

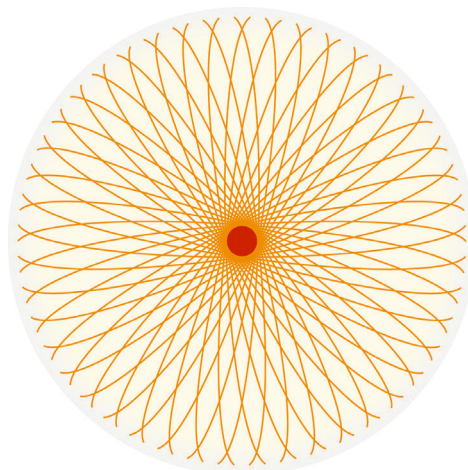
Report

Barriers to prevent and limit acute releases to sea

Environmental risk acceptance criteria and requirements to safety systems

Author(s)

Stein Hauge
Tony Kråkenes
Solfrid Håbrekke
Gorm Johansen
Mariann Merz
Tor Onshus



Report

Barriers to prevent and limit acute releases to sea

Environmental risk acceptance criteria and requirements to safety systems

KEYWORDS:

Safety barriers
Environmental
acceptance criteria
Performance
requirements

VERSION
1.0**DATE**
2011-10-16**AUTHOR(S)**

Stein Hauge, Tony Kråkenes, Solfrid Håbrekke, Gorm Johansen, Mariann Merz, Tor Onshus

CLIENT(S)
Multiclient**CLIENT'S REF.**
Håkon S. Mathisen**PROJECT NO.**
605051**NUMBER OF PAGES/APPENDICES:**
96 incl. appendices**ABSTRACT**

This report summarizes the result from PDS-BIP activity 1. Focus is on non-planned acute releases to sea and the barriers applied during drilling, workover and subsea production in order to prevent such releases.

The report discusses requirements to such barriers on two different levels: (1) on a high level in terms of environmental risk acceptance criteria (ERAC) and (2) on a more detailed level in terms of performance requirements for the barriers. The relationship between the overall acceptance criteria and the more detailed performance requirements is also discussed.

PREPARED BY
Stein Hauge**CHECKED BY**
Mary Ann Lundteigen**APPROVED BY**
Lars Bodsberg, Research Director**REPORT NO.** SINTEF A20727 **ISBN** 978-82-14-05227-5**CLASSIFICATION**
Unrestricted

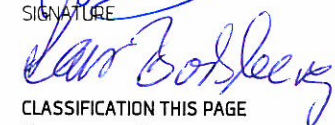
SIGNATURE



SIGNATURE



SIGNATURE

**CLASSIFICATION THIS PAGE**
Unrestricted

Document history

VERSION	DATE	VERSION DESCRIPTION
Version No. 1.0	2011-10-17	First official version of report based on previous project memos and comments to these memos.

Table of contents

Executive Summary	5
1 Introduction	7
1.1 Background.....	7
1.2 Objective and scope of report.....	7
1.3 Content of report.....	8
1.4 Limitations.....	8
1.5 Abbreviations.....	9
2 Relevant Standards and Regulations	12
2.1 Authority requirements.....	12
2.2 Requirements to barriers and overall acceptance criteria.....	13
3 Environmental risk analysis (ERA)	15
3.1 Introduction.....	15
3.2 ERA in regulations and standards.....	15
3.3 ERA in the MIRA guideline.....	16
4 Environmental risk acceptance criteria (ERAC)	17
4.1 General risk acceptance criteria.....	17
4.2 ERAC in PSA regulations.....	17
4.3 ERAC in the NORSOK Z-013 standard.....	19
4.4 ERAC in the MIRA guideline.....	19
4.5 ERAC applied in the Norwegian petroleum industry.....	21
5 Discussion of the current ERAC	22
5.1 Are today's criteria adequate?.....	22
5.2 How does ERA/ERAC impact on design and operation of frequency reducing barriers?.....	24
5.3 Who should determine the ERAC?.....	26
5.4 Uncertainty in environmental risk analyses.....	27
6 Safety Barriers and associated performance requirements	28
6.1 Type of barrier performance requirements.....	28
6.2 Performance requirements for drilling facilities.....	29
6.3 Performances requirements for well intervention equipment.....	31
6.4 Performances requirements for subsea ESD and PSD functions.....	32
6.5 Well barriers as described in NORSOK D-010.....	33
6.6 Summary of performance requirements.....	33
7 Relating the acceptance criteria to safety barrier requirements - alternative ERAC	36
7.1 Maximum acceptable frequency of specified scenario.....	36

7.2	Maximum acceptable frequencies of specified release volumes	39
7.3	Calibrated risk graph	40
8	Conclusions.....	45
9	References.....	47
APPENDICES.....		50
A	Safety Barriers Classification and Overview	51
B	Barrier Description.....	58
C	ERA in NORSOK Z-013.....	95

Executive Summary

This report has been developed as part of the on-going joint-industry project “Development of barriers and indicators to prevent and limit pollutants to sea”, funded by the Norwegian Research Council and the members of the PDS forum¹. The work has mainly been carried out by SINTEF and may therefore not express the view of all the PDS participants.

The purpose of the report is to identify and evaluate the environmental risk acceptance criteria (ERAC) applied in the oil and gas industry on the Norwegian Continental Shelf, to discuss pros and cons related to these criteria and to suggest possible alternative ways of setting such criteria. Furthermore, performance requirements for barriers that prevent and limit acute releases have been reviewed and the relationship between the overall acceptance criteria and these performance requirements are discussed. Focus is on non-planned acute releases to sea and the barriers applied during drilling, workover and subsea production in order to prevent such releases.

Based on the discussions in this report, some main conclusions and findings are presented below. These findings relate to the current environmental risk analysis (ERA), the ERAC, barrier performance requirements and the (missing) link between high level acceptance criteria and barrier performance requirements.

ERA as performed today has a one-sided focus on consequence modelling, to the possible detriment of frequency reducing measures

Today, the ERA focuses on the modelling of the consequences from accidental releases of oil/condensate. The analyses normally start with a set of release scenarios, and model the consequences of a release with respect to restitution time of vulnerable resources. The barriers prior to the release are generally not an explicit part of the ERA. Since frequency reducing measures shall be given priority, it is unfortunate that the current ERAC/ERA only direct focus towards consequences.

More ambitious ERAC are called for

In general the estimated risk figures in ERA are far below the ERAC. The current ERAC are therefore not strict enough to put focus on continuous improvement and risk reducing measures, in particular frequency reducing measures.

The authorities have set out very ambitious HSE goals for the Norwegian petroleum industry, including goals for environmental risk reduction. These very ambitious goals should be followed up by ambitious criteria for acceptable environmental risk.

The approach for defining ERAC needs to be reconsidered

Currently each operator defines the levels of acceptable risk – to personnel and environment – associated with their operations. Personnel are an operator asset, but the environment is a common good. Hence, it seems reasonable that the authorities should play a more active role in setting overall criteria and goals for the environment.

¹ PDS is a Norwegian acronym that translates into “reliability of safety instrumented systems”. For more information about PDS see: www.sintef.no/pds.

It appears that all companies operating in Norway use more or less the same ERAC adopted from the OLF MIRA guideline, but to a limited degree tailor the criteria to their particular situation. The authorities' intention of relating the criteria to the individual environmental resources and to consider the facilities in a larger context is therefore not properly implemented.

Performance requirements to important barrier functions are to some degree inadequate

According to the PSA Management Regulations § 5, barriers shall be established and personnel shall be aware of their intended function and what performance requirements have been defined for the identified barriers.

A review has been made of performance requirement to drilling systems, well intervention equipment and subsea ESD and PSD functions. It is concluded that the extent of such requirements given in relevant standards and guidelines are to some degree inadequate. In particular, integrity requirements (e.g. SIL/EIL requirements) are only provided for the drilling BOP function and the "isolation of subsea well" function.

In a future update of the OLF-070 guideline a number of new functions should therefore be considered included with recommended SIL/EIL requirements. Examples of possible candidate functions are emergency power, mud circulation/mixing, acoustic BOP activation back-up, emergency quick disconnect, drilling riser tension and inclination measurement, well intervention BOP and various subsea PSD functions (PAHH, LAHH, etc.).

The governing principle of independence between operations/control and safety functions are not consistently implemented for drilling and well intervention applications

For topside production systems, there is traditionally a well-defined split between safety and non-safety systems. This split is less clear for drilling and well intervention systems, where the same equipment is used during normal activities (e.g. mud control) and in response to hazardous events. This mix-up of control and safety should on a principal basis be further investigated (ref. e.g. PSA Facilities Regulations, § 33–34).

Alternative or additional acceptance criteria are called for to establish a better connection between overall ERAC and performance requirements to important barriers

There is a need to establish a connection between overall corporate ERAC and requirements to barriers applied during drilling, workover and subsea production. The current ERAC based on restitution times of vulnerable resources are not suitable for this purpose, so alternative and simpler ERAC are called for.

This report suggests additional ways of expressing ERAC on a level suitable for establishing a link to requirements for technical systems. The alternative ERAC are based on release frequencies and release volumes. The use of Calibrated risk graph is discussed as a method to arrive at EIL requirements similar to what is done when setting SIL requirements.

1 Introduction

1.1 Background

Kongsberg Maritime has on behalf of the PDS Forum members been awarded funding from the Norwegian Research Council to complete a project called “Development of barriers and indicators to prevent and limit pollutants to sea”). A brief summary of the work to be completed as part of this project is shown in Table 1.1.

The focus of this report is on Activity 1 “Environmental acceptance criteria and technical and operational requirements to safety systems”. The other activities in the PDS-BIP project will be addressed in separate SINTEF reports or memos. In particular, this report is based on two previous (draft) memos from sub-activity 1.1 [16] and 1.2 [17] and the comments received to these memos. The work has mainly been carried out by SINTEF and may therefore not express the view of all the PDS participants.

Table 1.1: Overview of activities in the PDS-BIB project.

Project Title: Development of barriers and indicators to prevent and limit pollutants to sea			
Main Activity		Sub-Activity	
1	Environmental risk acceptance criteria and technical and operational requirements to safety systems	1.1	Mapping and development of environmental acceptance criteria
		1.2	Technical and operational requirements to systems
2	Guidance for development of pro-active indicators	2.1	Development of indicators for environmental impact
		2.2	Guidance for data collection and follow-up of the environmental indicators
3	Developing analytical tools and guidelines for estimating the reliability of barrier functions to avoid environmental releases	3.1	Guidelines for design
		3.2	PDS method handbook 2013
		3.3	PDS data handbook 2013
		3.4	PDS example collection
		3.5	PDS tool
4	Publication of results and project information		Reports, memos, papers, articles, web, participation in standardisation work, etc.

1.2 Objective and scope of report

A number of safety barriers are installed to prevent and limit environmental releases from drilling, well intervention and subsea production. The main objective of this report is to identify and describe requirements that apply to these barriers, both on an overall level – in terms of environmental risk acceptance criteria (ERAC), and on a more detailed level – in terms of performance requirements to the specific safety systems.

Further, the report goes on to discuss the adequacy and pros and cons of these requirements and proposes some future improvement areas both with respect to overall acceptance criteria and performance requirements to safety systems.

The following tasks were identified as of special interest for this work:

- Which safety barriers apply during drilling, well intervention and subsea production?
- What are the overall authority requirements?
- What are the existing environmental risk acceptance criteria?
- Which performance requirements apply for the relevant safety barriers?
- Are the current requirements adequate?

The work presented in this report is based on a review of relevant literature, including authority regulations and referenced national and international standards. Other information sources include:

- Comments from the PDS members to two draft memos on technical barrier description and requirements [16] and environmental risk acceptance criteria [17].
- Input from discussions with members of the PDS forum. In particular, two workshops have been carried out with themes related to environmental risk analyses and environmental risk acceptance criteria.
- Experience from other relevant SINTEF projects, such as e.g. the Deepwater Horizon project [32].

1.3 Content of report

The content of the report includes:

- *Chapter 1:* Background information concerning the project scope, purpose and limitations;
- *Chapter 2:* Introductory information about relevant standards and regulations;
- *Chapter 3:* Brief description of environmental risk analysis (ERA) as described in relevant standards;
- *Chapter 4:* Description of current environmental risk acceptance criteria (ERAC) based on PSA regulations, industry standards and information received from the operators;
- *Chapter 5:* Discussion of pros and cons concerning today's ERAC, and possible areas of improvement;
- *Chapter 6:* Description and discussion of relevant barriers to avoid acute releases to sea. This includes a description of requirements relevant for these barriers as well as observations and findings related to the reviewed standards and guidelines;
- *Chapter 7:* Discussion of alternative ERAC and how these can be linked to barrier requirements;
- *Chapter 8:* Main conclusions and findings;
- *Chapter 9:* References to applied documentation;
- *Appendix A and Appendix B:* Overview of safety systems and barriers (Appendix A) and a more detailed discussion of drilling facilities, well intervention equipment and subsea related PSD and ESD functions (Appendix B);
- *Appendix C:* A somewhat more detailed presentation of how ERA is described in NORSOK Z-013.

1.4 Limitations

We often distinguish between non-planned releases and planned releases. *Non-planned releases* are hydrocarbon leaks resulting from unwanted events or accidents. These are mostly *acute* in nature, and the quantities involved may be large. Non-planned releases may be regarded as *continuous* when left undetected for a longer period. An example may be a very small subsea leak.

Planned releases (often termed *regular* or *operational releases*) are non-accidental releases associated with normal offshore operations. Such releases are normally an integrated and inevitable part of conducting

offshore operations, and have been accepted by the authorities. The quantities involved are small, and are considered to have a limited effect on the environment.

In this report focus is on acute accidental releases to sea and the safety instrumented systems implemented to prevent and limit such releases. We mainly consider drilling, well intervention and subsea related systems since topside process releases to a lesser degree have a potential to cause major environmental consequences.

Topside systems that are needed to support the operation of the subsea equipment, for example the mud system used during drilling, are also a part of the scope. It has not been within the scope to assess other types of (non-instrumented) safety-critical systems, such as procedures and passive (physical) barriers, like plugs, casing and cement barriers.

Typical scenarios representing acute releases to sea are:

- blowouts
- well leaks
- pipeline leaks
- riser leaks
- process leaks
- releases from storage tank
- releases when loading/offloading oil
- releases initiated from other accidents (e.g. fire, explosion, structure loss, collision, etc.)

Within each group of releases there are several possible scenarios. A blowout can occur during drilling, well testing, well completion, production or workover activities. Storage tank releases can be both topside and subsea, so can releases during loading/offloading, etc.

1.5 Abbreviations

Below is a list of abbreviations used in this report.

ALARP	- As Low As Reasonably Practicable
AMV	- Annulus Master Valve
APS	- Abandon Platform Shutdown
ASV	- Annulus Safety Valve
BIP	- <i>Brukerstyrt innovasjonsprosjekt</i> . Translates into “User directed innovation project” which represents a type of research activity that is funded by The Research Council of Norway
BOP	- Blowout Preventer
BPV	- Back Pressure Valve
BSR	- Blind Shear Ram
C	- Consequence
CIV	- Chemical Injection Valve
CT	- Coiled Tubing
DCV	- Directional Control Valve
DHSV	- Downhole Safety Valve
DNV	- Det Norske Veritas
EDS	- Emergency Disconnect System
EIF	- Environmental Impact Factor
EIL	- Environmental Integrity Level

ERA	- Environmental Risk Analysis
ERAC	- Environmental Risk Acceptance Criteria
ESD	- Emergency Shutdown
EQD	- Emergency Quick Disconnect
FAR	- Fatal Accident Rate
HIPPS	- High Integrity Pressure Protection System
IEC	- International Electro technical Commission
IL	- Integrity Level
IMO	- International Maritime Organization
KLIF	- <i>Klima og forurensningsdirektoratet</i> . Translates into "The Climate and Pollution Agency"
LAHH	- Level Alarm High-High
LMRP	- Lower Marine Riser Package
LOPA	- Layer Of Protection Analysis
LRP	- Lower Riser Package
LS	- Lower Stripper
MIRA	- <i>Metode for miljørettet risikoanalyse</i> . Translates into "Method for environmental risk analysis"
MODU	- Mobile Offshore Drilling Unit
NCS	- Norwegian Continental Shelf
NE	- Normally Energised
NDE	- Normally De-energised
NMD	- Norwegian Maritime Directorate
NORSOK	- <i>Norsk sokkels konkurranseposisjon</i> . Translates into "The competitive position of the Norwegian Continental Shelf"
OLF	- <i>Oljeindustriens landsforening</i> . Translates into "The Norwegian Oil Industry Association"
P	- Probability
PAHH	- Pressure Alarm High-High
PDO	- Plan for Development and Operation
PDS	- <i>Pålitelighet av datamaskinbaserte sikkerhetssystemer</i> . Translates into "Reliability of safety instrumented systems". Refers to a reliability prediction method for safety instrumented systems developed by SINTEF in co-operation with the Norwegian petroleum industry
PFD	- Probability of Failure on Demand
PIV	- Production Injection Valve
PLC	- Programmable Logic Controller
PLMV	- Production Lower Master Valve
PMV	- Production Master Valve
PSA	- Petroleum Safety Authority
PSD	- Production Shutdown
PSV	- Pressure Safety Valve
PUMV	- Production Upper Master Valve
PWV	- Production Wing Valve
QRA	- Quantitative Risk Assessment
RAC	- Risk Acceptance Criteria
RBD	- Reliability Block Diagram
RNNP	- <i>Risikonivå i norsk petroleumsvirksomhet</i> . Translates into "Risk level in the Norwegian petroleum activity"
ROV	- Remotely Operated Vehicle

SCSSV	- Surface Controlled Subsurface Safety Valve
SIF	- Safety Instrumented Function
SIL	- Safety Integrity Level
SIS	- Safety Instrumented System
SPWV	- Subsea Production Wing Valve
SSTT	- Subsea Test Tree
WB	- Well Barrier
WBE	- Well Barrier Element
WL	- Wireline
WOCS	- Workover Control System
WOR	- Workover Riser
WV	- Wing Valve
XOV	- Crossover Valve

2 Relevant Standards and Regulations

2.1 Authority requirements

The Petroleum Safety Authority Norway (PSA) is the regulatory authority for safety in the petroleum sector on the Norwegian continental shelf. PSA has developed a set of regulations and guidelines to govern the petroleum activities. Of these are the Facilities Regulations [4], the Management Regulations [5], the Framework Regulations [6] and the Activities Regulations [7] most applicable to the technical safety discipline.

The PSA regulations and guidelines frequently refer to other international and national standards for a detailed specification of the different functional requirements. An example of the relationship between regulations and standards that are frequently used with topside safety (instrumented) systems is shown in Figure 2.1. In general, the PSA regulations require compliance to IEC 61508 [1] and OLF-070 [3], but a number of additional national and international standards that shall be adhered to, such as the NORSOK standards, are also referenced.

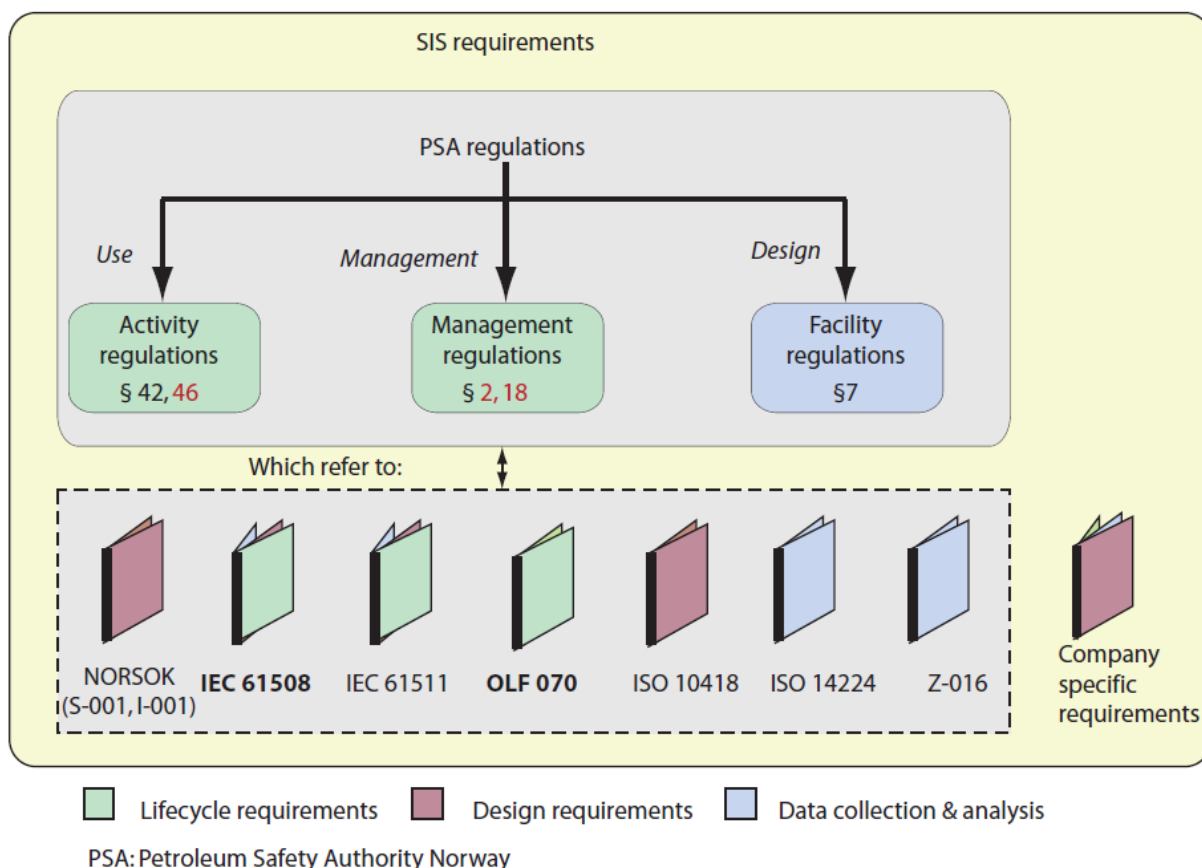


Figure 2.1: Standards and regulations [37].

The following standards were identified as being of particular relevance to the development of safety layers/barriers for drilling, well maintenance and subsea production operations:

- NORSOK S-001 “Technical Safety” [23]
- NORSOK D-001 “Drilling Facilities” [24]
- NORSOK D-002 “System Requirements Well Intervention” [25]

- NORSOK D-010 “Well integrity of drilling and well operations” [26]
- OLF Guideline 070 “Guidelines for the Application of IEC 61508 and IEC 61511 in the petroleum activities on the continental shelf” [3]
- IEC 61508 "Functional safety of electrical/electronic/ programmable electronic safety related systems" [1]
- ISO 13628 “Petroleum and natural gas industries - Design and operation of subsea production systems” [28]
- ISO 13624 "Petroleum and natural gas industries – Drilling and production equipment" [29]
- ISO 10417 “Petroleum and natural gas industries – Subsurface safety valve systems – Design, installation, operation and redress” [30]

For fixed drilling units on the Norwegian sector, these are generally subject to requirements given in the Facilities Regulations. For mobile drilling units, § 3 in the Framework Regulations states that for facilities following a maritime operational concept, relevant technical requirements in the Norwegian Maritime Directorate's regulations for mobile facilities (“the Red Book”) can alternatively be applied, with supplementary classification rules provided by DNV (or international flag state rules with supplementary classification rules providing the same level of safety).

When building drilling rigs, the shipyards basis for technical requirements will often be rules given by the classification company itself (such as DNV). These rules will typically be based on IMO / IMO MODU code. If the flag state (e.g. Norway) has specific national requirements that are stricter than the IMO code, these requirements must be implemented separately. Often, the foreign shipyards are not too familiar with for example the NORSOK standards or standards such as IEC 61508, and it may therefore be challenging to implement distinctive requirements related to for example safety integrity level (SIL).

To ensure that the drilling unit is fit for use on the Norwegian continental shelf, an “application for consent” needs to be prepared prior to drilling operations and submitted to the authorities (in this case the PSA) for approval. As part of the application for consent process, an acknowledgement of compliance must be obtained. This confirms based on an assessment, that the mobile facility’s technical condition and the applicant’s organisation and management system are in conformity with relevant requirements of Norwegian rules and regulations for the petroleum activities [19].

2.2 Requirements to barriers and overall acceptance criteria

Safety barriers are considered an important tool in order to reduce the risk. According to the PSA Management Regulations (§ 4 and § 5), barriers shall be established to reduce the risk, and performance requirements shall be stated for the barriers (including requirements for capacity, reliability, availability, efficiency, ability to withstand loads, integrity, and robustness). Furthermore, "the operator or the party responsible for operation of an offshore or onshore facility shall stipulate the strategies and principles that form the basis for design, use and maintenance of barriers, so that the barriers' function is safeguarded throughout the offshore or onshore facility's life".

On a more overall level, it is stated in § 9 of the Management Regulations that the operator shall set acceptance criteria for major accident risk and environmental risk.

The PSA regulations presume that the operators themselves define the overall acceptance criteria and that the criteria are broken down to performance requirements for the individual safety barriers. In practise (and as further discussed later in the report), this assumption is not consistently implemented throughout the

industry. In particular, safety critical equipment applied in drilling operations often seems to be lacking specific reliability requirements.

The OLF Guideline 070 [3], which is a national guideline and therefore applies to the Norwegian continental shelf, suggests the use of minimum safety integrity level (SIL) requirements for commonly used safety instrumented functions, as an alternative to the full risk based approach described in IEC 61508. The minimum SIL requirements are based on good engineering design practise to avoid human fatalities and injuries, and may not necessarily provide adequate reduction of environmental risk. In fact, the OLF-070 states that “special care should be taken” when these requirements are used to assess risk to environment and/or asset. It states: “For some cases, e.g. particularly vulnerable environmental areas, special considerations might result in a need for stricter requirements, whereas in other cases the requirements might be relaxed”.

3 Environmental risk analysis (ERA)

3.1 Introduction

Traditionally, offshore risk analyses have focused on the human asset, and still do. However, during the last few decades the awareness of environmental risk issues has increased, and today environmental risk analyses (ERA) are performed as part of all new developments on the Norwegian Continental Shelf (NCS). The importance of performing ERA has been made even more topical by the recent (April 2010) Deepwater Horizon accident in April 2010 and several other incidents related to loss of well control.

According to the PSA Framework Regulations [6] environmental risk equals the risk of pollution. By “risk of pollution” the regulations mean a *combination of probability and consequence of supply of solids, liquids or gas to the air, water or earth, as well as the influence of temperature that is, or may be, damaging or detrimental to the environment*. Further, PSA gives requirements on risk reduction, including environmental risk reduction, for all phases of petroleum activities. In this report we focus on acute releases to sea, so the pollution considered is therefore mainly limited to acute releases of hydrocarbons to sea. It should however be noted that the same barriers which protect the environment against acute releases (such as the BOP), will also protect personnel against hazardous events as well as the environment against acute gaseous releases to air.

Operators are required to assess the environmental risk from the offshore activities and to identify whether risk reducing measures are required in order to bring the risk to an acceptably low level. The ERA is to be approved by the authorities before the launch of the activities in question.

An uncontrolled release of oil may lead to large environmental damages, but fortunately such incidents occur very infrequently. Hence risk management related to avoiding large environmental releases cannot rely on learning from previous incidents only. Other methods for assessing the risk have to be applied, typically encompassing release scenario development, oil dispersion modelling and vulnerability modelling of marine and coastal resources.

3.2 ERA in regulations and standards

The purpose of an ERA is to provide decision makers with a tool that enables them to establish and maintain acceptable level of safety with respect to environmental protection for their operations. According to the PSA Management Regulations [5], an ERA shall be prepared for any exploration drilling, field development, and field operation on the NCS:

Section 16: Environmentally oriented risk and emergency preparedness analyses

Environmentally oriented risk analyses shall be carried out in respect of the individual facility. The analyses shall, inter alia, be carried out for acute pollution and for background load. It shall be possible to compare similar types of environmental risk contributions from various facilities unambiguously.

The NORSOK Z-013 standard on *Risk and emergency preparedness assessment* [14] gives requirements for the preparation of an ERA. The standard provides guidance on ERA objectives, main steps and content. Appendix C refers selected parts from NORSOK Z-013, from which we highlight the following points of particular relevance for the discussions in this report:

- Barriers on the installations that may prevent or reduce spills to the environment should be analysed
- Risk should be compared with the environmental risk acceptance criteria
- Risk contributions from different installations should be considered together

In order to meet the PSA requirements and to provide practical guidance on how to conduct an ERA, the industry has produced an ERA guideline called MIRA, which is discussed in the next section.

3.3 ERA in the MIRA guideline

MIRA is a method and guideline for environmental risk analysis developed by DNV on behalf of the Norwegian offshore industry (OLF). MIRA has been used on the NCS for more than 10 years. The methodology is continuously refined; the current version is the 2007 revision [8] which has been updated according to new knowledge on environmental risk analyses and existing regulations.

Main steps of the ERA described in the MIRA guideline are as follows:

1. Define acceptance criteria
2. Establish a description of the activity
3. Establish a probability estimate for an unwanted event
4. Establish a sufficient number of probable combinations of release durations and release rates in the environmental risk analysis
5. Oil spreading estimations
6. Perform estimations of harm
7. Estimate environmental risk

Also, the MIRA guideline specifies some general elements that should be included in an ERA:

- Acceptance criteria for environmental risk
- Spill scenarios (location, time, type of oil, oil spill rate, duration, progress)
- Data on wind and current conditions
- Occurrence of biological resources in the influence area
- The value of the resources (scientific value, preservation value)
- The resources' vulnerability to oil (on an individual and population level)

The objectives of MIRA are among others:

- Highlight the environmental risk related to an activity
- Highlight which activities/events related to an operation that contributes to environmental risk, in order to be able to implement frequency reducing measures (e.g. technical barriers, alterations to design, routines or other measures).
- Identify naturally present resources that will be vulnerable when acute releases occur, in order to carry out consequence reducing measures (e.g. oil-spill preparedness measures)

Regarding the frequency reducing measures, the guideline refers to PSA regulations stating that frequency reducing measures should be prioritised before consequence reducing measures, and that the effect of the risk reducing measures should be quantified. To identify frequency reducing measures, MIRA suggests that the acute release scenarios can be linked to specific activities contributing the most to acute release, e.g. completion or workover. The environmental risk from these activities will be influenced by barrier design and performance, e.g. of BOP and the kick detection systems. Further, MIRA proposes that the risk reducing effect from frequency reducing measures can be estimated either from updating the oil-drift calculations with new release rates, or by updating the risk estimate based on new release frequencies.

MIRA also gives guidance on the setting and use of environmental risk acceptance criteria; this is discussed in section 4.4.

4 Environmental risk acceptance criteria (ERAC)

This chapter gives a brief introduction to risk acceptance criteria in general and then presents regulations, standards and guidelines relevant for setting ERAC as required in the environmental risk analyses.

4.1 General risk acceptance criteria

Risk acceptance criteria (RAC) are used to express a risk level that is considered tolerable for the activity in question. Such criteria may be qualitative or quantitative and may refer to a phase or a specified activity.

Deciding how much risk is acceptable or tolerable is an important part of the risk management process. When performing quantitative risk analysis an estimate of the risk from hazardous events is obtained. This estimate can then be compared against the relevant risk acceptance criteria in order to consider whether the estimated risk is acceptable and for the further evaluation of risk reducing measures.

NORSOK Standard Z-013 [14] lists some qualities that are considered important for the RAC to be adequate as support for HES management decision. The RAC should (cf. section 5.2.2.7 of the standard):

- *Be suitable for evaluation of the activity/activities and/or system(s) in question.*
- *Be suitable for comparison with the results of the analysis 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. (But the application of RAC in risk evaluation will usually imply that one concept (or concepts) is (are) preferred over others, due to lowest risk).*

Further, Z-013 notes that due to uncertainty it is important that the RAC are satisfied with some margin.

It is further stated that the need for updating of RAC shall be evaluated on a regular basis, as an element of further development and continuous improvement of safety. Also, the RAC should be at a level where there is a reasonable balance between ambitions about continuous improvement, defined safety objectives and technology improvements on one hand and what is realistic to achieve on the other.

4.2 ERAC in PSA regulations

Below, references to important PSA regulations are given concerning ERAC. The most relevant text is highlighted with (*our*) italics.

4.2.1 The Framework Regulations

Section 11: Risk reduction principles

Harm or danger of harm to people, the environment or material assets shall be prevented or limited in accordance with the health, safety and environment legislation, including internal requirements and acceptance criteria that are of significance for complying with requirements in this legislation. In addition, the risk shall be further reduced to the extent possible.

In reducing the risk, the responsible party shall choose the technical, operational or organisational solutions that, according to an individual and overall evaluation of the potential harm and present and future use, offer the best results provided the costs are not significantly disproportionate to the risk reduction achieved.

4.2.2 The Management Regulations

Section 9: Acceptance criteria for major accident risk and environmental risk

The operator shall set acceptance criteria for major accident risk and environmental risk. Acceptance criteria shall be set for:

- a) the personnel on the offshore or onshore facility as a whole, and for personnel groups exposed to particular risk,
- b) loss of main safety functions as mentioned in Section 7 of the Facilities Regulations for offshore petroleum activities,
- c) acute pollution from the offshore or onshore facility,
- d) damage to third party.

The acceptance criteria shall be used when assessing results from risk analyses, cf. Section 17. Cf. also Section 11 of the Framework Regulations.

Guidelines to Section 9

Acceptance criteria as mentioned in the first subsection, shall express and represent an upper limit for what is considered an acceptable risk level for the various categories mentioned in literas a to d. Additional risk reduction shall always be considered, even if the results of risk analyses or risk assessments indicate a level of risk that is within the acceptance criteria, cf. Section 11 of the Framework Regulations.

The acceptance criteria shall be formulated so that they are in accordance with the requirement for suitable risk and preparedness analyses, cf. Section 17, and are suitable for providing decision-making support in relation to the risk analyses and risk assessments carried out. *The acceptance criteria should be formulated based on the damage potential and activity level represented by the activity.*

Offshore petroleum activities:

The [NORSOK Z-013](#) standard, Chapter 4, can be used to fulfil the requirements for acceptance criteria for major accident risk and environmental risk, with the following addition: When setting risk acceptance criteria as mentioned in the second subsection, litera a, an average risk determination should be made so that the acceptance criteria for the personnel as a whole, and for exposed personnel groups in particular, complement each other, see also the NORSOK Z-013 standard, Appendix A.2.1.4.

Acceptance criteria for environmental risk as mentioned in litera c, should be formulated so that the operator sees its own activities in an emergency preparedness region in an overall context. The acceptance criteria for environmental risk should be related to risky operations, and to facilities in the emergency preparedness region in question. The operators should cooperate on principles for establishing acceptance criteria, so that they are in a comparable form between operators, and so that they form a suitable basis for e.g. establishing joint emergency preparedness, cf. Section 42 of the Pollution Control Act (in Norwegian only) and Section 21 of the Framework Regulations.

When formulating and further developing the acceptance criteria for environmental risk, the operator should take into consideration the Storting White Papers and impact assessments that apply to the area.

4.3 ERAC in the NORSOK Z-013 standard

General aspects related to RAC were discussed in section 4.1 above. Acceptance criteria for environmental risk are treated in Annex A of the NORSOK Z-013 standard (section A.2.4 of the standard covers ERAC in particular). Here it is referred to the PSA Management Regulations for the requirements of ERAC for acute pollution. The NORSOK standard's description of ERAC is as follows:

Quantitative environmental RAC can be defined for various operations, e.g. drilling operation, operation of installations and/or fields. More than one type of RAC, per operation, can be established to be able to cover several analytical endpoints.

Environmental RAC should include frequencies of discharges to the environment that results in defined environmental consequences. As a simplification of this, frequencies of discharges to the environment of pollutants and their volume and consequence potential may be used.

Environmental consequences can be defined as recovery time of sensitive habitats or populations. It may also be defined as e.g. effect on individuals, populations or habitats, or exposure of areas/volumes of a certain environmental sensitivity, for instance length of polluted shoreline or areas with specifically sensitive resources.

An environmental RAC commonly applied for offshore activity on the NCS is based on recovery time for sensitive environmental resources. The RAC is divided into five consequence categories:

- 1. Insignificant damage: recovery time less than 1 month*
- 2. Minor damage: recovery time 1 month to 1 year*
- 3. Moderate damage: recovery time 1 year to 3 years*
- 4. Considerable damage: recovery time 3 years to 10 years*
- 5. Serious damage: recovery time more than 10 years*

The above mentioned environmental RAC based on recovery time, is specified as the upper limit for acceptable frequency for each of the consequence categories.

4.4 ERAC in the MIRA guideline

The MIRA method and guideline [8] issued by OLF, describes three approaches with different levels of detail for conducting environmental risk analyses.

The establishment of risk acceptance criteria for pollution is based on the guiding principle that the frequency of harm shall be “insignificant” compared to the consequence of the harm, measured in terms of the *restitution time* of affected marine and coastal resources. The restitution time is the time needed for a resource to return to its original state after being affected by pollution. With *resource* we understand any valued faunal or floral population or habitat, including shoreline, seabed or even bodies of water.

The responsibility of defining what corresponds to an “insignificant” (tolerable) frequency of harm in this context is left to the operators. This frequency may (according to the guideline) typically be 1 % or 5 % of the time, meaning that the environment should be unaffected 99 % or 95 % of the time respectively. Using 5 % implies that harm to the environment which lasts for instance 1 year should not occur more often than every 20th year on average, i.e. the *maximal return period* is 20 years (corresponding to a maximum annual acceptable frequency of $5 \cdot 10^{-2}$)

Based on a tolerance level of say 5 %, it is possible to derive at regional critical levels and maximal return periods.

Table 4.1 shows an example of possible resulting acceptance criteria when the activity level in the relevant region is defined as follows:

- 10 operations per facility per year
- 2 facilities per field
- 2 related fields in the region under consideration.

The assumed activity level and the relation between operations, facilities, fields and region is illustrated in Figure 4.1.

Table 4.1: Possible acceptance criteria when defining 5 % as the level of tolerable harm.

	Consequence category			
	Minor harm	Moderate harm	Significant harm	Serious harm
Restitution time (years)	0,1–1	1–3	3–10	> 10
Activity specific RAC (freq. per activity)	$1,25 \times 10^{-3}$	$4,25 \times 10^{-4}$	$1,25 \times 10^{-4}$	$2,5 \times 10^{-5}$
Facility specific RAC (freq. per year)	$1,25 \times 10^{-2}$	$4,25 \times 10^{-3}$	$1,25 \times 10^{-3}$	$2,5 \times 10^{-4}$
Field specific RAC (freq. per year)	$2,5 \times 10^{-2}$	$8,5 \times 10^{-3}$	$2,5 \times 10^{-3}$	5×10^{-4}
Regional RAC for fields seen together (freq. per year)	5×10^{-2}	$1,7 \times 10^{-2}$	5×10^{-3}	1×10^{-3}

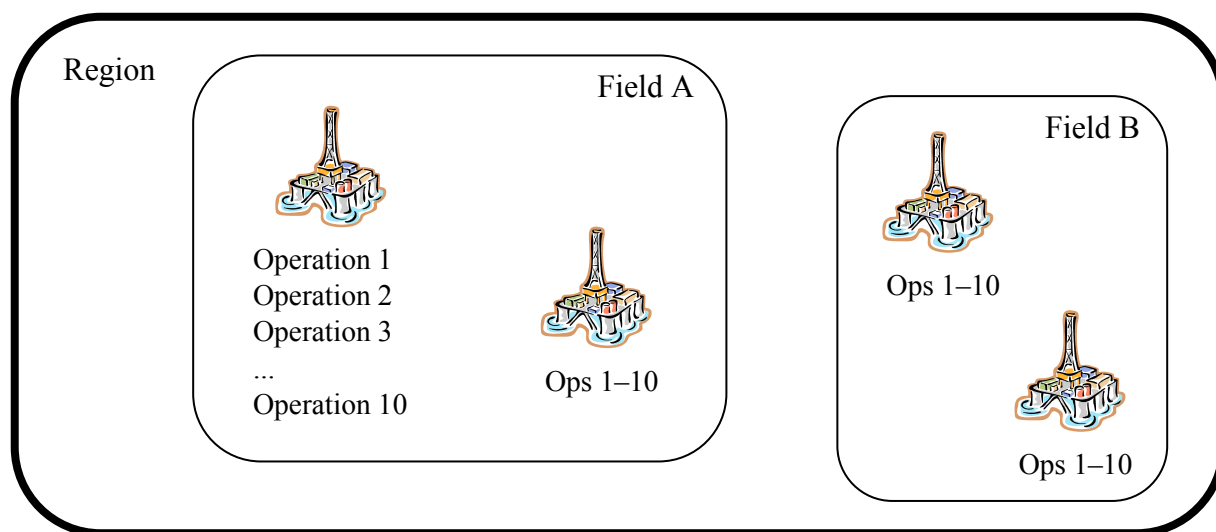


Figure 4.1: Illustration of the MIRA guideline example assuming 10 operations per facility per year, 2 facilities per field and 2 fields in the region.

In the MIRA guideline it is further recommended to establish specific acceptance criteria related to fields located in common emergency preparedness regions in order to achieve a good connection between environmental risk and emergency preparedness.

If the environmental risk exceeds the acceptance criteria, the activity is not acceptable and has to be modified. In practical terms this implies the introduction of risk reducing measures (focusing on probability reducing measures in preference to consequence reducing measures), or alternatively the activity must be terminated or not started. Even though the acceptance criteria are fulfilled, risk reducing measures shall be investigated according to the ALARP principle focusing on probability-reducing measures in preference to consequence-reducing measures.

In the MIRA method the ALARP area (defined as the risk from X % to 100 % of the acceptance criterion, where X is defined by each operator) is applied as guidance for the consideration of risk reducing measures. For example, a major operator defines X as 50, meaning that if estimated risk exceeds 50 % of the acceptance criterion, than risk reducing measures should be considered, otherwise not.

4.5 ERAC applied in the Norwegian petroleum industry

The different operators that are part of the PDS forum have been asked to provide their corporate ERAC. The general impression is that the operators have adopted the MIRA criteria approach. To our knowledge other types of ERAC have not been established by the operators.

When reviewing the operators' ERAC, it appears they have generally selected 5 % as the level of tolerable harm. The operators therefore end up with criteria similar to the example shown in Table 4.1. Table 4.2 illustrates how ERAC from an on-going development project are presented. They are based on the following assumptions:

- 5 % level of tolerable harm
- 5 fields per region
- 2 facilities per field
- 10 activities per facility

Table 4.2: Example of ERAC from an on-going development project.

Generic assessments					Field specific RAC		Facility specific RAC		Activity specific RAC	
Consequence category	Time for Restitution (year)	Average (year)	Regional limit (1/år)	Return period (year)	RAC for pollution	Return period (year)	RAC for pollution	Return period (year)	RAC for pollution	Return period (year)
Minor harm	< 1 year	0,5	$1,0 \times 10^{-1}$	10	$2,0 \times 10^{-2}$	50	$1,0 \times 10^{-2}$	100	$1,0 \times 10^{-3}$	1 000
Moderate harm	1– 3 years	2	$2,5 \times 10^{-2}$	40	$5,0 \times 10^{-3}$	200	$2,5 \times 10^{-3}$	400	$2,5 \times 10^{-4}$	4 000
Significant harm	3 – 10 years	5	$1,0 \times 10^{-2}$	100	$2,0 \times 10^{-3}$	500	$1,0 \times 10^{-3}$	1 000	$1,0 \times 10^{-4}$	10 000
Serious harm	> 10 years	20	$2,5 \times 10^{-3}$	400	$5,0 \times 10^{-4}$	2 000	$2,5 \times 10^{-4}$	4 000	$2,5 \times 10^{-5}$	40 000

From the review of the operators' criteria, it appears that the above table represents the "Norwegian petroleum industry ERAC standard".

5 Discussion of the current ERAC

When considering the ERAC as discussed in the previous chapter, a number of questions arises. These have been summarised in the following main questions that will be discussed in this chapter:

1. Are today's criteria adequate?
2. There is a general understanding that frequency reducing measures should have preference prior to consequence reducing measures. Do the current ERAC and ERA methodology encourage this? Are the acceptance criteria defined in such a way that they have any impact on design and/or operation?
3. Should the operators themselves define the acceptance criteria when the potential consequences will be harm to our common environment (fauna, flora, shoreline and beaches)?
4. The calculations of environmental impact are attached with a high degree of uncertainty. Can alternative or additional ways of establishing acceptance reduce this uncertainty?

5.1 Are today's criteria adequate?

It appears that all companies operating in Norway use the same criteria. These criteria are based on the MIRA ERAC example table and relate to consequence classes based on restitution times and maximum annual frequencies for events causing these consequences.

The MIRA ERAC is intended to be an *example* based on a set of assumptions about the activity in the region. The example table has nevertheless developed into some kind of static authority in the industry, and the figures therein are used more or less directly without paying any attention to the actual level of activity. Hence, the intention of making the criteria "field and region specific" does not seem to have been properly implemented.

There are several aspects of the MIRA approach that deserves attention. Below, some of them are discussed, in particular related to how the present ERAC are defined and interpreted. It is emphasised that many of these aspects are of principal nature and complex to deal with in practise. Nevertheless, they should be addressed and understood when applying the MIRA ERAC.

5.1.1 Tolerable harm and consequence categories which add up

As discussed above the operator has to define a level of tolerable harm in terms of the maximum acceptable proportion of time that the environment may be affected. However, the selection of 5 % instead of say 1 %, seem to be somewhat arbitrary. An interesting rhetorical question is therefore why it is acceptable that the environment is affected up to 5 % of the time.

MIRA employs four consequence categories (minor, moderate, significant and serious harm) according to the duration of the harm. In the MIRA example a 5 % level of tolerable harm is applied to each category independently. This means that in the long run, one accepts that the environment is affected 5 % of the time due to incidents in category "minor", but *in addition* also 5 % of the time due to incidents in category moderate, 5 % in category "significant" and 5 % in category "major". The *combined* level of tolerable harm from the four categories will therefore be close to 19 %!² This accumulating effect is not reflected or discussed in the MIRA guideline, and may therefore easily be disregarded when using the guideline.

² Calculation: $1-(1-0.05)^4=0.19$. Explanation: For a random point in time the probability of having an *unaffected* environment due to an incident in category "minor harm" is 95 %. The same probability applies for the other three categories, meaning that the probability of having an unaffected environment due to *any* incident is 95 % raised to the power of 4, i.e. $0.95^4 = 81$ %. Correspondingly, the probability of having an *affected* environment is 19 %.

- The restitution time measure directs focus towards consequence modelling but gives limited incentives to consider the frequency reducing barriers.

Since restitution time can be considered as a measure of the final consequences, it appears at the end of the event chain. This implies that a whole range of different parameters have to be taken into consideration (and quantified) in order to estimate the frequency of each consequence class. In brief, this will result in major uncertainties, as further discussed in section 5.4 below.

5.2 How does ERA/ERAC impact on design and operation of frequency reducing barriers?

5.2.1 Does today's ERA put focus on frequency reducing measures?

According to the PSA regulations [5], focus should be on *both* probability and consequences of pollution. From a review of some selected environmental risk analyses and discussions with experts, it appears that the ERA as per today focuses mainly on the modelling of the consequences of a release, i.e. the consequence reducing barriers. The analyses start with release frequencies (generic or field specific), so the barriers prior to the release are therefore not an explicit part of the ERA. Apparently these barriers are assumed covered by other analyses. Also, since the acceptance criteria applied in the ERA relates to the consequences of a release with respect to restitution time of selected vulnerable resources, it seems reasonable that the modelling in the ERA focus on consequences as well.

Further, it should be mentioned that neither the “environment part” of NORSOK Z-013 nor the MIRA guideline has a main focus on frequency reducing barriers. Hence, the industry has a considerable way to go in order to bridge the gap between restitution times and requirements to technical barriers – or said in another way: between biologists and engineers. There often appears to be some level of “dislocation” between those responsible for the design of the well and developing the drilling procedures and those tasked with the ERA.

It therefore seems fair to conclude that the present ERA has a limited ability to identify and suggest risk reducing measures. As discussed in the next section, the estimated environmental risk figures have generally been so low that identification of risk reducing measures has not been required. The analyses have therefore mainly functioned as a verification tool addressing company management and the authorities. A relevant question is therefore how to make the ERA or the ERAC more relevant for technical personnel.

5.2.2 Do current ERAC have any impact on design and operation?

One way of answering this question is to consider some typical generic blowout frequencies used in an ERA, as shown in Table 5.1.

Table 5.1: Basic blowout frequencies [9].

Type of operation	Frequency	Denomination
Exploration drilling	$2.9 \cdot 10^{-4}$	Per well
Production drilling	$7.4 \cdot 10^{-5}$	Per well
Completion	$9.2 \cdot 10^{-5}$	Per operation
Wire line operation	$7.1 \cdot 10^{-6}$	Per operation
Coiled tubing operation	$1.5 \cdot 10^{-4}$	Per operation
Snubbing	$3.6 \cdot 10^{-4}$	Per operation
Well overhaul	$2.7 \cdot 10^{-4}$	Per operation
Production	$9.8 \cdot 10^{-6}$	Per well-year
Gas injection	$1.9 \cdot 10^{-5}$	Per well-year
Water injection	$2.4 \cdot 10^{-6}$	Per well-year

How do these generic blowout frequencies compare to the given environmental acceptance criteria? Let us here consider a “worst case” scenario where we choose the strictest criterion, i.e. the criterion related to single activities (such as e.g. drilling of a well) causing severe environmental impact. Such catastrophic events shall, according to Table 4.2, not occur with a frequency exceeding $2.5 \cdot 10^{-5}$ per operation.

First remember that the acceptance criteria relate to the ultimate consequences, i.e. all the barriers, both frequency and consequence reducing, are included. Regarding the generic blowout frequencies, these incorporate only the frequency reducing barriers (e.g. mud and BOP in the case of drilling). Hence, when going from the frequency of a release (e.g. a blowout) and all the way through the event chain to the final consequences, the consequence reducing barriers will also have to be included in the calculations. I.e. there will be an additional risk reduction from the blowout occurs to the final consequences due to factors such as blowout rate and duration, weather conditions, wind and waves, distance to shore, oil collection on surface and shore, use of chemicals for decomposition of oil, burning of surface oil, vulnerability of fish and birds, stock sizes, etc. The average size of this “post-spill risk reduction” is difficult to generalize and depends on a number of these factors.

For this “worst case” consideration let us choose the drilling of an exploration well, an operation with a relatively high generic blowout frequency of $2.9 \cdot 10^{-4}$ per well (cf. Table 5.1). Now, observe that only a risk reduction factor of approximately 12 (from $2.9 \cdot 10^{-4}$ to $2.5 \cdot 10^{-5}$) is required in order to meet the acceptance criterion. In a typical ERA the “post-spill risk reduction” will include:

1. The first risk reduction factor associated with the release will be *blowout rate and duration*. In order to get severe environmental consequences with >10 years restitution time, the rate and duration has to be of a considerable size and length. Only a limited proportion of the generic blowouts fall into this category.
2. Secondly, as discussed above, once the oil is released there will be several mechanisms available that can limit the amount of oil that actually affect the vulnerable resources.
3. Finally, in order to experience severe environmental impact a relatively high proportion of the exposed resources (i.e. fish, marine mammals or birds) have to be killed. This only occurs with a certain (limited) probability.

In one ERA considered, the risk reduction from these factors was so large that the resulting frequency of “severe impact” was far below the acceptance criterion (actually less than 1 % of the criterion). Hence, no incentives to change design or operation arose from this analysis.

Note that the basic blowout frequency per well for exploration drilling has recently been reduced from $2.9 \cdot 10^{-4}$ to $1.5 \cdot 10^{-4}$ based on updated information from the SINTEF Offshore Blowout Database [21].³ Using this updated frequency, the required risk reduction factor decreases from 12 to 6, emphasizing even stronger how easy it is to meet the current ERAC given the historic blowout frequencies.

The environmental risk analyses as carried out today focus on oil drift and dispersion simulations and the emergency preparedness resources in place to limit the consequences of a spill. Based on the discussions above it seems fair to say that the current ERAC and ERA methodology do not direct similar attention to the frequency reducing barriers. For this purpose one will have to consult QRA studies or probably more relevant; specific reliability studies. However, such analyses traditionally focus on personnel safety and do not have any links to the environmental acceptance criteria. Hence, the quality of the technical barriers to a small degree affects the result of the ERA (and vice versa).

Further, current ERAC are not easy to understand for non-biologists as they relate to response time of organisms and how the organisms are exposed to oil given a set of environmental parameters and a given release scenario.

The overall impression, confirmed by discussions with ERA experts and authorities, is that risk estimates from ERA are generally well within the acceptance criteria. The current ERAC are therefore not strict enough to support the objective of continuous improvement as they do not put focus on risk reducing measures.

5.3 Who should determine the ERAC?

Today, each operator establishes their own ERAC that is adapted from the MIRA guideline (cf. discussion in section 4.5). Whether the authorities should have a more active role in setting overall criteria and goals for the environment is clearly a political question also affecting the principle of internal control. However, there are several arguments why this question needs to be raised:

1. As opposed to personnel risk which relates to the company's own employees, we are here dealing with national resources in terms of our common environment. Hence, the environment is like a third part which has to be considered across operators and beyond each company's interests. How do we measure the "cost" of the general public getting oil contamination on their beaches? And should the allowed frequency of such an event be decided by the oil industry alone?
2. It will be easier to coordinate the requirements across companies, areas and regions when an overall authority states or co-ordinates the requirements (rather than each company setting their own requirements). The guidelines to section 6 of the PSA Management Regulations states that "*The level of acceptable risk should be clarified in co-operation with other operators, if there be any, in the area that may be affected by the activities of the facility*". With today's regime this co-operation to a limited degree seems to have been implemented.
3. The idea of continuous improvement in the petroleum industry is laid down e.g. in the Ministry of Labour and Inclusion – White paper No. 12 (2005–2006) concerning Health, Environment and

³ Note that such numbers are based on very rare events, and are therefore very sensitive to the addition or removal of single blowout events in the observation period. In addition, the predictive value of averaging historical blowout observations can be questioned, particularly when there is a trend (towards improvement in this case). Furthermore, experience data relating to well events is often specific to the actual well conditions or to the area conditions and thus may be difficult to apply more generally.

Safety in the Petroleum Industry, where it is stated that “*The Government objective is to be world leading in Health, Environment and Safety*” and further in the Soria Moria 2 proclamation [20] which e.g. says that (our translation) “*The petroleum industry on the NCS shall be world leading in terms of oil-spill preparedness and environmental condition monitoring*”. These very ambitious goals should be followed up by ambitious criteria for acceptable environmental risk. As discussed in section 5.2.2, this does not seem to be the case given today’s practice.

From discussions in the PDS forum, it appears that the operators themselves want the authorities to be more active with respect to definition and follow-up of ERAC. Implementation of stricter acceptance criteria may push the operators further in order to identify measures to reduce the risk of acute releases to sea.

5.4 Uncertainty in environmental risk analyses

It should be noted that the results from ERA and estimated restitution times are attached with a high degree of uncertainty, due to the many factors that influence the environmental impact of an oil spill, including spill location, spill rate and duration, oil characteristics, waves, wind direction, current, time of year, presence and vulnerability of resources, etc. Consequently, the figures that are compared against the acceptance criteria will be attached with major uncertainties.

Figure 5.2 illustrates four phases of the consequence chain of a blowout and indicates that there is a considerable amount of uncertainty attached to calculations of restitution times for affected resources. Moving along the consequence chain, the total scenario uncertainty increases as the calculations incorporate an increasing amount of assumptions and input parameters. Normally, the environmental impact calculations are performed for a restricted set of relevant scenarios. In addition to the blowout frequency, the blowout rate and the duration of the blowout are mandatory inputs to the calculations. For oil drift calculations both location, time of year, wind, current and oil characteristics are important parameters. Furthermore there are many types of environmental resources on which the effect from the oil varies (illustrated as resources A, B and C in the two rightmost phases in the figure).

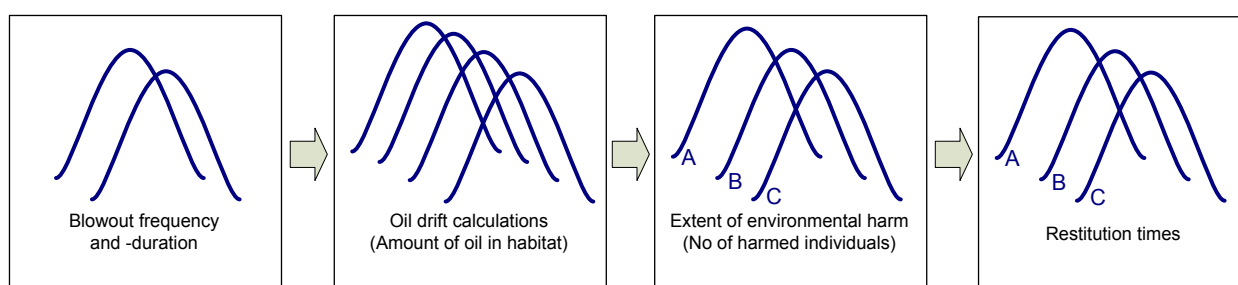


Figure 5.2: Total scenario uncertainty increases along the event chain – here represented with four phases – as the calculations incorporate an increasing amount of assumptions and input parameters [13].

Observe that if the acceptance criteria are expressed in terms of parameters earlier in the event chain (e.g. blowout frequency), the uncertainty may be reduced, and it will probably become easier for the operators to understand and have control with the criteria. Alternative ways of expressing the ERAC are further discussed in chapter 7.

6 Safety Barriers and associated performance requirements

In the preceding chapters focus has been on overall acceptance criteria and environmental acceptance criteria in particular. In this chapter we consider safety barriers to prevent and limit accidental releases to the environment and the associated performance requirements that are given for these barriers. This chapter summarizes the more detailed discussions in Appendix B.

The following safety barriers are discussed in this chapter with respect to barrier performance requirements:

- Drilling Facilities
 - Emergency Power
 - Mud and Cementing Systems
 - Well Control Systems (incl. BOP)
 - Drilling Instrumentation
 - Drilling ESD system
- Well Intervention Equipment
 - Well Intervention Activities
 - Requirements to Well Intervention Equipment
 - Typical Safety Functions during Well Intervention – an Example
- Subsea Production Safety Functions – ESD and PSD
 - Emergency Shutdown (ESD)
 - Process Shutdown (PSD)
- Well Barriers as Described in D-010
- Summary of Performance Requirements

6.1 Type of barrier performance requirements

In general and based on the PSA Management Regulations § 5 concerning barriers, performance requirements can be seen as comprising three elements:

- *Functional requirements*; i.e. qualities such as capacity and efficiency related to the effect that the barrier has on the event/accident chain given that it functions;
- *Integrity requirements*; i.e. qualities such as availability and reliability related to the barrier's ability to function when required and/or demanded;
- *Vulnerability requirements*; i.e. qualities related to robustness and the barrier's ability to withstand relevant accidental loads.

In this report, focus has been on functional and integrity requirements, since such requirements (to some degree) can be found in the referred standards and guidelines (such as e.g. NORSOK and OLF-070). Vulnerability requirements are normally specified on a more case by case basis in design and engineering projects and have therefore not been covered here.

Note that the barrier requirements discussed in this chapter are based on the national and international standards and guidelines that are referenced by the PSA. Company internal documents (which may contain additional requirements) have not been considered in particular.

6.2 Performance requirements for drilling facilities

Drilling emergency power

Emergency power shall facilitate operations to secure the well and associated equipment by maintaining the mud column barrier in case of loss of main power.

- A number of functional requirements concerning which operations that emergency power shall facilitate are given in NORSOK D-001. These requirements apply in the case of main power failure where emergency power is required to secure the well and associated equipment by maintaining the main barrier (i.e. mud balancing). However, if loss of main power and transfer to emergency power is caused by an ESD, securing the well by activating the BOP may be more relevant.
- OLF-070 does not include any SIL requirements to drilling emergency power (or no requirements to emergency power at all)

Mud and cementing systems

The mud column is one of the two main barriers for drilling and completing a well. The mud column and its control is an operations function, even though loss of control can lead to an emergency situation. The mud and cementing systems include the bulk system, mud mixing and storage systems, the high pressure mud pumping system, the mud treatment system and cementing systems.

- A number of functional requirements (e.g. concerning capacity) for the mud and cementing systems are given in NORSOK D-001.
 - A general requirement to drilling facilities in D-001 is that regularity requirements shall be defined prior to the design. For the high pressure mud system the requirement is “regularity as high as possible”. This is not a precise or verifiable requirement.
 - Only single level transmitters are required in the mud storage and mud treatment tanks although level measuring is known to be fairly unreliable
- There is no SIL requirement set in the OLF-070 guideline. The mud circulation system is regarded as an operations function. The OLF-070 guideline compares the mud circulation system with the process control function of a process plant.

Well control systems (incl. BOP)

Well control systems are in NORSOK D-001 [24] defined as the mechanical well control and associated equipment and systems. This includes BOP, choke & kill system, diverter system, riser system, wellhead connectors and the control system for the BOP.

- According to NORSOK D-001 the BOP blind shear ram (BSR) shall be capable of shearing the drill pipe as well as closing off the well bore. There are no requirements that the BSR shall be able to cut tool joints. The position of the tool joint has to be known, or dual shear-rams have to be installed in order to shear the drill pipe over/under the drill pipe tool joints.
- In case of BOP failure and a topside blowout, the diverter system appears as the “last line of defence” with respect to reducing the amount of flammable hydrocarbons on the rig. The design requirements for the diverter system are relatively vague (ref. details in Appendix B.1.3.5). It should therefore be considered to review today’s systems and update relevant standards (in particular NORSOK D-001) to reflect current best practice. In general, when activating the diverter system it should only be possible to route the flow overboard [32].

- Explicit SIL Requirements have only been put upon the Drilling BOP function. The OLF-070 discussion concludes:
The required PFD/SIL for the BOP function for each specific well should be calculated and a tolerable risk level set as part of the process of applying for consent of exploration and development of the wells. As a minimum the SIL for isolation using the annulus function should be SIL 2 and the minimum SIL for closing the blind / shear ram should be SIL 2.”
- The marine drilling riser emergency quick disconnect (EQD) function is discussed in the OLF-070 guideline. The OLF-070 conclusion is:
Required SIL level for emergency disconnect for each specific well should be calculated and a tolerable risk level set as part of the application for consent process for exploration and development wells. The emergency disconnect for the marine drilling riser should have a minimum SIL level of SIL 2. This is based on historical information more than a detailed assessment of existing emergency disconnect systems. It is not known whether this can be documented for existing systems.
- Some relevant findings from different Deepwater Horizon accident investigation reports are given below:
 - According to BPs own investigation report [30], one fault (missing battery power) was found in one pod, and an erroneous solenoid valve was found in the other pod. This illustrates the importance of proper condition monitoring and testing of redundant equipment.
 - Given the above mentioned pod errors alone, an acoustic backup system might have been able to close the Deepwater Horizon BOP. It has however been claimed that acoustic systems are sensitive to mud clouds and gas plumes and that an acoustic system might not be functional in the event of a blowout (ref. [35]).
 - Even with redundant pods and acoustic backup the shuttle valve will be a single source of failure for a given BOP. This valve, however, is considered to be a simple and highly reliable component [30].
 - An important recommendation from the recent BOEMRE report into the Deepwater Horizon accident [33] is that better and more clear-cut procedures on when to activate the emergency disconnect function are required. In the case of Deepwater Horizon, this function was activated too late and the hydraulic/power/signal lines to the lower marine riser package were probably already torn off by the explosion.

Drilling instrumentation

The Drilling Instrumentation Package shall monitor and log parameters related to drilling and well activities. The system shall also be designed to handle alarms, status and hours in operation for equipment as required in NORSOK standards or recommendation from equipment suppliers.

- Quite detailed design requirements for the drilling instrumentation have been set in NORSOK D-001.
- In D-001 there are no requirements for kick detection systems. For marine risers at considerable water depths an early kick detection device “should be considered”. The OLF-070 guideline discusses kick detection systems. According to the guideline it is not recommended to set a minimum SIL requirement for kick detection due to the following:
 - *“Kick detection is only one of the information elements required in the decision process for activating the BOP”.*

- *"Kick detection is required for process control of the mud column. It does not automatically initiate an action".*

Drilling ESD system

Requirements to ESD systems can be found in NORSOK S-001. This standard does not, however, focus on drilling applications but merely topside production. For emergency shutdown principles on drilling rigs, reference is made to NMD's "Brannforskrift" and/or DNV OS-A101 ("Safety principles and arrangements") which include a separate chapter on special provisions for drilling units. Figure B-4 and B-5 in Appendix B show two examples of possible shutdown hierarchies for a mobile offshore drilling unit (MODU).

- The number of possible operational scenarios and situational variety involved in drilling operations, e.g. related to which barriers are available and therefore shall be included in the ESD hierarchy for a given situation, indicate that developing an unambiguous and general shutdown logic for a mobile drilling unit is extremely challenging.
- The remedy for this complexity tends to be extensive manual response and manual activation of technical barriers such as diversion of flow, activation of BOP/EDS and initiation of shutdown actions related to ignition sources and stop of main machinery.

6.3 Performances requirements for well intervention equipment

Well intervention is any operation carried out on an oil or gas well during, or at the end of its productive life, that alters the state of the well or provides additional well diagnostics. Well intervention activities as well as relevant systems and requirements are further discussed in Appendix B.2. Some main observations are summarized below.

General observations

- Requirements to well intervention equipment are described in NORSOK D-002 [25] and NORSOK D-010 [26]. Also, other standards may apply (e.g. NORSOK Z-015 for temporary equipment)
- In addition to specific requirements stated in D-002, the standard requires that planning, design, fabrication, operation and maintenance of well equipment shall be according to a list of other standards. (See Tables 1-5 in D-002). The NORSOK D-010 standard focuses on well integrity and requirements to well barrier elements that shall be present during different drilling and well operations, including well intervention activities.

Well intervention equipment

- Well intervention equipment is normally taken on board in temporary containers. The requirements for such temporary equipment seem somewhat diffuse and there are a lot of cross-references between standards. It has been commented that containers with well service equipment frequently are treated as "ignition group 1" equipment and are therefore disconnected on single gas detection.
- It has also been commented that BOPs applied during well intervention often are designed according to API 16D where the definition of failsafe and NE/NDE are not necessarily in line with NORSOK D-002.
- It is a concern that well intervention safety functions (ESD, PSD and EQD) and control functions are often implemented into one single PLC, since a PLC failure may then affect more than one function. Independence between ESD, PSD and EQD is not ensured and furthermore the safety functions are

not independent of well control used during normal operation. Also, there may be utility systems, such as purge and power supply, which upon failure may leave the PLC unable to operate.

- The OLF-070 guideline discusses well intervention BOP functions with respect to setting SIL but concludes that the background for stating a minimum SIL requirement is not found to be available.
- If the SIL concept is adapted, it may be found that the level of hardware fault tolerance mandated by the architectural constraints in IEC 61508 and OLF-070 conflicts with other design considerations for well intervention systems.

6.4 Performances requirements for subsea ESD and PSD functions

In Appendix B, a major part of the discussion concerns performance requirements for drilling related systems. In addition, instrumented functions with the purpose of protecting subsea production installations are also discussed. This includes (among others) subsea ESD and PSD functions that are identified in OLF-070 [3].

General observations

- Currently, commonly used standards on SIS focus mainly on topside facilities (e.g. Norsok S-001). When it comes to subsea production facilities and drilling operations there seems to be some more confusion related to which standards to use for emergency shutdown and production shutdown functions.
- The Norsok S-001 standard [23] only includes two sections that can be regarded as relevant for subsea production applications: Emergency Shutdown (ESD) and Process Safety / Production Shutdown (PSD). These subsea shutdown systems and associated requirements are further discussed in Appendix B.3.
- The Facilities Regulations § 33 requires *independence* between ESD and systems for management, control and other safety systems and it has traditionally been mandated to have a relatively clear split between safety and non-safety systems. Yet, this level of independence is being challenged by the technological solutions that are being selected for subsea production systems.

Emergency shutdown (ESD) functions

- The SIL concept has been adopted, in light of standards such as IEC 61508, IEC 61511, and OLF-070. Only one subsea production related ESD function is included in OLF-070. This function is "isolation of subsea well" and a SIL 3 requirement is stated.

Production shutdown (PSD) functions

- SIL requirements concerning subsea PSD functions are per today not included in OLF-070. Since subsea production equipment including pumps/compressors and separators are increasingly taken into use, this should be included in a future update of the OLF-070 guideline.
- Furthermore, minimum SIL requirements are missing for several other types of subsea functions. An example here is subsea leakage detection which, given the right technology, may have a large effect, in particular with respect to environmental risk.
- Possibly off topic, but it should be mentioned that requirements to offshore loading equipment seem to be missing. It may be that systems not being defined as safety critical, such as offshore loading, should be redefined as safety critical in light of being contributors to environmental risk.

6.5 Well barriers as described in Norsok D-010

Norsok D-010 [26] focuses on well integrity by defining minimum requirements and guidelines for well design, planning and executions of well operations on the Norwegian continental shelf. Well integrity is described as the application of technical, operational and organizational solutions to reduce the risk of uncontrolled release of formation fluids throughout the entire life cycle of the well, as well as other safety aspects. The Norsok D-010 standard is currently under revision.

Selected parts of Norsok D-010 are further discussed in Appendix B.4. Some main observations concerning the standard are summarized below.

- Norsok D-010 has established a well barrier terminology in lack of international standard definitions. The standard is not exhaustive with respect to activities and operational situations covered.
- The terminology and definitions given in Norsok D-010 are to some degree ambiguous. For example the relationship between well barrier element (WBE) and well barrier (WB) is somewhat unclear (see Appendix B.4. for details).
- The standard states that the primary and secondary well barriers to the extent possible shall be independent, but allows for common well barrier elements if "a risk analysis be performed and risk reducing/mitigating measures applied to reduce the risk as low as reasonable practicable". Since, the primary well barrier to a large degree must be considered as an operational (control) measure, this potential mix-up of control and safety must on a principal basis be questioned (ref. e.g. PSA Facilities Regulations [4], § 33–34).
- Norsok D-010 includes some requirements to deepwater wells. In particular, the riser instrumentation (current and inclination measurement systems) has an important safety function as part of an emergency disconnect, and may therefore be subject to possible SIL/EIL requirements.
- Norsok D-010 includes a separate section on "Activity and operation shut-down criteria" (i.e. section 4.6). It would have been beneficial if this section included more specific criteria as to when an activity shall be halted. Experience from a number of well incidents both on the NCS and abroad shows that numerous danger signals have been present prior to the event, but the operation has been carried on. More explicit and specific stop criteria would therefore be beneficial and should be considered included as part of the on-going Norsok D-010 update.

6.6 Summary of performance requirements

Based on the above sections and the more detailed discussions in Appendix B, Table 6.1 provides a summary of performance requirements for the systems under consideration. This includes integrity requirements (e.g. SIL requirements), functional requirements (e.g. closing time, accumulator capacity, etc.) and other relevant requirements (such as testing requirements). The table is by no means exhaustive, but highlights some requirements that are considered relevant for the safety instrumented parts of the barriers to prevent and limit releases to sea.

Table 6.1: Summary of performance requirements for safety barriers under consideration.

System	Type of performance requirement		Comments / references / other requirements
	Integrity	Functional	
Drilling			
• General			A general requirement to drilling facilities is that regularity requirements shall be defined prior to detailed design.
• Emergency Power	No SIL requirements given in OLF-070	Some requirements given in NORSOK D-001	The functional requirements apply in the case of main power failure where emergency power is required to secure the well and associated equipment by maintaining the main barrier (i.e. the mud column).
• Mud and Cementing Systems	No SIL requirements given in OLF-070	Various functional (incl.capacity) requirements are given in NORSOK D-001	The mud circulation system is regarded as an operations function. The OLF-070 guideline compares the mud circulation system with the process control function of a process plant
• Well Control Systems (incl. BOP)	Drilling BOP - SIL 2, i.e. the annulus function should be SIL 2 and the minimum SIL for closing the blind/shear ram should be SIL 2	A number of functional requirements concerning response time, accumulator capacity, etc. given in NORSOK D-001 and also in NORSOK D-010	NORSOK D-001 describes minimum structural requirements of BOP system.
• Drilling Instrumentation	No SIL requirements given in OLF-070	A number of functional requirements given in NORSOK D-001	No specific requirements to kick detection given in NORSOK D-001. Kick detection discussed in OLF-070 but no SIL requirements given. Further reference to NORSOK standards I-001 and Z-010 given in D-001.
• Drilling ESD system	No SIL requirements given in OLF-070	Section 5 (and partly section 8) of DNV-OS-A-101 [34] include requirements relevant for drilling ESD systems, e.g. concerning fail safe functionality	The operational variety involved in drilling operations results in extensive manual response and activation of technical barriers such as diversion of flow, activation of BOP and initiation of shutdown actions related to ignition sources and stop of main machinery. Manual functions are generally not given any SIL requirements.
Well intervention			
• General	OLF 070 has not found sufficient background information to set any SIL	A number of functional requirements concerning response time, accumulator capacity, power	A general requirement to well intervention equipment is that regularity requirements shall be defined prior to detailed design.

System	Type of performance requirement		Comments / references / other requirements
	Integrity requirements	Functional packages, etc. given in Norsok D-002	
<ul style="list-style-type: none"> Well intervention BOP 	No SIL requirements given in OLF-070	A number of functional requirements for BOP systems during well intervention is given in Norsok D-002 and also in Norsok D-010	From other SINTEF projects it is known that a SIL 2 requirement has been stated for BOP workover functions
Subsea ESD functions			
<ul style="list-style-type: none"> Isolation of subsea well 	SIL 3 (OLF-070)	Functional requirements given in Norsok S-001, but unclear to which degree these requirements apply for subsea equipment	<p>The only subsea ESD function defined in OLF-070 is "Isolation of subsea well" which in general is given a SIL 3 requirement.</p> <p>I should be noted that when a SIL requirement is given, this is related to some standard/conventional designs as further described in OLF-070.</p>
<ul style="list-style-type: none"> Subsea Well, APS Subsea Well, Hydraulic bleed Subsea Well, Electrical cut 	SIL 3 (OLF-070)	Maximum response times must be defined	In order to fulfil the OLF-070 requirement, 6 monthly valve testing has been assumed in the guideline
	SIL 3 (OLF-070)		
	SIL 2 (OLF-070)		
Subsea PSD functions			
<ul style="list-style-type: none"> General 	No SIL requirements identified for subsea PSD functions	-	No subsea PSD functions described explicitly in OLF-070

7 Relating the acceptance criteria to safety barrier requirements - alternative ERAC

In this chapter we discuss what is required in order to establish a link between environmental risk acceptance criteria and the reliability requirements for barriers applied during drilling, workover and subsea production. An important question is how to express acceptance criteria to make them more suitable for resulting in specific requirements to the barriers.

The ERAC currently used are related to restitution times. As discussed in the previous chapter, the restitution time measure is somewhat difficult to estimate, not straightforward to comprehend and it depends on a large number of factors attached with a considerable degree of uncertainty. In this chapter we will therefore discuss some alternative and simpler measures for expressing the ERAC. It is emphasized that such alternative ERAC measures are not meant to *replace* the existing restitution time measure, but could come as a *supplement* to be considered in cases where there is a need for simpler criteria in order to be able to establish requirements to technical systems.

The ERACs suggested in this chapter are simpler in the sense that they focus on release frequencies and volumes, i.e. "cutting off" the event chain at a much earlier stage compared to the ERAC based on restitution times (cf. Figure 5.2). Important characteristics of specific release scenarios – such as type of oil, drift and dispersion, and the presence and vulnerability of valued resources – are therefore disregarded. These aspects may be incorporated in various ways, making the analysis more nuanced, but at the same time increasing the complexity and reducing the possibility to establish a logical link between the criteria and the technical barriers.

7.1 Maximum acceptable frequency of specified scenario

A possible option for expressing ERAC can be to state a maximum acceptable frequency, either for a set of scenarios in total or for specific scenarios or activities. Relevant scenarios with respect to acute releases to sea were listed in section 1.4, and some important ones include:

- blowouts
- pipeline leaks
- releases from storage tank
- releases when loading/offloading oil

For blowouts and releases during loading/offloading there will be several frequency-reducing barriers involved. It may therefore be appropriate to give ERAC in terms of maximum allowable release frequency for a given operation (e.g. for a drilling operation or an offloading operation) or for a specified period of operation (e.g. one year). This requirement can then be "broken down" to specific requirements on an equipment level (see section 7.1.1).

Pipeline leaks and releases from storage tanks are mainly related to integrity of the containment barrier, but can also depend on the successful operation of frequency reducing barriers such as subsea HIPPS (for pipelines) and ESD isolation valves (to isolate cargo tanks).

When defining a maximum acceptable frequency of a specified scenario, this can e.g. be done analogous to the common acceptance criteria for over-pressurisation of a topside pressure vessel. This criterion is normally expressed as an acceptable hazard rate, i.e. frequency of events per year that can cause rupture of a pressure vessel (i.e. "the 10^{-5} criterion"). A comparable risk acceptance criterion for a drilling operation can for example be:

The maximum acceptable frequency of a blowout is $5 \cdot 10^{-5}$ per drilling operation.

In order to make this criterion more nuanced, the acceptable frequency could also be adjusted based on application specific conditions related to the facility and the vulnerability of the area under consideration. It may for example be possible to define “vulnerability classes” where parameters such as distance to shore, type of released oil, presence of vulnerable resources, activity level, etc. are applied for deciding whether the overall vulnerability of the area is either high, medium or low (as an example). The maximum acceptable blowout frequency could then be expressed in terms of vulnerability as indicated in Table 7.1.

Table 7.1: Example of possible ERAC related to maximum blowout frequency based on vulnerability.

Vulnerability of area	Maximum acceptable blowout frequency (per operation)
Low	$1 \cdot 10^{-4}$
Medium	$5 \cdot 10^{-5}$
High	$1 \cdot 10^{-5}$

ERACs based on maximum acceptable blowout frequencies are simple and appealing, but also have a number of challenges related to them. As per today, considerable efforts are made to reduce the probability of a blowout but these often result from qualitative assessments by those responsible for the drilling operation. Hence, there seems to be potential for more effective use of quantitative risk analysis (QRA) when evaluating the risk of blowout or well releases.

Models, tools and techniques for estimating well specific blowout frequencies exist and are used in various projects. Comments from users of these models indicate that they are useful, and give considerable additional qualitative insight. It is also commented that the models to a variable degree are sensitive with respect to reflecting the quantitative effects from changes in well design, operational procedures, performance of the physical barriers, equipment specifications or physical/hydraulic characteristics of the specific well. To have a risk criterion on acceptable blowout frequency is therefore appealing, but may require some further development of models and input data for estimating well specific blowout and kick frequencies.

In order to adjust the ERAC according to vulnerability along the lines of Table 7.1, effort needs to be put into analysing the particular area under consideration as well as characteristics of the release situation. This will involve analyses similar to those performed in ERA today, where the vulnerability of each area and the environmental consequences are considered. Since preparations for PDO (Plan for Development and Operation) shall include an impact assessment with respect to the environmental consequences⁴, it should be possible to categorise a given area according to vulnerability classes as given in Table 7.1 at a quite early project stage.

In the next section an example is given of how such a “frequency criterion” could result in requirements on a technical barrier level.

7.1.1 Example – requirement to BOP from maximum tolerable blowout frequency

Consider as an example a drilling operation where the following assumptions apply:

⁴ Ref. PSA Guidelines for plan for development and operation of a petroleum deposit (PDO); <http://www.npd.no/en/Regulations/Guidelines/>

- The well kick frequency will vary depending on the type of drilling operation, but is here set to 0.2 per operation (i.e. 5 drilled wells for each kick)
- The acceptable blowout frequency for the operation under consideration is set to $5 \cdot 10^{-5}$
- Available risk reducing functions include the mud column and the BOP.

Let us start with the general risk reduction scheme as given in the IEC 61508/61511 standards. Associated with a given operation or activity, here drilling of a well, there will be a certain associated risk. In order to bring this risk below a tolerable level, risk reducing measures are introduced. The starting point will be the risk present during normal operation, i.e. in our example a normal drilling operation with a mud column present to balance the pressure in the well. A *demand* arises when the presence of this mud column is no longer sufficient to balance the pressure in the well (i.e. a kick). Circulation of heavier mud is then the preferred and most common method to regain control of the well in such a kick situation. If this is not successful, it will be possible to close the BOP. It should be noted that operation of these two barriers are interrelated since the BOP is used while pumping heavy mud into the well and allowing gas and light mud to exit through the choke lines. However, for the purpose of this example they can be considered independent since the BOP includes additional shut down devices such as annular preventers, bore rams and the shear ram.

The scenario as described above is illustrated in Figure 7.1.

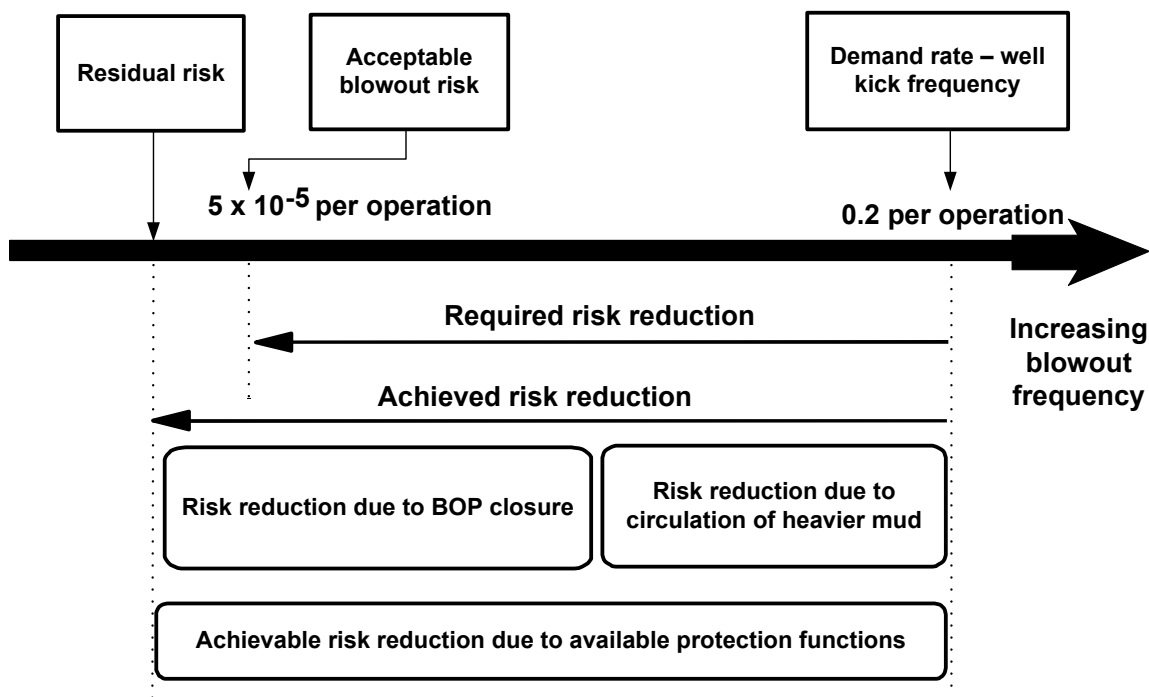


Figure 7.1: General risk reduction scheme for drilling operation.

From Figure 7.1 it is seen that a risk reduction from 0.2 to $5 \cdot 10^{-5}$ is required, corresponding to a factor of 4 000. This required risk reduction factor can be applied to derive at equipment requirements as illustrated in Figure 7.2.

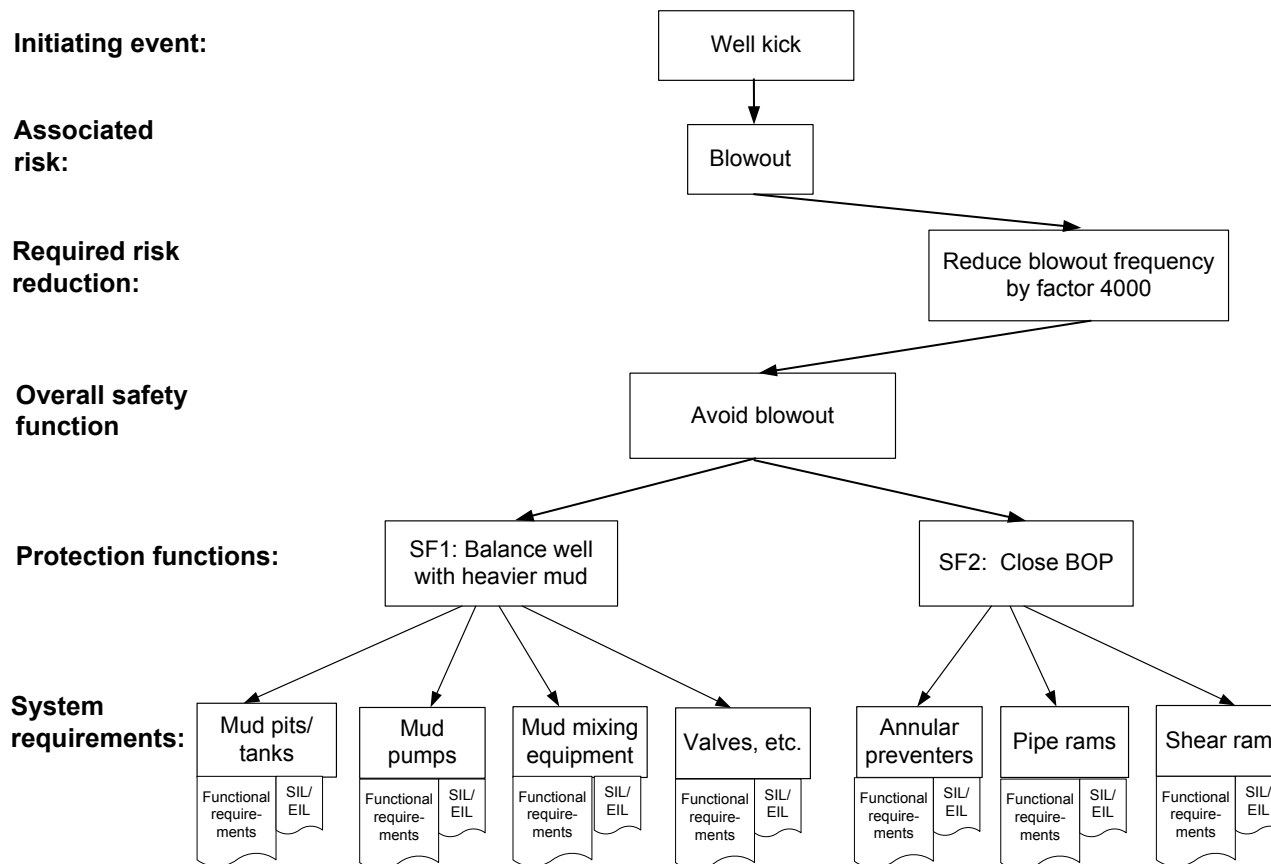


Figure 7.2: Risk reduction and resulting system requirements for drilling operation.

Hence, with the given assumptions, and by stating or assuming a certain reliability of the heavy mud function, it will be possible to deduce a requirement to the BOP. If for example it can be assumed that circulation of heavier mud is successful in 80 out of 100 demands (i.e. $PFD_{\text{mud}} = 0.2$)⁵, the resulting PFD_{BOP} requirement on the BOP stack will become:

$$PFD_{\text{mud}} \cdot PFD_{\text{BOP}} \cdot \text{demand rate} < 5 \cdot 10^{-5} \rightarrow PFD_{\text{BOP}} < 5 \cdot 10^{-5} / (0.2 \cdot 0.2) \rightarrow PFD_{\text{BOP}} < 1.25 \cdot 10^{-3}$$

I.e. PFD for the BOP must be less than $1.25 \cdot 10^{-3}$. This corresponding to a SIL/EIL 2 function, but note that the requirement is quite close to a quantitative SIL 3 requirement (i.e. a PFD between 10^{-3} and 10^{-4}).

7.2 Maximum acceptable frequencies of specified release volumes

In the above section we considered an ERAC expressed as the maximum allowable frequency of a specified scenario, such as e.g. a blowout. A possible “refinement” of such a criterion is to define classes of release volumes, and for each of these classes give an associated acceptable frequency. An example of how such acceptance criteria could be expressed is given in Table 7.2.

⁵ The justification for using this PFD value can be found in [22].

Table 7.2: Example of possible ERAC related to released volumes of oil to sea.

Consequence class	Released volume of oil to sea	Acceptable annual frequency
Minor harm	< 10 m ³	10 ⁻¹
Moderate harm	10–100 m ³	10 ⁻²
Significant harm	100–1000 m ³	10 ⁻³
Serious harm	1000–10 000 m ³	10 ⁻⁴
Major/Catastrophic harm	> 10 000 m ³	10 ⁻⁵

When for example considering the consequence class “major/catastrophic harm” where the released volume exceeds 10 000 m³, the maximum acceptable frequency of such an event is here set to 1·10⁻⁵ per year, corresponding to a return period of 100 000 years. Comparable to the example in the previous section, the risk of such an event occurring given no protection functions (i.e. the demand rate) can be estimated, and requirements to the protection functions can be derived.

In an on-going Norwegian offshore development project the operator has, instead of restitution times, used released amount of oil in order to define equivalent consequence classes for a calibrated risk graph. Using calibrated risk graph is further discussed in section 7.3.

Similar to the criterion of maximum acceptable blowout frequency discussed above, the acceptable frequency of released volumes could also be adjusted based on application specific considerations related to the facility and the vulnerability of the area under consideration.

7.3 Calibrated risk graph

Calibrated risk graph is a semi-quantitative method described in IEC 61511-3, Annex D [2], enabling the safety integrity level of a SIF to be determined from knowledge of the risk factors associated with the process and basic process control system. The risk graph approach can also be used to determine the need for risk reduction where the consequences include acute environmental damage (and also asset loss).

Calibration of the risk graph is the process of assigning numerical values to risk graph parameters. The objectives of the calibration process are as follows:

- 1) To describe all parameters in such a way as to enable the SIL/EIL assessment team to make objective judgments based on the characteristics of the application
- 2) To ensure the SIL/EIL selected for an application is in accordance with corporate risk criteria and takes into account risks from other sources
- 3) To enable the parameter selection process to be verified

An example of a calibrated risk graph from a Norwegian offshore project is shown in Figure 7.3.

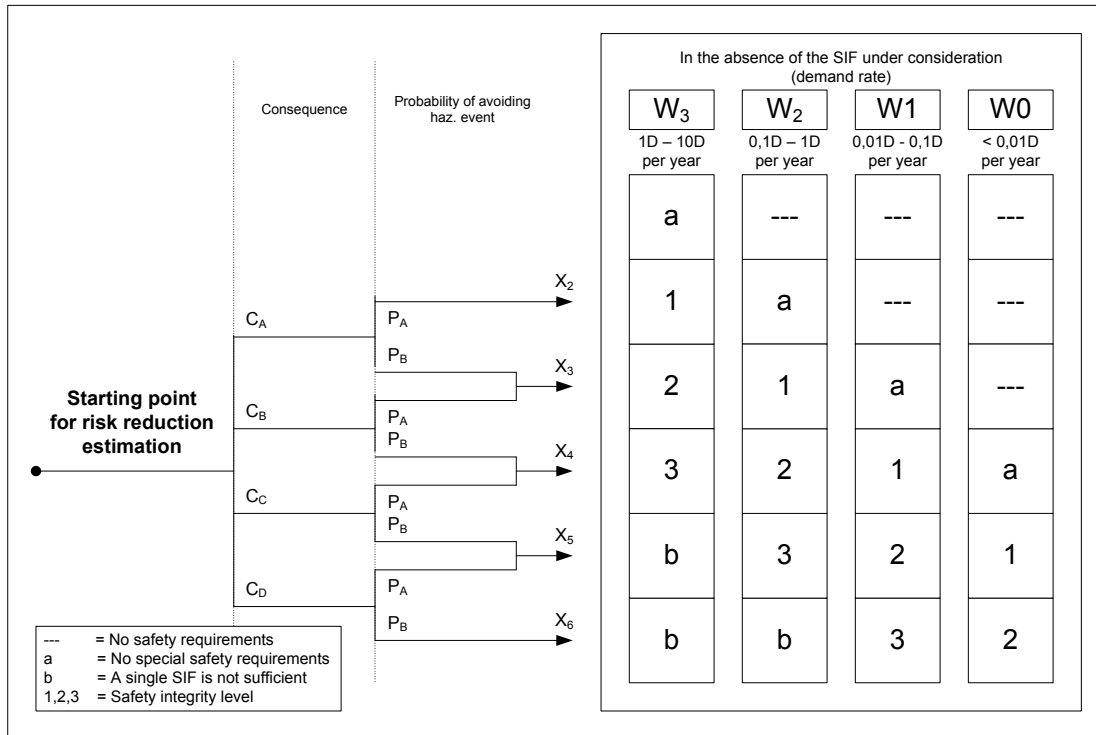


Figure 7.3: Calibrated risk graph for determination of EIL – example from project.

The associated consequence classes have been defined as shown in Table 7.3. Note that in the calibrated risk graph, consequence classes based on restitution time have been substituted with the consequence parameter C based on released volume, which is a more manageable quantity.

Table 7.3: Calibration of C parameter – example from project.

C parameter	Classification	Released Volume	Comments
C _A	A release large enough to be reported to plant management. Small scale liquid spill	< 1 m ³	All spills are to be reported to management. The effects of small spills are expected to be negligible; however, the potential for harm to marine organisms is present.
C _B	Release with significant damage. Spill within the vicinity of the installation, but with potential for significant damage and risk of spreading to surrounding environments.	1–100 m ³	Typical process leaks or minor spills from offloading. Scenario would most likely involve mobilization of local oil spill resources, but is expected to have minor potential for significant harm.
C _C	Release to environment with major damage which can be cleaned up quickly. Temporary damage to plants or fauna	100–1000 m ³	Larger leaks/spills where oil spill resources will be mobilized and utilized in order to contain spills. Effects most likely to be local but with potential for major damage to shoreline and remote habitats.
C _D	Release to environment which cannot be cleaned up quickly or with lasting damage to flora/fauna.	> 1000 m ³	Large uncontrolled spills with full mobilization of oil-spill resources. Significant potential for major damage to environment

The P parameter is the probability of avoiding the hazardous event if the protection system fails to operate. Classification of the P parameter is shown in Table 7.4.

Table 7.4: Classification of P parameter (IEC 61511-3, Annex D [2]).

P-parameter	Classification
P _A	Use parameter if all conditions in the bulleted list below are satisfied
P _B	Use parameter if any of the conditions in the bulleted list below are not satisfied

P_A should only be selected if all the following are true⁶:

- **Warning:** Facilities are provided to alert the operator about a hazardous event that may, if not stopped, lead to an environmental release.
- **Barriers:** Independent facilities are provided that are capable of stopping or mitigating the consequences of the hazardous event.
- **Time:** There is sufficient time for the operator to activate and for the independent facility to respond to stop the environmental release.

Note that when considering environmental risk, the interpretation of the P parameter will be slightly different from personnel risk considerations. E.g. if a BOP is the barrier under consideration, alternative means to shut down will often not exist (given that balancing with heavier mud has failed) and the available time for action will probably be short. Further, the time aspect is less important since environmental harm will occur regardless of whether the exposure is postponed. Hence, P_B will be the natural choice for environmental risk.

7.3.1 Discussion – using the risk graph on the blowout example

Let us, for the purpose of illustration, consider the same example as in section 7.1.1 for deciding an EIL for the BOP using the calibrated risk graph. We then need to make some additional assumptions:

- Only one well is drilled that year, so the kick frequency per operation (0.2) will be the starting point for estimating the demand rate (W parameter in risk graph) per year.
- Only 50 % of the blowouts (due to release point and duration) have the potential to cause the worst possible consequence C_D.⁷

When using the risk graph method, the demand rate W “in the absence of the SIF under consideration” shall be used. Here the SIF under consideration is the BOP, and therefore the demand rate shall be taken as the product of the kick frequency (0.2), the risk reducing effect from balancing with heavier mud (0.2) and the likelihood of experiencing the worst consequence (0.5). Therefore the resulting demand rate on the BOP, in terms of the number of potential blowout situations which can cause the worst possible consequence C_D, becomes: 0.2 per year · 0.5 · 0.2 = 0.02 per year, corresponding to W1 in the risk graph. Further, we assume that the BOP is the ultimate barrier so that the P parameter will be P_B.

Now using the risk graph in Figure 7.3 and combining C_D, P_B and W1, we see that an EIL 3 requirement will result for the BOP.

A main question concerning the calibrated risk graph and as discussed in section 7.3 above, is how “to ensure the SIL/EIL selected for an application *is in accordance with corporate risk criteria* and takes into

⁶ Original text from IEC 61511-3, Annex D modified to fit to environmental risk considerations.

⁷ The assumption of 50 % of the blowouts having a potential to cause the worst consequence may be conservative for many cases but is here only applied as an example to illustrate the methodical approach.

account risks from other sources”. In other words: How do we know that by using the risk graph in Figure 7.3, we will fulfil the ERAC as given in Table 4.2 or alternatively the criteria given in section 7.1 or 7.2?

First, in order to be able to calibrate the risk graph it is necessary to have an acceptable frequency for each of the consequences C_A – C_D . In addition it will be necessary to have an idea about the total number of different events or scenarios that can fall into each consequence category in order to take into account the complete risk picture.

Note that by adapting the ERAC suggested in section 7.2, it will be possible to establish such an explicit connection. This is illustrated below when the P parameter is always set to P_B (and therefore can be disregarded) and the acceptance criteria are as given in Table 7.5 (same as Table 7.2).

Table 7.5: Acceptance criteria for the risk graph example.

Consequence class		Released volume of oil to sea	Acceptable annual frequency
C_A	Minor harm	$< 10 \text{ m}^3$	$1 \cdot 10^{-1}$
C_B	Moderate harm	$10\text{--}100 \text{ m}^3$	$1 \cdot 10^{-2}$
C_C	Significant harm	$100\text{--}1000 \text{ m}^3$	$1 \cdot 10^{-3}$
C_D	Serious harm	$1000\text{--}10\,000 \text{ m}^3$	$1 \cdot 10^{-4}$
C_E	Major/Catastrophic harm	$> 10\,000 \text{ m}^3$	$1 \cdot 10^{-5}$

The specified SIL (or EIL) will then correspond to the required risk reduction (or span) between the demand rate and the acceptable annual frequencies. The resulting risk graph is shown in Figure 7.4.

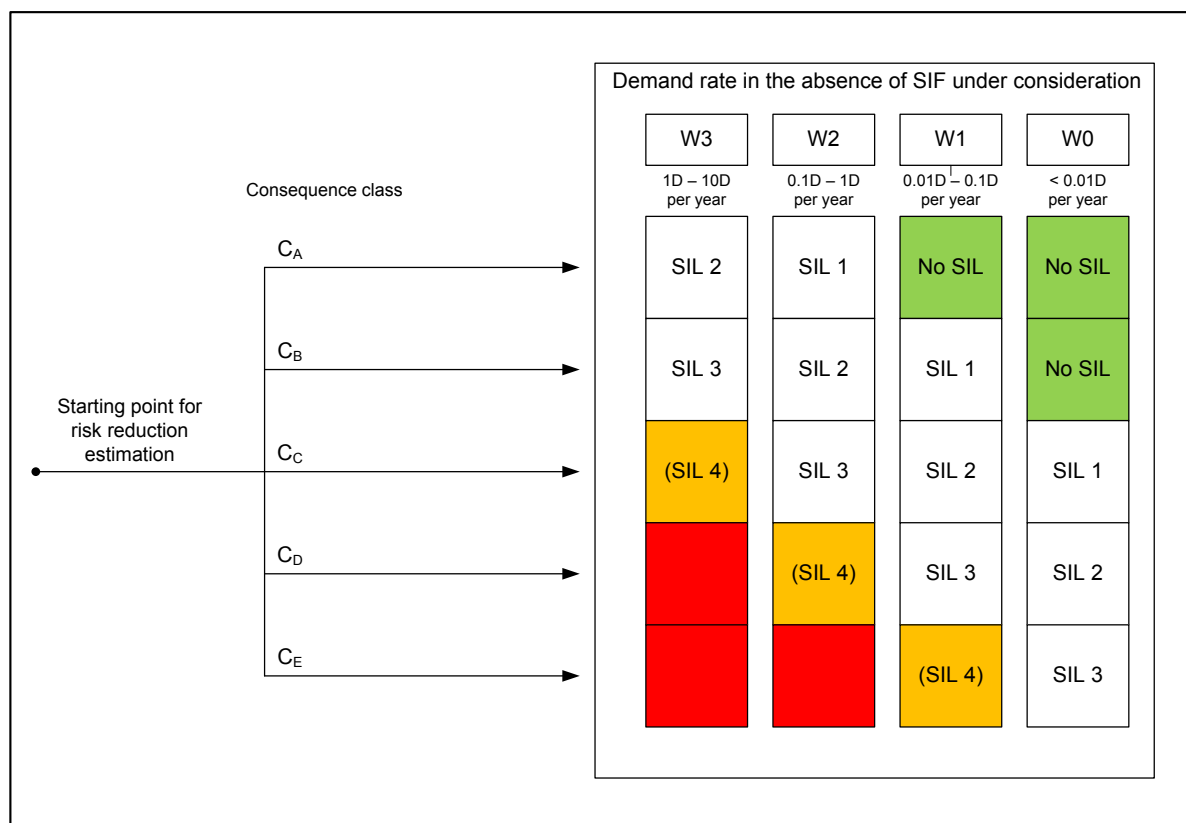


Figure 7.4: Calibrated risk graph when applying acceptance criteria in Table 7.5.

The reasoning behind the SIL (or EIL) requirements is as follows: Consider as an example a scenario, e.g. a blowout, with a potential of causing the worst consequence C_E and with a demand rate W_0 . The required risk reduction will then be from $1 \cdot 10^{-2}$ (the demand rate) to $1 \cdot 10^{-5}$ (i.e. the acceptance criterion for the worst consequence C_E), corresponding to a PFD of maximum $1 \cdot 10^{-3}$. Therefore the requirement in the lower rightmost column becomes SIL 3 (and so on). Consequently, an explicit link between the acceptance criteria and the required SIL (or EIL) is established.

8 Conclusions

Based on the discussions in this report, some main conclusions have been summarised below.

On the establishment of ERAC

- ERA as performed today seems to focus on the consequence side of risk, rather than on the causal side. The analyses normally start with a set of release scenarios, and model the consequences of a release with respect to restitution time of vulnerable resources. The barriers prior to the release are generally not an explicit part of the ERA. Since frequency reducing measures shall be given priority, it is unfortunate that the current ERAC/ERA only direct focus towards consequences.
- The estimated risk from an ERA is generally far below the ERAC. The current ERAC therefore does not seem to be strict enough to put focus on continuous improvement and risk reducing measures, in particular frequency reducing measures.
- The authorities have set out very ambitious HSE goals for the Norwegian petroleum industry, including goals for environmental risk reduction. These very ambitious goals should be followed up by ambitious criteria for acceptable environmental risk.
- What is defined as acceptable risk – to personnel and environment – is determined by each oil company. Personnel are an operator "asset", but the environment is a common good. Hence, it seems reasonable that the authorities should play a more active role in setting overall criteria and goals for the environment.
- It appears that all companies operating in Norway use more or less the same ERAC adopted from the OLF MIRA guideline, but to a limited degree tailor the criteria to their particular situation. The authorities' intention of relating the criteria to the individual environmental resources and to consider the facilities in a larger context is therefore not properly implemented.

On the need for additional or alternative ERAC

- There is a need to establish a connection between overall corporate ERAC and requirements to technical safety systems, in particular barriers applied during drilling, workover and subsea production. The current ERAC based on restitution times of vulnerable resources are not suitable for this purpose, so alternative and simpler ERAC are called for.
- This report suggests additional ways of expressing ERAC on a level suitable for establishing a link to requirements for technical systems. The alternative ERAC are based on release frequencies and release volumes. The use of Calibrated risk graph is discussed as a method to arrive at EIL requirements similar to what is done when setting SIL requirements.

On the current status on barrier performance requirements

- Performance requirements to safety barriers needed to prevent environmental releases are to some degree inadequately defined. In particular, integrity requirements (e.g. SIL/EIL requirements) are only provided for the drilling BOP function and the "isolation of subsea well" function. Furthermore, it has not been properly verified that these (existing) requirements and "strict enough" in terms of environmental risk.

- In a future update of OLF-070 a number of new functions should therefore be considered included with recommended SIL/EIL requirements. Examples of possible candidate functions are emergency power, mud circulation/mixing, acoustic BOP activation back-up, emergency quick disconnect, drilling riser tension and inclination measurement, well intervention BOP and various subsea PSD functions (PAHH, LAHH, etc.).
- For production systems, there is normally a well-defined split between safety and non-safety systems. This is generally not the case for drilling and well intervention systems, where the same equipment is used during normal activities (e.g. mud control) and in response to hazardous events. This mix-up of control and safety must on a principal basis be questioned (ref. e.g. PSA Facilities Regulations, § 33–34).

9 References

- [1] IEC 61508. Functional safety of electrical/electronic/programmable electronic safety related systems, ver. 1.0, 2010
- [2] IEC 61511. Functional safety - safety instrumented systems for the process industry sector, part 1-3,
- [3] Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry, OLF Guideline 070
- [4] The Facilities Regulations, Petroleum Safety Authority Norway, version last amended April 2010, <http://www.ptil.no/facilities/category400.html>
- [5] The Management Regulations, Petroleum Safety Authority Norway, version last amended April 2010, <http://www.ptil.no/management/category401.html>
- [6] The Framework Regulations, Petroleum Safety Authority Norway, version last amended February 2010, <http://www.ptil.no/framework-hse/category403.html>
- [7] The Activities Regulations, Petroleum Safety Authority Norway, version last amended April 2010, <http://www.ptil.no/activities/category399.html>
- [8] OLF, Metode for miljørettet risikoanalyse (MIRA) Revisjon 2007, Report No. 2007-0063 (In Norwegian)
- [9] Frekvenser for akutte utslipp i Norskehavet, SINTEF report A4735, January 2008 (In Norwegian)
- [10] Bruk av BAT (Beste Tilgjengelige Teknikker)-prinsippet for miljøsikkerhet, SINTEF report A4531, February 2008 (In Norwegian)
- [11] Risikonivå i petroleumsvirksomheten, Metoderapport for Pilotprosjektet, Overvåkning av risiko for uønskede hendelser som kan føre til akutte utslipp på Norsk sokkel, Ptil, Preventor, 2010 (In Norwegian)
- [12] Risikonivå i petroleumsvirksomheten, Pilotprosjekt, Overvåkning av risiko for uønskede hendelser som kan føre til akutte utslipp, Norsk sokkel 2005–08, Ptil, Preventor, 2010 (In Norwegian)
- [13] OLF, Retningslinjer for beregning av utblåsningsrater og -varighet til bruk ved analyse av miljørisiko, 15.01.07 (In Norwegian)
- [14] NORSOK Standard Z-013, Risk and emergency preparedness assessment, Edition 3, October 2010
- [15] Drill, not spill, SINTEF memo, K. L. Sørstrøm and Y. Liao, 2010-11-18
- [16] Barriers to Prevent and Limit Pollutants to Sea – Environmental Risk Acceptance Criteria, SINTEF draft memo, February 2011
- [17] Barriers to Prevent and Limit Pollutants to Sea – Description of Barriers and Associated Performance Requirements, SINTEF draft memo, December 2010

- [18] Foundations and fallacies of risk acceptance criteria, I. L. Johansen, NTNU, 2010-02-23
- [19] OLF/NOFO - Summary of differences between offshore drilling regulations in Norway and U.S. Gulf of Mexico, DNV report, 26.08.2010
- [20] Soria Moria 2 http://www.regjeringen.no/upload/SMK/Vedlegg/2009/Ny_politisk_plattform_2009-2013.pdf (In Norwegian)
- [21] Scandpower - Blowout and well release frequencies based on SINTEF offshore blowout database 2010 (revised), 5 April 2011
- [22] Barriers to Prevent and Limit Pollutants to Sea – Environmental Barrier Indicators, SINTEF report (To be published)
- [23] NORSOK Standard S-001 Technical Safety, Edition 4, February 2008
- [24] NORSOK Standard D-001 Drilling Facilities, Rev 2, July 1998
- [25] NORSOK Standard D-002 System Requirements Well Intervention Equipment, Rev 1, October 2000
- [26] NORSOK Standard D-010 Well integrity in drilling and well operations, Rev 3, August 2004
- [27] API RP 53, Recommended Practices for Blowout Prevention Equipment Systems for Drilling Wells, third edition, March 1997
- [28] ISO 13628, Petroleum and natural gas industries – Design and operation of subsea production system
- [29] ISO 13624, Petroleum and natural gas industries – Drilling and production equipment
- [30] ISO 10417, Petroleum and natural gas industries – Subsurface safety valve systems – Design, installation, operation and redress
- [31] Deepwater Horizon Accident Investigation Report, 2010-09-08, BP
- [32] Deepwater Horizon-ulykken: Årsaker, lærepunkter og forbedringstiltak for norsk sokkel. SINTEF report A19148, May 2011 (in Norwegian).
- [33] BOEMRE (The Bureau of Ocean Energy Management, Regulation and Enforcement): Report Regarding the Causes of the April 20, 2010 Macondo Well Blowout (14.09.11).
- [34] Offshore Standard, DNV-OS-A-101, Safety Principles and Arrangements, April 2011
- [35] Evaluation of Secondary Intervention Methods in Well Control, West Engineering Services Inc., March 2003
- [36] Sklet, S.: Safety barriers: Definition, classification, and performance. Journal of Loss Prevention in the Process Industries, 19 (2006) 494-506.

- [37] Lundteigen, M.A.: PhD thesis: Safety instrumented systems in the oil and gas industry: Concepts and methods for safety and reliability assessments in design and operation, 2009, ISBN 978-82-471-1385-1

APPENDICES

A Safety Barriers Classification and Overview

A.1 Definition and Classification of Safety Barriers

The main purpose of a safety barrier is to prevent or mitigate the consequences of hazardous events. In general terms, it may be defined as “*Safety barriers are physical and/or non-physical means planned to prevent, control, or mitigate the consequences of undesired events and accidents.*” [36]. A classification of safety barriers according to their main characteristics is sometimes useful. Classification may be done according to e.g.:

- Where, in the sequence of events that may lead to an accident, the safety barrier is intended to act: When using the bow-tie model as basis (see Figure A-1), the safety barriers are usually split into preventive (probability/frequency reducing) and reactive (consequence reducing) barriers. Preventive barriers are used to stop or prevent a potential hazard from developing into a hazardous event and will therefore impact the frequency of hazardous events. Reactive barriers are used to stop, control or mitigate the hazardous event from developing into an accident, and will therefore act as consequence reducing measures.
- The technology used: Pure mechanical systems or systems that include one or more electrical, electronic, or programmable electronic devices. The latter is often referred to as safety instrumented systems.
- How frequent the barrier is demanded: IEC 61508 distinguishes between low demand mode, where the safety barrier is demanded less than once per year, high demand, where the safety barrier is demanded more than once per year, and continuous demand mode, where the safety barrier retains the safe state as part of the normal operation.
- Duration of the demand: Some barriers are barriers designed to function on demand (e.g., close a valve), while others must also operate for a longer period of time, once demanded (e.g., continue to run a pump for a specified period of time).
- Temporary versus permanent: Temporary barriers are barriers designed to function for a relatively limited time period during a specific activity and which may require on-going attention to ensure their effectiveness. Examples are kill weight fluid and down hole tubing plugs which do not remain in well.
- In what way the barrier is activated: It is sometimes distinguished between passive and active barriers. Passive barriers do not take action in order for it to achieve its function, while active barriers take an action in response to a measurement or a human action. Examples of passive barriers are cement and manifold piping. Examples of active barriers are down hole safety valves.

The annual report on risk level in the Norwegian oil and gas industry which is published by the PSA (the RNNP report) uses the following classification of barriers:

- Barriers used to prevent, reduce, or mitigate the consequences of process leakage
 - Detection
 - Shutdown
 - Pressure relief
 - Spill collection
- Barriers used to control well incidents
- Barriers used to prevent structural damage
- Barriers used to prevent or mitigate leakage and damage on subsea production equipment, risers and piping

The bow-tie model is illustrated in Figure A-1. In this project, a hazardous event is defined as loss of containment such as the release of hydrocarbons or other substances that may lead to environmental damages. The main focus of the project is directed to instrumented preventive barriers, i.e., the measures taken to prevent loss of containment and the requirements that should be set to these barriers.

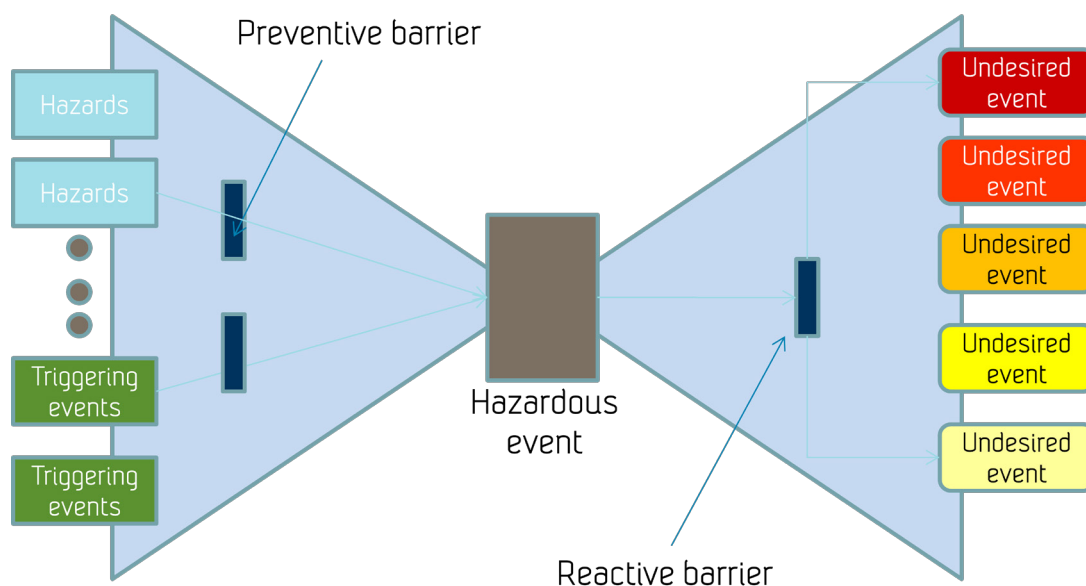


Figure A-1: Preventive vs. reactive barriers.

Following the above classification of barriers, the project aims to identify and assess the technical and operational requirements for safety barriers that are used to:

- Detect
- Shut down
- Control well incidents

The specification of reliability performance requirements to these systems should include aspects such as:

- Demand frequency
- Demand duration
- Means of activation (automatic or manual)

A.2 Overview of Safety Systems and Barriers

A.2.1 Technical Safety Disciplines and Systems for Production

The NORSOK standard “S-001 Technical Safety” [23] includes 20 sections describing technical equipment that may constitute safety barriers (see Table A-1).

Technical disciplines and systems marked with red (items 1–17) are located topside and are not a part of the scope for this project. The containment function (item 18) shall prevent the release of hydrocarbons, chemicals and/or toxic gases. Requirements are given for piping, flanges and connections. No instrumented systems are involved (except during testing) and the containment function is not further described. NORSOK S-001 focuses on production and does not cover drilling and well integrity.

Items marked with green (items 19 and 20) are topside located safety control systems controlling safety equipment located topside and subsea. These systems are described in Appendix B.3.

Table A-1: Technical safety disciplines and systems for production of oil and gas.

Id	Technical safety as identified by NORSOK S-001	Location
1.	Fire detection	Topside
2.	Gas detection	Topside
3.	Escape and evacuation	Topside
4.	Rescue and safety equipment	Topside
5.	Marine systems and position keeping	Topside
6.	Emergency power and lightning	Topside
7.	PA , alarm and emergency communication	Topside
8.	HVAC	Topside
9.	HMI – Status, alarm and activation	Topside
10.	Layout of installation	Topside
11.	Structural integrity	Topside
12.	Passive fire protection	Topside
13.	Fire fighting systems	Topside
14.	Ignition source control	Topside
15.	Blow down and flare vent	Topside
16.	Ship collision barrier	Topside
17.	Open drain	Topside
18.	Containment	Topside/Subsea
19.	Emergency Shutdown Control System (ESD)	Topside/Subsea
20.	Process Safety	Topside/Subsea

A.2.2 Drilling Facilities and Well Intervention

Table A-2 presents a corresponding list of systems for drilling and well intervention, which have been identified in the NORSOK standard “D-001 Drilling Facilities” [24] and the NORSOK standard “D-002 System Requirements Well Intervention Equipment” [25]. Some of these systems play an important role in preventing loss of containment or in mitigating the potential consequences.

Systems marked with red in Table A-2 (items 21 and 23–27) are located topside only, with little relevance to subsea barriers, and are not a part of the scope for this project. The items marked with a yellow colour (items 22, 28–31 and 33–34) are topside systems needed for the fluid column barrier to be functional, and they are briefly discussed in Section B.1. The green items 32 and 35 are discussed in Sections B.1 and B.2.

Table A-2: Drilling Facilities and Well Intervention Equipment.

Id	Drilling facilities (NORSOK D-001) and Well Intervention (NORSOK D-002)	Location
21.	Layout	Topside
22.	Emergency power	Topside
23.	Drilling structures	Topside
24.	Hoisting and rotary systems	Topside
25.	Motion compensating systems	Topside
26.	Pipe handling systems	Topside
27.	Associated equipment (Drill floor, derrick, substructure)	Topside
28.	Bulk systems	Topside
29.	Mud mixing and storage systems	Topside
30.	High pressure mud systems	Topside
31.	Mud treatment systems	Topside
32.	Well control system	Topside/Subsea
33.	Cementing system	Topside
34.	Drilling instrumentation	Topside/Subsea
35.	Well intervention equipment	Topside/Subsea

A.2.3 Well Barriers (full life cycle, including production, drilling and well intervention)

The major modules of a production well are the X-mas tree, the wellhead, the casing and the completion string as illustrated in Figure A-2. All these modules contain well barrier elements.

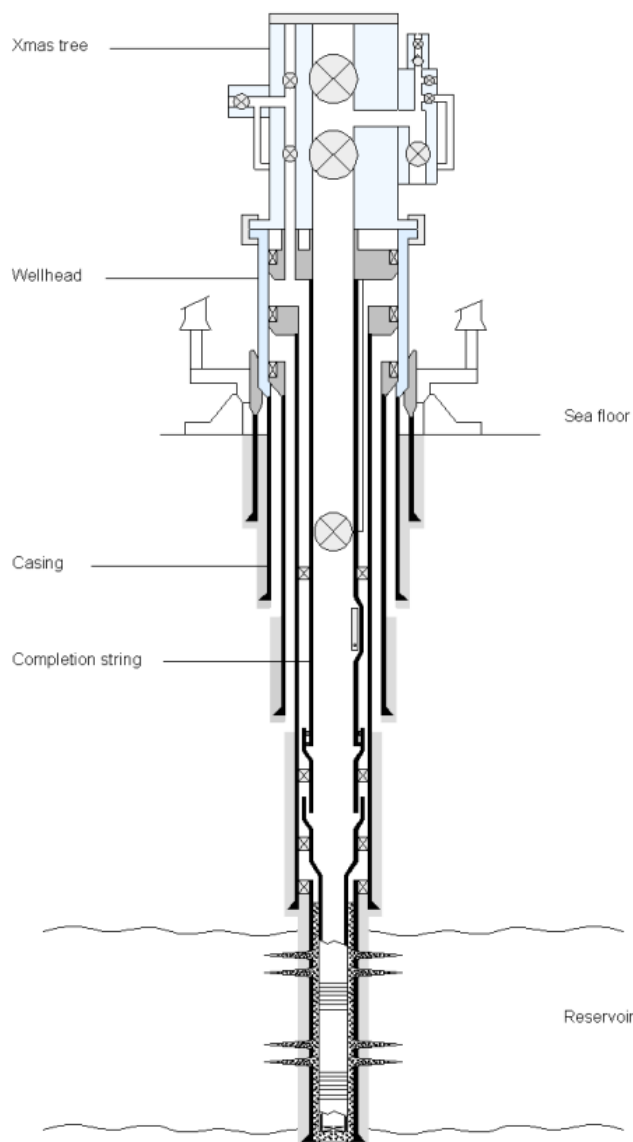


Figure A-2: Major well modules (Source: ExproSoft AS).

The NORSOK standard D-010 “Well integrity of drilling and well operations” [26] focuses on well barrier elements for the whole life cycle of a well, including production, drilling and well intervention activities. The standard is further described in Section 0. NORSOK D-010 has identified and described a total of 50 different well barrier elements. The most relevant within this scope are listed in Table A-3.

Instrumented well barrier elements are typically controlled by a process control systems with control units located both topside and subsea. Some instrumented well barriers are in addition controlled by safety systems which activate the well barriers either by manual initiation or automatic initiation.

Some well barrier elements are described in the following sections. For a complete description of well barriers, NORSOK D-010 can be used. Figure A-3 shows a well barrier diagram illustrating well barrier elements and possible leak paths.

Table A-3: Relevant well barrier elements from D-010 [26].

Id	Well Barrier Elements (D-010), the whole life cycle	Location
36.	Fluid column	Topside/Subsea
37.	Well Head	Topside/Subsea
38.	Drilling BOP	Topside/Subsea
39.	Subsea production tree	Subsea
40.	Subsea test tree	Subsea
41.	SCSSV	Subsea
42.	Annulus SCSSV	Subsea
43.	Annulus accumulator line and valve	Subsea
44.	Downhole tester valve	Subsea
45.	Subsea lubricator valve	Subsea
46.	Wireline BOP (backup WBE)	Subsea
47.	Lower riser package	Subsea
48.	Coiled tubing BOP	Subsea
49.	Coiled tubing safety head	Subsea
50.	Snubbing BOP	Subsea
51.	Snubbing safety head	Subsea
52.	Rotating control device	Subsea
53.	Downhole isolation valve	Subsea
54.	Production tree isolation tool	Subsea

The mapping between the above tables and descriptions in the next Appendix is illustrated below.

<u>Appendix A</u>		<u>Appendix B</u>
Safety disciplines and Systems for Production	Table A-1	B.3 Subsea Production
Drilling Facilities and Well Intervention	Table A-2	B.1 Drilling Facilities B.2 Well Intervention Equipment
Well Barriers (full life cycle, including production, drilling and well intervention)	Table A-3	B.4 Well Barriers as Described in D-010

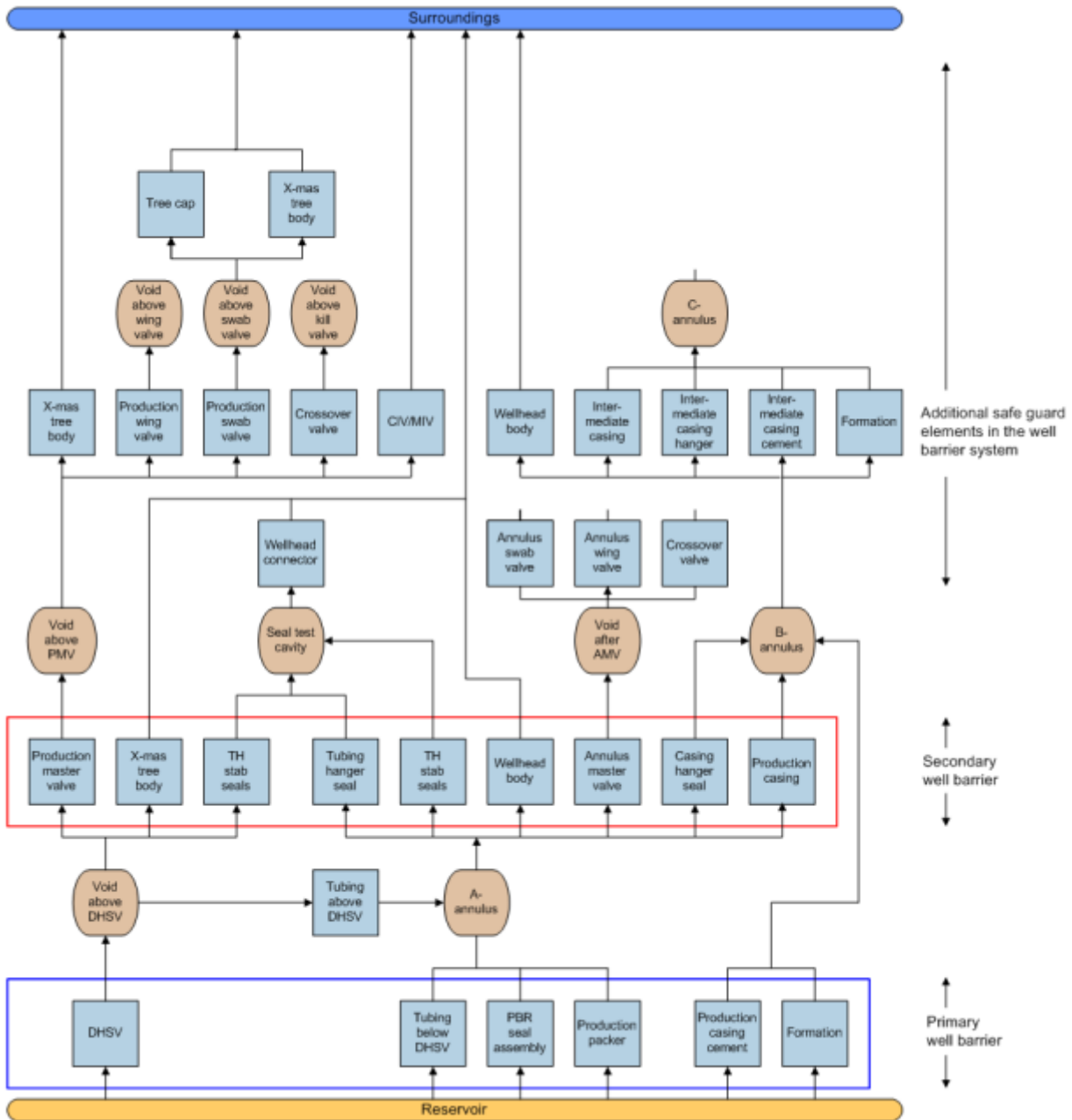


Figure A-3: Well barrier diagram for a simple production well (Source: ExproSoft AS).

B Barrier Description

Barrier elements being a part of, or being controlled by, or being supervised by one of the systems or facilities marked with a green or yellow colour in Table A-1 and Table A-2 are further described in this appendix. The following systems and facilities are covered in this Appendix:

B.1 Drilling Facilities

- B.1.1 Emergency Power⁸
- B.1.2 Mud and Cementing Systems
- B.1.3 Well Control Systems (incl. BOP)
- B.1.4 Drilling Instrumentation
- B.1.5 Drilling ESD system

B.2 Well Intervention Equipment

- B.2.1 Well Intervention Activities
- B.2.2 Requirements to Well Intervention Equipment
- B.2.3 Typical Safety Functions during Well Intervention – an Example

B.3 Subsea Production Safety Functions – ESD and PSD

- B.3.1 Emergency Shutdown (ESD)
Process Shutdown (PSD)

B.4 Well Barriers as Described in D-010

B.5 Summary of Performance Requirements

B.1 Drilling Facilities

Requirements for Drilling facilities are given in NORSOK D-001. The most relevant requirements within the scope of this project are presented in the following sections. Requirements are written in *italic*. A short description has been included for some systems.

B.1.1 Emergency Power

The emergency power shall be sufficient to facilitate the following operations, not simultaneously, but in relevant combinations:

- *Circulate mud at reduced rate*
- *Mix and transfer mud as required*
- *Move tubulars at limited speed*
- *Complete cement job*
- *Rotate drill at limited RPM/torque*
- *Operation of pipe handling equipment at limited speed*
- *Operate and recharge secondary well control equipment*

It should be noted that the above requirements apply in the case of main power failure where emergency power is required to secure the well and associated equipment by maintaining the main barrier (i.e. mud balancing). However, if loss of main power and transfer to emergency power is caused by an ESD, securing

⁸ Emergency power during production (item 6) is not covered by this memo, while emergency power during drilling (item 22) is. The rationale is that subsea safety barriers during production normally are failsafe de-energized. That is not always the case for drilling operations. The fluid column barrier is for example dependent on power to the mud pumps.

the well by maintaining the main barrier may not be first priority. In such case “non-essential” personnel may already be mustered and securing the well by activating the BOP is more relevant.

Observations (Emergency Power)

- Emergency power is not covered by the present version of the OLF-070 guideline.

B.1.2 Mud and Cementing Systems

The mud column is one of the two main barriers for drilling and completing a well. The mud column and its control is an operations function, even though loss of control can lead to an emergency situation.

B.1.2.1 Bulk System

The bulk system shall be designed to receive, store and deliver required volume of bulk material to the mud and cementing system.

All valves used for loading, discharge, pumping and circulation shall be remotely operated.

B.1.2.2 Mud Mixing and Storage Systems

The total capacity of the mud, bulk and storage system shall be sufficient to replace 100% of any hole volume including the riser if applicable.

All valves in daily use shall be remotely operated.

All tanks shall be equipped with a minimum of one level sensor.

A control room for remote operation of the mud and bulk systems shall be included, unless satisfactory working environment is ensured by other means.

Two separate mixing lines shall be available simultaneously to facilitate the mixing of dry bulk materials, powder additives and liquid additive in both the active and storage systems

The level monitoring system should be of a load cell type and have a heave and list compensating system when applicable.

Electrical equipment shall be zone certified.

B.1.2.3 High Pressure Mud System

The high pressure mud pumping system shall be capable of delivering all drilling and completion fluids in normal use. Minimum 2 pumps are normative. Normally 3 pumps are used. Early in the drilling phase, the focus is on large volumes. Later, when pressure increases, some of the pump internals are replaced with new (smaller) size components. One of the pumps is often down due to this type of activities. The mud pumps are also used for testing of well barriers, such as BOP.

The high pressure mud pumping system shall be capable of delivering all drilling and completion fluids in normal use at the specific pressures and volumes. The system shall be designed for continuous service, and have regularity as high as possible.

The HP mud pumps and supercharge pumps shall be operated from the drillers cabin.

Electrical equipment shall be zone certified.

The HP mud pumps shall be located to allow gravity feed from mud tanks in case of failure of super charge pumps. Super charge pumps shall have gravity feed bypass piping.

Provisions shall be made to enable sectioning of the suction system as well as the discharge system.

B.1.2.4 Mud Treatment System

The mud treatment system reduces the amount of water, oil and drilling particles from the drilling slurry in order to reuse the mud. A system may include centrifuges, shakers, degassers, mud cleaners, flow dividers and cutting handlers.

Electrical equipment shall be zone certified. All tanks shall be equipped with (minimum one) mud level sensors.

The equipment and control system shall be arranged such as to minimise manual operation.

The mud treatment equipment shall as a minimum have start/stop controls and running indication for shale shakers in drillers cabin as well as locally.

The treatment system shall be operated from a control station.

A combined control room, sound proofed and ergonomically laid out shall be arranged for cement and mud system operations.

B.1.2.5 Cementing Systems

The cementing systems shall be designed for normal mixing and pumping of cement slurries, pressure testing, well circulation, well killing and bullhead operations for intermittent services.

The operation of necessary functions shall take place from a suitable control facility at a safe distance from the high pressure equipment. Examples of necessary functions may be; gears/velocity, stop/start and opening and closing of necessary valves.

The cement unit shall be connected to a data registration unit, measuring and recording the following data during mixing and pumping:

- *Specific gravity*
- *Pump pressure*
- *Pump rates*
- *Cumulative volume pumped*

Observations (Mud and Cementing Systems)

- A general requirement to drilling facilities in D-001 is that regularity requirements shall be defined prior to the design. For the high pressure mud system the requirement is “regularity as high as possible”. This is not a precise or verifiable requirement.
- There is no SIL requirement set in the OLF-070 guideline. The mud circulation system is regarded as an operations function. The OLF-070 guideline compares the mud circulation system with the process control function of a process plant.

- Note that only single level transmitters are required in the mud storage and mud treatment tanks although level measuring is known to be fairly unreliable.

B.1.3 Well Control Systems (incl. BOP)

B.1.3.1 BOP – Description

A blowout preventer (BOP) is a specialized equipment developed to cope with erratic pressures and uncontrolled flow (kick) emanating from the well during drilling. The BOP is also used for non-safety activities: to centre the drill string and to hang off the drill string in the wellbore.

Blowout preventers often contain a stack of independently-operated cut-off mechanisms, so there is redundancy in case of failure, and the ability to work in all normal circumstances with the drill pipe in or out of the wellbore. A typical BOP stack with a short explanation to the different stack elements is shown in Figure B-1. The control pods named YELLOW POD and BLUE POD in the figure are redundant units. The names “yellow pod” and “blue pod” have become a de facto standard.

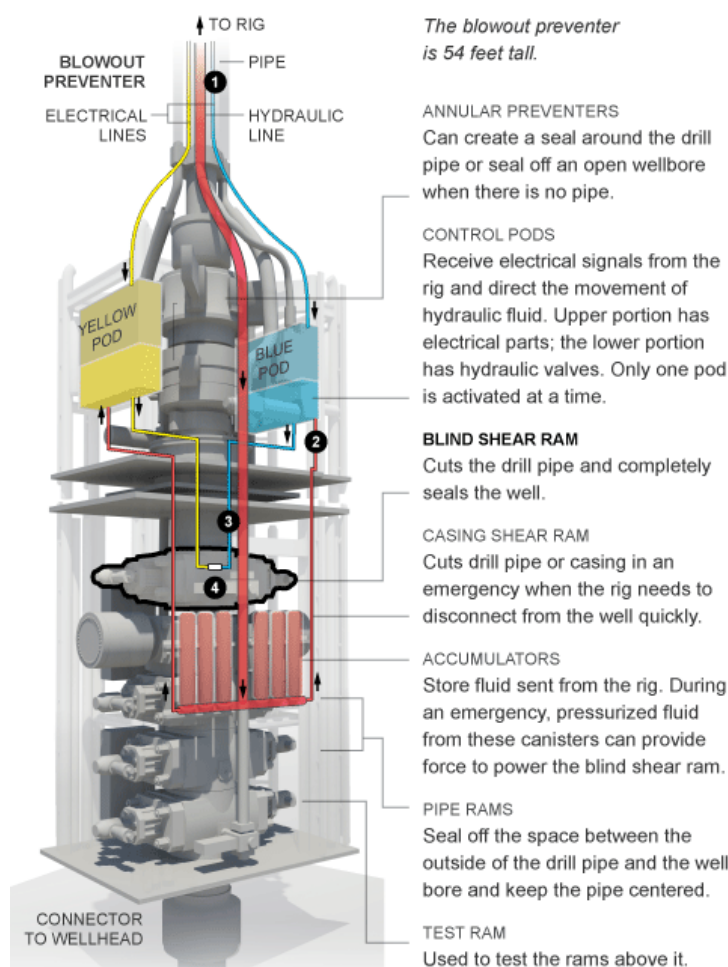


Figure B-1: Deepwater Horizon BOP stack (the New York Times).

Figure B-2 shows a typical blind shear ram. Hydraulic fluid enters the shuttle valve from either the yellow or the blue pod (1) causing a piston (2) to push the rams (4) together with great force. Once the rams has closed and cut off the drill string (if present), a mechanical wedge lock (3) prevents the rams from moving back. Rubber seals on the ram close off the well. Oil (or gas or mud) pushing up from the well adds pressure below and behind the ram, helping to keep the ram closed.

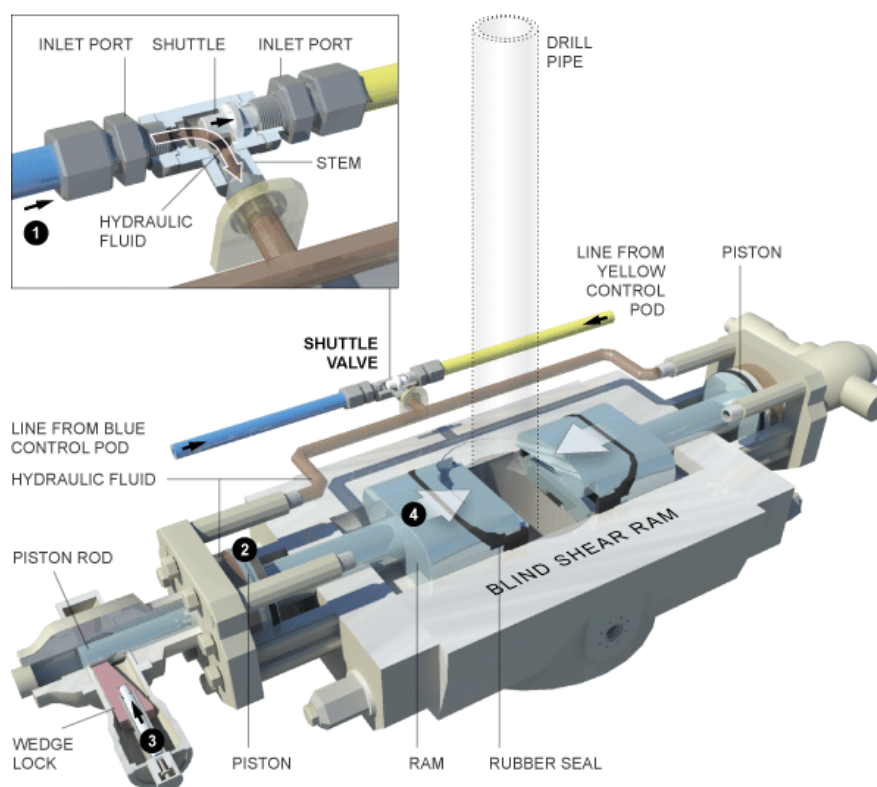


Figure B-2: Typical blind shear ram with shuttle valve (the New York Times).

Figure B-3 shows a Reliability Block Diagram (RBD) for a typical close ram operation. On the Norwegian shelf there is a requirement for an acoustic or other back-up activation system when a Mobile Offshore Drilling Unit (MODU) is drilling with the BOP on the seabed (see Section B.1.3.6). The RBD below illustrates dependencies for a typical setup of a blue pod, yellow pod and acoustic backup. Only typical major components have been included in the RBD. Wedge lock components and check valves are examples of components that have been excluded from the RBD.

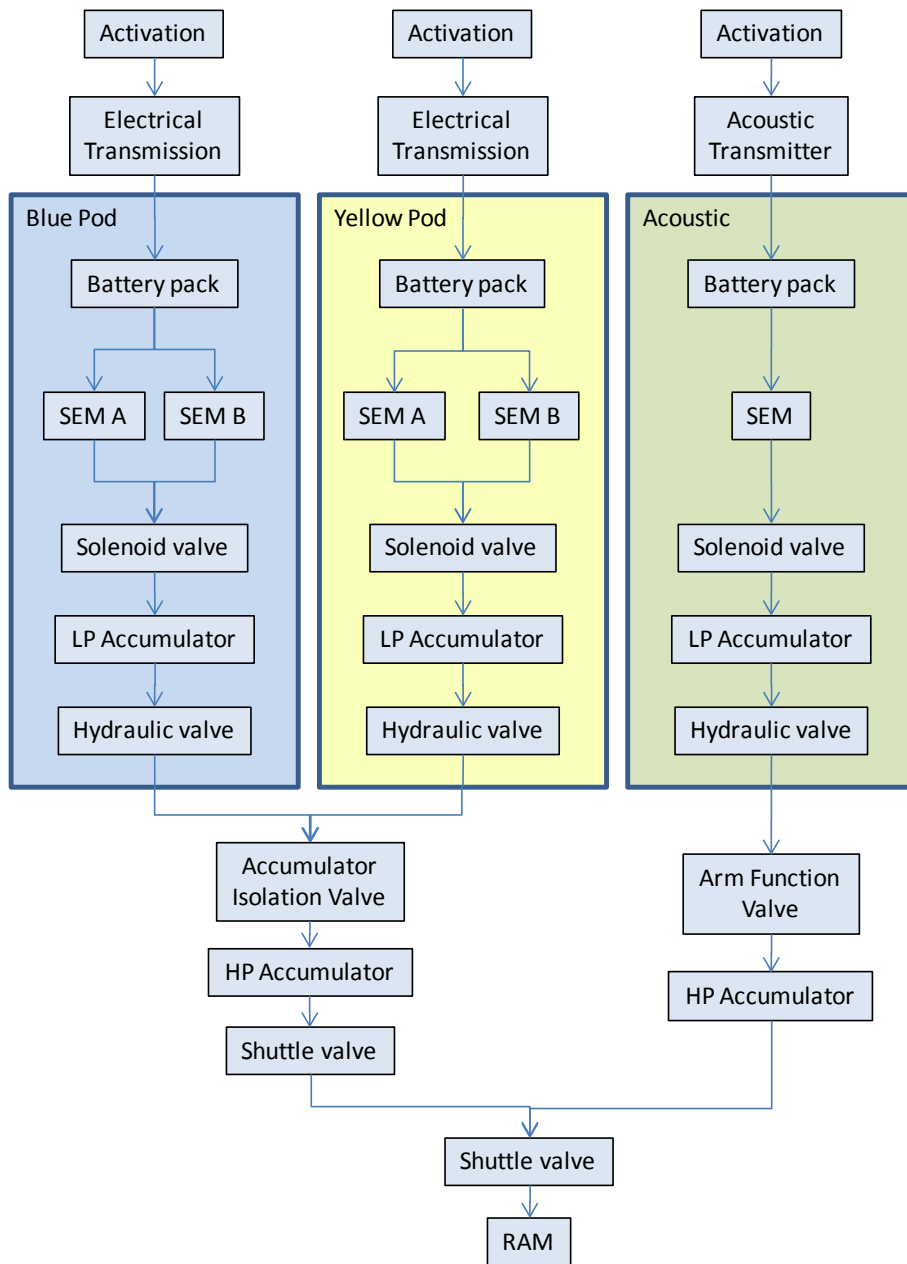


Figure B-3: Reliability Block Diagram for a typical ram close operation.

B.1.3.2 BOP – General Requirements

The BOP system shall as a minimum consist of:

- *One (1) annular preventer*
- *One (1) shear ram preventer*
- *Two (2) pipe ram preventers*
- *Minimum one (1) Choke Line outlet*
- *Minimum (1) Kill Line outlet*
- *One(1) wellhead coupling or connector*
- *Minimum two manual gate valves*
- *Minimum two remote hydraulic operated gate valves*

This valve arrangement applies to fixed installations where the BOP is readily accessible.

The shear ram shall be capable of shearing the pipe body of the highest grade drill pipe in use, as well as closing off the wellbore.

Shear and pipe ram shall be fitted with a mechanical locking in closed position.

The position of the choke and kill line outlets shall be arranged so that circulation for well control can be carried out with the drill string suspended in the BOP and the shear ram closed.

Subsea BOPs for MODUs normally comprise of three main components:

- *Wellhead connector*
- *BOP stack*
- *LMRP (Lower Marine Riser Package)*

The LMRP shall be connected to the BOP stack by means of a remotely controlled hydraulic connector.

The LMRP shall incorporate the disconnectable choke- and kill stabs and the pods for the BOP Control System.

Testing of the BOPs at the surface shall be possible with the BOP and LMRP connected.

Each of the Choke and Kill outlets on the BOP stack shall be fitted with two gates arranged in series and installed close to the BOP. One choke outlet should be located below upper annular in order to handle trapped gas.

All of the gate valves shall be hydraulically operated and of remote control type. The valves shall be of the “fail-safe” closing type, and shall be capable of closing under dynamic flow conditions.

For DP operated vessels dual shear rams should be given due consideration.

B.1.3.3 BOP – Control System

This section describes the control system required for remote control of the BOP stack on fixed and mobile installations.

The control system shall consist of the following:

Control panels which clearly indicate whether the functions are in open or closed position. Furthermore it shall indicate pressures (accumulator and manifold) and volume (flow meter reading) for the functions and operations performed.

The control panels shall be equipped with a securing device against unintentional operation of essential functions (e.g. shear ram, riser connection).

The panels to be equipped with alarms for:

- *Low accumulator pressure*
- *Loss of power supply*
- *Low levels of control fluid*

All functions shall be operated independently from the main BOP accumulator unit and remote panel on the drill floor.

The main BOP accumulator unit shall be located in a safe area in order to avoid exposure in the event of an uncontrolled well situation.

Maximum response time when the BOP is located on a surface installation is 30 seconds. (In the case of annular preventers exceeding 20", a response time of up to 45 seconds is acceptable). Response time refers to the time it takes from the closing function is activated from the panel, until the BOP function is in closed position.

The accumulator capacity for operating BOP stack with associated systems shall have as a minimum sufficient volumetric capacity to close, open and close all the installed BOP functions, plus 25 per cent of the volume for one closing operation for each one of the said BOP rams.

Accumulators shall have sufficient pressure capacity to enable cutting of the relevant drill string. There shall be sufficient remaining accumulator pressure to enable cutting of the drill string after having used a volume corresponding to as follows:

- *Closing and opening of one annular preventer*
- *Closing, Opening and Closing of one pipe ram preventer*

Alternatively a dedicated shear ram auxiliary pressure system (Shear boost system) may be installed to meet the minimum requirements to cut the drill string if the remaining accumulator pressure is not sufficient to enable cutting after having performed operations as described above.

B.1.3.4 Choke and Kill System

The choke and kill system provides for stopping production from a well by injecting a fluid from the outside of the well conduit into the well bore.

The choke manifold shall as a minimum include:

- *3 chokes*
- *Minimum one shall allow for remote control, and minimum one for manual operation.*

Operation of remote controlled chokes shall take place from a suitable panel, which shall at least indicate:

- *Drilling pressure*

- *Choke manifold pressure*
- *Choke position indicators*
- *Volume pumped*
- *Drilling fluid pump rate*

The choke manifold shall furthermore be fitted with a valve on each of the outlet/inlet pipes, so that lines to and from the manifold can be isolated.

Where high pressure/low pressure zones interfaces in the manifold system, two valves arranged in series shall be installed.

Manifolds for 345 bar pressure rating or higher shall be equipped with at least two valves before each of the chokes.

B.1.3.5 Diverter System

The diverter system is used to protect the personnel and equipment by rerouting the flow of shallow gas and wellbore fluids through an overboard vent line. The diverter system is not designed to shut in or halt flow, but permits routing of the flow away from the rig.

The diverter shall have a suitable diverter piping arrangement leading to opposite sides of the installation.

The diverter system shall as a minimum be remotely operable from drillers position and main BOP control unit, and be able to close around relevant drill string dimensions.

A trip tank system of two tanks shall be provided. Two level controls with drill floor operated interlock valves between tanks.

B.1.3.6 Special Requirements for Mobile Offshore Drilling Units

With regard to floating offshore units with BOP located on the sea bed, there shall in addition be sufficient remaining pressure to enable the LMRP to be disconnected after completion of cutting the drill string.

Pressure regulators in the system shall remain unaffected in the event of loss of power supply, e.g. loss of compressed air.

Maximum response time for closing of BOP when located on the seabed can be up to 45 seconds.

When drilling with the BOP system installed on the seabed, an acoustic or an alternative control system shall in addition be installed. This system shall as a minimum be able to operate:

- *Pipe ram preventers*
- *Shear ram preventer*
- *Marine Riser Connector*

The accumulators for this system shall have sufficient capacity for closing off:

- *Two (2 ea.) pipe ram preventers*
- *One (1) shear ram preventer*
- *Opening of the riser connector*
- *Plus 50%*

The acoustic accumulators shall have sufficient pressure for cutting the drill string, after having closed a pipe ram preventer.

In addition the pressure shall be sufficient to carry out a disconnection of the LMRP after cutting of the drill string has been completed.

A portable unit (which can be handled by one person) shall be available for operation of the above mentioned functions in the event of evacuation from the platform.

Observations (Well Control Systems)

- The shear-ram is not required to cut the tool joints. The position of the tool joint has to be known, or dual shear-rams have to be installed in order to shear the drill pipe over/under the drill pipe tool joints.
- According to one of the Deepwater Horizon accident investigation reports [30] one fault (missing battery power) was found in one pod, and an erroneous solenoid valve was found in the other pod. This illustrates the importance of proper condition monitoring and testing of redundant equipment.
- Given the above mentioned pod errors alone, an acoustic backup system might have been able to close the Deepwater Horizon BOP. It has been claimed that acoustic systems are sensitive to mud clouds and gas plumes and that an acoustic system might not be functional in the event of a blowout (ref. [35]).
- Even with redundant pods and acoustic backup *the shuttle valve* will be a single source of failure for a given BOP. This is however, considered to be a simple and highly reliable component.
- In case of BOP failure and a topside blowout, the diverter system appears as the "last line of defence" with respect to reducing the amount of flammable hydrocarbons on the rig. The possibility of mal-operating the system therefore needs to be minimised. The design requirements for the diverter system are relatively vague (ref. section B.1.3.5). It should therefore be considered to review today's systems and update relevant standards (in particular NORSOK D-001) to reflect best available practice. In general, when activating the diverter system it should only be possible to route the flow overboard.
- Explicit SIL Requirements have only been put upon the Drilling BOP function. The OLF guideline discussion concludes:
"Setting a SIL 3 level to either function would lead to a significant increase in the standard for drilling BOPs. The challenge lies mainly in the need for documentation of the system reliability. Setting a SIL 3 level would most certainly also result in the need for changing existing control system. It would also be necessary to include additional rams in standard BOP assemblies. The required PFD/SIL for the BOP function for each specific well should be calculated and a tolerable risk level set as part of the process of applying for consent of exploration and development of the wells. As a minimum the SIL for isolation using the annulus function should be SIL 2 and the minimum SIL for closing the blind / shear ram should be SIL 2."
- The marine drilling riser emergency disconnect function is discussed in the OLF-070 guideline. The OLF-070 conclusion is:
Required SIL level for emergency disconnect for each specific well should be calculated and a tolerable risk level set as part of the application for consent process for exploration and development

wells. The emergency disconnect for the marine drilling riser should have a minimum SIL level of SIL 2. This is based on historical information more than a detailed assessment of existing emergency disconnect systems. It is not known whether this can be documented for existing systems.

- An important recommendation from the recent BOEMRE report into the Deepwater Horizon accident [33] is that better and more clear-cut procedures on when to activate the emergency disconnect function is required. In case of Deepwater Horizon, this function was activated too late and the hydraulic/power/signal lines to the lower marine riser package were already torn off by the explosion.

B.1.4 Drilling Instrumentation

The DIP (Drilling Instrumentation Package) shall monitor and log parameters related to drilling and well activities. The system shall in addition be designed to handle alarms, status and hours in operation for equipment as required in NORSOK standards or recommendation from equipment suppliers. Time based data logged shall be available online for three days. Older data shall be available on off-line storage media, if required.

The different systems shall not be mixed within the same I/O card or be powered from the same fuse. Duplicated I/Os shall have separate card and fusing.

There shall be segregation between DIP and safety systems, i.e. fire and gas, shutdown systems, BOP/choke control systems.

Annex B (in D-001) details the minimum parameter requirements for monitoring and logging of drilling and well activities.

Field instrumentation shall be selected and installed according to NORSOK standard I-001 and Z-010.

Observations (Drilling Instrumentation)

- Quite detailed design requirements for the drilling instrumentation have been set in NORSOK D-001. If the SIL concept was adapted, it may be found that the level of hardware fault tolerance mandated by the architectural constraints in IEC 61508 and OLF-070 conflicts with the more detailed requirements and design considerations for drilling systems.
- In D-001 there are no requirements for kick detection systems. For marine risers at considerable water depths an early kick detection device “should be considered”. The OLF-070 guideline discusses kick detection systems. According to the guideline it is not recommended to set a minimum SIL requirement for kick detection due to the following:
 - Kick detection is only one of the information elements required in the decision process for activating the BOP.
 - Kick detection is required for process control of the mud column. It does not automatically initiate an action.

B.1.5 Drilling ESD system

Requirements to ESD systems can be found in NORSOK S-001. This standard does not, however, focus on drilling systems. For emergency shutdown principles on drilling rigs, reference is made to NMD’s “Brannforskrift” and/or DNV OS-A101 (“Safety principles and arrangements”) which include a separate

chapter on special provisions for drilling units. Some relevant requirements from DNV OS-A-101 are referred (*in italics*) below:

Shutdowns shall normally be automatically initiated, however solely manually initiated actions may be provided where automatic action could be detrimental to safety, e.g. during drilling and dynamic positioning.

Upon failure of the shutdown system, all connected systems shall default to the safest condition for the unit or installation. The safest conditions for the systems onboard shall be defined.

This is defined in Table C.1 ("Safest conditions and corresponding output circuit configuration") in the DNV Offshore Standard and it is here specified that the drilling system shall normally remain operational with output circuit configuration NDE.

A shutdown logic shall be implemented to determine the response to different degrees of emergency or upset condition. The shutdown logic should be as simple as possible.

Observations (Drilling ESD system)

- The number of possible operational scenarios and situational variety involved in drilling operations, e.g. related to which barriers are available and therefore shall be included in the ESD hierarchy for a given situation, indicate that developing an unambiguous and general shutdown logic for a mobile drilling unit is extremely challenging.
- The remedy for this complexity tends to become extensive manual response and activation of technical barriers such as diversion of flow, activation of BOP and initiation of shutdown actions related to ignition sources and stop of main machinery.

Figure B-4 and B-5 show typical shutdown hierarchies for a mobile drilling unit.

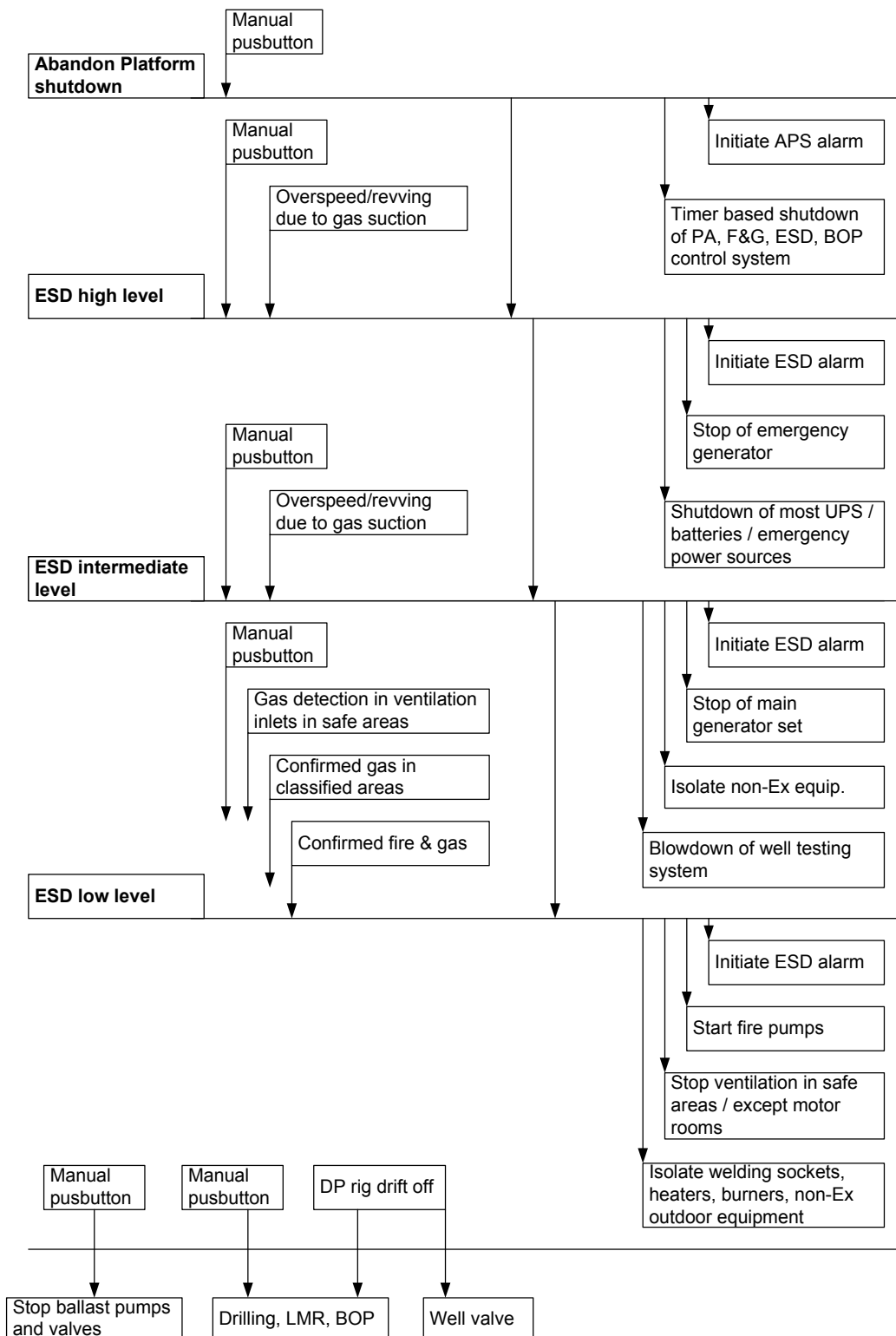


Figure B-4: Typical ESD logic for drilling rig (based on input from Bjørn Arstad, NMD).

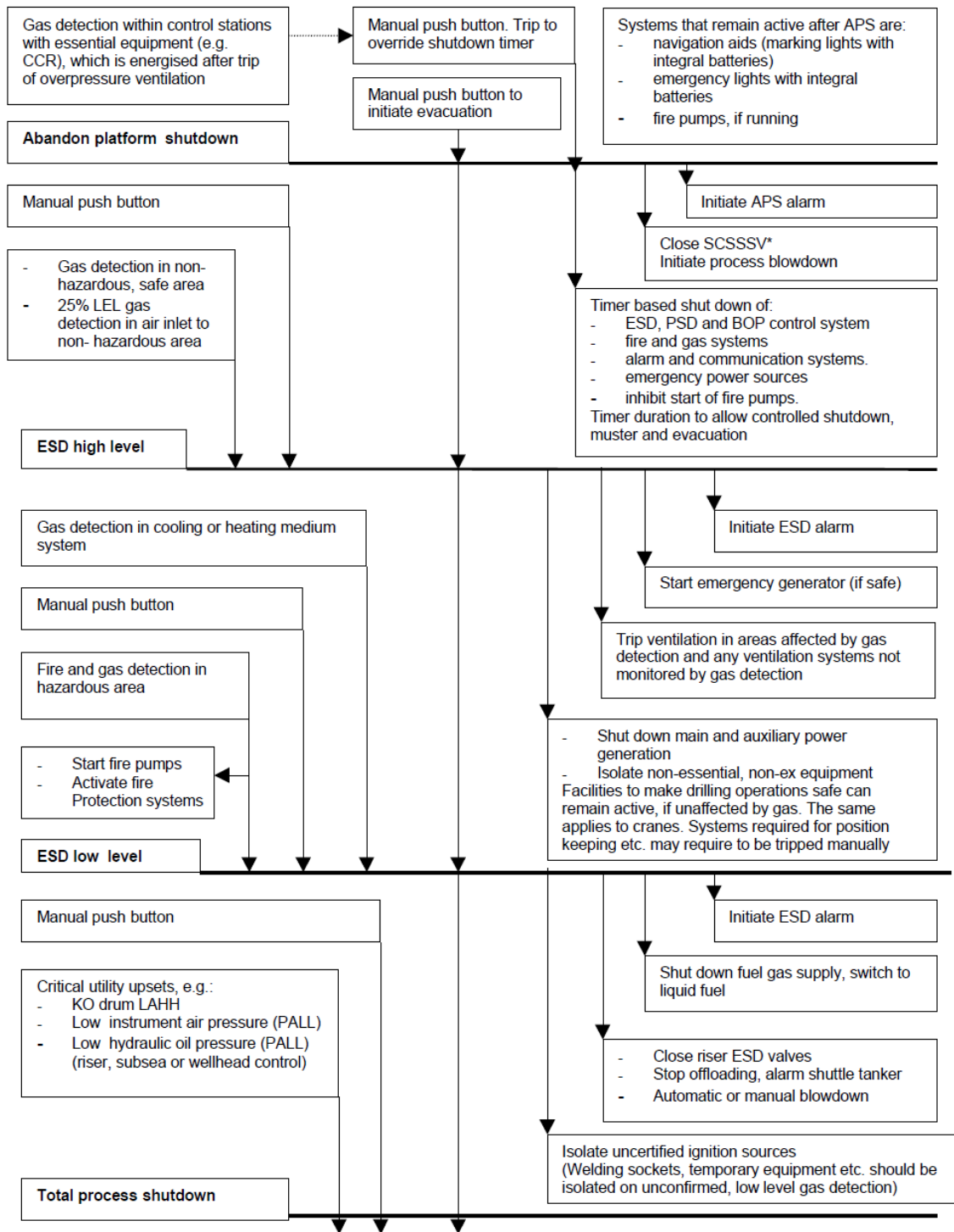


Figure B-5: Outline of emergency shutdown logic for mobile drilling unit (from DNV-OS-A101).

B.2 Well Intervention Equipment

B.2.1 Well Intervention Activities

Well intervention is any operation carried out on an oil or gas well during, or at the end of its productive life, that alters the state of the well or provides additional well diagnostics. Some different types of well work are: (Text is mainly based on NORSOK D-010 and http://en.wikipedia.org/wiki/Well_intervention).

Pumping

This is the simplest form of intervention as it does not involve putting hardware into the well itself. It often involves rigging up valves on the X-mas tree and pumping (injecting) chemicals and fluids into a well through tubing and annuli. The duration of the pumping operations might be short term, when performing stimulation, corrosion treatment, scale treatment, or long term, when disposing slurryfied drill cuttings or waste.

Wellhead and X-mas tree maintenance

The complexity of this operation can vary depending on the condition of the wellhead or X-mas tree. Scheduled annual maintenance may simply involve greasing and pressure testing the valve on the hardware. Sometimes the downhole safety valve is pressure tested as well.

Wireline

A wireline operation is a technique for deployment of various electrical or mechanical downhole tools (logging tools, plugs, packers, perforating guns, shifting tools, pulling tools etc.) on electrical cables, slickline⁹ or braided line¹⁰. The operations are performed in pressurised wells or in dead wells

Coiled tubing

A coiled tubing operation is a technique for deployment of various tools (logging tools, drilling tools, packers, etc.) and as a conduit for circulating or placing fluids in the well. Coiled tubing is used when it is desired to pump chemicals directly to the bottom of the well, such as in a circulating operation or a chemical wash. It can also be used for tasks normally done by wireline if the deviation in the well is too severe for gravity to lower the tool string and circumstances prevent the use of a wireline tractor¹¹. Coiled tubing can be deployed in pressurised wells or in dead wells.

Snubbing

Also known as hydraulic workover, this involves forcing a string of pipe into the well against wellbore pressure to perform the required tasks. The rig-up is larger than for coiled tubing and the pipe more rigid.

Workover

Workover is complex and expensive. The production tubing may have become damaged or downhole components such as tubing retrievable downhole safety valves or electrical submersible pumps may have malfunctioned. The reason for a workover may not be that the completion itself is in bad condition, but the changed reservoir conditions make it unsuitable. Casing strings might also lose integrity and have to be replaced. This is significantly more difficult and expensive than replacing the completion string.

⁹ Slickline operations may be used for fishing, gauge cutting, setting or removing plugs, deploying or removing wireline retrievable valves and memory logging.

¹⁰ Braided line is generally used when the strength of the slickline is insufficient for the task. Braided line includes both the core-less variety used for heaving fishing and electric-line used for logging and perforating.

¹¹ Wireline tractors are electrical tools used to push the tool string into the hole overcoming the wireline's disadvantage of being gravity dependant

These different interventions are commonly executed from light/medium intervention vessels. Mobile Offshore Drilling Units (MODUs) are often used for the heavier interventions such as snubbing and workover.

B.2.2 Requirements to Well Intervention Equipment

Requirements to well intervention equipment are described in NORSOK D-002 (“System requirements well intervention equipment”) and NORSOK D-010 (“Well integrity in drilling and well operations”). Also, other standards may apply (e.g. NORSOK Z-015 for temporary equipment, see below discussion).

The NORSOK D-002 standard is an overall improvement and expansions of the former standards for coiled tubing, snubbing and wire line equipment. In addition to the specific requirements stated in D-002, the standard requires that planning, design, fabrication, operation and maintenance of well equipment shall be according to a list of other standards. (See Tables 1-5 in D-002). The NORSOK D-010 standard focuses on well integrity and requirements to well barrier elements that shall be present during different drilling and well operations, including well intervention activities.

B.2.2.1 Some General Requirements

An overall objective for well activities shall be the requirement that no single failure shall entail a life-threatening situation for the involved personnel, or significant damage to material and the environment.

Function testing of all components including all accessory equipment shall be performed prior to each job. Function testing of the positive and negative weight indicator system shall be performed prior to each job. Function testing of all interfaces to permanently installed equipment and systems. Documentation and verification to be submitted to verify acceptable rig up versus forces and bending momentums, downhole tools, well control system, frames, main equipment and pumps expected work conditions inside set safety limits.

The BOP control system and panels shall be equipped with alarms for low accumulator pressure, loss of power and low level of control fluid.

Maximum response time when the BOP is located on a surface installation: 30 seconds.

Stripper ram maximum response time for snubbing: 5 seconds.

Equalizer, bleed off, kill line and choke line valves maximum response time for snubbing: 1 second.

The accumulator capacity for operating a BOP stack with associated systems shall as a minimum have sufficient volumetric capacity to close, open and close all the installed BOP functions plus 25% of the volume for one closing operation for each one of the said BOP rams.

Systems shall be equipped with a data acquisition system to display and record operational parameters. The data-sampling rate shall be sufficient to record relevant variations in the displayed and recorded parameters.

The power package shall be capable of supplying sufficient power to operate all operating systems of the snubbing unit on a continuous basis and at peak demand.

For snubbing, two independent power packages are required at the work site. Minimum one unit shall be diesel driven.

B.2.2.2 BOP Requirements during Well Intervention

Minimum requirements to the BOP system from NOROK D-002 are shown in the next tables.

Table B-1: BOP minimum requirements – Primary well control system (from D-002).

Primary well control system is defined as follows:		
Equipment	External well control	Internal well control
<p align="center">Snubbing</p> <ul style="list-style-type: none"> • Stripper bowl or active stripper. • Two stripper rams • Equalising loop system • One annular preventer • Workstring • Two back pressure valves in the BHA 	<p>X</p> <p>X</p> <p>X</p> <p>If used</p>	<p>X</p> <p>X</p>
<p align="center">Coiled tubing</p> <ul style="list-style-type: none"> • Dual stripper. • Coiled tubing body (string) • End connector • One dual check valve in the BHA • Alternatively – plugged end of coiled tubing. 	<p>X</p>	<p>X</p> <p>X</p> <p>X</p> <p>X</p>
<p align="center">Wireline</p> <p>Slickline operations Stuffing box for solid wireline.</p> <p>Braided cable Grease injection head with relevant sized flowtubes.</p> <p>Open hole operations Hydraulic line wiper and stuffing box, if applicable.</p> <p>Primary well control system for wireline operations is dependant on type and size of line and is located above the secondary well control system.</p>	<p>X</p> <p>X</p> <p>X</p>	

Table B-2: BOP minimum requirements – Secondary well control system (from D-002).

Secondary well control system is defined as follows:			
Equipment	External well control		Internal well control
<p align="center">Snubbing</p> <ul style="list-style-type: none"> • One combined blind/shear ram • Two pipe rams (fixed or variable) • One annular preventer • Minimum one choke line outlet • Minimum one kill line inlet • Minimum one manual gate and/or plug valve on each choke and kill line and minimum one remote hydraulic operated gate and/or plug valve. Alternatively the remote valve on the kill line can be replaced with one manual valve and a check valve. • One nipple profile in the BHA • One stabbing valve 	X	X	X
<p align="center">Coiled tubing</p> <ul style="list-style-type: none"> • One combined shear/seal ram • One pipe ram • One slip ram • Minimum one kill line inlet • Minimum one manual gate valve and/or plug valve on the kill line and minimum one remote hydraulic operated gate and/or plug valve. Alternatively remote valve can be replaced with one manual valve and a check valve. 	X	X	
<p align="center">Wireline</p> <ul style="list-style-type: none"> • One wireline ram • One wireline ram (inverted) • A double valved kill inlet connection shall be included in the rig up during a live well intervention • One combined shear/ seal ram 	X	X	
	X	X	
	X	X	
	X	X	

Table B-3: BOP minimum requirements – Tertiary well control system (from D-002).

Tertiary well control system is defined as follows:		
Equipment	External well control	Internal well control
General The safety head BOP shall be mounted as close as possible to the wellhead.		
Snubbing One safety head BOP	X	X
Coiled tubing One safety head BOP	X	X
Wireline One shear/seal ram (safety head BOP)	X	X
The need for separate shear/seal ram (safety head BOP) should on the individual facility be considered if the height distance between the valves is short or if remote control valve on the x-mas tree is documented as a shear/seal valve.		

B.2.2.3 Temporary Well Intervention Equipment

Most installations do not have permanent facilities for well intervention installed. Rather, well intervention equipment is taken on board in temporary containers. Such containers are subject to requirements given in NORSOK Z-015 (“Temporary equipment”). In particular, section 4.2.2 and section 4.7.3 of Z-015 deal with well intervention equipment.

In section 4.2.2 of NORSOK Z-015, well service containers are mentioned but no specific requirements to such containers are given as such. It has however been commented that since well service containers are grouped as type B containers together with offices and coffee bars, they are frequently treated as ignition source group 1 equipment and there disconnected on single gas detection. Since these containers in practice make out the CCR for the well subject to intervention, this may be an unfortunate practice¹².

In section 4.3.7 of NORSOK Z-015, well service equipment is further mentioned. For detailed requirements to different types of drilling equipment, reference is however made to NORSOK D-002 (see above).

B.2.3 Typical Safety Functions during Well Intervention – an Example

Consider a light intervention system (LIS) and its associated workover control system (WOCS) applied during coiled tubing and wireline operations for a subsea well. Such a system may typically comprise of a surface flow tree (located on the rig) an Emergency Disconnect Package (EDP) and a Lower Riser Package (LRP) located on top of the subsea well (i.e. the workover BOP).

The intervention system has different safety functions, including PSD, ESD and EQD, implemented in order to assure a safe operation and provide isolation of the well. The purpose of the PDS, ESD and the EQD function will typically be:

¹² However, when considering NORSOK S-001 and the definition of ignition source groups therein (section 3.1.11) it appears that well service containers should be classified as group 2 equipment.

- *The ESD* function will isolate the well by closing production and annulus valves in the lower riser package. The LRP will also include a shear ram which is capable of cutting any lines/tubing running through the lower riser package. Depending on whether a wireline or a coiled tubing operation is performed, the downhole safety valve (DHSW) may or may not be available as a barrier element.
- In case of an uncontrolled event on the rig, *the PSD* may typically be activated by closing valve(s) on the surface flow tree. By doing this, the well is isolated from the test area on the rig.
- *The EQD* function shall include the necessary functionality to allow disconnection of the workover riser from the lower riser package, leaving the well in a safe state with valves closed on the LRP valves, in the event of an emergency situation.

The PSD, ESD and EQD are typically activated manually by operators and are located inside a dedicated WOCS container and in specific rig areas. Often a programmable logic controller (PLC) is located inside the WOCS container, performing both control functions as well as safety functions.

Observations (Well Intervention)

- Well intervention equipment is normally taken on board in temporary containers. The requirements for such temporary equipment seem somewhat diffuse and there are a lot of cross-references between standards. It has been commented that containers with well service equipment frequently are treated as ignition group 1. equipment and are therefore disconnected on single gas detection.
- It has also been commented that BOPs applied during well intervention often are designed according to API 16D where the definition of failsafe and NE/ NDE are not necessarily in line with NORSOK D-002.
- It is a concern that well intervention safety functions (ESD, PSD and EQD) and control functions are often implemented into one single PLC, since a PLC failure may then affect more than one function. Independence between ESD, PSD and EQD is not ensured and furthermore the safety functions are not independent of well control used during normal operation. Also, there may be utility systems, such as purge and power supply, which upon failure may leave the PLC passive.
- The OLF-070 guideline discusses well intervention BOP function with respect to setting SIL but concludes that the background for setting a minimum SIL requirement is not found to be available.
- If the SIL concept is adapted, it may be found that the level of hardware fault tolerance mandated by the architectural constraints in IEC 61508 and OLF-070 conflicts with the more detailed requirements and design considerations for well intervention systems.
- The nomenclature is more precise in NORSOK D-010 compared to D-002.
- The notion “Tertiary well control system” is not used in D-010.
- Function testing of all equipment is required prior to each job. The test interval used in PFD calculations is thus short.

B.3 Subsea Production Safety Functions – ESD and PSD

The NORSOK standard “S-001 Technical Safety” includes several sections describing technical equipment that may constitute safety barriers. Only two sections in S-001 are regarded as subsea related: Emergency Shutdown (ESD) and Process safety / Production Shutdown (PSD).

B.3.1 Emergency Shutdown (ESD)

The purpose of the ESD system is to prevent escalation of abnormal conditions. The ESD system shall operate as an independent system, but will have interfaces to other systems, such as the PSD system, F&G detection, ignition source control, blowdown, flare/vent system and PA communication system. ESD may be activated automatically or manually according to a shutdown hierarchy. Figure B-6 shows a typical emergency shutdown hierarchy taken from NORSOK S-001. This hierarchy represents a typical production installation (for drilling rig ESD system reference is made to section B.1.5).

In OLF-070, the following ESD sub-functions are included:

- Isolation of riser
- Segregation with one ESD valve
- Blowdown
- Isolation of topside well
- Isolation of subsea well

The function “Isolation of subsea well” is subsea related and is further described below.

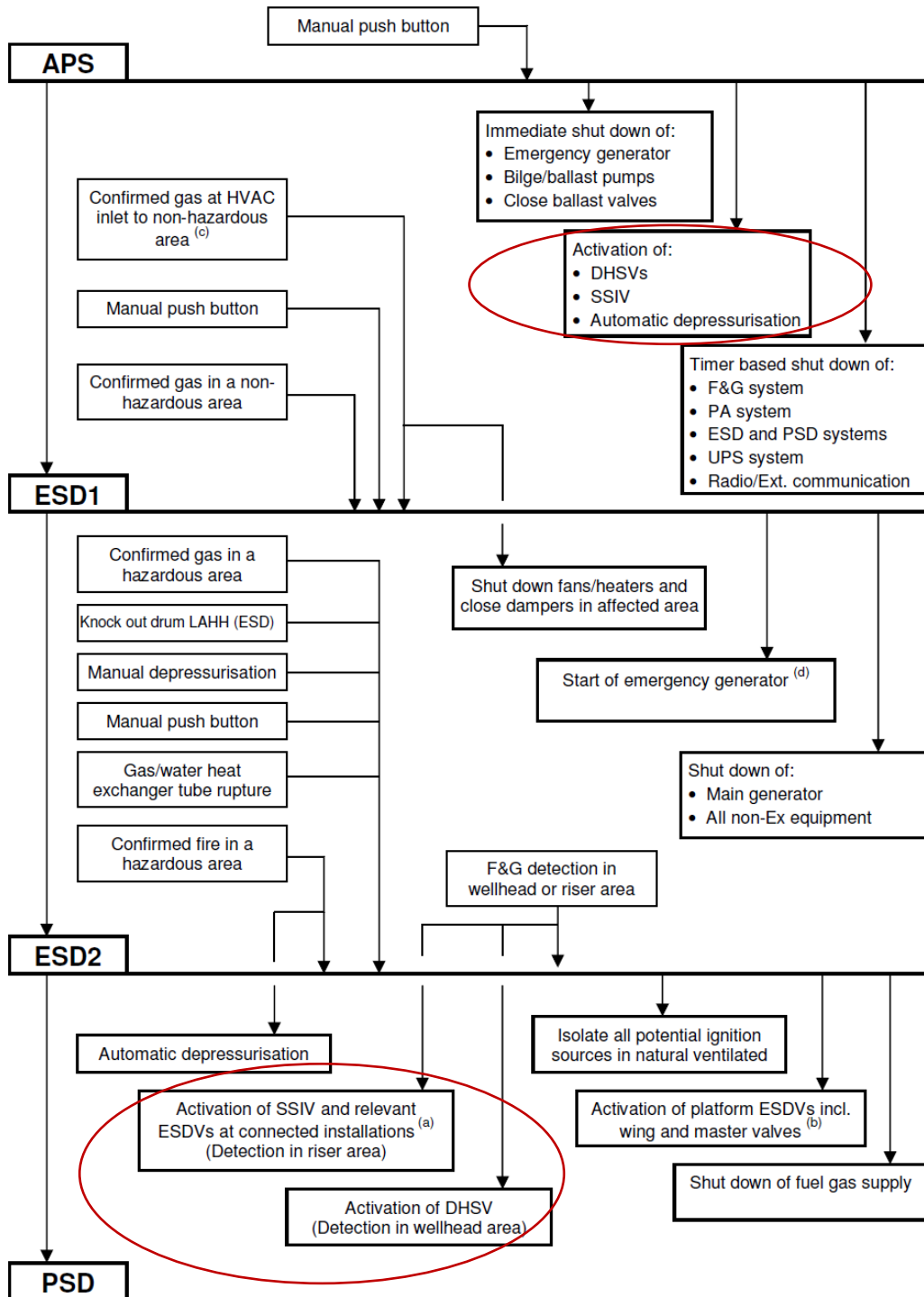


Figure B-6: ESD principle hierarchy (from S-001). Subsea related equipment is marked.

B.3.1.1 Isolation of Subsea Well

For isolation of a standard subsea well, the OLF-070 guideline analyses an ESD sub-system consisting of the following equipment:

- Topside located ESD node
- Topside located ESD hydraulic bleed down solenoid valves in HPU
- Topside located ESD electrical power isolation relay in EPU
- Production Wing Valve (PWV) including actuators and solenoids (in X-mas tree)
- Chemical Injection Valve (CIV) including actuators and solenoids (in X-mas tree)
- Production Master Valve (PMV) including actuators and solenoids (in X-mas tree)
- Down Hole Safety Valve (DHSV) including actuators and solenoids

Note that during well intervention operations, several of the above ESD valves will not be available. The workover BOP will then take over some of the shutdown functions. This BOP is not necessarily directly connected to the installations ESD system, but may be operated from the PLC in the workover container, ref. discussion in section B.2

The locations of PMV, CIV and PWV for a typical horizontal X-mas tree are shown in Figure B-7.

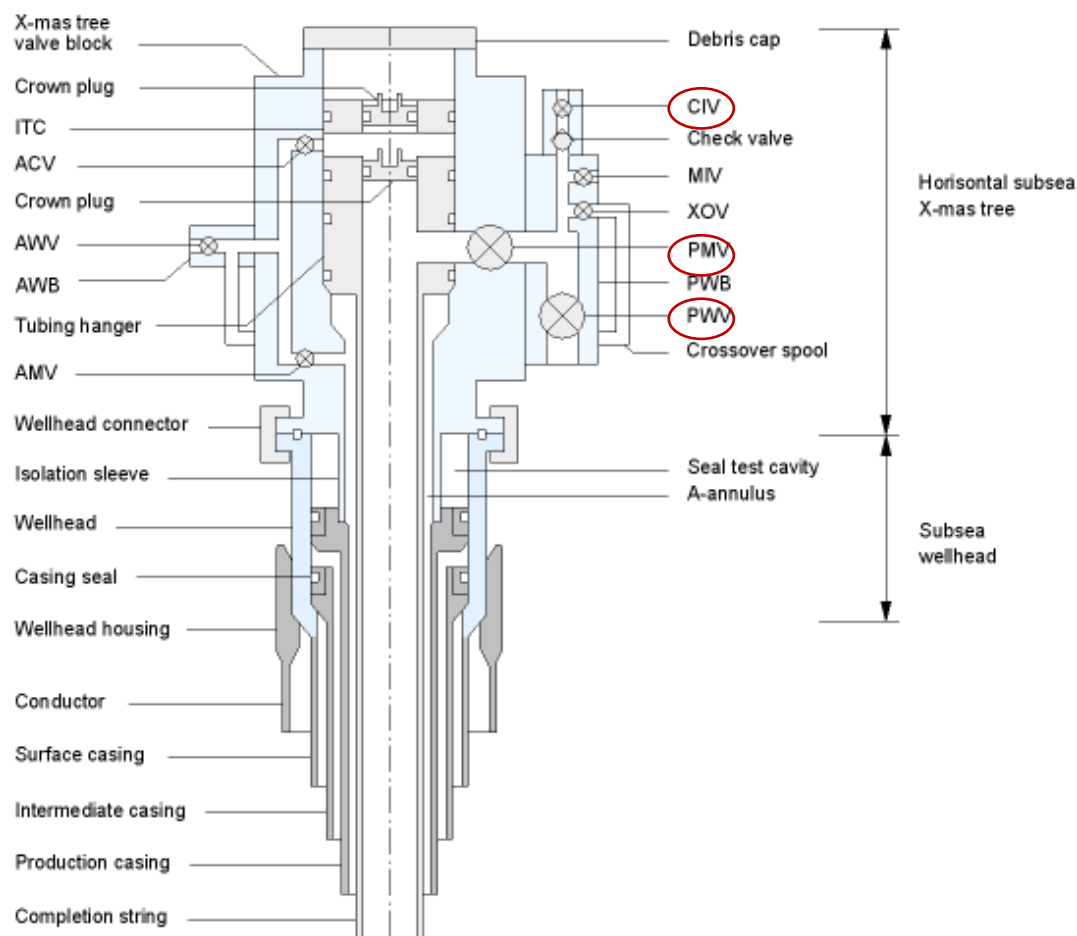


Figure B-7: Typical horizontal X-mas tree, CIV, PMV and PWV are marked (Source, ExproSoft).

OLF-070 states a SIL 3 requirement for the “Isolate subsea well” ESD function.

B.3.2 Process Shutdown (PSD)

B.3.2.1 Description

The process shutdown (PSD) system shall control abnormal operating conditions to prevent hydrocarbon release. This includes:

- Stopping hydrocarbon flow
- Shutdown process and utility equipment
- Pressure relief

The PSD system has interfaces with ESD and BD and flare/vent system. A functional PSD system is typically dependant on UPS, hydraulic power and instrument air.

It should be noted that as per today, no subsea related PSD functions are defined in OLF-070. Since more and more production related equipment is being located subsea, there is obviously a need for new functions to be included in OLF-070.

The only subsea PSD related function covered by the OLF-070 guideline is an example description of a recommended methodology for handling of functional deviations from standard ISO 10418 designs. A case with a flowline/riser not designed for full well shut-in conditions is described. In order to protect the flowline and riser against overpressure, subsea PSD and HIPPS are implemented (see OLF-070 guideline Appendix C).

B.3.2.2 Requirements

Relevant requirements from S-001 are:

Process and auxiliary systems shall be designed such that no single failure during operations can lead to unacceptable hazardous situations. Two independent levels of protection shall be provided. The design shall be in accordance with ISO 10418¹³ (alternatively API RP 14C may be applied).

The PSD system shall be independent from the process control system.

Maximum response time of the process safety function shall be defined in order to ensure that the total reaction time for each safety function can be fulfilled.

Logic solver compliance with the intended use and safety integrity requirements shall be demonstrated.

Observations (subsea production ESD and PSD)

- Concerning ESD and PSD functions, today's safety standards focus mainly on topside facilities (e.g. NORSOK S-001). When it comes to subsea production facilities and drilling operations there seems to be some more confusion related to which standards to use for emergency shutdown functions.

¹³ ISO 10418:2003 provides objectives, functional requirements and guidelines for techniques for the analysis, design and testing of surface process safety systems for offshore installations for the recovery of hydrocarbon resources.

- The SIL concept has been adopted, in light of standards such as IEC 61508, IEC 61511, and OLF-070. A subsea production related ESD function is included (ESD isolation of subsea well) in OLF-070
- SIL requirements concerning subsea PSD functions are per today not included in OLF-070. Furthermore, safety standards such as NORSOK S-001 focus mainly on topside applications. Since subsea production equipment including pumps/compressors and separators are increasingly taken into use, this should be included in a future update of the OLF-070 standard.
- Furthermore minimum SIL requirements are missing for several other types of subsea functions. An example here is subsea leakage detection which, given the right technology, may have a large effect, in particular with respect to environmental risk.
- Possibly off topic, but it should be mentioned that requirements to offshore loading equipment seem to be missing. It may be that systems not being defined as safety critical, such as offshore loading, should be redefined as safety critical in light of being contributors to environmental risk.
- The Facilities Regulations § 33 requires *independence* between ESD and systems for management, control and other safety systems and it has traditionally been mandated to have a relatively clear split between safety and non-safety systems. Yet, this level of independence is being challenged by the technological solutions that are being selected for subsea production systems.

B.4 Well Barriers as Described in D-010

NORSOK D-010 [26] focuses on well integrity by defining minimum requirements and guidelines for well design, planning and executions of well operations on the Norwegian continental shelf. Well integrity is described as the application of technical, operational and organizational solutions to reduce the risk of uncontrolled release of formation fluids throughout the entire life cycle of the well, as well as other safety aspects. NORSOK D-010 requires that the well control equipment and arrangement shall be according to the previously referred standards NORSOK D-001 and NORSOK D-002. The NORSOK D-010 standard is currently under revision.

NORSOK D-010 describes the following activities:

- Drilling
- Well testing
- Well completion
- Production
- Side-tracks, suspension and abandonment
- Wireline operations
- Coiled tubing operations
- Snubbing operations
- Under balanced drilling and completion operations
- Pumping operations

Note that many of the activities in the bullet list above are well intervention activities which have been described in Section B.2.

For each of these activities, well barrier schematics and acceptance criteria are presented and design requirements are given for the equipment. Well barriers are thoroughly described in NORSOK D-010. A well barrier (WB) is defined as an envelope of one or several dependent barrier elements preventing fluids or gases from flowing unintentionally from the formation, into another formation or to surface. Furthermore, D-010 defines a Well Barrier Element (WBE) as an object that cannot prevent flow from one side to another by itself. Figure B-8 illustrates well barriers and terminology used in NORSOK D-010.

Table B-4 and B-5 below present a summary of all the instrumented elements included in NORSOK D-010 that are part of the well barriers for the different activities. The fluid column is included in the table since it is dependent on various instrumented equipment. The activities covered by Table B-4 and Table B-5 represent typical scenarios and are not complete. D-010 states that the activities described are not comprehensive and that schematics for the actual situations during an activity or operation should be made.

General technical and operational requirements and guidelines relating to WBEs are collated in tables in a dedicated section of the D-010 standard. References to these tables are also included in Table B-4 and Table B-5.

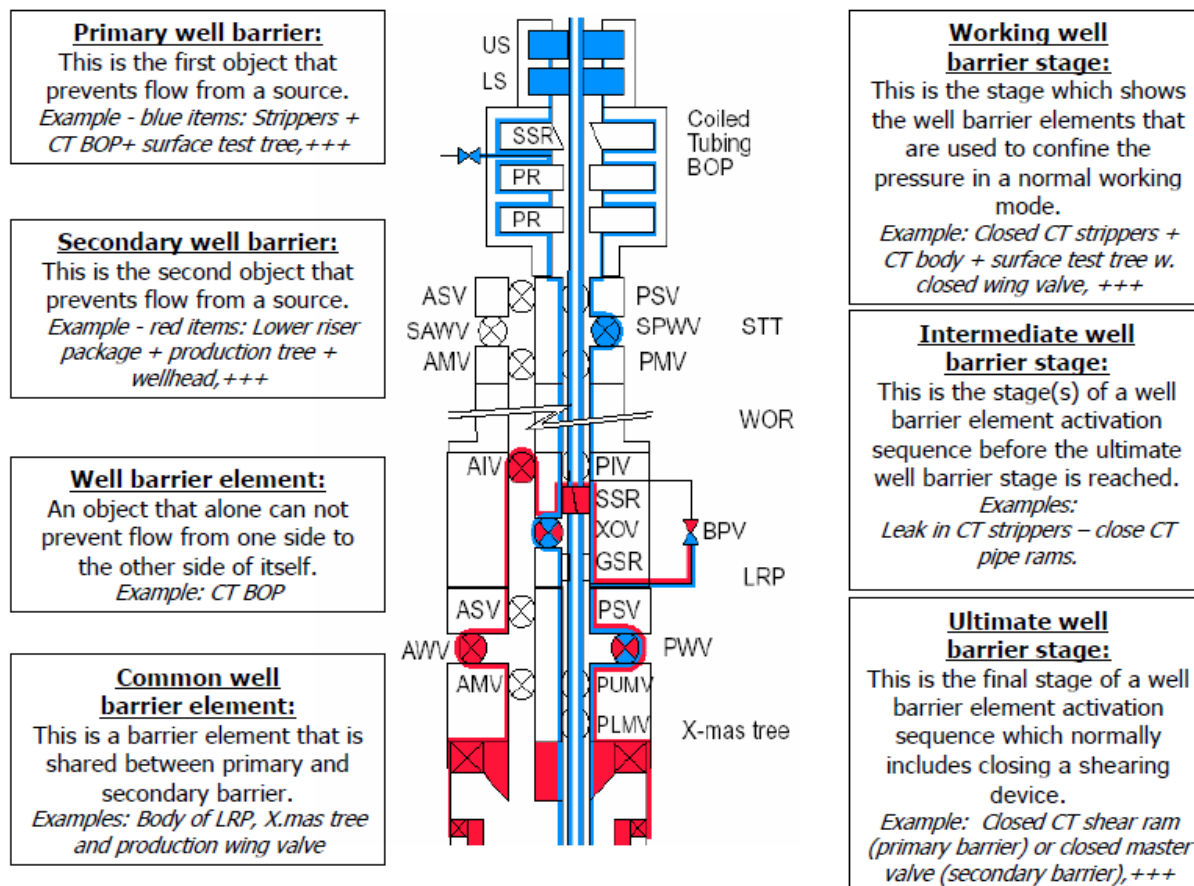


Figure B-8: Well barriers and terminology (from NORSOK D-010).

NORSOK D-010 includes two sections (sections 4.2.5.2 and 4.2.5.3) concerning well control equipment for HTHP and deepwater wells that are interesting with respect to requirements to instrumented safety systems. This includes among others:

- The installation shall [for HTHP wells] be equipped with:
 - a failsafe-open, remotely operated valve in the overboard line,
 - a cement line pressure gauge in the choke panel
- [For deepwater wells] the riser shall have the following:
 1. current meter;
 2. riser inclination measurement devices along the riser;
 3. riser tensioning system with an anti-recoil system to prevent riser damage during disconnection;
 4. flex joint wear bushing to reduce excessive flex joint wear.

In particular the riser instrumentation have an important safety function as part of an emergency disconnect, and as such could be considered subject to SIL/EIL requirements.

Another interesting paragraph in D-010 concerns criteria for shut-down of the activities or operations (section 4.6 in D-010). It is first stated that criteria for shut-down of the activities or operations shall be established. Furthermore it is stated that activities and operations should cease, when:

- having a weakened/impaired well barrier/WBE or failure/loss of a well barrier/WBE,
- high probability for exceeding allowable operating limits of well control equipment and other critical equipment,
- hydrocarbon gas level in air exceeds the specified limit, see Norsok S-001,
- H₂S gas level in air exceeds a time weighted average of $10 \cdot 10^{-6}$ or instantaneous reading of $20 \cdot 10^{-6}$ for a period of maximum 10 min,
- H₂S content of fluids or gases exceeds operating limits of the well control equipment and other critical equipment.

Observations (NORSOK D-010)

- Norsok D-010 has established a well barrier terminology in lack of international standard definitions. D-010 covers the entire life cycle of the well and describes 50 well barrier elements that may prevent uncontrolled release of formation fluids. The life cycle includes several modes of operation and possible SIL requirements should reflect the different modes. Norsok D-010 has established a well barrier terminology in lack of international standard definitions. The standard is not exhaustive with respect to activities and operational situations covered.
- The terminology and definitions given in Norsok D-001 are to some degree ambiguous. For example the relationship between well barrier element (WBE) and well barrier (WB): It is stated that a WBE cannot prevent flow from one side to the other by itself, whereas a WB can. In such case, the WB must comprise two or more WBEs, but the definition says that a WB is an "envelope of *one* or more dependent barrier elements...".
- The standard states that the primary and secondary well barriers to the extent possible shall be independent, but allows for common well barrier elements if "a risk analysis be performed and risk reducing/mitigating measures applied to reduce the risk as low as reasonable practicable". Since, the primary well barrier to a large degree must be considered as an operational (control) measure, this potential mix-up of control and safety must on a principal basis be questioned (also ref. PSA Facilities Regulations [4], § 33–34).
- Norsok D-010 includes a number of interesting requirements to HTHP and deepwater wells. In particular the riser instrumentation (current and inclination measurement systems) have an important safety function as part of an emergency disconnect, and are therefore candidates for SIL/EIL requirements
- In SINTEF's report concerning the Deepwater Horizon accident [32] it is recommended that Norsok D-010 is updated with respect to the cement as a primary barrier, and the use of new technology.
 - *Why:* Failure of the cement barrier and the lack of adequate qualification was an important direct cause of the DWH accident and Montara accident. Shortcomings in relation to application of new technology (such as "managed pressure drilling") were a contributing cause to the Gullfaks C event.
 - *How:* Norsok D-010 should be updated in terms of improved procedures for planning, mixing, pumping and qualification of cement as a primary barrier. The method of placement and qualification of cement as a primary barrier should be better described. Moreover, the standard should be updated based on existing new technologies.
 - *Objective:* An improved best practice will increase understanding of the criticality of cement as the primary barrier and increase the likelihood of successful cementing. Description of best practices regarding new technologies will increase the likelihood of safe applications.

- NORSOK D-010 includes a separate section (4.6) on "Activity and operation shut-down criteria". It would have been beneficial if this section included more specific criteria as to when an activity shall be halted. Experience from a number of well incidents both in Norway and abroad show that numerous danger signals have been present prior to the event, but the operation has been carried on. More explicit and specific stop criteria would therefore be very beneficial and should be considered included as part of the D-010 update. For example the criteria "*having a weakened/impaired well barrier/WBE or failure/loss of a well barrier/WBE*" for ceasing the operation could be more precise. What kind of BOP control pod failures is for example acceptable or not before stopping the operation?

Table B-4: Well barrier elements (WBE) overview (1 of 2)

Well Barrier Elements	Ref	Drilling				Well testing				Suspension	Completion			Production			
	Reference to WBE table in D-010	Drilling with shearable drill string	Running non-shearable drill string	Running non-shearable casing	Through tubing drilling and coring	Running closed end well test string	Flowing and shut-in periods	Landing string disconnected	R/U and R/D WL equip. and changing WI**	Hang off / Disconnect of mariner riser	Running open end completion string	Running non-shearable items through BOP	Pulling BOP and subsea tree	Well capable of flowing – Shut-in	Gaslift platform production well	Subsea production well – vertical tree	Subsea production well - horizontal tree
Fluid column	1	P	P	P	P	P	P	P	P	P	P	P					
Well Head	5	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S
Drilling BOP	4	S	S	S	S	S	S	S	S	S	S	S					
Surface production tree	33				S*									S	S		
Subsea production tree	31				S*											S	S
Surface test tree	34						P		P								
Subsea test tree	32						P	P	P								
SCSSV	8												S	P	P	P	P
Annulus SCSSV	9														P		
Annulus acc. line and valve	12				S								S	S			
Downhole tester valve	46					P		P	P								
Subsea lubricator valve	45						P		P								

P = Element in primary barrier
S = Element in secondary barrier

* Either subsea or surface production tree

** during well testing

Table B-5: Well barrier elements (WBE) overview (2 of 2)

Well Barrier Elements	Ref	Wireline operations					Coiled tubing				Snubbing		UB Drill.		Pumping		
	Reference to WBE table in D-010	Rigging WL equip. above surface tree	Running WL through surface tree	Running WL through vert. ss tree *	Running WL through horizontal ss tree **	Pipe conveyed wireline logging	Rigging CT equip. above surface tree	Running CT through surface tree	Running CT through vert. ss tree *	Running CT through horizontal ss tree **	Rigging snubbing equip. above prod. tree	Running workstring into live well ****	Drilling and tripping of work string *****	Tripping workstring using DIV	Pumping through tubing- SCSSV isolated	Pumping through tubing *****	Pumping fluid down B annulus *****
Fluid column	1					P											P
Well Head	5	S	S	S	S	S		P/S	S	S	S	P/S	S	S	S	S	S
Drilling BOP	4				S	S				S			P/S	S			
Surface production tree	33	S	P/S				S	P/S		S	P/S			P/S			
Subsea production tree	31			P/S	P/S				P/S	P/S							
Surface test tree	34			P	P				P	P							
Subsea test tree	32									P							
SCSSV	8	P					P				P					S	
Wireline stuffing/ grease box head	39		P	P	P												
Wireline BOP(backup WBE)	37		P	P	P												

P = Element in primary barrier
S = Element in secondary barrier

ss tree = subsea tree

* With LRP
** With Drilling BOP and SSTT installed
*** Shear RAM able to shear
**** in UB fluid
***** Production tree isolation tool installed
***** No ASCCV installed

Well Barrier Elements	Ref	Wireline operations					Coiled tubing				Snubbing		UB Drill.		Pumping		
	Reference to WBE table in D-010	Rigging WL equip. above surface tree	Running WL through surface tree	Running WL through vert. ss tree *	Running WL through horizontal ss tree **	Pipe conveyed wireline logging	Rigging CT equip. above surface tree	Running CT through surface tree	Running CT through vert. ss tree *	Running CT through horizontal ss tree **	Rigging snubbing equip. above prod. tree	Running workstring into live well ***	Drilling and tripping of work string ****	Tripping workstring using DIV	Pumping through tubing- SCSSV isolated	Pumping through tubing *****	Pumping fluid down B annulus *****
Lower riser package	42			S				S									
Coiled tubing BOP	14						P	P	P								
Coiled tubing safety head	16						P/S										
Snubbing BOP	19										P						
Snubbing safety head	21										S						
Rotating control device	48											P					
Downhole isolation valve	49												P				
Production tree isolation tool	23														P		

B.5 Summary of Performance Requirements

Table B-6 gives an overview of the following types of requirements:

- SIL requirements
- Timing requirements, typically closing time.
- Requirements to number of operations and accumulator capacity
- Testing requirements

Requirements have been found in the following documents unless otherwise specified:

- For ESD, PSD: NORSOK S-001 [23]
- For drilling facilities: NORSOK D-001 [24]
- For well intervention equipment: NORSOK D-002 [25]
- SIL requirements: OLF-070 guideline [3]

Table B-6: Summary of Performance Requirements

System	SIL	Timing	No of operations	Testing	Comment
ESD Isolation	See below	Fast.	Local accumulators shall have capacity for at least three operations (close-open-close).	Shall be facilities for testing of internal leakage. OLF calculations are based on 6 months test interval.	
- Subsea Well, APS	SIL 3 (OLF)	Shall be defined.			Bleed off time might be too high to be acceptable
- Subsea Well, Hydraulic bleed	SIL 3 (OLF)				
- Subsea Well, Electrical cut	SIL 2 (OLF)	Travel time for ESD valves should not exceed 2s/in.			
PSD	No SIL requirements identified for subsea PSD functions.	Shall be defined.	No requirements identified	No requirements identified	
Drilling Facilities	A general requirement to drilling facilities is that regularity requirements shall be defined prior to detailed design. For mud circulation, the OLF-070 guideline does not recommend to set a general SIL requirement (<i>see text below this table*</i>).			General requirements are given to FAT and startup phase only.	
- Emergency Power	See general requirement above	No requirements identified	NA	Se general requirement above.	
- Bulk System		NA	NA		
- Mud Mixing and Storage		NA	NA		Capacity requirements are

System	SIL	Timing	No of operations	Testing	Comment
Systems					given.
- High Pressure Mud System	Regularity as high as possible	NA	NA		Minimum 2 pumps are normative. Normative capacities are defined.
- Mud Treatment System	See general requirement above	NA	NA		Capacity requirement is given for mud/gas separator system
- Well Control Systems	Drilling BOP - SIL 2 The OLF guideline conclusion regarding BOP SIL is quoted below this table.	Max responsetime when the the BOP is located on a surface is 30 seconds. For annular preventers exceeding 20", a response time of up to 45 seconds is acceptable. Maximum response time for subsea BOP is 45 seconds.	Accumulator capacity for operating BOP stack with associated systems shall have minimum capacity to close, open and close all BOP functions plus 25% of the volume for one closing operation for each of the BOP rams. Additional (to above) accumulator capacity requirements are given (see D-001 for details). For MODUs there shall in addition be sufficient remaning pressure to enable the LMRP to be disconnected after completion of cutting the drillstring. The acoustic accumulator shall have sufficient pressure for cutting the drillstring, after having	Testing shall be possible in a safe and efficient manner. Testing of MODU BOPs at the surface shall be possible with both BOP and LMRP connected. Suitable BOP test stumps shall be available. It shall be possible to perform testing of BOPs on test stump and x-mas trees while normal drillfloor operations are ongoing.	

System	SIL	Timing	No of operations	Testing	Comment
			closed a pipe ram preventer.		
- Cementing Systems	See general requirement for drilling facilities.	NA	NA	See general requirement for drilling facilities.	2 pumps are normative. Min 1 pump is normative for emergency circulation.
- Drilling Instrumentation		Continuously monitoring is required	NA		Some self tests are required: " <i>System design shall include diagnostics...</i> " (see S-001 for details).
Well Intervention Equipment	<p>A general requirement to well intervention equipment is that regularity requirements shall be defined prior to detailed design.</p> <p>The OLF guideline have not found sufficient background information to set a SIL requirement (see text below this table).</p>	<p>Max response time for surface BOP is 30 seconds.</p> <p>Max responsetime for stripper ram during snubbing is 5 seconds.</p> <p>Max responsetime for equaliser, bleed off, kill line and choke line valves is 1 second.</p> <p>Data sampling rate for the data aquisition system shall be sufficient to record relevant variations.</p>	<p>The accumulator capacity for operating a BOP stack with associated systems shall as a minimum have sufficient capacity to close, apen and close all installed BOP functions plus 25% of the volume for one closing operation for each one of the BOPs. Additional (to above) requirements are given depending on operation (see D-002 for details).</p>	<p>General requirements are given to FAT and startup phase.</p> <p>Function testing of all components including all accessory equipment shall be performed prior to each job, including interfaces to permanently installed equipment and systems.</p>	

The OLF-070 guideline discusses the following drilling related safety functions with respect to setting SIL:

- Drilling BOP function
- Well Intervention BOP function
- Kick detection function
- Mud circulation function
- Kill function
- Marine Drilling Riser – Anti Recoil function
- Marine Drilling Riser – Emergency Disconnect function
- Lifting, Rotation and Pipe Handling

Explicit SIL Requirements have only been put upon the Drilling BOP function. The OLF-guideline discussion concludes:

“Setting a SIL 3 level to either function would lead to a significant increase in the standard for drilling BOPs. The challenge lies mainly in the need for documentation of the system reliability. Setting a SIL 3 level would most certainly also result in the need for changing existing control system. It would also be necessary to include additional rams in standard BOP assemblies.

The required PFD/SIL for the BOP function for each specific well should be calculated and a tolerable risk level set as part of the process of applying for consent of exploration and development of the wells. As a minimum the SIL for isolation using the annulus function should be SIL 2 and the minimum SIL for closing the blind / shear ram should be SIL 2.”

For the other safety functions in the above bullet list, no explicit minimum SIL requirements have been stated. For the well intervention BOP the background for setting a minimum SIL requirement is not found to be available. For the other functions the OLF-070 guideline states that it is not recommended to set a minimum SIL requirement for various reasons discussed in the guideline.

C ERA in NORSOK Z-013

Annex G of NORSOK Z-013 provides guidance on how to perform environmental risk analysis in different life cycle phases of an activity. Below, selected parts from Annex G are referred.

The ERA will often be part of an overall risk assessment process for personnel, environment and assets. The approach should be the same irrespective of the context. The environmental risk analysis should address all acute release scenarios which may affect the environment.

Objectives

The objectives of an ERA can vary as follows:

- Present environmental risk picture resulting from activities and operations, for short and long term effects
- Input to risk assessment with respect to comparison with operator's acceptance criteria and environmental goals
- Input to decision-making related to different development concepts and design/decommissioning options
- Input to decision-making with focus on consideration of environmental risk reducing measures for activities and operations, including environmental preparedness and response.

ERA steps

The following steps may form part of an environmental risk analysis:

1. Identify release scenarios to the environment, based on an environmental HAZID as well as the scenarios from quantitative risk analyses.
2. Analyse barriers on the installations that may prevent spills or reduce amount of spilled volume to the environment, including reduction of discharge rates and duration of spills.
3. Establish release scenarios (e.g. leak location (geographical, topside and subsea), contaminant characteristics, discharge rates and durations.
4. Simulation of the drift and dispersion of the contaminant (e.g. oil) for relevant scenarios. This includes spread on the sea surface, contamination of water column, drift time, evaporation, emulsification and eventually stranding of oil on shore.
5. Establish the occurrence of environmental resources within the influence area and their vulnerability/sensitivity towards the contaminant. (Indicators for sensitivity can be vulnerability of the resources (individual and/or population/habitat level) to the contaminant and/or the scientific value or administrative protection value of the resources.)
6. Calculate drift time to and the exposure of these environmental resources to the contaminant (overlap between the contaminant and scenarios for distribution of the biological resources).
7. Assess (qualitatively or quantitatively) the short and long term effects on these environmental resources, e.g. on individuals and populations (establish relevant, reliable and valid consequence categories).
8. Assessments shall be based on updated science and monitoring and mapping of biological resources.
9. Calculate the risk as a combination of the probability of a certain event causing environmental damage and the degree of seriousness of this damage.
10. Compare the risk with the environmental acceptance criteria.
11. ALARP evaluations.

Contents

The following should be performed for offshore facilities in relation to environmental risk and environmental preparedness and response analysis:

- a) the operator should perform risk and emergency preparedness analyses for acute pollution from its own installations and activities. The risk contributions from different installations shall be considered together. Unmanned installations shall be considered together with the manned installations to which they are connected. It shall be possible to compare the environmental risk contributions from different installations in an unambiguous way;
- b) the operator should establish goals for protection of prioritized, vulnerable resources. Alternative equipment solutions and their availabilities should be identified at an early stage, and their effect should be analysed. The analyses shall include the categories sea surface, water column, coast and shoreline when relevant, and should ensure that different vulnerabilities in different geographical areas are considered;
- c) the characteristics of oil and chemicals and actual effectiveness values for preparedness equipment should be included in the basis for analyses;
- d) the analyses should use the event sequences that may result in acute pollution. The initiating events should be ranked, preferably based on analyses of transport and spreading. In addition, the event sequences should be supplemented with other types of incidents and conditions that also can result in acute pollution;
- e) for the identified release scenarios, discharge rate and duration distributions shall be established. Selected scenarios shall be subject to transport and spreading analyses, based on discharge rate and duration distributions. The transport and spreading calculations shall include the periods for the planned activity and the subsequent month;
- f) with respect to risk reduction, it is required that all risk contributions are considered together. This implies that the analyses shall have the possibility to classify results into applicable and comparable categories;
- g) consideration of vulnerable environmental resources shall be made visible in the environmental risk and environmental preparedness and response analyses. The environmental preparedness and response analysis shall, where relevant, consider fields and areas as well as regions in the same context.



Technology for a better society

www.sintef.no