety and environment, a risk reduction for only one of these aspects, or have an opposing influence, reducing the risk for one aspect whilst increasing the risk for the other.

Table 2-4 gives examples of risk reduction measures and their likely influence on safety and environment risks.
Where risk management measures may result in an opposing influence on safety and environmental risk, careful consideration shall be required to determine the most appropriate and acceptable balance in risk. There may be a requirement for additional specific risk management measures to be considered to reduce a consequential risk increase created from implementation of a measure. The selection of risk management measures and the process to follow when a measure may have an opposing influence on safety and environmental risk levels needs to be documented within an organization’s risk management procedures.

Barrier analysis

Risk management measures that play a critical role in the management of MEI and MPI risks can be identified through various approaches. In many cases, conforming to recognised good practice will result in effective risk management. Where good practice is not relevant or in more complex situations QRA approaches may be used in the identification of risk reduction. It is recommended that unless there is a suitable alternative (e.g. a QRA), barrier analysis using barrier diagrams (e.g. bow-tie) should be undertaken to identify risk management measures (i.e. barriers).

A bow-tie is a simple graphical tool to identify the potential causes and consequences together with the relative barriers in place to prevent the event and mitigate its possible outcomes. Figure 2-3 below illustrates an example of a bow-tie.

The objective of bow-tie analysis is to identify the barriers that allow these hazards to be effectively managed such that they can be assessed for tolerability and reduced to ALARP. This might involve assessing the risk reduction delivered by barriers and if necessary improving the effectiveness of existing barriers or adding more barriers.

<table>
<thead>
<tr>
<th>Category</th>
<th>Risk Reduction Measure</th>
<th>Influence on Risk</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Safety</td>
<td>Env</td>
</tr>
<tr>
<td>Prevention</td>
<td>Structural integrity</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Prevention</td>
<td>Ship radar system</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Prevention</td>
<td>Impact protection on oil export pipeline</td>
<td>None</td>
<td>+</td>
</tr>
<tr>
<td>Control</td>
<td>Emergency shutdown system</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Control</td>
<td>Plated deck bunds</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Control</td>
<td>Grated deck</td>
<td>+</td>
<td>-</td>
</tr>
<tr>
<td>Control</td>
<td>Fire water deck drains</td>
<td>+</td>
<td>-</td>
</tr>
<tr>
<td>Mitigate</td>
<td>Passive fire protection on key structural members</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Mitigate</td>
<td>Escape routes, emergency lighting, protected muster point</td>
<td>+</td>
<td>Low</td>
</tr>
<tr>
<td>Mitigate</td>
<td>Lifeboats, life rafts, personal protective equipment</td>
<td>+</td>
<td>None</td>
</tr>
</tbody>
</table>

Table 2-4 Examples of risk reduction measures and risk benefit for safety and environment
A barrier is a physical and/or non-physical means to prevent, control, and/or mitigate undesired events or accidents. It is important that a barrier is clearly defined. Guidance on barrier definition as well as on DNV GL’s recommended approach to barrier analysis is contained within App.B.

Barrier analysis identifies functions related to each barrier system and the elements or procedures necessary to fulfil the function (sub-function can also be established where this is found necessary):

— Barrier Function (what the barrier aims to do, e.g. prevent leaks).
— Barrier System (what device completes the function, e.g. leak detection system).
— Barrier Elements (e.g. the individual parts of the leak detection system including the leak detection equipment).

When considering additional risk reduction barriers, in addition to the hierarchy of risk reduction previously detailed, the following, in priority order, should also be considered:

1) Passive hardware barriers.
2) Active hardware barriers.
3) Administrative or procedural barriers.

Hardware barriers should be considered before procedural barriers as they are likely to be more effective and reliable (assuming that they are well designed and maintained).

The barrier analysis should ideally be visualized in barrier diagrams. A bow-tie diagram is the preferred means of such documentation, but other equivalent means are acceptable. Bow-ties may be presented with different levels of detail.

Effective risk management requires complete and fully functioning barriers to be identified and defined. A complete barrier will be formed by a number of barrier systems or elements, which collectively deliver the required function of the risk reduction measure. It is recommended, to be meaningful, that barriers shown on bow-ties should be complete and fully functioning barriers with each system or element that delivers all or part of a barrier function also being shown. Systems may be hardware or procedural and generally would include several barrier elements that collectively deliver the system objective (e.g. “emergency shutdown system”, “bund”, “emergency response procedures”).

**Figure 2-3  Example of a bow-tie diagram**

A barrier is a physical and/or non-physical means to prevent, control, and/or mitigate undesired events or accidents. It is important that a barrier is clearly defined. Guidance on barrier definition as well as on DNV GL’s recommended approach to barrier analysis is contained within App.B.

Barrier analysis identifies functions related to each barrier system and the elements or procedures necessary to fulfil the function (sub-function can also be established where this is found necessary):

— Barrier Function (what the barrier aims to do, e.g. prevent leaks).
— Barrier System (what device completes the function, e.g. leak detection system).
— Barrier Elements (e.g. the individual parts of the leak detection system including the leak detection equipment).

When considering additional risk reduction barriers, in addition to the hierarchy of risk reduction previously detailed, the following, in priority order, should also be considered:

1) Passive hardware barriers.
2) Active hardware barriers.
3) Administrative or procedural barriers.

Hardware barriers should be considered before procedural barriers as they are likely to be more effective and reliable (assuming that they are well designed and maintained).

The barrier analysis should ideally be visualized in barrier diagrams. A bow-tie diagram is the preferred means of such documentation, but other equivalent means are acceptable. Bow-ties may be presented with different levels of detail.

Effective risk management requires complete and fully functioning barriers to be identified and defined. A complete barrier will be formed by a number of barrier systems or elements, which collectively deliver the required function of the risk reduction measure. It is recommended, to be meaningful, that barriers shown on bow-ties should be complete and fully functioning barriers with each system or element that delivers all or part of a barrier function also being shown. Systems may be hardware or procedural and generally would include several barrier elements that collectively deliver the system objective (e.g. “emergency shutdown system”, “bund”, “emergency response procedures”).

**Figure 2-3  Example of a bow-tie diagram**

A barrier is a physical and/or non-physical means to prevent, control, and/or mitigate undesired events or accidents. It is important that a barrier is clearly defined. Guidance on barrier definition as well as on DNV GL’s recommended approach to barrier analysis is contained within App.B.

Barrier analysis identifies functions related to each barrier system and the elements or procedures necessary to fulfil the function (sub-function can also be established where this is found necessary):

— Barrier Function (what the barrier aims to do, e.g. prevent leaks).
— Barrier System (what device completes the function, e.g. leak detection system).
— Barrier Elements (e.g. the individual parts of the leak detection system including the leak detection equipment).

When considering additional risk reduction barriers, in addition to the hierarchy of risk reduction previously detailed, the following, in priority order, should also be considered:

1) Passive hardware barriers.
2) Active hardware barriers.
3) Administrative or procedural barriers.

Hardware barriers should be considered before procedural barriers as they are likely to be more effective and reliable (assuming that they are well designed and maintained).

The barrier analysis should ideally be visualized in barrier diagrams. A bow-tie diagram is the preferred means of such documentation, but other equivalent means are acceptable. Bow-ties may be presented with different levels of detail.

Effective risk management requires complete and fully functioning barriers to be identified and defined. A complete barrier will be formed by a number of barrier systems or elements, which collectively deliver the required function of the risk reduction measure. It is recommended, to be meaningful, that barriers shown on bow-ties should be complete and fully functioning barriers with each system or element that delivers all or part of a barrier function also being shown. Systems may be hardware or procedural and generally would include several barrier elements that collectively deliver the system objective (e.g. “emergency shutdown system”, “bund”, “emergency response procedures”).

**Figure 2-3  Example of a bow-tie diagram**

A barrier is a physical and/or non-physical means to prevent, control, and/or mitigate undesired events or accidents. It is important that a barrier is clearly defined. Guidance on barrier definition as well as on DNV GL’s recommended approach to barrier analysis is contained within App.B.

Barrier analysis identifies functions related to each barrier system and the elements or procedures necessary to fulfil the function (sub-function can also be established where this is found necessary):

— Barrier Function (what the barrier aims to do, e.g. prevent leaks).
— Barrier System (what device completes the function, e.g. leak detection system).
— Barrier Elements (e.g. the individual parts of the leak detection system including the leak detection equipment).

When considering additional risk reduction barriers, in addition to the hierarchy of risk reduction previously detailed, the following, in priority order, should also be considered:

1) Passive hardware barriers.
2) Active hardware barriers.
3) Administrative or procedural barriers.

Hardware barriers should be considered before procedural barriers as they are likely to be more effective and reliable (assuming that they are well designed and maintained).

The barrier analysis should ideally be visualized in barrier diagrams. A bow-tie diagram is the preferred means of such documentation, but other equivalent means are acceptable. Bow-ties may be presented with different levels of detail.

Effective risk management requires complete and fully functioning barriers to be identified and defined. A complete barrier will be formed by a number of barrier systems or elements, which collectively deliver the required function of the risk reduction measure. It is recommended, to be meaningful, that barriers shown on bow-ties should be complete and fully functioning barriers with each system or element that delivers all or part of a barrier function also being shown. Systems may be hardware or procedural and generally would include several barrier elements that collectively deliver the system objective (e.g. “emergency shutdown system”, “bund”, “emergency response procedures”).

**Figure 2-3  Example of a bow-tie diagram**

A barrier is a physical and/or non-physical means to prevent, control, and/or mitigate undesired events or accidents. It is important that a barrier is clearly defined. Guidance on barrier definition as well as on DNV GL’s recommended approach to barrier analysis is contained within App.B.

Barrier analysis identifies functions related to each barrier system and the elements or procedures necessary to fulfil the function (sub-function can also be established where this is found necessary):

— Barrier Function (what the barrier aims to do, e.g. prevent leaks).
— Barrier System (what device completes the function, e.g. leak detection system).
— Barrier Elements (e.g. the individual parts of the leak detection system including the leak detection equipment).

When considering additional risk reduction barriers, in addition to the hierarchy of risk reduction previously detailed, the following, in priority order, should also be considered:

1) Passive hardware barriers.
2) Active hardware barriers.
3) Administrative or procedural barriers.

Hardware barriers should be considered before procedural barriers as they are likely to be more effective and reliable (assuming that they are well designed and maintained).

The barrier analysis should ideally be visualized in barrier diagrams. A bow-tie diagram is the preferred means of such documentation, but other equivalent means are acceptable. Bow-ties may be presented with different levels of detail.

Effective risk management requires complete and fully functioning barriers to be identified and defined. A complete barrier will be formed by a number of barrier systems or elements, which collectively deliver the required function of the risk reduction measure. It is recommended, to be meaningful, that barriers shown on bow-ties should be complete and fully functioning barriers with each system or element that delivers all or part of a barrier function also being shown. Systems may be hardware or procedural and generally would include several barrier elements that collectively deliver the system objective (e.g. “emergency shutdown system”, “bund”, “emergency response procedures”).
Examples of barriers identified on a bow-tie, using the Guidance in Appendix B, are presented in Appendices C and D.

It is recommended that procedural barriers should be identified and detailed on the bow-ties as these are effective means of control and deemed good practice to include them to ensure critical tasks are adequately assessed and executed.

Should an existing offshore installation already have a QRA, barrier analysis bow-ties, or equivalent for the management of safety risks, these analyses should be used as the basis for MEI and MPI risk management.

Identification of critical elements

Whether using QRA, barrier analysis or other appropriate approaches, all SECEs and ECEs need to be identified.

SECEs and ECEs shall be any structure, plant, equipment, system (including computer software) or component part whose failure could cause or contribute substantially to a MEI and MPI, and which purpose is critical to prevent or limit the effect of a MEI and MPI. Under the EU Offshore Safety Case Directive SECEs are mainly hardware based and cannot be purely procedural. DNV GL recommends that where risk management has significant dependency on procedures to prevent a MEI and MPI then they should be recognised as, or within, SECEs and ECEs in order that they are, and remain, effective.

A systems approach is necessary to identify those systems that constitute SECEs and ECEs. Within such systems, many individual components may be SECEs and ECEs, but others may not. The term ‘contribute substantially to a major accident’ is used in the EU Offshore Safety Directive and is intended to include those parts whose failure would not directly initiate a MA, but would make a significant contribution to a chain of events that could result in a MA.

Consideration of SECEs and ECEs should include systems for the prevention, detection, control and mitigation of MEI and MPI. Items improving reliability by providing redundancy or diversity should also be considered. Although many items will be critical on every installation, there will be some variation because of the specific circumstances of design and operation of the installation.

It is recognised that individual operators will likely develop their own criteria and approach for identification of SECE and ECEs.

A list of typical SECEs and ECEs is contained within App.A.

Main results

The main results from Stage 4 are:

— a documented record of the process undertaken to identify all reasonably practicable risk reduction measures that will maintain MEI and MPI risk at acceptable levels (e.g. ALARP)

— barrier visualisation diagrams (bow-ties or equivalent)

— a list of all critical elements (SECEs and ECEs) that are required within the management of MEI and MPI risk.

2.5 Stage 5 - performance standards for SECEs and ECEs

Main objectives

The main objective for Stage 5 is to define the minimum level of performance that must be achieved over the lifetime of the operation for all identified SECEs/ECEs in a Performance Standard.

Recommended method

Identification and management of ECEs is outside the scope of EU Offshore Safety Directive. As good practice, it is recommended that Performance Standards are developed for ECEs following the same approach used for SECEs.

Methodologies for developing Performance Standards for SCEs are well established and guidance can be found in the Step Change in Safety Assurance and Verification Practitioner’s Guide, Managing Risks to prevent and minimize the impact of Major Accidents /5/. For SECEs and ECEs, it is recommended to follow these existing methodologies.
A Performance Standard is a statement, which can be expressed in qualitative or quantitative terms, of the performance required of a barrier, and which is used as the basis for managing the hazard through the lifecycle of the installation. Performance Standard’s should take account of the circumstances on a particular installation. The parameters detailed in Table 2-5 should be included in each Performance Standard.

Table 2-5 Performance standard parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role</td>
<td>What is the exact role that the SECEs and ECEs will perform? The role must be defined with respect to the particular hazards the SECEs and ECEs are helping to manage.</td>
</tr>
<tr>
<td>Functionality</td>
<td>What are the SECEs and ECEs required to do? The functional standards define the minimum performance necessary to fulfil the role (but do not define how that performance should be achieved, see App.B).</td>
</tr>
<tr>
<td>Reliability &amp; availability</td>
<td>How likely is the critical element to perform on demand and for what proportion of time will it be available to perform on demand? The criticality of a system will determine how reliable and available it must be.</td>
</tr>
<tr>
<td>Survivability</td>
<td>How will the system perform after the event (i.e. during or after a MEI or MPI)? If a system has to operate or maintain its integrity during or after an event, it must have sufficient strength, protection or redundancy so that it can fulfill its role and meet the functional standards. These will be expressed in terms of the severity of the event that it should survive.</td>
</tr>
<tr>
<td>Interdependencies</td>
<td>What other SECEs and ECEs are required to function in order for the one in question to also operate effectively, or vice versa? If a system is either dependent upon another system or other systems are dependent on it, then this interdependency should be detailed. This is to ensure a holistic understanding of hazard management is maintained.</td>
</tr>
</tbody>
</table>

For organisations which already manage safety risk using SCEs, Performance Standards will already exist. It is appropriate to keep the format for SECEs and ECEs given that they follow the parameters above.

Safety Performance Standard’s may already be in place for the identified SECEs. For each SECE, the existing Performance Standards shall be re-evaluated to ensure that it is adequate to prevent or mitigate the identified MEI and MPIs. If it is not adequate, the Performance Standard’s shall be modified and updated accordingly.

If no Performance Standards are in place for the identified SECEs and ECEs, Performance Standards shall be developed and put in place. For SECEs it is recommended to coordinate the work from the safety and environmental perspective, so that unified Performance Standards are established.

The list of identified SECEs and their Performance Standards shall be reviewed by those responsible for assurance and verification activities to confirm that they are appropriate. This is described in [2.7].

Main results

The main result from Stage 5 is a set of Performance Standards for all identified SECEs and ECEs, preferably based on or combined with Performance Standards from safety.

2.6 Stage 6 - design and operate

Main objectives

The main objectives of Stage 6 are to:

- Ensure that SECEs and ECEs, in order to meet their Performance Standards, are designed, installed and maintained in an efficient state, in efficient working order and in good repair.
- Ensure that recording and reporting of maintenance and repair activities is carried out.
- Ensure risk management process is maintained up to date and used in decision making.
Recommended method

Management processes should be put in place to ensure the initial and continued suitability of critical elements throughout the period they are required.

There should be a robust maintenance strategy that identifies the components of the critical elements and the inspection and maintenance required on them. These requirements should assure that the critical elements continue to work as intended. The system must be capable of recording and reporting on those maintenance and repair activities.

There should also be the capability to monitor critical element performance through suitable reports and key performance indicators (KPIs) (e.g. trend analysis of maintenance failures, critical element maintenance backlog, deferrals, corrective work orders, and impairment risk assessments) and report to appropriate management levels offshore and onshore.

There should be provision for consistently applying a management of change (MOC) procedure that assesses the impact of changes on critical elements.

For impaired critical elements (i.e. ones found not to meet their PERFORMANCE STANDARD or are defective), a procedure for determining whether safe operation is still possible should exist.

All relevant factors that could lead to the degradation of, or changes in, a critical element’s performance should be identified, assessed and where possible actions taken to prevent or limit them before they could lead to the critical element failing to deliver its required level of performance. Factors such as aging, the environment to which it is exposed, frequency of use, potential misuse or overload, dependency on other elements, etc., all need to be considered within the processes put in place to ensure continued adequacy of the critical elements.

Throughout the design and operation of an offshore installation the risk assessment process should be used and kept up to date to reflect the current design and operation. During the life of an offshore installation critical elements will change or require to be changed to maintain the effectiveness of the risk management.

Main results

All SECEs and ECEs will:

— Be designed and maintained fit for service to deliver the requirements specified in the Performance Standards.
— Be working, or capable of working, at all times.
— Have records kept of maintenance and repair activities.
— Reflect the requirements determined through up to date risk assessment.

2.7 Stage 7 - SECEs and ECEs assurance and verification

Main objectives

The main objective of Stage 7 is to put in place assurance and verification processes to demonstrate that the SECEs and ECEs will perform their required functions when required to do so.

Note: Stages 6 and 7 overlap with activities undertaken in one feeding into and/or influencing the other.

Recommended method

Assurance activities

Assurance activities include inspection and testing to provide early detection of impaired performance and to assure maintenance activities are achieving their intent. It also includes activities to monitor Performance Standard compliance through suitable management reports and KPIs (e.g. SECEs maintenance backlog).

It is recommended that assurance activities for each Performance Standard criteria are included. The Performance Standard’s ensure close and demonstrable alignment between each Performance Standard criteria and the assurance activities in place to assure performance.

Assurance requirements should include:

— details of assurance activities to be undertaken
— frequency of the assurance activities
— responsible personnel
— recording of findings.

Relevant technical personnel (e.g. operations, maintenance teams, etc.) should be involved for discussion and consultation to ensure that the identified assurance activities are suitable, effective and realistic.

Where it is found that criteria in a Performance Standard cannot be met, an appropriate plan should be developed to understand the impact of the lack of performance and put in place measures and/or changes to the operation to ensure hazard risks are maintained at an acceptable level. Failure of SECEs and ECEs to achieve a minimum level of performance may require immediate operational risk reduction measures, including process or operation shutdown.

The assurance processes should be undertaken by competent people who have appropriate levels of impartiality and independence from pressure, especially of a financial or operational nature, which could affect sound judgement.

Verification activities

Verification should be performed by an independent party. Verification activities are required as part of the EU offshore safety directive such that:

— Companies operating under the EU Offshore Safety Directive are required to establish schemes for independent verification to give independent assurance that the SECEs and the schedule of their examination and testing are suitable, up-to-date and operating as intended.
— Verification of SECEs. No verification is stipulated for ECEs under the directive.
— The verification activities need to be tailored to the relevant project phase. Typically desktop verification will be appropriate in early design phase, while during construction or operations, inspections (and testing, reviews) may be the most suitable activity. As mentioned in [2.5], the performance requirements will normally be the same regardless of the project phase as they shall reflect the expected performance during operation.
— For a production installation, the verification scheme shall be in place prior to the completion of the design. For a non-production installation, the scheme shall be in place prior to the commencement of operations in the offshore waters of EU Member States.

Verification scheme

The purpose of the verification scheme is to ensure that SECEs are, and will remain, compliant with the PERFORMANCE STANDARD through each phase of an installations lifecycle. Implementation of the verification scheme provides additional confidence, independent of the company’s assurance process, that the parts of the installation deemed to be safety and environmentally critical are suitable or actions necessary to support their suitability are identified and implemented.
Typically, an operational verification scheme can specify the following types of verification activities:

**Table 2-6 Activities typically covered by verification scheme**

<table>
<thead>
<tr>
<th>Type</th>
<th>Verification Activities (nature)</th>
</tr>
</thead>
</table>
| Offshore                          | — Witness SECEs assurance activities (e.g. test/inspections/musters etc.)  
— Visually examine condition of SECEs (e.g. piping, vessels, hazardous area equipment etc.)  
— Audit compliance with SECEs assurance process (e.g. control of temporary equipment, management of control inhibits or overrides, control of locked open/locked closed valves, management of defined life repairs etc.) through inspection and testing and the review of any offshore records. |
| Onshore - Assurance Management System | — Review maintenance and inspection records confirming they are:  
— suitable for assuring the Performance standard,  
— conducted at the specified frequency,  
— reported correctly stating ‘As-Found’ and ‘As-Left’ condition, and  
— reporting remedial work and ensuring it has been correctly prioritised/executed  
— Review planned maintenance deferrals.  
— Detailed procedural compliance audits of specific inspection strategy encompassing the RBI implementation, defined life repairs etc. |

**Verifier competency**

Each Verification Body should have a system of documented competence with traceable means of assessment clearly stating the competence criteria and method of assessing the individual Verifier.

In principle, a verification body’s competency scheme should contain the following aspects:

— competency criteria by engineering discipline or SECEs-specific  
— detailed criteria to define competence – in general a combination of technical knowledge and experience is required  
— frequency of review and assessment  
— definition of which lifecycle phase the person is considered competent for  
— increasing levels of competency may be defined.

The verification body has a responsibility to:

— comment on the list of identified SECEs, including the robustness of the methodology used to establish the MA and resulting SECEs  
— if asked to by the duty holder, the verifier can draw up the verification scheme. The verifier must agree the scheme with the duty holder  
— perform verification activities as defined in the verification scheme  
— report on the suitability of SECEs detailing examinations/witness of tests/reviews performed, findings and remedial actions recommended  
— communicate any reservations on the list of SECEs, content of verification scheme or ongoing suitability to high level company management.
SECTION 3 DOCUMENTATION AND UPDATE PROCESS

Section 2 describes how to identify and manage MEIs and MPIs using SECEs and ECEs. This section recommends how to document the process and reflect changes.

3.1 Process documentation

The sections below provide information on what should be documented during each stage in the MEI and MPI identification and risk management process (SECEs and ECEs).

Stage 1: Establishing context

Stage 1 sets the framework and guiding parameters for the risk management process. The information shall be documented. Additional information that should be included for the environmental risk management process is:

— criteria for what constitutes an MEI and MPI
— inventory of hazardous material to the environment
— overview of local environmental receptors
— environmental risk acceptance/tolerability criteria to be used during risk evaluation.

Stage 2: Hazard identification

HAZID-ENVID process shall be documented within a report which should contain a record of the:

— methodology applied i.e. HAZID-ENVID combined
— information used as a basis for the identification process (e.g. design documents, description of local environmental resources and their sensitivity, inventory of materials hazardous to the environment standards, etc.)
— personnel involved in HAZID-ENVID
— criteria used for screening of MEI and MPI. Criteria will be the same for both MEI and MPI
— identified hazards and associated hazardous events, their causes and characteristics, risk management measures.

Stage 3: Risk analysis and evaluation

Consequence analysis, likelihood analysis and risk evaluation of MEIs and MPIs shall be documented, and should include:

— a record of the methodologies applied and tools used
— assumptions taken and sources of data used, as well as any related uncertainties
— outcome of the sensitivity evaluation of environmental receptors, and reasoning behind selection of environmental impact indicators
— consequence results compared against MEI and MPI criteria, including justification for any incidents that are de-selected as being ‘major’
— the likelihood assigned to the MEIs and MPIs
— risk results compared against risk acceptance criteria, and key risk drivers highlighted.

Stage 4: Risk management and identification of critical elements

The ALARP process conducted should be documented, including:

— criteria used to assess whether additional mitigation is reasonable
— ALARP process findings and reasoning
— the selection of risk management measures and the process to follow when a measure may have an opposing influence on safety and environmental risk levels within an organization’s risk management procedures.
The barrier analysis process shall be documented. The documentation should include:

— methodology and approach used
— information used as a basis for the barrier analysis (e.g. design details, operation procedures)
— all the updated/created barrier diagrams (bowties or equivalent)
— a list of SECEs and ECEs.

**Stage 5: Performance standards for SECEs and ECEs**

The Performance Standards for SECEs and ECEs shall be documented.

During the Performance Standard development the following should be documented:

— basis for the Performance Standard requirements (e.g. Guidelines, Standards, Company specific documents used)
— in case of reviewing an existing SCE Performance Standard, the following should also be documented:
  — if there are no changes to the Performance Standard, justification should be made that existing requirements are appropriate for the environment
  — if there are changes made, basis for the changes to the requirements should be recorded.

**Stage 6: Design and operate**

Full details of the design, operation, maintenance, repairs, modifications and changes with respects to SECEs and ECEs shall be documented. This will include records of SECEs and ECEs:

— design and operation basis
— operation procedures
— maintenance procedures
— inspection procedures
— assurance processes
— verification scheme
— maintenance failures
— maintenance back-log
— anomalies
— deferrals
— testing records
— inspection records
— corrective work orders.

The documentation will detail the initial and continued suitability of the SECEs and ECEs for the installation.

The risk assessment and management documentation (as developed through each of the stages detailed within this RP) will need to be kept up to date to reflect the current status of the offshore installation and its operation.

**Stage 7: SECEs and ECEs assurance and verification**

**Assurance**

Assurance activities shall be documented within reports. Assurance reports are likely to cover:

— the examination and testing carried out
— the findings
— any remedial actions recommended
— actions taken.
### Verification

The following verification aspects shall be documented:

- details of SECEs and ECEs Performance Standards subject to verification
- method of verification to be used for Performance Standards
- person or Body completing the verification including the justification of their competence to do so
- details of the verification activities completed, any instances of non-compliance with the verification scheme and any remedial actions recommended
- verification report detailing suitability of SECEs detailing examinations/witness of tests/reviews performed, findings and remedial actions recommended
- communication of any reservations on the list of SECEs, content of verification scheme or ongoing suitability to high level company management
- any actions taken by the installation operator.

### 3.2 Review and updating

The design and operation of the installation shall be systematically reviewed and if required changes shall be made to the Performance Standard or the identification of SECEs and ECEs updated.

The Performance Standard shall reflect the current design and operation of the installation and the risk management requirements. In order to ensure this, the update of the performance standard shall be a part of the MOC process. This implies that the performance standard should be a dynamic and formal document which is updated when there are for example:

- new and/or updated company and/or regulatory requirements
- modification on the installations design
- changes in the process conditions (higher/lower pressure and/or temperatures)
- changes in the fluids composition (e.g. introduction of H2S in production, new chemicals)
- new knowledge, resulting in a change in the existing design basis during a design phase.

In some circumstances it may be also required to update the identification of SECEs and ECEs. Any change from the basis for the SECEs and ECEs identification should be assessed with respect to effects on the MA (with MEI potential) and MPI selection, barrier analysis and/or validity of the assessment and its results. Examples of changes include but are not limited to:

- changes in the design or modifications of existing facilities
- changes in the location (e.g. drilling rig moving to new site)
- significant changes in environmental conditions or environmental sensitivity (e.g. new knowledge becomes available for physical or ecological factors)
- significant changes in data used as for risk ranking (e.g. new failure frequencies).

When updating, the complete basis for the SECEs and ECEs identification process should be reviewed. This review should be documented.
APPENDIX A  EXAMPLES OF SECES AND ECES

Below is a list of typical SECEs across different types of installations. It is noted that critical elements would be defined as SECEs even if there is no potential environmental consequences as per the EU Offshore Safety Directive.

Table A-1  List of typical SECEs

<table>
<thead>
<tr>
<th>Safety and Environmental Critical Elements (SECEs)</th>
<th>Applicability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Structures</td>
<td>Relevant for: All installations</td>
</tr>
<tr>
<td>Well integrity</td>
<td>Relevant for: All production installations, drilling installations &amp; subsea wells</td>
</tr>
<tr>
<td>Flowlines and risers</td>
<td>Relevant for: In vicinity of all production installations</td>
</tr>
<tr>
<td>Process hydrocarbon containment</td>
<td>Relevant for: All production and drilling installations</td>
</tr>
<tr>
<td>Drains</td>
<td>Relevant for: All production installations</td>
</tr>
<tr>
<td>Ballast and bilge systems</td>
<td>Relevant for: All floating installations</td>
</tr>
<tr>
<td>Fire and gas detection</td>
<td>Relevant for: All production and drilling installations</td>
</tr>
<tr>
<td>Shutdown (emergency shutdown)</td>
<td>Relevant for: All production and drilling installations</td>
</tr>
<tr>
<td>Blowdown &amp; pressure relief</td>
<td>Relevant for: All production and drilling installations</td>
</tr>
<tr>
<td>Firewater system</td>
<td>Relevant for: All production and drilling installations</td>
</tr>
<tr>
<td>Well control process equipment (BOP)</td>
<td>Relevant for: Drilling installations</td>
</tr>
<tr>
<td>Mud systems</td>
<td>Relevant for: Drilling installations</td>
</tr>
<tr>
<td>Navigation lights</td>
<td>Relevant for: All installations</td>
</tr>
<tr>
<td>Mooring systems (anchor lines, dynamic positioning systems, etc.)</td>
<td>Relevant for: All floating installations</td>
</tr>
</tbody>
</table>

Table A-2  Potential list of ECEs that would prevent and minimize a potential MPI.

<table>
<thead>
<tr>
<th>Environmental Critical Elements (ECEs)</th>
<th>Applicability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hydraulic oil containment for riser tensioning systems / heave compensation systems</td>
<td>Relevant for: Semi-submersibles, drill ships</td>
</tr>
<tr>
<td>Methanol containment system</td>
<td>Relevant for: Production installations</td>
</tr>
<tr>
<td>Offloading cargo hose (crude oil) between installation and shuttle tanker or loading buoy</td>
<td>Relevant for: FPSO, FSO, FSU</td>
</tr>
<tr>
<td>Hydrocarbon containment subsea (e.g. &gt; 500 m zone production or oil export pipelines, subsea separation systems)</td>
<td>Relevant for: Pipelines, Subsea systems</td>
</tr>
</tbody>
</table>
APPENDIX B  DNV GL GUIDANCE ON DEFINING A ‘BARRIER’

DNV GL has identified that the term ‘barrier’ is widely used within industry, but often poorly defined. SECEs and ECEs are in effect barriers. Defining what constitutes a barrier in a consistent manner enables barrier and risk management techniques to be utilised effectively. DNV GL is in the process of publishing its own RP in this area, and this is expected to be published in late 2015 / early 2016. In this Appendix, DNV GL sets out some guidance and recommendations in this area.

The offshore regulator in Norway, Petroleum Safety Authority (PSA) Norway, is one of the few Regulators to actually define what a barrier is. The PSA require that a barrier has a Function, System and Elements and DNV GL believe this approach works well as a general principal. The PSA set outs and defines these terms as stated below:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
<th>Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Barrier Function</td>
<td>A term used by the PSA in Norway who define this as “The task or role of a barrier. Examples include preventing leaks or ignition, reducing fire loads, ensuring acceptable evacuation and preventing hearing damage”. It should be an abstract system, property or purpose, and not an object. It can often be best described in verb form and can be to prevent, control, or mitigate undesired events or accidents.</td>
<td>Outside of Norway it is recommended that barriers should not be represented on bow-ties at this level.</td>
</tr>
<tr>
<td>Barrier System</td>
<td>A term used by the PSA in Norway who define these as being “made up by technical, operational or organizational barrier elements, are the means by which the barrier function(s) are carried out, and which without the barrier function(s) could not be accomplished or realized”. DNV GL recommends that a barrier system should ideally be independent and complete (fully functioning).</td>
<td>DNV GL would recommend that barriers on bow ties are displayed at this level.</td>
</tr>
<tr>
<td>Barrier Element</td>
<td>A term used by the PSA in Norway who define these as “technical, operational or organizational measures or solutions that are part of the realization of a barrier function”. These individual parts make up a Barrier System.</td>
<td>Outside of Norway it is recommended that barriers should not be represented on bow-ties at this level.</td>
</tr>
</tbody>
</table>

DNV GL would normally recommend that when defining barriers that the PSA approach is a good basis to be used to check that the barrier is clearly defined and all constituent parts are included in this.

SECEs and ECEs are normally defined at either barrier system or barrier element level.

It should just be noted that a pure procedure alone would not normally be seen as a barrier under the PSA rules. DNV GL thinks that it is good practice to recognise procedural controls as barriers when developing bow-ties so long as they meet the following criteria that should apply to all barriers.
Barriers categorisation

When considering barriers as displayed on a standard bow-tie (as typically shown above) DNV GL recommend that preventative barriers should be able to fully prevent the top event occurring on their own without interaction with other barriers. Once the top event has occurred; mitigation barriers need not be able to fully prevent the consequences, but reduce the severity of these.

— Prevention barrier – a barrier lying on the left side of the bow tie and capable of terminating a cause sequence before reaching the Top Event.
— Mitigation barrier – a barrier lying on the right side of the bow tie and capable of terminating or at least reducing the scale the potential consequences.

DNV GL recommends that barriers on bow-ties are displayed at barrier system level (as outline above) and are then categorised using the following approach:

— Passive barrier – a barrier system that is continuously present and provides its function without any required action i.e. a bund.
— Active barrier – a barrier system requiring some action to occur, usually involving detection, determination, then action where all components are automated and do not require human input i.e. a gas detection system leading to activation of an emergency shutdown system. It human input is required to complete the barrier function then the barrier becomes a Procedural Barrier.
— Procedural barrier – a barrier system that relies to some degree on human intervention following a procedure / instruction including detection, determination (decision making), then action. i.e. an operating procedure.

Passive Barriers need no additional input to complete the barrier function and are ‘complete’ or ‘fully functioning’ in effect. However Procedural or Active Barriers will need a number of component elements in order to complete their barrier function and should contain three barrier elements: sensor, decision making and action (or ‘sense-think-do’):

Barrier Elements should be defined by the part they play in this. It is recommended that fully Procedural Barriers be checked to ensure that each part is included in them.
Finally, DNV GL would recommend that all barriers on any given threat or consequence line are independent of each other as shown in the diagram below. This will help to reduce the likelihood of common cause failure causing the failure of multiple barriers.

It is DNV GL’s view that a structure barrier approach such as the one outlined above will assist in creating consistent bow-tie diagrams and thus help with the implementation of barrier management and risk management techniques.
APPENDIX C EXAMPLE: MA (MEI POTENTIAL) BOW-TIE DIAGRAM
Driven by our purpose of safeguarding life, property and the environment, DNV GL enables organizations to advance the safety and sustainability of their business. We provide classification and technical assurance along with software and independent expert advisory services to the maritime, oil and gas, and energy industries. We also provide certification services to customers across a wide range of industries. Operating in more than 100 countries, our 16,000 professionals are dedicated to helping our customers make the world safer, smarter and greener.