PDS

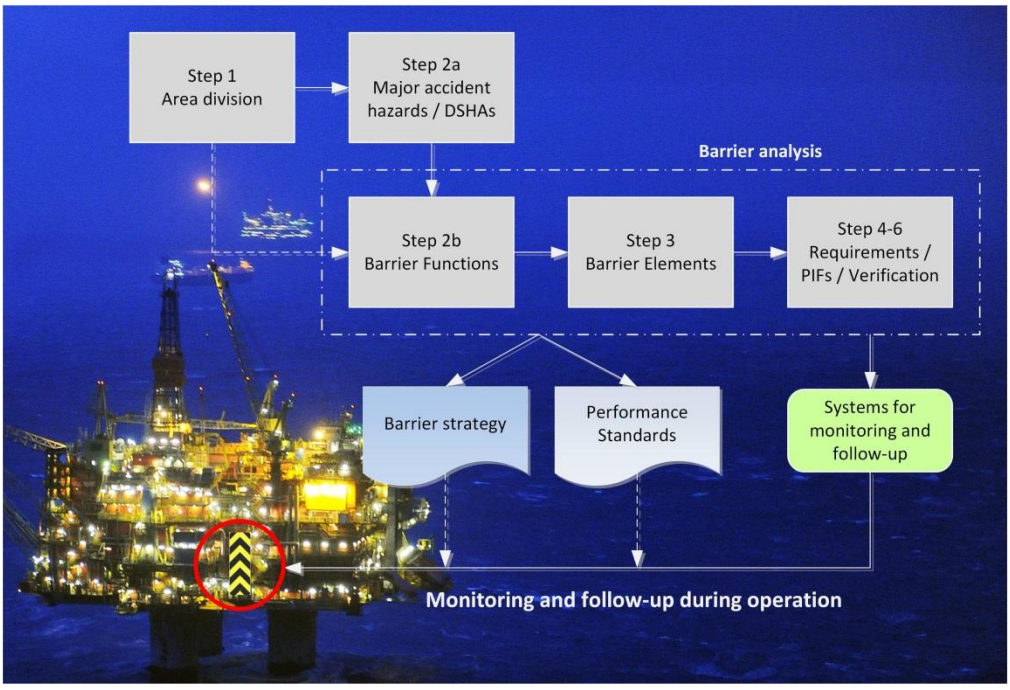
SINTEF

SINTEF A27623 - Unrestricted

Report

Guidance for barrier management in the petroleum industry

Authors
Stein Hauge and Knut Øien



SINTEF Technology and Society
Safety Research
2016-09-23

(Empty page)

SINTEF

SINTEF Teknologi og samfunn
SINTEF Technology and Society

Address:
Postboks 4760 Sluppen
NO-7465 Trondheim
NORWAY

Telephone:+47 73593000
Telefax:+47 73592896

ts@sintef.no
www.sintef.no
Enterprise /VAT No:
NO 948007029 MVA

KEYWORDS:
Safety
Barrier management
Petroleum Industry

Report

Guidance for barrier management in the petroleum industry

VERSION
Version 02

DATE
2016-09-23

AUTHOR(S)
Stein Hauge and Knut Øien

CLIENT(S)
PDS forum

CLIENT'S REF.
Håkon S. Mathisen

PROJECT NO.
102001170

NUMBER OF PAGES/APPENDICES:
62

ABSTRACT

The purpose of this report is to provide practical guidance on barrier management with focus on establishing systems and solutions for maintaining the function of the barriers throughout the lifetime of an offshore or onshore petroleum facility. It covers guidance on how to identify and define barriers and barrier elements, how to formulate performance requirements for the barrier elements and how to monitor the status of the barriers and verify that the requirements are fulfilled during operation. This includes examples of approaches, methods and specific tools for barrier management. Operational and organisational barriers and barrier elements are emphasized, since main industry focus so far has been on technical barriers. The report has been developed as part of the PETROMAKS innovation project "Tools and guidelines for overall barrier management and reduction of major accident risk in the petroleum industry", funded by the Norwegian Research Council and the members of the PDS forum.

PREPARED BY
Stein Hauge and Knut Øien

SIGNATURE

CHECKED BY
Lars Bodsberg

SIGNATURE

APPROVED BY
Stian Antonsen, Research Director

SIGNATURE

REPORT NO.	ISBN	CLASSIFICATION	CLASSIFICATION THIS PAGE
SINTEF A27623	978-82-14-06031-7	Unrestricted	Unrestricted

Document history

VERSION	DATE	VERSION DESCRIPTION
Version No. 01	2016-04-06	Draft for PDS member comments
Version No. 02	2016-09-23	Final version

Preface

This report has been developed as part of the PETROMAKS innovation project "*Tools and guidelines for overall barrier management and reduction of major accident risk in the petroleum industry*", funded by the Norwegian Research Council and the members of the PDS forum. The report expresses the views of the authors, and may not express the views of all the PDS participants.

The project comprises the following five main activities:

1. Development of an overall method for barrier management /1/
2. Development of improved methods and data for modelling of dependencies between barriers and barrier elements /2/
3. Evaluation of how new technology – and wireless technology in particular – may affect the performance of the barriers /3/
4. Development of industry guidance for overall barrier management including technical, operational and organisational barrier elements for all relevant lifecycle phases
5. Publication of results

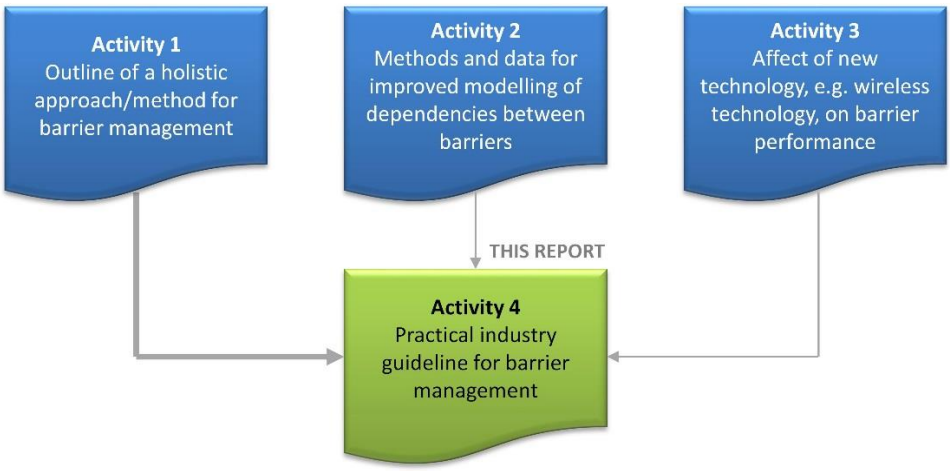


Figure 0.1 Link between the various project activities and reports

This report documents Activity 4. It builds on the work carried out in Activity 1 and incorporates some results from Activity 2 and 3.

Many examples in this document are based on barrier management work performed in the Goliat FPSO project. In this project, Safetec, ABB and SINTEF have collaborated closely with Eni Norge, and we greatly appreciate their contributions and consent to issue this report. In particular, we will emphasise Safetecs contribution to the methodology presented in this report.

In 2014, DNV GL on behalf of the Norwegian Shipowners' Association issued the document *Barrier Management in Operation for the Rig Industry; "Good practices"* /7/, where most of the examples are related to barrier functions on a drilling rig. In this PDS guidance document, the examples are generally focusing on topside production; thus, this document supplements the DNV GL good practice document.

About PDS forum

PDS forum is a co-operation between oil companies, engineering companies, drilling contractors, consultants, vendors and researchers, with a special interest in safety instrumented systems in the petroleum industry. The main objective is to maintain a professional meeting place for:

- Exchange of experience and ideas related to design and operation of safety instrumented systems (SIS)
- Exchange of information on new field developments and SIS application areas
- Developing guidelines for the use of new standards on safety and control systems
- Developing methods and tools for calculating the reliability of SIS
- Exchange and use of reliability field data

Participants PDS forum

Oil companies / Operators:

A/S Norske Shell
BP Norge AS
ConocoPhillips Norge
Det norske oljeselskap ASA
Eni Norge AS
ENGIE (GDF SUEZ E&P)
Odfjell Drilling & Technology
Lundin Norway AS
Statoil ASA
Repsol Norge (Talisman Energy Norge)
Teekay Petrojarl ASA
Total E&P Norge AS

Governmental bodies (observers):

The Norwegian Maritime Directorate
The Petroleum Safety Authority Norway

Control and Safety System Vendors:

ABB AS
FMC Kongsberg Subsea AS
Honeywell AS
Kongsberg Maritime AS
Origo Solutions AS
Siemens AS
Simtronics ASA / Tyco

Consultants / Engineering companies:

Aker Engineering & Technology AS
Aker Subsea AS
DNV GL Norge AS
Lilleaker Consulting AS
Lloyd's Register Consulting
Safetec Nordic AS

For more information about PDS forum see: www.sintef.no/pds

SINTEF

Table of contents

Executive Summary

Introduction

This report provides practical guidance on barrier management covering both design and operation. Operational and organisational barriers and barrier elements are emphasized, since main industry focus so far has been on technical barriers.

The report provides guidance on how to identify and define barriers and barrier elements, how to formulate performance requirements for the barrier elements and how to monitor the status of the barrier elements and verify that the requirements are fulfilled during operation. This includes examples of approaches, methods and specific tools for barrier management.

This guidance document is not prescriptive. Concepts, definitions, approaches, methods and tools may be adopted or adapted to the degree found suitable for the individual user.

Risk reduction through multiple – and independent – barriers

The petroleum industry is facing the risk of major accidents, i.e. accidents with major consequences, which may cause multiple fatalities and/or massive oil spills. Fortunately, such accidents have low probability of occurrence. One reason for the low probability is multiple layers of protection (barriers), or what is also called "defense in depth". Single failures can and will occur, but single failures should not be allowed to result in catastrophic events. This is why we have multiple barriers in place, which need to be managed throughout the life cycle of the facility.

Traditionally, barrier management focuses on single barriers and technical aspects and - to a lesser degree - operational conditions. This focus on single barriers rather than the entire barrier system may fall short of preventing major accidents that are characterized by multiple barrier failure. It is important that barrier management focus on the entire barrier system including technical, organizational and operational measures, in order to avoid potential multiple barrier failures.

Barrier management overview

We distinguish mainly between the design phases (*establish barriers*) and the operations phase (*maintain and follow-up barriers*). In the design phases, the focus is on identifying and designing barriers to ensure that necessary risk reduction can be obtained during operation. In the operations phase, the focus is on follow-up and maintaining the barriers to ensure that they are available at all time, to implement compensating measures if barriers are impaired, and to verify required performance.

Overall principles and framework for barrier management provide a foundation for barrier management processes on specific facilities or projects. A barrier strategy shall be established for each facility based on the unique characteristics of the facility. Thus, the purpose of the strategy is to describe a logical relationship between the unique risk picture, as described in safety and reliability studies from design and engineering, and the selected barriers. Detailed performance requirements for barrier elements are included in corresponding performance standards.

Establish barriers – barrier management in design – preparing for operation

The main steps to establish a barrier strategy and corresponding performance standards include the following topics:

1. Facility description and area division
2. DSHAs and barrier functions per area (based on the risk picture)

3. Barrier elements in each area (or globally)
4. Performance requirements
5. Performance influencing factors (PIFs)
6. Verification activities (and intervals) for monitoring of barrier performance

After having identified the technical, operational and organizational barrier elements, and defined the associated performance requirements and verification activities, it is important to prepare for the operations phase, including the development of information systems and tools that can be applied during operation. Such systems and tools should be developed during the design and engineering phase in order to ensure readiness for operation.

The frequency of information needed for these systems and tools vary from real time (instantaneous) to infrequent data (years); thus, they cover both short term and longer-term perspectives. Short-term tools (e.g. a barrier panel/dashboard) provide information needed on a daily basis for e.g. planning of work and work order approval. Medium-term tools capture threats to the barriers that gradually develop over time, and methods covering long-term perspectives are needed for verification purposes.

Maintain and follow-up barrier performance – barrier management in operation

Barrier management activities in operation include:

1. Normal (safe) operation
    - Operating within design envelope, including monitoring of barrier status
    - Keeping overview, logging and control of inhibits and overrides
    - Daily reporting of safety critical failures and non-conformances
    - Handling of non-conformances
    - Identifying and evaluating need for modifications or changes
2. Maintaining barrier performance

    2a. Testing and maintenance of technical barriers
    - Maintenance, testing and inspection according to maintenance programme / test procedures
    - Review of maintenance/testing back-log

    2b. Maintenance of organizational and operational barriers
    - Follow-up of required offshore competence and resources
    - Keeping safety critical procedures updated
3. Verification and evaluation of barrier performance
    - Verification of performance of technical barrier elements and performance standards
    - Verification of performance of organizational and operational barrier elements
    - Annual reviews to verify compliance with required performance
    - Audits, inspections, and management reviews to verify long-term performance
4. Evaluation, decision, and implementation of measures to counteract performance deviations
5. Keeping the basis for barrier operation updated (e.g. barrier strategy and performance standards)

A description of these activities are provided, including indication of responsible position/role, and suggested frequencies of the various barrier management activities.

1 Introduction

1.1 Scope

The original scope of this report is to provide "a practical industry guideline for overall barrier management including technical, operational and organizational barrier elements for all relevant lifecycle phases".

We distinguish mainly between the design phases (establish barriers) and the operations phase (maintain and follow-up of barriers).

Overall barrier management is described in the report *"Towards a holistic approach for barrier management in the petroleum industry"* /1/. In the present report, the focus is on practical guidance, emphasizing important aspects and challenges, i.e. to answer questions such as:

1. How to identify and define the barriers, in particular organisational and operational barrier elements?
2. How to define performance requirements to the barrier elements?
3. How to establish practical solutions and systems for barrier management?
4. How to apply these solutions and systems during operation, including:
    a. How to monitor the status of the barriers?
    b. How to maintain the performance of the barriers?
    c. How to verify that the performance requirements are fulfilled?
    d. How to manage changes to the barriers?

We propose answers to these questions, but they are by no means the only possible answers. This report does not prescribe an exact recipe, but provides *guidance* on how to establish and manage barriers during design and operation.

1.2 Input and approach

This report is based on:

- Work performed earlier in this research project (/1/, /2/, /3/)
- Review of relevant documents, e.g. the PSA "barrier memo" /4/, PSA regulations /5/ and industry initiatives such as the DNV GL / NSA "good practices" document /7/
- Review of barrier performance data, such as RNNP data /8/ and company/project specific data in a SINTEF report for PSA /9/
- Experience gained through participation in industry and authority projects on barrier management
- Discussions in PDS forum meetings and workshops
- Experience from industry representatives
- Comments from the industry on draft revision of the report

Many examples presented in this document are based on barrier management work performed in the Goliat FPSO project. In this project, Safetec, ABB and SINTEF have collaborated closely with Eni Norge, and we greatly appreciate their consent to issue the report. In particular, we will emphasise Safetecs contribution to the methodology presented in this report.

1.3 Limitations

Major accidents, i.e. accidents that may lead to multiple fatalities, major environmental harm or loss of assets (major economic losses), are of main concern for the industry, and this report considers barriers in the

context of major accident risk. In a wider sense and according to regulations, barrier management should also address risks related to working environment, personal injury, security, and production regularity. This is however outside the scope of this report.

The aim of this report has been to cover important aspects and challenges related to barrier management. As discussed in /1/, barrier management is a wide-ranging topic and there are certainly challenges that are beyond the scope of this report.

The area of barrier management is rapidly evolving, and there are ongoing initiatives, e.g. company specific initiatives, for which information is not publicly available.

1.4 Abbreviations

API	American Petroleum Institute
BSP	Barrier Status Panel
CCF	Common Cause Failure
CCR	Central Control Room
CM	Corrective Maintenance
CMMS	Computerized Maintenance Management System
DNV GL	Det Norske Veritas Germanischer Lloyd
DP	Dynamic Positioning
DSHA	Defined Situations of Hazard and Accident
EPA	Emergency Preparedness Analysis
EPP	Emergency Preparedness Plan
ESD	Emergency Shutdown
ESRA	European Safety and Reliability Association
ESV	Emergency Shutdown Valve
FAR	Fatal Accident Rate
FPSO	Floating Production, Storage and Offloading
HAZID	Hazard Identification
HAZOP	Hazard and Operability Study
HC	Hydrocarbons
HF	Human Factors
HMI	Human Machine Interface
HR	Human Resource
HSE	Health, Safety and Environment
HVAC	Heating, Ventilation and Air Conditioning
IEC	International Electrotechnical Committee
IMS	Information Management System
IOGP	International association of Oil & Gas Producers
IR	Infrared
ISO	International Standardization Organization
JRCC	Joint Rescue Coordination Centre
LEL	Lower Explosion Limit
MEG	Methanol and Glycol
MR	Management Regulations
NORSOK	The Norwegian shelf's competitive position (*Norw.*: "Norsk sokkels konkurranseposisjon")
NSA	Norwegian Shipowners' Association
OCS/OTS	Operational Condition Safety / Operasjonell Tilstand Sikkerhet

OIM	Offshore Installation Manager
O&O	Operational and Organisational
PAHH	Pressure Alarm High High
PDS	Reliability of Safety Instrumented Systems (*Norw.*: "Pålitelighet av Datamaskinbaserte Sikkerhetssystem")
PFD	Probability of Failure on Demand
PIF	Performance Influencing Factor
PM	Preventive Maintenance
PS	Performance Standards
PSA	Petroleum Safety Authority
PSD	Process Shutdown
PSV	Pressure Safety Valve
P&ID	Piping and Instrumentation Diagram
QRA	Quantitative Risk Analysis
RNNP	Risk Level in the Norwegian Petroleum Industry *(Norw.:"* RisikoNivå i Norsk Petroleumsvirksomhet")
SAS	Safety and Automation System
SCTA	Safety Critical Task Analysis
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented Systems
SRS	Safety Requirement Specification
TBD	To Be Decided
TCS/TTS	Technical Condition Safety / Teknisk Tilstand Sikkerhet
TIMP	Technical Integrity Management Project
TO&O	Technical, Operational and Organisational
XV	On/off (shutoff) Valve

1.5 Report structure

In Chapter 2, we describe the need for risk reduction through multiple barriers, and the importance of independent barriers[1]. We also present relevant definitions and discuss differences between some of the definitions. Chapter 3 presents an overview of barrier management, mainly based on the PDS report: *"Towards a holistic approach for barrier management in the petroleum industry"* /1/. Chapter 4 gives guidance on the establishment of barriers, i.e. barrier management in design. Chapter 5 gives examples of supporting systems and tools for barrier management and verification. Finally, Chapter 6 gives guidance on maintaining the performance of barriers during operation, i.e. barrier management in operation.

[1] Independence between barriers and common cause failures are core issues covered in a separate PDS project report (Activity 2): *"Common Cause Failures in Safety Instrumented Systems – Beta Factors and Equipment Specific Checklists based on Operational Experience"* /2/.

2 The barrier concept and barrier definitions

2.1 The barrier concept – risk reduction through multiple barriers

The petroleum industry, like the nuclear industry, aviation and others, is facing the risk of major accidents, i.e. accidents with major consequences, which may cause multiple fatalities and/or massive oil spills. Fortunately, such accidents have low probability of occurrence; they are what we call "low probability, high consequence" events.

A main reason for the low probability is multiple layers of protection, which is also called "defense in depth". This is achieved through multiple barriers, as illustrated in Figure 2.1 by "cheese slices with holes" in the so-called "Swiss Cheese model" /Reason/.

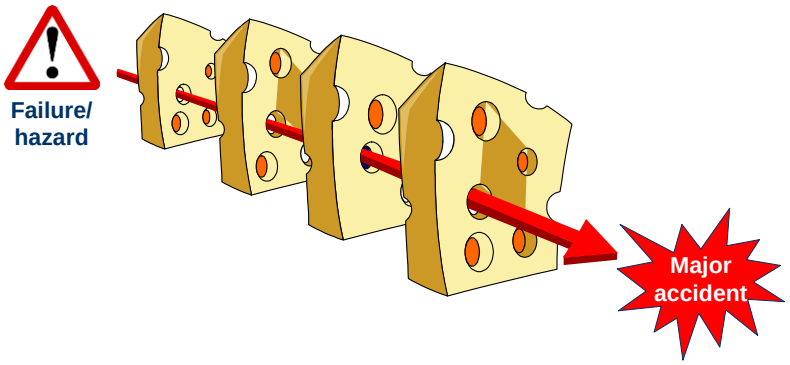


Figure 2.1 Swiss Cheese model (adapted from /12/)

Single failures can and will occur, but single failures should not be allowed to result in catastrophic events. This is why we have multiple barriers in place.

Evidently, even multiple barriers sometimes break down ("the holes in the Swiss cheese slices aligns"), resulting in a major accident, such as the Deepwater Horizon accident in the Gulf of Mexico in 2010, causing the loss of 11 lives and the largest oil spill in U.S. history /10/.

Copyright: Getty Images

Figure 2.2 The Deepwater Horizon accident in 2010

The Management Regulations, Section 5 (Barriers), is one of the key requirements that frames the design and operation of safety barriers in the Norwegian petroleum industry /5/. It outlines the principle of having multiple, and sufficiently independent, barriers to control risk and the need to prevent multiple barrier failure or degradation from single events or conditions.

According to the Management Regulations, Section 5, second subsection: *"Where more than one barrier is necessary, there shall be sufficient independence between barriers"*. /5/

In the Guidelines regarding the management regulations, Section 5, it is stated: *"The requirement for independence as mentioned in the second subsection, entails that it should not be possible for multiple important barriers to be impaired or malfunction simultaneously, e.g. as a result of a single fault or a single incident"*. /19/

Avoiding such failures or incidents therefore becomes an important part of barrier management and accident prevention. Design and/or operational measures must be in place to avoid simultaneous failure of several barrier elements.

Dependencies are often included in reliability assessments by modelling the effects of multiple failures with shared causes. Such common cause failures (CCFs) are sometimes the main contributor to the total safety unavailability for systems with redundancy. This is illustrated in Figure 2.3.

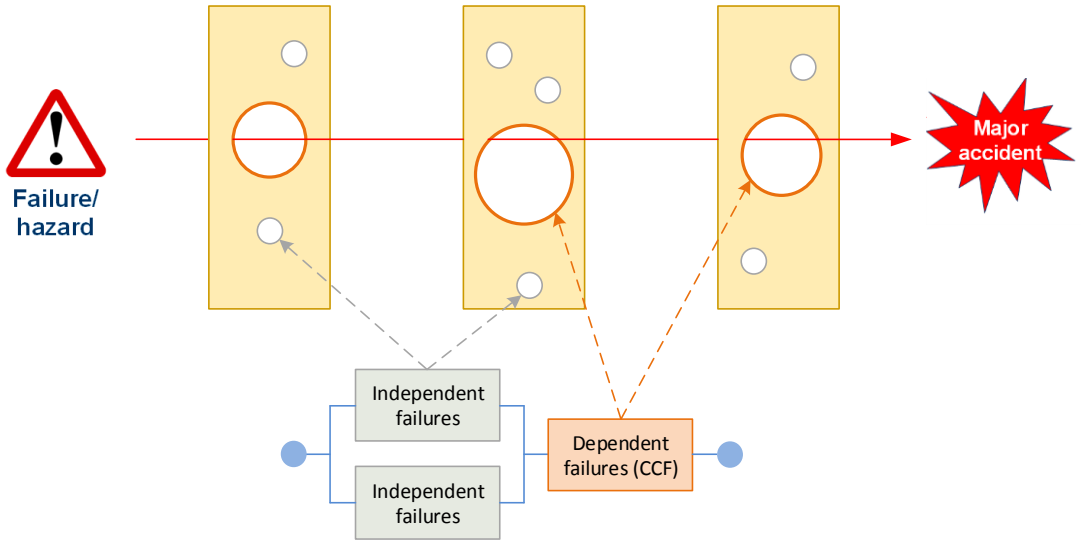


Figure 2.3 Possible effect on safety barriers from common cause failures

Modelling of dependencies and common cause failures (CCFs) are traditionally only included in assessments of technical systems. Standards like IEC 61508 /15/ and IEC 61511 /16/, require that the contribution from CCFs shall be included in the quantification of reliability. Among the most popular models is the beta-factor model using the parameter β to represent the fraction of all item failures that are CCFs. CCF models and data based on operational experience for safety instrumented systems (SIS) are further described in /2/.

When investigating major accidents and tracing the course of events beyond/behind the immediate causes, it is often found that such events can be seen as a result of some kind of organizational neglect. I.e. investigations of major accidents rarely stop at simple technical failures or human errors, but often identify organizational weaknesses that affect multiple barriers. E.g., in /10/ it is concluded: "*The Deepwater Horizon*

accident did not happen as a result of one crucial misstep or a single technical failure, but as a result of a series of events, decisions, misjudgments and omissions that reveal a systemic breakdown".

Traditionally, barrier management focuses on single barriers and technical aspects and - to a minor degree - operational conditions. This focus on single barriers rather than the entire barrier system may fall short of preventing major accidents that are characterized by multiple barrier failure. It is important that barrier management focus on the entire barrier system including technical, organizational and operational measures, in order to avoid potential multiple barrier failures.

In summary, maintaining the functionality of each single barrier, avoiding dependencies between the barriers and focusing on organizational and operational measures/solutions, as well as the technical solutions, are all key ingredients in successful barrier management.

2.2 Barrier related definitions

In order to perform barrier management, it is important to have a common understanding of what constitutes a barrier /7/. Experience from various projects show that the agreed definitions, and in particular how broadly a barrier is defined, influence the scope of the barrier management activities. Establishing baseline definitions early in the project is therefore important.

Although the definitions discussed in this section have some minor differences, the main message is to agree on a set of common definitions that are suitable for the project under consideration, and use these consistently to identify barriers, barrier functions, barrier elements and associated performance requirements.

In the following discussions, we use the concepts and definitions recommended by PSA as a starting point. Complying with the regulators is hardly a disadvantage, but definitions are not normative. Hence, PSA allows for alternative definitions as long as regulatory requirements are otherwise fulfilled. We will therefore also discuss some alternative definitions. A main objective has been to present a logical breakdown of barrier functions into sub-functions and tasks, and associated definitions that clarify the relationship between these sub-functions and tasks and the elements used to realize them.

2.2.1 Barrier management

The Petroleum Safety Authority (PSA) has issued a memo; *"Principles for barrier management in the petroleum industry"* /4/ hereafter referred to as the "Barrier memo", where the purpose of barrier management is expressed as:

The main purpose of barrier management is to establish and maintain barriers so that the risk faced at any given time can be handled by preventing an undesirable incident from occurring or by limiting the consequences should such an incident occur. Barrier management includes the processes, systems, solutions and measures, which must be in place to ensure the necessary risk reduction through the implementation and follow-up of barriers (/4/, page 1).

The associated definition of "barrier management" provided by PSA /4/ is:

Barrier management:	*Coordinated activities to establish and maintain barriers so that they maintain their function at all times*

2.2.2 Barrier

There exists a number of definitions of "barrier", from regulators, standards, etc. We present and discuss a selection of these definitions.

The definition of "barrier" as suggested by PSA /4/ is:

Barrier:	*Technical, operational and organisational elements which are intended individually or collectively to reduce possibility for a specific error, hazard or accident to occur, or which limit its harm/disadvantages*

An objection to this definition has been that almost anything, such as maintenance, training and audits, can *reduce the possibility* for a specific error, hazard or accident to occur, hence implying a very wide definition of barriers. However, based on discussions in the "barrier memo" /4/, it is quite clear that PSA is concerned about a too broad definition of barriers; they do not want "everything" to be included as barriers (e.g. they make a clear distinction between barrier elements and performance influencing factors).

The ambiguity concerning how to interpret the extent of the barrier concept recurs when considering the Management Regulations, Section 4 (Risk reduction) and Section 5 (Barriers) /5/. Here it is stated (excerpt) – underlined by author:

Section 4
Risk reduction

In reducing risk as mentioned in Section 11 of the Framework Regulations, the responsible party shall select technical, operational and organisational solutions that reduce the likelihood that harm, errors and hazard and accident situations occur.

Furthermore, barriers as mentioned in Section 5 shall be established.

Section 5
Barriers

Barriers shall be established that at all times can

a) identify conditions that can lead to failures, hazard and accident situations,
b) reduce the possibility of failures, hazard and accident situations occurring and developing,
c) limit possible harm and inconveniences.

From Section 4 concerning risk reduction, we interpret that barriers shall be established in addition ("*furthermore*") to *"solutions that reduce the probability that harm, errors and hazard and accident situations occur"*. However, Section 5 point a) and b) can again be interpreted as giving a very wide barrier definition. Hence, Section 4 and Section 5 from the Management Regulations must be read in conjunction.

In the DNV GL / NSA report /7/, the following barrier definition is suggested:

Barrier:	*Barriers refer to measures established with an explicit purpose to (1) prevent a hazard from being realized, or (2) to mitigate the effects of a hazardous event*

This definition specifies that barriers shall prevent and mitigate hazardous events. With respect to the extent of the definition, it is more restrictive than the PSA definition, since it can be interpreted that it focuses on avoiding hazardous failures, not any failures. Still, it can be questioned how "far back" in the causal chain "prevent" shall be interpreted. In the report /7/, some examples of this are given.

Based on /1/, SINTEF proposes a more narrow definition:

Barrier:	*Planned measures to regain control, to mitigate development of situations of hazard and accident, or to mitigate consequences* *NOTE 1: Barriers come in addition to inherent safety and control measures, which shall prevent failures and loss of control* *NOTE 2: Detection measures to regain control is included*

This definition reserves the use of barriers to "abnormal" situations when some kind of deviation, failure or malfunction have already occurred. I.e., barriers are only needed after loss of control; first to regain control, second to mitigate further development, and third to mitigate (or limit) consequences. Prior to loss of control other measures are in place, i.e. inherent safety (inherent design solutions) and control measures[2].

The abnormal situations, after having lost control, will often correspond to the defined situations of hazard and accident (DSHAs) with major accident potential, since we are focusing on major accident hazards. The DSHAs are familiar for all personnel, which is useful when communicating about barrier management with operations personnel. Hence, barriers against major accidents are planned measures against already defined situations of hazard and accident.

Note that in order to regain control, detection of the abnormal situations will be required. Hence, detection of situations outside the normal operational envelope is included as part of the barrier definition. Examples will be gas detection, leak detection, detection of a well kick, detection of high-high pressure, detection of ship on collision course and detection of loss of stability. Early detection that is implemented to ensure operation within the normal operational envelope is considered a control measure (or a control barrier). Examples of this will be detection of high pressure in a vessel (by the process control system), detection of too low mud weight or detection of a stuck ballast control valve (that in combination with other failures can result in loss of stability).

2.2.3 Barrier function, sub-functions and safety critical tasks

As seen from the barrier definitions, a barrier is a planned measure implemented to prevent hazards and accidents or mitigate their consequences. Since a barrier is a planned measure, it also has a predefined purpose or role referred to as the *barrier function*. The following definition is given by PSA /4/:

Barrier function:	*The task or role of a barrier* *NOTE: Examples include preventing leaks or ignition, reducing fire loads, ensuring acceptable evacuation and preventing hearing damage*

A barrier function, such as "prevent HC leak" can be further broken down into sub-functions and possibly sub-sub functions. The sub-functions can be performed automatically by technical systems, and/or manually by personnel.

When the sub-functions (or sub-sub functions) are performed automatically by technical safety systems, they are often referred to as *safety functions*, or more specifically, if performed by safety instrumented systems (SIS) they are named *safety instrumented functions (SIFs)*.

When personnel perform or they are involved in realising the barrier sub-(or sub-sub) functions, these functions may be denoted *safety critical tasks*.

[2] Control measures (or just "controls") could alternatively be denoted "control barriers" as opposed to "safety barriers".

Figure 2.4 illustrates the relationship between the different terms for the barrier function "prevent HC leak".

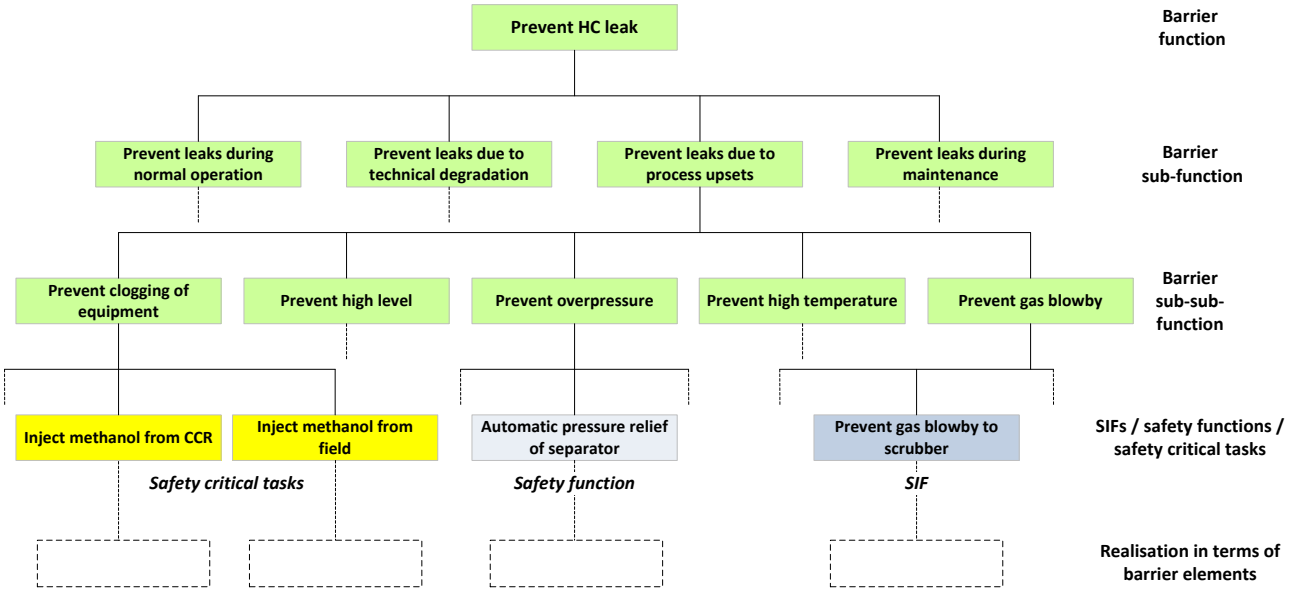


Figure 2.4 Types of barrier sub- (or sub-sub-) functions; safety critical tasks, safety functions and SIFs

In Figure 2.4, three types of barrier functions are illustrated; safety critical tasks, safety functions and SIFs, i.e., also safety critical tasks are functions.

It should be noted that barrier sub- and sub-sub-functions often depend on *both* personnel and technical systems to be realised. For example in Figure 2.4, the CCR operator must manually initiate methanol injection, but successful realisation also depends on proper function of a pushbutton on the operator display and chemical injection valves in the field.

2.2.4 Barrier element

Barrier elements are measures or solutions, which play a part in *realising* a barrier function (cf. Figure 2.4). PSA introduces three categories of barrier elements: Technical, operational and organisational (TO&O) barrier elements, and proposes the following definitions (/4/, /25/):

Barrier element:	*Technical, operational or organisational measures or solutions, which play a part in realising a barrier function*
Technical barrier element:	*Equipment and systems which constitute a part of realising a barrier function*
Operational barrier element:	*Actions and activities the personnel have to perform to constitute a part of realising a barrier function*
Organizational barrier element:	*Personnel with defined roles or functions and specific competence which constitute a part of realising a barrier function*

As seen from these definitions, PSA has chosen to define the safety critical tasks (actions) as the *operational barrier elements*, whereas the personnel who perform these tasks are defined as the *organizational barrier elements*.

Due to the interrelationship between the organizational and operational barrier elements, it is in the DNV GL / NSA report /7/, argued that it is not considered practical to apply both terms. Therefore, only the term operational barrier element is applied, represented by the safety critical tasks. The personnel performing these tasks (the organizational barrier elements in PSAs context) are captured through performance requirements for the operational barrier elements. As an example: the corrosion coupons shall be checked *by the inspection team* every 3rd month.

Statoil /26/ has chosen a similar approach. The *operational barrier elements* are defined as the "safety-critical tasks performed by a person, or team of personnel, which realizes one or several barrier functions", whereas the *organizational barrier elements* are not explicitly defined.

SINTEF proposes that the barrier definitions should highlight the logical relationship between

1. Function/task, i.e. what the barrier must do to prevent or mitigate an undesirable event sequence, and
2. Measures/solutions that play a part in realizing the barrier function

As seen from Figure 2.4, the safety critical tasks and the safety functions/SIFs result from a functional breakdown of the overall barrier function. They are sub-functions and at "the same level" in the functional breakdown. SINTEF proposes that the term barrier element should not include the sub-functions, but rather the measures and solutions required to implement these tasks and functions /1/.

Tasks and functions are implemented by technical equipment/systems and personnel. In some cases, personnel will depend on written or electronic aids to perform the safety critical tasks. When the written (or electronic) description of the safety critical task is required *there and then* to perform the task, SINTEF proposes to include it as an operational barrier element, since it is a necessary element to realize the barrier function.

Operational barrier element:	*The description of the actions or activities that must be carried out by the personnel in order to realise a barrier function* *NOTE: Only those procedures that are required there and then to perform the actions or activities are considered as barrier elements*

How the safety critical tasks should be manually realized is typically covered by operational procedures, checklists, instructions, manuals, handbooks, etc., describing how, when and under which circumstances/ conditions the organizational element (e.g. the operator) should act. This is a specific prerequisite for action, whether or not the procedure itself is a necessary aid during the realization of the barrier function. Those procedures etc. that are needed *during the realization* of the barrier function – and only those – are regarded as operational barrier elements. Examples of such safety critical procedures can be:

- Checklist applied during start-up of subsea wells to avoid overpressure in case of full «shut-in» pressure
- Use of communication protocol when preparing for launch of lifeboat (between lifeboat captain, emergency management team and standby vessel)
- Procedures for actions to take in case of ship on collision course
- Procedures for gas-freeing of ballast tanks upon gas detection in tank

This interpretation of operational barrier elements is also practical since the identification of specific operational procedures as barrier elements is a necessary and important part of preparation for operation. It has also been applied in practice in this way, referring to acute medical procedures, helideck manual, the emergency response plan, etc. as *operational measures or elements*, in emergency preparedness analyses.

Further, note that in this scheme, the safety critical tasks will result from the functional breakdown of the barrier functions and will typically appear through performance requirements for the organizational barrier elements. As an example: the inspection team shall *check the corrosion coupons* every 3rd month.

The *organizational barrier element* is constituted by the personnel (roles) directly involved in the realization of the safety critical tasks, e.g. the central control room (CCR) operator who manually activates blowdown or manually performs a production shutdown, the driller or mud logger who detects a kick, or the lifeboat captain who is responsible for evacuation with lifeboat. It also includes authorization to realize a barrier function.

The similarities and differences can be summarized in the following sequence of defining barrier elements:

1. Identify the barrier functions
2. Break down the barrier functions into barrier sub-functions (and sub-sub functions) including:
   a. Safety functions
   b. Safety instrumented functions
   c. Safety critical tasks (denoted operational barrier elements in the PSA and DNV/Statoil frameworks)
3. Identify and describe the technical equipment and systems required to realize the barrier sub-functions (denoted technical barrier elements in all the frameworks)
4. Identify and describe the personnel and roles responsible for performing the safety critical tasks (denoted organizational barrier elements in the PSA and the SINTEF frameworks)

In addition, we will also emphasize the importance of identifying the safety critical procedures that are required there and then when performing the safety critical tasks (denoted operational barrier element in the SINTEF framework).

2.2.5 Performance influencing factor (PIF)

The following definition has been provided by PSA /4/ for performance influencing factors:

Performance influencing factors:	*Conditions which are significant for the ability of barrier functions and elements to perform as intended*

Some examples of performance influencing factors are maintenance and testing, environmental conditions, training and exercises, competence, accessibility, document handling systems, management and safety culture.

Performance influencing factor is a collective term used about factors or conditions that influence the performance of both technical systems and humans. Often, the term performance shaping factors (PSFs) is used to denote factors with a significant influence on human performance. In /7/, the following definition is provided:

Performance shaping factors:	*Human, workplace or other contextual factors which have a significant effect on an operator's or crew of operator's performance*

3 Barrier management – overview

As stated in Section 1.1 (Scope), we distinguish mainly between the design phases (*establish barriers*) and the operations phase (*maintain and follow-up barriers*). In the design phases, the focus is on identifying and designing barriers to ensure that necessary risk reduction can be obtained during operation. This implies that it is necessary already in design to have a good understanding of the installation specific risk picture in order to be able to specify the required barriers. If major accident risks are neglected, overlooked or underestimated, the result may be that insufficient barriers are implemented in design. Guidance for barrier management in design is described in Chapter 4.

As part of design and engineering, it is important to prepare for the operations phase, including the development of information systems and tools that can be applied during operation to verify the performance as well as the status of the barrier elements. Such systems and tools are described in Chapter 5.

In the operations phase, the focus is to follow-up and maintain the barriers, to ensure that they are available at all time, and to implement compensating measures if barriers are impaired. Guidance for barrier management during operation is described in Chapter 6.

In this chapter, we provide a brief overview of barrier management (for more details see /1/). It includes:

1. Barrier management principles and framework
2. Barrier management process, including the development of a barrier strategy and performance requirements (standards)

This is illustrated in Figure 3.1.

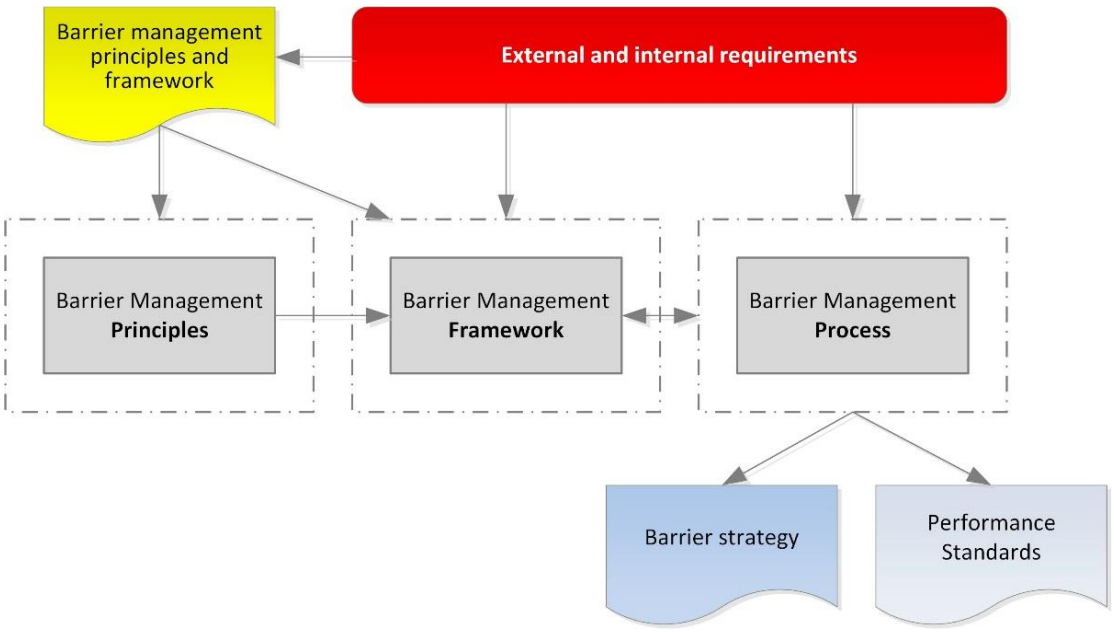


Figure 3.1 Barrier management overview

3.1 Barrier management principles and framework

Overall principles and framework for barrier management provide a foundation for establishing barrier management processes on specific installations or projects. It is recommended to have a document describing barrier management principles and framework at company level. It should include e.g.:

- References to the most important rules and regulations, codes, standards and guidelines relevant for barrier management
- Company internal documents and requirements that should be adhered to as part of the barrier management process
- Definitions and abbreviations related to barrier and barrier management that shall apply across the company (to ensure a common understanding)
- High level guiding principles for barrier management in various life cycle phases
- Description of the barrier management framework
- An outline of the barrier management process to be followed

For further details, see /1/.

3.2 Barrier management process

An overview of main barrier management activities in various life cycle phases is given in Table 3.1.

Table 3.1 Main barrier management activities in various life cycle phases

Early design	Detailed design	Operation
Prepare plan for barrier management	Update plan for barrier management	Prepare plan to assure barrier performance (update if necessary)
Define areas	Verify areas	Review area definition
Perform or review HAZID	Review refined HAZID	Update HAZID (e.g. during modifications)
Identify/define major hazards/DSHAs	Revise DSHAs	Review and update risk analyses and DSHAs
Perform barrier analysis	Refine barrier analysis	Update barrier analysis
Establish initial barrier strategy	Refine barrier strategy	Review and update barrier strategy
Establish initial performance standards	Refine performance standards	Review and update performance standards
	Establish system for monitoring of barrier status (e.g. barrier panel)	Monitor barrier status and consider need for compensating measures
	Establish systems and processes for follow-up of barrier performance	Monitor and verify barrier performance

The barrier strategy (document) is one of the outcomes of the barrier management process. We define barrier strategy as "*a result of a process which, on the basis of the risk picture, describes and clarifies the barrier functions and elements to be implemented in order to reduce risk*" (/1/, /4/).

The barrier strategy should typically include:

1. Introduction (objective, scope and structure of document)
2. Terminology, abbreviations and references

3. Methodology (including description of the barrier management process)
4. Description of the facility and area division
5. Description of DSHAs and barrier functions per area
6. Description of identified barrier elements in each area (or globally)
7. Description of performance requirements for barrier elements or references to requirements documented elsewhere (e.g. in Performance Standards)
8. Description of performance influencing factors (PIFs) affecting the barrier elements
9. Description of verification activities (and intervals) for monitoring of barrier performance

The main part of the detailed information referred to in point 6-9 above, including the detailed performance requirements, may be included in a separate document (denoted Performance Standards, Barrier Function Performance Standards, or something similar).

This is further elaborated in Chapter 4 (design phases) and Chapter 6 (operations phase).

4 Establish barriers – barrier management in design

The proposed barrier management process in design is illustrated in Figure 4.1.

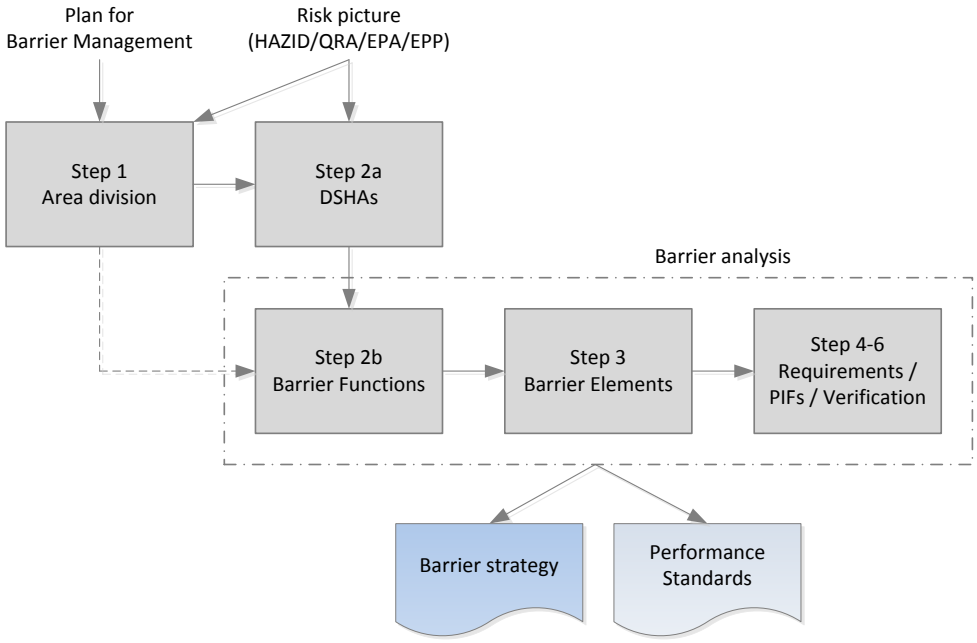


Figure 4.1 Main steps of the barrier management process

The main steps to establish a barrier strategy and corresponding performance standards include:

1. Facility description and area division
2. Defined Situations of Hazard and Accident (DSHAs) and barrier functions per area (based on the risk picture)
3. Barrier elements in each area (or globally)
4. Performance requirements
5. Performance influencing factors (PIFs)
6. Activities (and intervals) for verification of performance requirements

The installation specific risk picture provides a basis and a main input for these steps. This report does not go into detail on how to establish the risk picture. We refer to NORSOK Z-013 /17/ and ISO 17776 /22/ for further reading.

4.1 Facility description and area division (Step 1)

A short description of the facility should be provided. Since the barrier strategy needs to be area-specific addressing the specific needs (barriers against hazards/accidents) in each area of the facility /4/, a suitable division of the facility in areas should be defined.

The main criteria for area division in the barrier strategy should be the risk picture, i.e. the risk level within a defined area should not vary significantly. If the risk level, and hence the barrier elements, varies within an area, it should be considered split into several sub-areas when described in the barrier strategy.

For practical purposes, we recommend to limit the number of main areas. This to avoid a too comprehensive barrier management process and to reduce the extent of the barrier strategy document.

Typical "main areas" (on an offshore installation without drilling) are broad areas such as:

- Process area
- Riser area (and/or wellhead area)
- Utility area
- Living Quarter
- Shafts
- General functions

4.2 DSHAs and barrier functions per area (Step 2)

There is a close relationship between the major accident hazards identified and analyzed in the Quantitative Risk Analysis (QRA) and the Defined Situations of Hazard and Accident (DSHAs) identified and analyzed in the Emergency Preparedness Analysis (EPA) and in the Emergency Preparedness Plan (EPP). Since the Emergency Preparedness Plan is often the most familiar document for the personnel onboard the installation, the DSHA numbers and names from this document should preferably be used in the barrier strategy. These major accident hazards or DSHAs, which are part of the risk picture, should be reviewed at stages throughout the design phases.

Identification of the required barriers is an important part of effective barrier management and requires a comprehensive understanding of the risk picture related to the installation and/or the activity under consideration.

In a typical oil & gas development project, analysing and understanding the risk picture is not covered by one single activity, but by different types of analyses and project activities. Some of the most important ones typically include HAZID, QRA, HAZOP, Emergency Preparedness Analysis, various SIL/SIS analyses as well as different design reviews.

Although these analyses and activities are related to barriers and barrier identification, it seems like the industry has no single coordinated activity or analysis targeted towards systematic barrier identification and description. Rather, the barriers have naturally resulted from the use of NORSOK standards, API standards and standardised design. This particularly applies for technical barrier elements, whereas O&O barrier elements until recently has not been well defined, identified or analysed.

On this background, PSA has stressed the requirement for developing a facility specific barrier strategy /4/, i.e., a document that consistently, and on an area basis, describes the relationship between the hazards present in an area and the barriers needed to protect against these hazards. Hence, the purpose of the barrier strategy document is to describe a logical relationship between the barrier functions and barrier elements and the unique risk picture as described in safety and reliability studies from design and engineering.

When performing barrier identification, it is necessary to use a structured approach to ensure that all relevant barriers are covered, i.e. all required barrier elements are identified and described. This will typically start with a Hazard Identification (HAZID), where the relevant major accident hazards / DSHAs (with major accident potential) are identified (Step 2a).

The next step (Step 2b) is to identify and define the barrier functions that need to be in place to prevent and mitigate these hazards. Examples of typical major accident hazards and associated barrier functions for a floating offshore installation without drilling is shown in Table 4.1.

Table 4.1 Examples of typical major accident hazards and associated barrier functions

Major Accident Hazards / DSHAs	Associated barrier functions
Hydrocarbon (HC) leakage	Prevent HC leak from process equipment Prevent HC leak from risers and pipelines Prevent HC leak from cargo/slop tank Prevent HC leak during offloading operation Limit size of HC leak from process equipment Limit size of HC leak from risers and pipelines Limit Size of HC leak from cargo/slop tank Limit size of HC leak from offloading hose
Fire and explosion	Prevent ignition Prevent explosive or dangerous atmosphere in cargo/slop tank Prevent HC in ballast tank Prevent escalation to other equipment Prevent escalation to other area Prevent fatalities during escape / mustering Prevent fatalities during evacuation
Acute pollution	Prevent spill to sea Limit consequences of spill to sea
Dropped object	Prevent dropped objects from crane operations Limit consequences in case of dropped objects
Ship on collision course / drifting object	Prevent collision with passing or visiting vessel
Ship collision	Prepare evacuation due to vessel or drifting object on collision course
Loss of buoyancy / stability	Prevent loss of buoyancy/stability Regain buoyancy/stability
Loss of position	Prevent loss of position
Helicopter accident at installation	Prevent helicopter accident Prevent escalation from helicopter accident
Extreme weather	Ensure contingency in case of extreme weather forecast
Structural failure	Prevent loss of structural integrity Prevent fatalities upon loss of structural integrity
Non HC fire	Prevent non-HC fire Limit consequences from non-HC fires

Having identified the necessary barrier functions, the next step (Step 3) is to perform a detailed functional breakdown of each of these functions to identify which technical, operational and organisational barrier elements that are required to implement and realize each of the sub-functions. This is described in the next section.

4.3 Barrier systems and elements in each area (Step 3)

Figure 4.2 illustrates that each barrier function – which mitigates an occurred event or prevents a succeeding event – may be divided into a set of barrier sub-functions (at one or more levels), which in turn are realized through a combination of technical, operational and/or organizational barrier elements.

As illustrated in Figure 4.2, the *organizational barrier element* of a barrier function constitutes the personnel (roles) directly involved in the realisation of the function, and the *operational barrier element* is (in our scheme) the procedures etc. that are required there and then to perform the action.

When identifying barrier elements, we ask the question "What are the necessary technical, operational and organizational elements to realize the sub-function"?

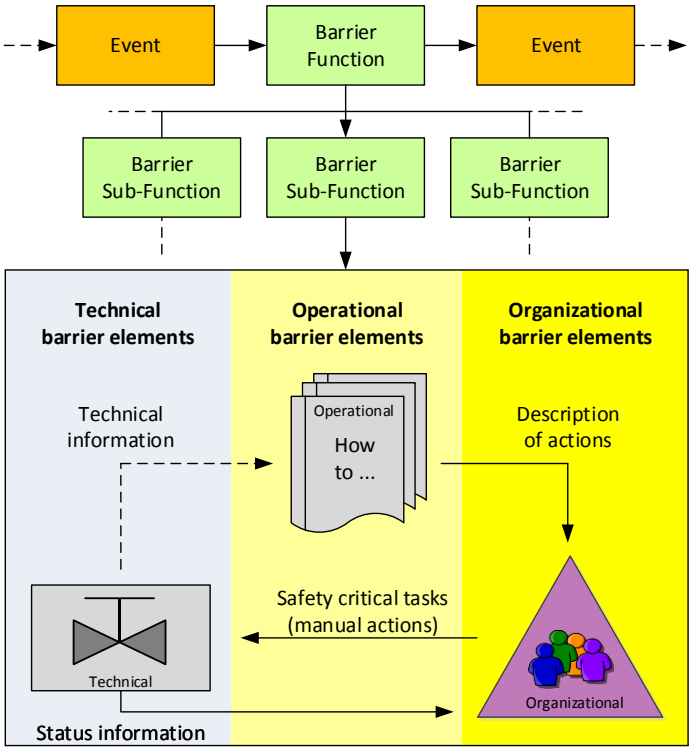


Figure 4.2 Barrier functions implemented through barrier elements

The main purpose of the functional breakdown is to clarify and communicate the role of the barrier elements realizing the barrier function. Example *breakdown structures* for the barrier functions "prevent HC leaks from process equipment", "prevent collision with visiting vessel" and "prevent fatalities during evacuation", are illustrated in Figure 4.3, 4.4, and 4.5, respectively.

An example of a *detailed functional breakdown* of the barrier function "prevent HC leak from process equipment" is shown in Figure 4.6.[3] This barrier function is broken down into sub-functions and ultimately safety critical tasks, safety functions and SIFs (cf. Figure 2.4). These tasks and functions are then realised in terms of technical, operational and organisational (TO&O) barrier elements.

Similarly can be done for all barriers functions, thus providing a good overview of the TO&O barrier elements that are required to realize the different barrier sub-functions.

In the following we will discuss the identification of TO&O barrier elements.

[3] This breakdown structure is largely based on work performed by Safetec in the Goliat barrier management project.

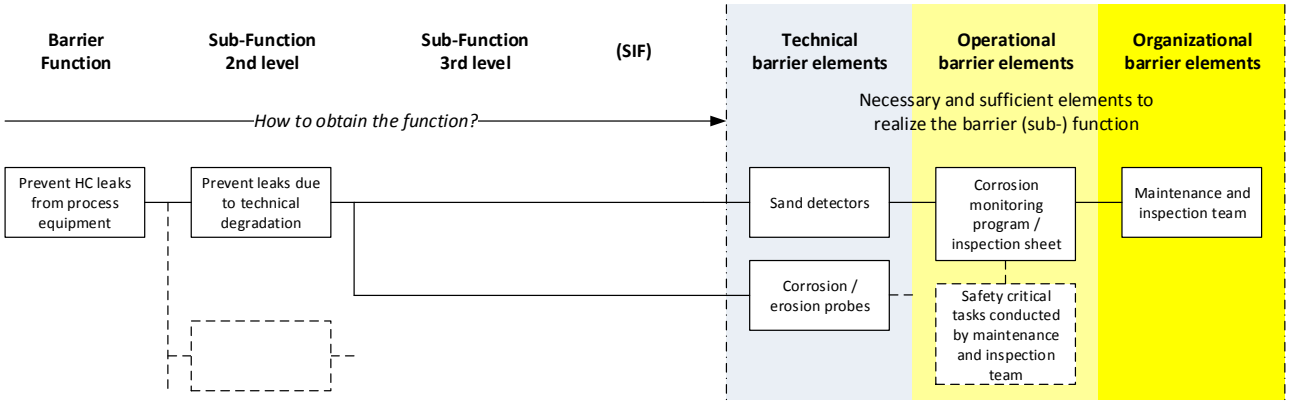


Figure 4.3 Breakdown structure for barrier function "prevent HC leaks" (example)

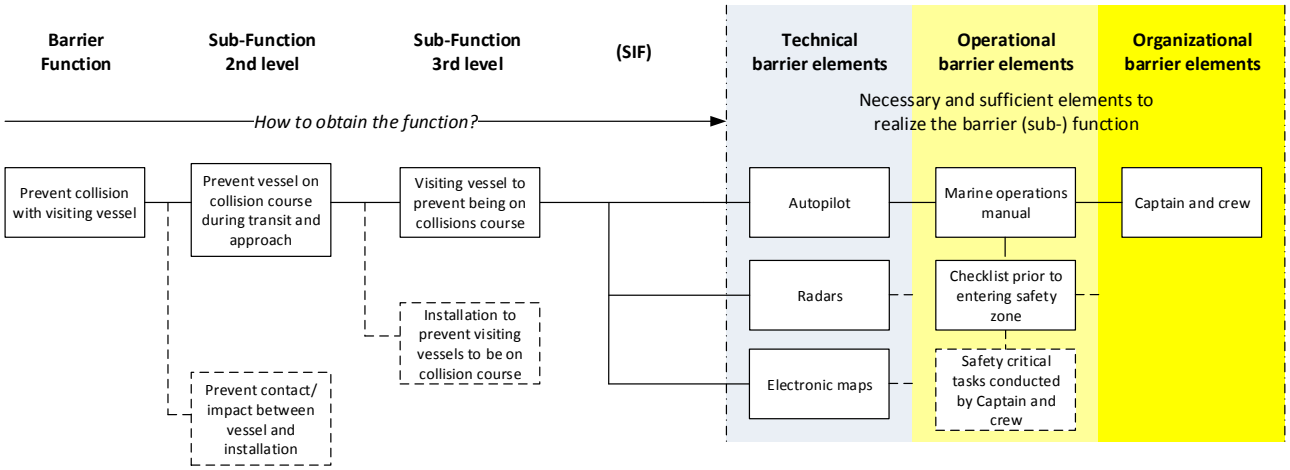


Figure 4.4 Breakdown structure for barrier function "prevent collision with visiting vessel" (example)

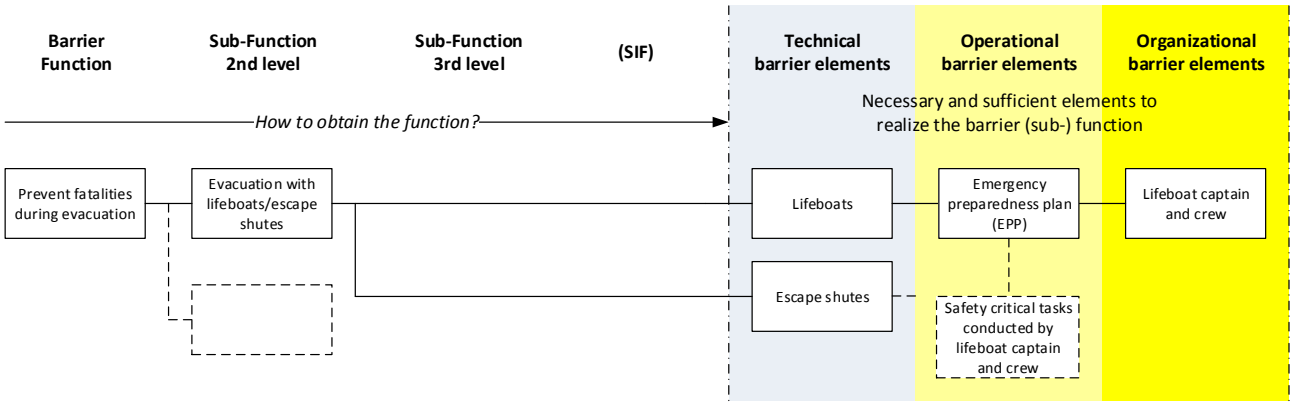


Figure 4.5 Breakdown structure for barrier function "prevent fatalities during evacuation" (example)

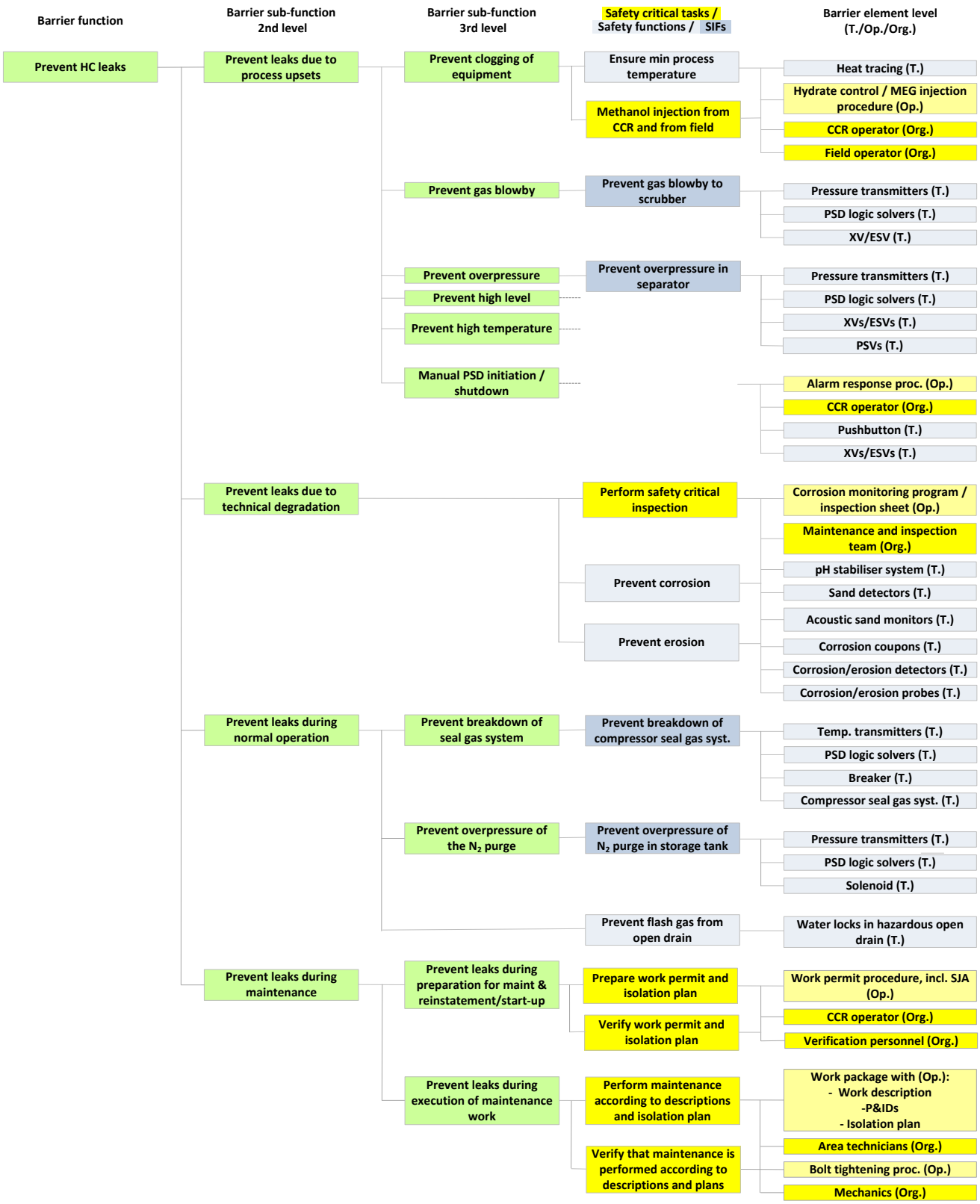


Figure 4.6 Detailed functional breakdown of BF "Prevent HC leak from process equipment" (example)

4.3.1 Technical barrier elements

Using standard engineering documentation, the identification of the technical barrier elements realizing a barrier sub-function is relatively straightforward, at least compared to the operational and organisational (O&O) barrier elements.

The functional breakdown is a top-down approach, and it must be made sure that all relevant barrier elements are captured. This is particularly true for the technical barrier elements, since there is typically an extensive amount of technical barrier elements required. (The amount of O&O barrier elements are quite limited compared to the technical barrier elements). The top-down approach should therefore be accompanied by a bottom-up verification approach. This could be a mapping against existing performance standards (from early phases), relevant NORSOK standards, or some logical model showing the relations between all barrier elements within a barrier function.

4.3.2 Organisational barrier elements

The functional breakdown ease the identification of the personnel (roles) that are responsible for performing certain safety critical tasks related to each barrier function and associated sub-functions. As it appears from Figure 4.3 – 4.6, identification of personnel/roles will depend on whether the task is part of normal operation or emergency response. Therefore, when identifying the organizational barrier elements, it is beneficial to distinguish between the normal operational organization and the emergency response organization, e.g. whether it is the field operator (normal operation role) or the lifeboat captain (emergency role) that is responsible for a given task.

Most of the barrier functions are either part of normal operation (to prevent a deviation/event to occur), or part of emergency response. However, some of the barrier functions may be initiated during normal operation, and then continue to be ensured after the organization has changed to an emergency response organization. E.g., ship on collision course is identified during normal operation, but follow-up is done by the emergency response organization, if the situation threatens the installation. Similarly, an extreme weather forecast during normal operation will be followed-up after confirmation of extreme weather by establishment ("scrambling") of the emergency response organization.

When performing a functional breakdown as discussed above, it is typically found that a few roles are responsible for several safety critical tasks. CCR operators in particular are involved in realising many barrier functions, but also other operational personnel such as maintenance and inspection personnel, area technicians / field operators will typically have many tasks. This, of course, depends on how the organisation is structured.

It is often sharp end personnel, responsible for the *realization* of the barrier functions, who are identified when performing a functional breakdown as described above. Blunt end personnel can also be involved in realisation of barrier functions, e.g. the operation & maintenance manager will typically verify isolation plans prior to isolation and opening of process equipment (cf. Figure 4.6). Nevertheless, blunt end and support personnel are to a larger degree responsible for the conditions or factors that will affect the performance of the barrier functions (i.e. the PIFs). This includes e.g. competence management, writing of procedures, developing work practices, planning the work packages, etc., which is an argument for also setting performance requirements to the PIFs (see discussion in Section 4.4).

Similar as for the technical elements, organizational barrier elements can be included in some logical model to ensure that all relevant elements have been identified[4]. In addition, the emergency roles can be checked by reviewing e.g. the emergency preparedness plan.

4.3.3 Operational barrier elements

Within our proposed framework the operational barrier elements are defined as the safety critical *procedures* (including checklists, instructions, diagrams, etc.), which provide necessary aids in performing a safety critical task[5].

It should be noted that there may be safety critical tasks, which are performed without any other direct aid than knowledge and experience (e.g. pushing a button), i.e. it is carried out without any explicit descriptions. Thus, for these sub-functions, there will not be any associated operational elements.

The variation of descriptions (safety critical procedures) in terms of providing aid is large. It may therefore be beneficial to distinguish between different categories when reviewing the safety critical procedures. A possible categorization scheme is shown in Table 4.2.

As discussed in Section 2.2.4, PSA and some companies have chosen to define the operational barrier elements as safety critical tasks (sub-function). SINTEF has however chosen to highlight the difference between a barrier function and barrier element by stressing that a barrier element is not a task, but a measure for realizing a task (cf. e.g. Figure 2.4 and Figure 4.6).

Table 4.2 Possible categorization of safety critical procedures

Category	Description
1	Procedure, process, etc. critical for the activation of a barrier function *after the occurrence of a failure or event* (i.e. *time critical*), which needs to be available at the time of activation. This may be a specific sequence or a series of steps, which is not reasonable to memorize, or possible to perform only based on competence and experience.
2	Procedure, process, etc. important in order to *prevent a failure or initiating event to occur* in the first place. It needs to be available; however, it is *not time critical*. This may be a specific sequence or a series of steps, which is not reasonable to memorize, or possible to perform only based on competence and experience.
3	Procedure, process, etc. being a potential aid in preventing or limiting the consequences of failures/events; however the procedure/checklist or similar is not strictly required to be available to realize the barrier function; the actions can be performed only based on competence and experience.
4	Reference document describing required actions (what to do and/or how to perform them), but not foreseen as an aid during the activation of a barrier function.
5	Procedure, process, reference document or similar is missing (or it has not yet been finally categorized).

Only the two first categories are considered as operational barrier elements, since it can be argued that they are needed "there and then" in order to activate a barrier. These are the operational barrier elements, for which performance requirements should be established and followed-up (see Step 4 in the next section).

[4] Using the top-down function analysis approach (as illustrated in Figures 4.3-4.6), it is possible to overlook some relevant sub-functions. Thus, a separate verification method should be used to ensure completeness.

[5] The information aids will often be in the form of procedures, and we use "safety critical procedures" as a general term. Operational barrier elements are only those safety critical procedures needed when performing a barrier task ("there and then").

4.4 Performance requirements (Step 4)

According to PSA Management Regulations, Section 5 /5/ performance requirements shall be developed for the technical, operational and organizational barrier elements. Two examples of performance requirements for the TO&O barrier elements are given in Figure 4.7 and 4.8. Note that the safety critical tasks appear as performance requirements to the operational personnel, i.e. the organizational barrier elements (and not as an operational barrier element). I.e., the required performance of safety critical tasks are ensured by (and measured through) the personnel (organizational barrier elements).

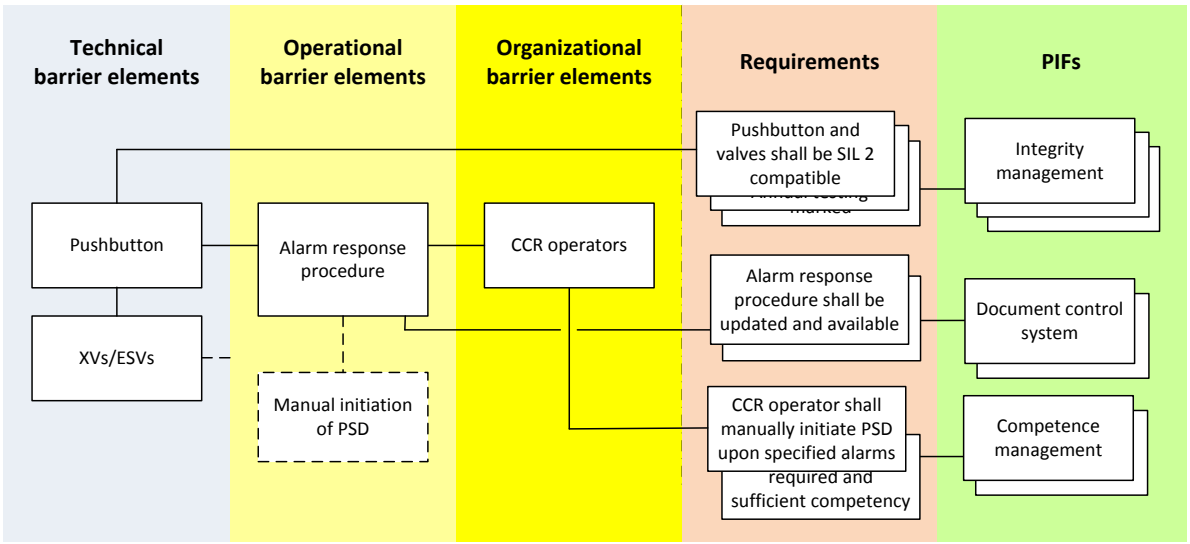


Figure 4.7 Performance requirements for TO&O barrier elements – example with PSD initiation

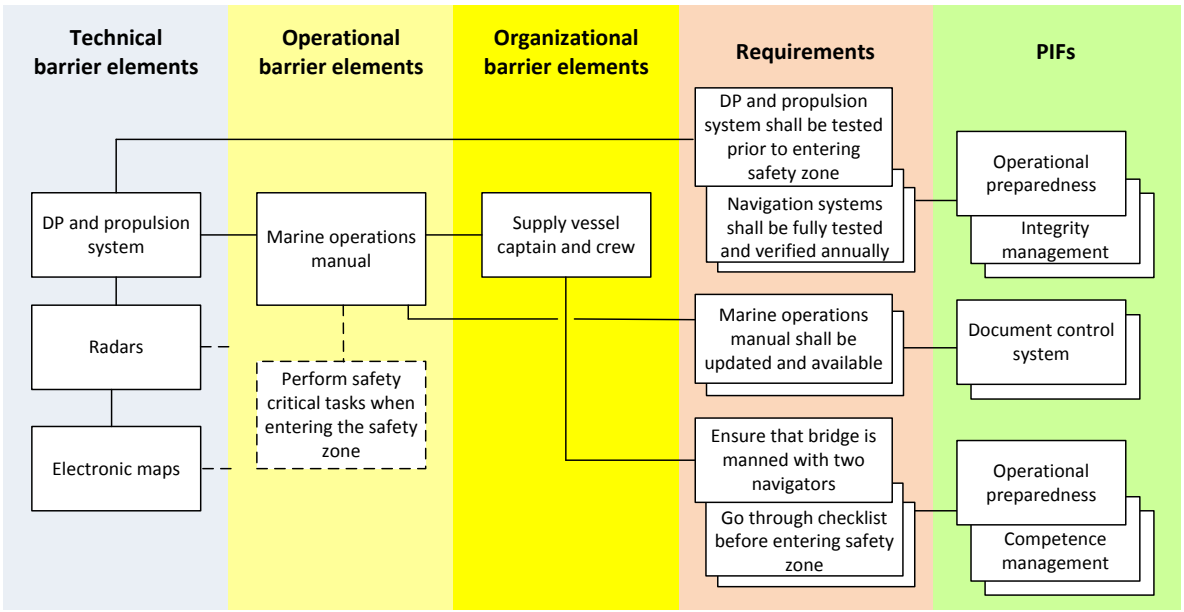


Figure 4.8 Performance requirements for TO&O barrier elements – example with prevent collision

Performance requirements should reflect the facility specific risk picture, e.g. required response times, manning requirements and required fire and explosion load resistance. Performance requirements for technical barrier elements are derived from regulations, standards and guidelines, company specific requirement documents, as well as relevant project documentation. Whereas there are a large number of requirements defined for the technical barriers/-elements, the situation for O&O barriers/-elements is often the opposite. This is a challenge, since verifiable performance requirements need to be established for all barrier elements /1/. Although performance requirements are mainly developed "directly" for the barrier elements themselves, it may be relevant, especially for O&O elements, also to develop "indirect" performance requirements, i.e. performance requirements for the PIFs, instead of, or in addition to, the barrier elements.

Relevant types of performance requirements

The Management Regulations, Section 5 Barriers, states in the fourth subsection /5/:

"Personnel shall be aware of what barriers have been established and which function they are intended to fulfil, as well as what performance requirements have been defined in respect of the concrete technical, operational or organisational barrier elements necessary for the individual barrier to be effective."

It is further stated in the guidelines regarding the management regulations, Re Section 5 Barriers /5/[6]:

"Performance as mentioned in the fourth subsection, means verifiable requirements to, inter alia, capacity, reliability, accessibility, efficiency, ability to withstand loads, integrity and robustness."

In the "Barrier memo" /4/, PSA has provided the following definition of performance requirements:

"Verifiable requirements related to barrier element properties to ensure that the barrier is effective. They can include such aspects as capacity, functionality, effectiveness, integrity, reliability, availability, ability to withstand loads, robustness, expertise and mobilisation time."

Thus, they have added functionality, availability, expertise, and mobilization time to the definition in the regulations.

Finally, we include the following discussion from the "Barrier memo" /4/:

"Performance requirements related to the specific operational and organisational barrier elements could include specific stipulations for expertise in doing the work as well as criteria for action, response time, notification to the central control room, number of personnel and availability. Such requirements for technical, operational and organisational barrier elements may often display the same characteristics – capacity, functionality, effectiveness, integrity, robustness and availability, for example. ... Personnel, for example, could be required to have taken a specific course in order to secure correct performance of a job required to realise a barrier function."

Thus, in the "Barrier memo" PSA have added requirements with respect to criteria for action, response time, notification to the CCR, number of personnel and specific courses to the previously mentioned types of requirements.

[6] Underlining is inserted to highlight the types of performance requirements (properties) referred to by PSA. Underlining in subsequent paragraphs are restricted to additional types of requirements, not mentioned earlier.

In summary, the following types of performance requirements (properties) may be relevant for TO&O barrier elements, according to PSA:

- Functionality
- Capacity
- Effectiveness
- Reliability
- Availability
- Integrity
- Ability to withstand loads
- Robustness
- Accessibility
- Expertise
- Mobilization time
- Criteria for action
- Response time
- Notification to the CCR
- Number of personnel
- Specific courses

The structuring of the performance requirements is not straightforward; it can be done in various ways. In the "Barrier memo" /4/, and in /20/, some of the main types of performance requirements have been grouped in three main properties, i.e. functionality, integrity and survivability. This is illustrated in Figure 4.9.

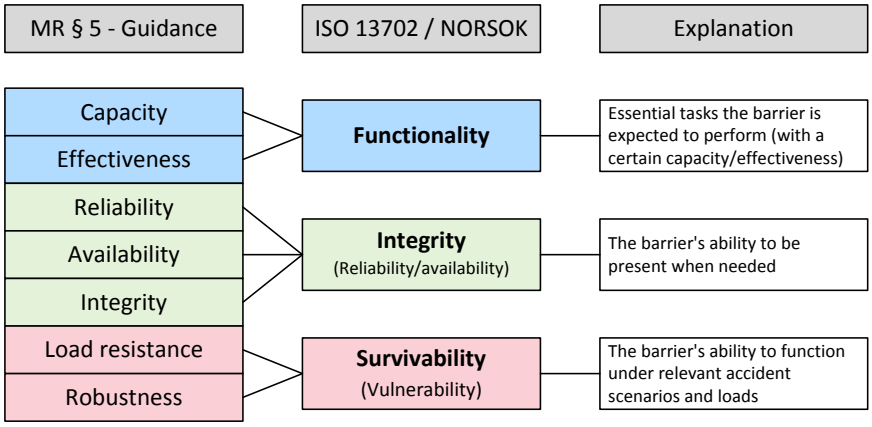


Figure 4.9 Relations between types of performance requirements (adapted from /4/)

These three main properties are most relevant for technical barrier elements, but may also be interpreted in an O&O barrier element context. An attempt of doing this for the above list of performance requirements is summarized in Table 4.3.

As seen from the table, most types of requirements (properties) are found relevant for the organizational barrier elements, but just a few for the operational barrier elements.

There may be some different views about how to interpret, or "translate", technical types of performance requirements into O&O types of performance requirements, and how comprehensive this "translation" should be. We have performed an assessment and a subjective screening of what we consider as the most relevant O&O types of performance requirements (properties).

The main purpose of this list (Table 4.3) is to use it as a checklist, by asking questions such as:

- Do any *criteria for action* constitute a relevant performance requirement for the personnel/role performing this task/sub-function?
- Are there *specific competence/courses* that are required/mandatory for the personnel/role performing this task/sub-function?
- Are there *specific roles* that require a certain number of personnel and/or substitutes?

Table 4.3 Assessment of relevance and grouping of O&O performance requirements

Type of requirement	Organizational	Operational
Functionality	Specified through capacity and effectiveness, e.g. response time	-
Capacity	(Certain roles are "heavy duty" such as number of deck operators during heavy lifting and number of bridge officers during supply ship approach)	-
Effectiveness	See response time	-
Reliability	(May be relevant with respect to reliability of performing certain tasks)	Correctness/updating of procedures
Availability	E.g. having available substitutes for all emergency response functions	Availability of procedures
Integrity	May be related to fatigue/overtime and the ability of personnel to perform safety critical tasks over time	(E.g. lamination of procedures to increase the durability)
Ability to withstand loads	(Substitute in case of incapacitation. See also capacity and availability)	-
Robustness	(Certain roles are "heavy duty". See also capacity and integrity)	(For certain procedures, it may be relevant to set requirements concerning their robustness related to e.g. various operational conditions or varying personnel)
Accessibility	(See availability)	Use of passwords to obtain access to written documentation is an issue. See also availability of procedures
Expertise	Specific competence, including specific courses	-
Mobilization time	Often similar to response time. Specific type of response time	-
Criteria for action	E.g. shutdown or abortion of actions at certain weather criteria, e.g. maximum wave heights	-
Response time	Relevant for certain safety critical tasks such as e.g. "activation of manual ESD within 2 minutes"	-
Notification to CCR	This is included as actions	-
Number of personnel	Related to availability of personnel, e.g. number of persons in CCR during certain situations	-
Specific courses	Related to expertise and may include requirements to certain mandatory courses, e.g. flange assembling course	-

(Text in parenthesis indicated that the requirement may in theory be relevant), '-' = Not relevant

In Figure 4.10, we have provided an overview of types of performance requirements (with brief explanations) for the technical, organizational and operational barrier elements. It may be additional types of performance requirements missing from the list in Table 4.3, especially for the O&O barrier elements.

Therefore, in Figure 4.10 we have added an additional type of "other requirements", to capture any specific requirements that are not included in the properties presented above.

Note that the requirements related to availability and integrity for organizational barrier elements may not be relevant to treat for each individual action, or each individual actor. It may be more suitable to consider the entire workforce/shift, e.g. whether the emergency response organization fill all the roles and has required substitutes/backup available.

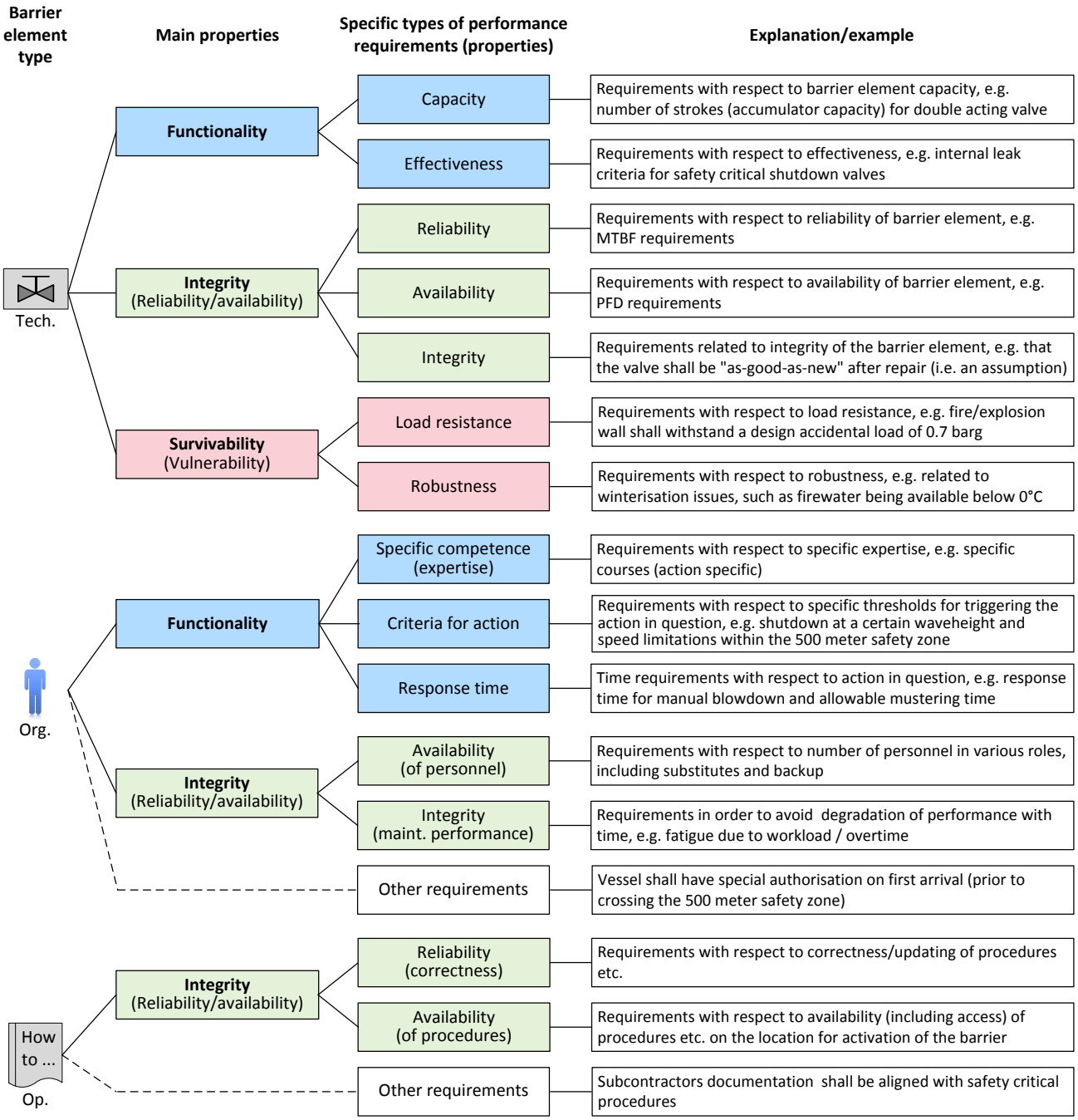


Figure 4.10 Types of performance requirements relevant for TO&O barrier elements

4.5 Performance influencing factors (Step 5)

Establishing performance requirements (Step 4) is closely linked to the identification of performance influencing factors (PIFs) (Step 5) – since we may indirectly establish performance requirements on the PIFs, instead of, or in addition to, the direct performance requirements on the elements.

Performance influencing factors (PIFs) are defined as conditions, which are significant for the ability of barrier functions and elements to perform as intended /4/, cf. section 2.2.5 and Figure 4.7 and 4.8. Typical relevant PIFs for O&O barrier elements are:

- Generic competence
- Training and exercises
- Experience
- Staffing and workload
- Document control
- Working conditions incl. environmental conditions
- Other PIFs (related to other relevant requirements for the specific actions in question)

According to PSA, the establishment of performance requirements is only strictly required for the barrier elements, not the PIFs. The PIFs must be followed-up, but not necessarily against any performance criteria. They are mainly relevant as indirect measures of the status of the barrier elements, in lack of direct measures.

This means that we should include additional PIFs to the extent necessary to ensure the performance of the barrier elements, focusing on the most important PIFs. The potential number of PIFs is large; however, the aim here is not to cover as many PIFs as possible. The aim is to identify a manageable number of important factors for which indicators can be developed and used as indirect measures of the status of the barrier elements. It is recommended not to make the list of PIFs too comprehensive.

In addition, many of the PIFs are managed regularly through various other management systems, and may not need to be included as a dedicated part of the barrier management system.

If it is desired to implement a more extensive and unifying approach to the management and follow-up of factors affecting the O&O barrier elements, one such approach is the Operational Condition Safety (OCS) verification scheme /14/. This scheme includes PIFs such as:

- Work practice
- Workload and physical working environment
- Communication
- Management
- Management of change

Task complexity, HMI, and Teamwork are additional examples of PIFs for which performance requirements may be considered developed and followed-up.

In order to assess the status and integrity of performance influencing factors, different human reliability assessment (HRA) and human factors (HF) methods may be applied (e.g. /23/ and /24/). Such methods may also be useful when identifying barrier elements, when assessing their vulnerability to human errors and when considering measures to improve human performance.

Safety critical task analysis (SCTA) is a technique highlighted by both DNV GL /7/ and Statoil /26/. In a task analysis, the main task, e.g. "prevent HC leak during pump maintenance", is further broken down into sub-tasks, e.g. "prevent leak during preparation for pump maintenance" and "prevent leak during execution of pump maintenance". Each sub-task (or safety critical task) is made subject to assessment in terms of what can go wrong (human errors), how likely it is to go wrong (human reliability analysis) and what conditions, or PIFs will influence the human reliability. Such analyses can be performed as part of project development and risk analyses, and they will provide information needed to define performance requirements and identify critical performance-influencing factors[7].

4.6 Verification of performance requirements (Step 6)

Verification of performance requirements (either direct performance requirements for the barrier elements or indirect through performance influencing factors), should be carried out efficiently, utilizing existing information systems to the extent possible. Verification activities and intervals should be planned for and described during the design phase. The actual verification will however take place during operations and the verification activities are therefore further described in Chapter 6 (barrier management in operation).

Dedicated supporting systems and tools need to be developed both for monitoring of the present barrier status and for longer-term verification of fulfilment of performance requirements. Such supporting systems and tools should be developed in the design phase, to be ready for operation, and are presented in a separate chapter – Chapter 5.

[7] Further guidance for safety critical task analysis can be found in http://www.energyinst.org/scta. See also /28/

5 Supporting systems and tools for barrier management and verification

Having identified the TO&O barrier elements, and defined the associated performance requirements and verification activities, it is important to prepare for the operations phase, including the development of information systems and tools that can be applied during operation. Such systems and tools should be developed during the design and engineering phase in order to ensure readiness for operation.

During operations, we can have both short-term and long-term perspectives for the follow-up of barriers.

We may distinguish between three types of information needed:

1. Information to display the current status of barrier elements
2. Information to verify the performance requirements, through indicator measurements
3. Information to verify the performance requirements, through inspection and audits

The first is related to the requirement of being aware of which barriers and barrier elements are not functioning or have been impaired (Management Regulations, Section 5, fifth subsection /5/).

The last two are related to the requirement of being aware of what performance requirements have been defined in respect of the barrier elements (Management Regulations, Section 5, forth subsection /5/) and to verify these requirements.

This distinction is useful, because the status of a barrier element with respect to performance requirements (type 2 and 3), and the status of the barrier element at a given point in time (type 1), are two different things.

For technical equipment, we typically have reliability requirements, such as failure to open the blowdown valve that must be compliant with a SIL 2 requirement (e.g. probability of failure on demand (PFD) < 0.005 for a single valve). We perform function tests and we may also record the results from all planned/unplanned valve operations, but we will need to perform such tests and activations over a quite long period (for the entire comparable blowdown valve population) to see if we meet the PFD requirement. Moreover, the result from the last test or activation does not necessarily tell us anything about the status of the blowdown valve *right now*[8].

Similarly, the status right now of the O&O barrier elements are not necessarily related to the status with respect to the performance requirements. E.g., we may require a certain response time to alarm a ship on collision course or to perform manual blowdown, and we may test this during exercises, drills and simulations, but from this information, we cannot conclude on the status *right now*. The present status is related to e.g. missing, sick or otherwise incapacitated personnel ("known failures"), overdue exercises and drills, or missing courses/competence, increasing the probability of not meeting the response time requirement.

Thus, different types of information is needed, providing information on different time-scales: short-term, medium-term and long-term.

[8] It is however advantageous to consider what has happened in the recent past pointing to potential issues or uncertainty about the condition of a barrier element. For example, if a shutdown valve failed during the last activation, was re-tested and functioning, but has not been operated for a while, there may be some additional degree of uncertainty concerning the valve status. Hence, knowledge about the recent history may influence the confidence concerning whether a barrier element will operate successfully upon the next demand.

This is illustrated in Figure 5.1. Instantaneous information from e.g. the safety and automation system (SAS), information management system (IMS) and condition monitoring system may also be utilized as additional short-term information sources, as well as on-line (instantaneous) information.

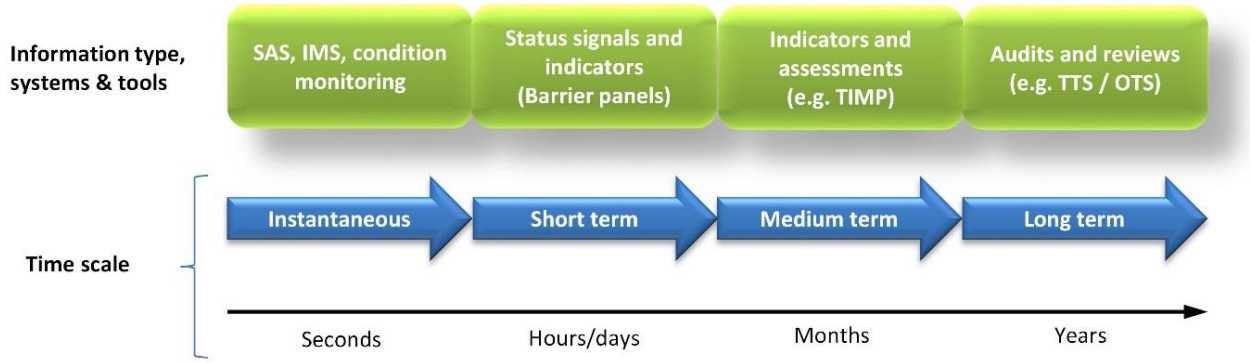


Figure 5.1 Information type, systems and tools during operation

Short-term information
This is information about the "immediate" status (here and now) of the barrier elements. Some of this information, e.g. from SAS, is typically displayed on operator stations in the CCR, and a selection of such information together with information from e.g. the maintenance management system may also be displayed in a barrier status panel (sometimes referred to as a "barrier status dashboard"). In addition to status information on technical barrier elements, it may be relevant to display online available information about O&O barrier elements. This is further discussed in Section 5.1.

Medium-term information
This is status information about the barrier elements obtained through indicator measurements and through periodic verification activities that are conducted on a quite frequent basis, e.g. monthly or bi-monthly. Results from recent tests or activations of technical barrier elements will be examples of indicators in this category. These indicators concern the recent history of the barrier elements, and provide additional knowledge when assessing the status of these elements.

An example of a system based on periodic assessment of medium-term information is Statoil's Technical Integrity Management Project (TIMP), which is further discussed in Section 5.2.

Long-term information
Long-term information is provided by audit and review type of information. For technical information, verification schemes such as Statoil's Technical Condition Safety (TCS; Norw: "Teknisk Tilstand Sikkerhet" – TTS) has been developed. The O&O counterpart is Operational Condition Safety (OCS; Norw: "Operasjonell Tilstand Sikkerhet" – OTS). This is further discussed in Section 5.3.

5.1 Short-term monitoring – Barrier status panel (BSP)

There are no explicit requirements in the PSA regulations to establish a barrier status panel (BSP). On the other hand, the regulations, e.g. the Management Regulations, Section 5 Barriers, states in the fifth subsection /5/:

"Personnel shall be aware of which barriers are not functioning or have been impaired."

The development of a BSP may be considered as a practical way of responding to this requirement. A BSP should display status information about the barrier elements. It can also include drill down functionality to provide the operators with more details about specific barrier elements and tags (e.g. more detailed information about present status and about recent history).

Several installations on the Norwegian continental shelf have developed such barrier panels (or dashboards), which provide status information about the barriers. However, the information presented and the frequency of updating of the information (how up-to-date it is), differ.

Figure 5.2 shows the intro page of the barrier status panel at Goliat FPSO. This BSP will initially monitor technical barrier elements, but it will be extended to include also operational and organizational barrier elements.

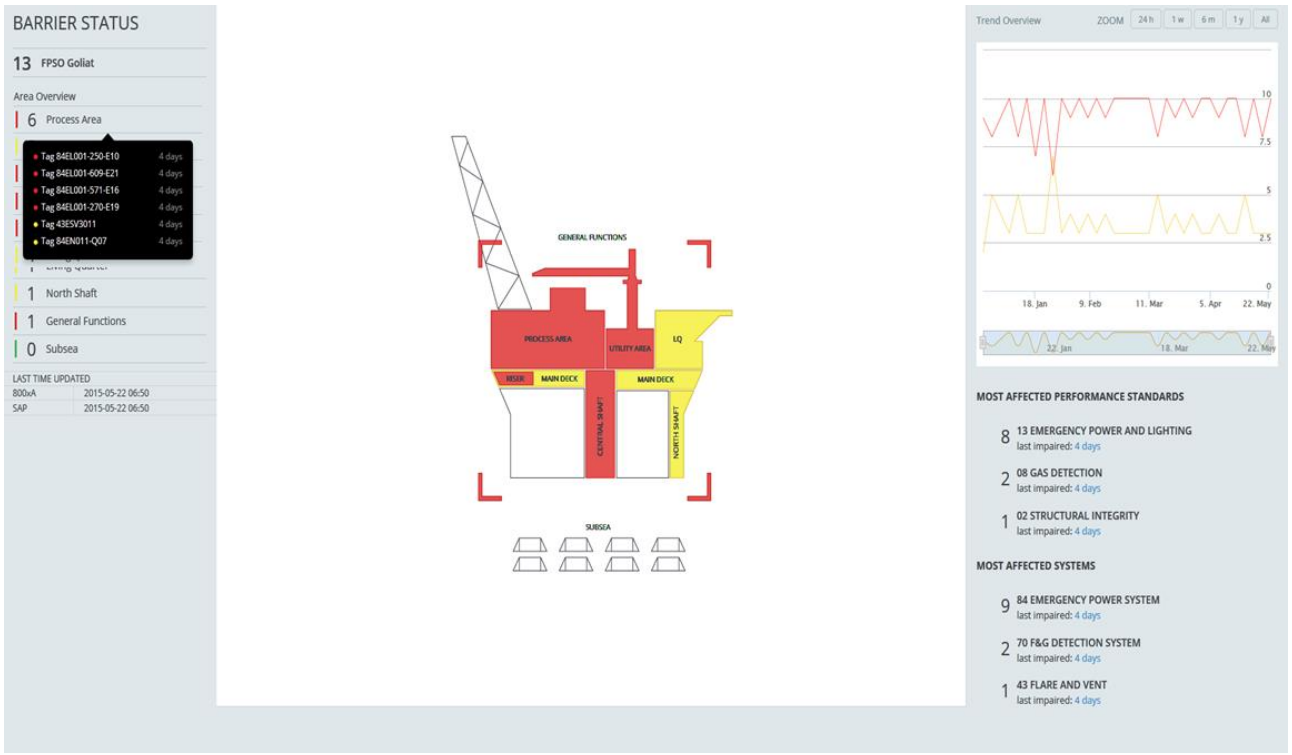


Figure 5.2 Intro page of barrier status panel (BSP) at Goliat FPSO

In this barrier panel, it is possible to drill down to areas, systems, performance standards and barrier functions and get an overview of the failed or degraded tags in the respective area, system, etc. All tags considered as safety critical (i.e. part of a barrier element) are included in the panel and the status of each tag is – at any time – set as either green, yellow or red based on a number of indicators. The selected indicators are automatically collected from different on-line systems, through the BSP interface, and they include:

- Condition monitoring alarms with a certain criticality, indicating a failed or degraded tag
- Safety fault alarms from SAS, indicating a failed or degraded tag
- Signal from SAS of a manually blocked/inhibited or suppressed tag, indicating a disabled tag
- Open or overdue corrective maintenance (CM) on high (or medium) priority work orders, indicating a failed (or degraded) tag

- Delayed preventive maintenance (PM) / testing, indicating increased uncertainty as to whether the tag is functioning

In addition, some operators have chosen to include the result from the last test or activation of the barrier element to provide additional information about the recent history of the elements.

Based on these status indicators, basic rules for setting the traffic lights on a (technical) tag level can be defined, and the tags that are failed or degraded are then displayed in different presentations or "views" as illustrated in Figure 5.3 (here showing the "barrier function view").

Figure 5.3 Example of presentation of failed or degraded tags in BSP ("barrier function view")

In Figure 5.3, the status of each tag and associated barrier function (and sub-function) is shown in terms of a yellow or red light (green tags supressed). Hence, there is an underlying logic or algorithm, which aggregates all underlying tags up to sub-function and function level. Such an algorithm can be very simple, e.g. saying that any yellow or red tag gives the same status on all higher levels, i.e. aggregated status information is just based on the worst status on a lower level. Alternatively, the algorithm can be made more risk based by e.g. allocating a predefined risk criticality to each tag and letting this criticality be part of the aggregation rules.

The BSP is a decision support and risk-communication tool both for operational personnel offshore and onshore support personnel. Some main objectives of installing a barrier status panel are:

- To provide all users with up-to-date readily accessible information regarding the barriers' health status, and thereby important information about the current risk picture
- To provide operational personnel with relevant information during planning and preparation for maintenance activities, e.g. to give an overview of barriers that are unavailable or degraded in a certain area
- To provide maintenance personnel with overviews of degraded and failed barrier elements to assist in prioritizing maintenance tasks

- To show trends on how the status of the barriers develop over time, which provide information about e.g. the need to consider modifications regarding the equipment itself or its use and/or maintenance

Some challenges related to barrier panels include:

- *Design and functionality of interfaces*; the BSP will typically collect information from a number of systems. The harvesting of data should be automatic, which requires design and preparation of dedicated interfaces with the source systems. The establishment of necessary interfaces is sometimes challenging, both technically and administratively
- *Data quality*; the information presented in the BSP is obtained from a number of systems, and the quality of the presented information will never be better than the quality of the input, e.g. the quality of notifications in the computerized maintenance management system (CMMS) impacts the quality of the information presented in the BSP
- *Keeping the BSP up-to-date*; design changes and modifications will take place during the operations phase and must be reflected and updated in the underlying structure of the BSP and associated supporting information systems/tools

In general, any concerns from the users of the BSP (whether related to coverage and correctness of input data, aggregation and presentation issues, or user interface, etc.) should be acted on promptly. If not, the users will soon distrust the BSP and may consequently avoid using it.

5.2 Medium-term verification and follow-up – TIMP

A BSP will capture changes to the status of individual barrier elements from day to day, but it will only to a limited degree incorporate detailed development over time (beyond trend graphs), or knowledge held by the personnel responsible for the systems.

To compensate for this, verification systems have been developed to capture threats to the barriers that may gradually develop over some time and to present barrier status information in a more medium-term perspective (e.g. monthly or bi-monthly). One example of this is Statoil's Technical Integrity Management Programme (TIMP) /9/:

"*The purpose of this program is to establish a holistic and standardized approach on risk of failures. By connecting tools, competence and people to a best practice work process, we can evaluate risk and, when necessary, initiate risk reducing actions in order to achieve a desired risk level.*" /5/.

TIMP makes use of relevant data (or indicators) for technical barriers, including notifications from the maintenance system, backlog of PM and CM, test reports, inspection reports, incident reports, TTS findings (see Section 5.3) and dispensations /5/, as illustrated in Figure 5.4.

The data or indicators are collected and presented in the TIMP portal and manually assessed by technical experts such as system responsible personnel. Based on the status of the input data (indicators) and the subjective judgements by the experts, the barrier performance is evaluated on an equipment, system, PS (performance standard) and plant level. The results (in terms of a mark/score per performance standard) are presented in a generic bow-tie diagram, as illustrated in Figure 5.5.

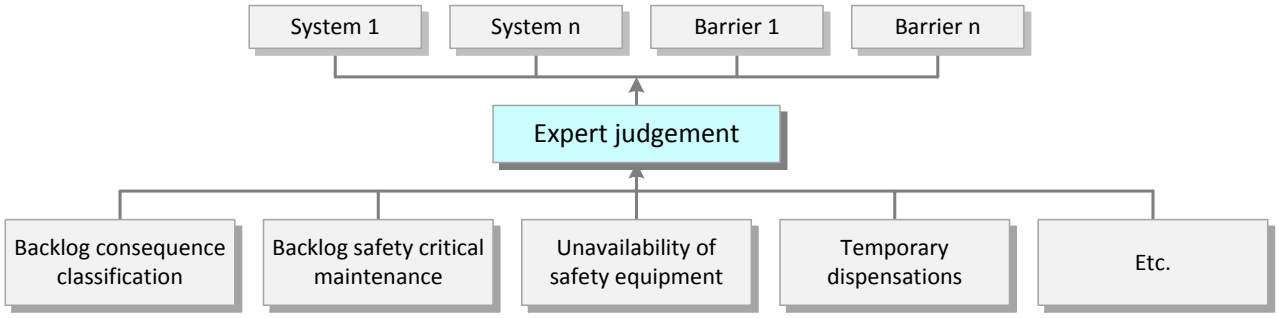


Figure 5.4 Manual/expert assessment of status of equipment, systems and barriers (/9/)

Figure 5.5 Statoil's TIMP visualization of technical barrier status (/9/)

A TIMP evaluation is typically updated on a monthly or bi-monthly basis (i.e. a medium-term perspective). In /5/, the following advantages of introducing TIMP have been pointed out:

- Increased understanding and awareness of technical barriers
- Improved ability to prioritize efforts and resources, both with respect to safety and productivity
- TIMP offers a standardised approach across installations for following up technical integrity
- The work process with aggregation of information, combined with expert judgment, is in itself an important strengthening of safety culture and awareness
- The information presented in the TIMP portal is transparent and well documented
- TIMP also facilitates experience and knowledge transfer as well as easier reporting (to authorities, partners, customers, upper management, etc.)
- "Continuous" overview of technical integrity for each plant enables increased predictability

TIMP focuses on technical integrity and mainly on technical indicators. It would be desirable to develop and include indicators for operational and organizational barriers to ensure proper and complete medium-term verification and follow-up of barriers.

5.3 Long-term verification and follow-up – TTS/OTS

In addition to supporting systems and tools for short- and medium-term barrier management and verification, detailed long-term verifications of barrier elements are carried out by some companies using a TTS/TCS (Teknisk Tilstand Sikkerhet / Technical Condition Safety) type of methodology. This is a thorough review and assessment, which in some companies takes place every 5th year, whereas in other companies a comparable review of defined barrier functions and systems is performed every 2nd or 3rd year.

The TTS verification is focusing on technical aspects of barriers. The approach was developed by Statoil in cooperation with DNV GL and similar approaches have been adopted by several Norwegian offshore operating companies. Based on offshore reviews and onshore interviews, each system and performance standard is given a mark/score (A-F).

A comparable approach for the assessment of operational safety conditions has also been developed; denoted OTS/OCS (Operasjonell Tilstand Sikkerhet / Operational Condition Safety). In /14/, OTS verification is defined as "a systematic and independent assessment of the status of the operational safety barriers". It is argued that OTS reveals non-compliance with requirements and best practice within different relevant levels in an organization and that it is suitable as a basis for the development of risk reducing measures. The OTS method comprises seven operational performance standards, which correspond to PIFs, i.e. factors that influence the performance of the operational and organisational barrier elements. The descriptions/ definitions are summarised in Table 5.1.

Table 5.1 Performance standards in OTS /14/

Performance standard (PS)	Description/definition
Work practice	Work practice is the way work tasks are routinely or usually carried out at an installation or a plant. Good work practices shall contribute to safe and accurate work performance in accordance with procedures and documentation so that major accidents are avoided.
Competence	Competence entails knowledge, skills and abilities that can contribute to adequate work performance and/or problem solving. Competent and skilled personnel contribute to task performance and problem solving in a safe manner and with good quality so that major accidents are avoided.
Procedures and documentation	Procedures and documentation are written and electronic aids that describe the design and status of the plant and routines for operation and maintenance. Governing documents contain best practice to ensure safe and efficient operations. Procedures and documentation shall support safe operation and maintenance to prevent major accidents by describing current procedures for operation, maintenance and modifications of the plant, document the current (updated) design of the physical plant, and describe the status of systems, equipment and organization.
Communication	Communication is the dissemination of information and knowledge of importance to correct performance of work tasks on the installation/plant. Good communication will help ensure that those involved in a work process has access to the information required, and that the involved have a common understanding of the tasks so that major accidents are avoided.
Work load and physical working environment	Workload and physical working environment contains two factors. Workload is associated with planning and execution of work where adequate resources and time are available for completion of the work in an accurate and safe manner. The physical working environment entails the environmental conditions (including the design and maintainability) in a workplace that may affect the potential for major accidents. Appropriate workload will contribute to having enough time for planning and execution of work in an accurate and safe manner, both to avoid stress and so that there is enough time for rest and restitution to be able to work safely. High standard on the physical working environment will ensure that work activities are executed in a safe manner without negative influence from external conditions in order to prevent major accidents.
Management	Management is crucial to planning, coordination, monitoring and follow-up of activities and improvement efforts. The role of management is to govern the business in a way that ensures that employees have a strong focus on safety in their daily work, and that they are engaged and feel a commitment to the company's safety strategies so that major accidents are avoided. Management shall also ensure that the conditions, which affect the risk of major accidents, are followed-up and improved.
Management of change	Management of change is related to the overview and control of changes so that they are implemented effectively to reach set goals and do not lead to unforeseen problems associated with the operation and maintenance of the existing plant or an unacceptable risk of major accidents. The function of change management is to ensure that all technical, operational and organizational change is managed in such a way that major accidents are avoided.

Note that "operational barriers" in the OTS context corresponds to both organisational and operational barrier elements as defined in Section 2.2.4. Also, note that according to our definitions the most critical procedures are considered as operational barrier elements in themselves (not PIFs).

5.4 Examples of other barrier monitoring systems and tools

5.4.1 ConocoPhillips' iSee system

Several companies in the petroleum industry have implemented barrier status panels on their facilities, as discussed in Section 5.1. Typically, a barrier panel/dashboard provides an overview of degraded or failed barrier elements and tags on different levels, e.g. on tag, element, system, performance standard, function and/or area level (cf. Figure 5.2 and 5.3).

Some systems present status information using simple tables or graphs, whereas other systems also visualise the status of degraded or failed barrier elements on layout drawings. One example is ConocoPhillips' iSee system /11/. Here, information per area is visualised on 2D drawings, as illustrated in Figure 5.6. This figure provides a screenshot of a web-based visual graphical interface containing:

- Location of on-going and planned work permits
- Overview of barrier and deviation status and development
- Risk analysis data (graph in red box)

Figure 5.6 Visualization of risk/barrier status information using area charts /11/

In addition to risk/barrier status information, the area charts could also visualize other data such as e.g. manning data, bypasses of safety systems, ongoing work on HC systems, hot work permits and other critical

activities, and static QRA data (e.g. overall FAR level and risk distribution in relevant area). This type of visualization may be characterized as "live area risk charts". The advantage of combining barrier status information with critical activities indicators, as well as other indicators, is that it provides a more complete decision support tool for planning purposes. Such a tool combines information from several input sources that traditionally has been treated separately.

5.4.2 The risk barometer

Common to the tools or approaches discussed above, is that they present barrier status information without indicating the effect of the failures or degradations on the overall risk level. According to PSA, there is a need to strengthen the understanding of the relationship between risk management and barrier management[9]. This could include answering questions such as: "What is the effect on risk of having certain degraded or failed barrier elements/tags?" Answering this question provides current risk status based on the status of barriers, i.e. providing a "dynamic risk picture".

The difference between, and the benefit of risk information as opposed to pure barrier status information, are discussed and exemplified in the following. In a barrier panel, the status of each identified barrier element or tag is typically presented in terms of a green, yellow or red traffic light (functioning, degraded or failed barrier element/tag). In addition to the latest status, the development of the numbers of failed and degraded elements (yellow and red elements) over time, i.e. the trends, can be presented. This is illustrated in Figure 5.7 (left part) showing a positive trend in the period July-October 2014.

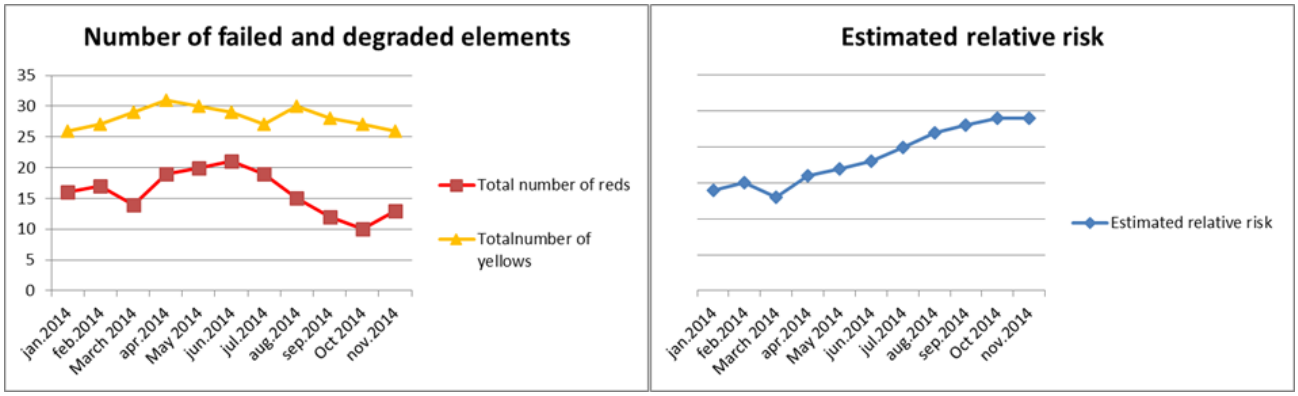


Figure 5.7 Benefit of adding risk information to barrier status

This information could be supplemented with additional information about the development in relative risk. Assume that the reduction in total number of red elements for the period July-October 2014 is due to a large number of low-criticality barrier elements having been repaired, at the same time as a few high-criticality elements have failed and have actually caused the overall risk to increase, as illustrated in Figure 5.7 (right part).

Consequently, although the total number of failed (red) barrier elements shows a positive trend, the relative risk may – on the contrary – have increased. This illustrates the benefit of estimating the associated risk in addition to the number of failed or degraded barrier elements.

Developing a complete dynamic risk model that can predict the effect on risk of failed or degraded barrier elements (and planned and unplanned activities, etc.) is a very complicated task, due to several reasons. This

[9] http://www.psa.no/barriers/category960.html

includes incompleteness of the current risk models, the complexity, variety and extent of the activities taking place on an oil and gas installation, lack of technical and operational input data, and the fact that human activities are generally challenging to capture in a risk model.

In lack of a complete dynamic risk model, simplified approaches are considered. One such approach is the "Risk barometer" /21/. It uses a simple hierarchical model to predict changes in risk based on the status of barrier functions, systems and barrier elements. A display from the risk barometer is shown in Figure 5.8, and it can be used to obtain the relative change in risk as indicated in Figure 5.7 (right part).

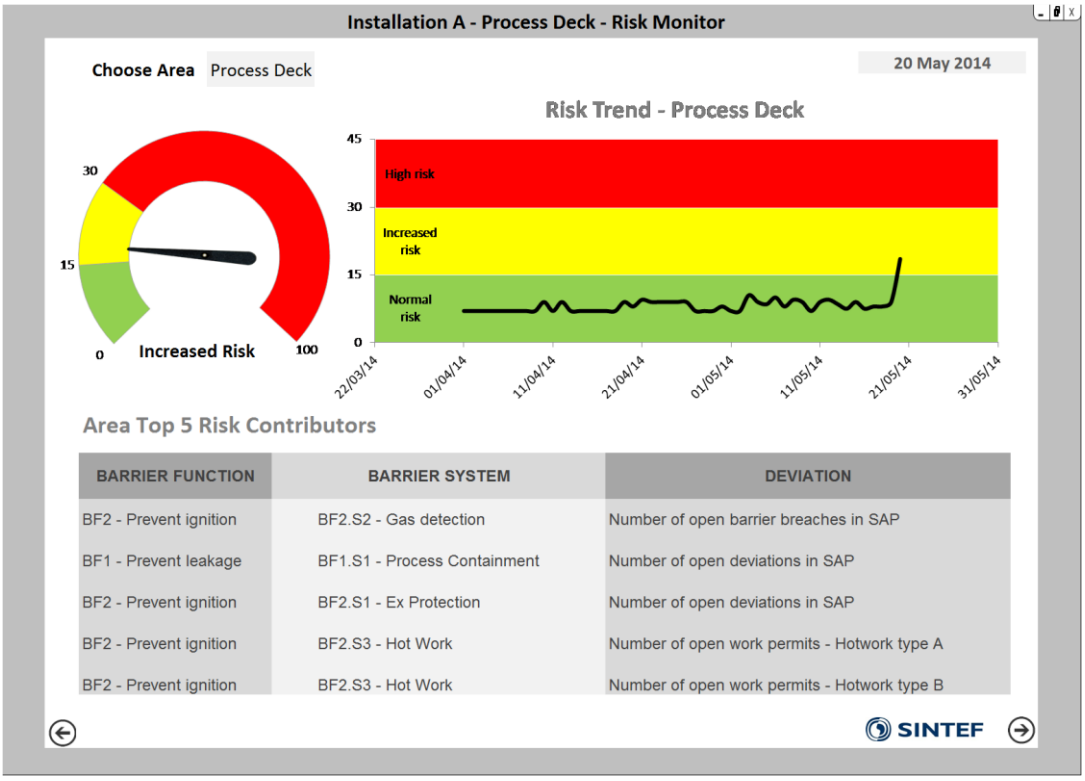


Figure 5.8 Risk barometer display for area level (process deck) /21/

6 Maintain and follow-up barrier performance – barrier management in operation

Barrier management in operation[10] includes all activities carried out to maintain the functionality and integrity of the barriers throughout operation, during all operational modes. A simplified illustration of barrier management in operation is shown in Figure 6.1.

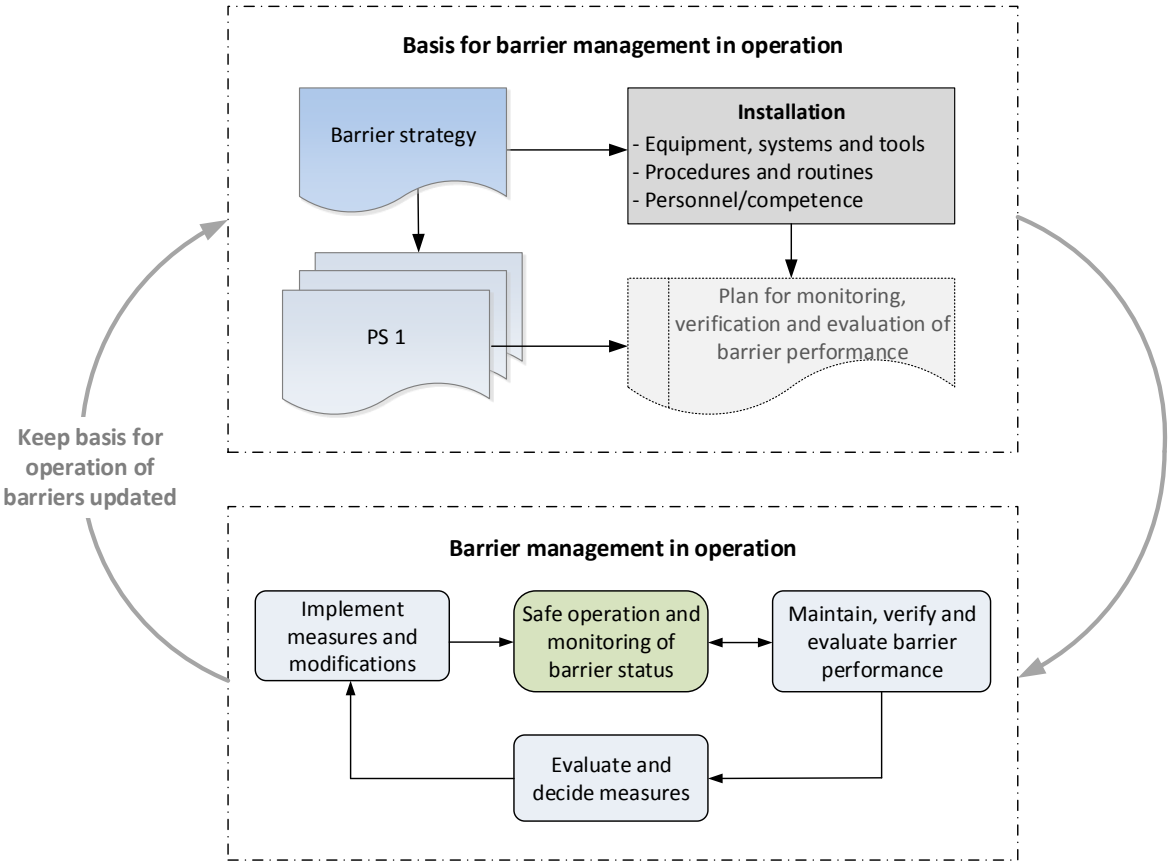


Figure 6.1 Barrier management in operation

The main barrier management activities in operation include:

1. Safe operation and monitoring of barrier status, including handling of barrier non-conformances (lost or impaired barriers)
2. Maintain and ensure the integrity of barriers throughout operation, including verification and evaluation of barrier performance
3. Evaluate and decide on measures, e.g. in case of deviations from performance requirements
4. Implement measures and modifications, including new barriers if required
5. Keep the basis for operation of the barriers updated at any time, including the installation specific barrier strategy, other relevant documentation, procedures and routines as well as systems and tools that are applied for operating and maintaining the integrity of the barriers

[10] Follow-up of safety instrumented systems (SIS) and the associated SIL requirements in the operational phase will be an integrated part of the barrier management process. SIS follow-up during operation is described in quite detail in "Norsk olje og gass retningslinje 070" /13/ and will therefore not be further elaborated here.

As illustrated in Figure 6.1, barrier management activities related to monitoring, verification and evaluation of barrier performance may be described in a separate plan (see also Section 4.6). Such a plan is not explicitly described in this report, but the related activities are further discussed in the next sections.

6.1 Safe operation and monitoring of barrier status

During normal operation, the installation and the associated production processes should operate under stable conditions and within the safe operating limits. In such a stable situation, there will be few demands on the barriers, and the operational personnel's daily interface with the barriers mainly include:

- Monitoring the status of the TO&O barrier elements
- Handling of impaired or lost barriers in connection with e.g. maintenance activities, missing competence, equipment malfunction, start/stop, in/out of service, etc.

6.1.1 Monitoring the status of the TO&O elements

The status of the barriers should be known to relevant operational personnel at all times. A practical solution for monitoring of the barrier status will be through the implementation of a barrier status panel as described in Chapter 5. Such a status panel may facilitate automatic collection and presentation of relevant barrier status information, highlighting failed or degraded barrier elements and giving an overview of inhibits and overrides. Active compensating measures may also be visualized in the barrier status panel.

If a barrier status panel is not in place, all the relevant BSP information will, as discussed in Section 5.1, be available in other systems, and monitoring of relevant data and parameters directly from these (dispersed) systems will be required.

In addition to continuous monitoring of the status of TO&O elements, follow-up of relevant operational parameters and any deviations from these parameters will be important to ensure operation within "the safe operational envelope". Examples are monitoring of critical process parameters through control and safety system alarms, surveillance of ship traffic and objects on collision course, monitoring of crane alarms, monitoring of stability and tension calculations, weather forecasts, etc.

Furthermore, it must be ensured during daily operation that:

- Operation of the barriers is performed according to relevant procedures and the basis for barrier operation, including the fulfilment of relevant assumptions, e.g. related to crane lifting restrictions, hot work hours/restrictions and manning assumptions
- Safety critical failures revealed during activities other than testing are reported and followed-up
- Relevant and competent personnel are involved in day-to-day activities, both offshore and onshore
- Non-conformances related to organisational and operational barriers are reported and followed-up
- Modifications or changes to procedures based on reported failures, degradations, non-conformances or process changes are evaluated and implemented

6.1.2 Handling of impaired or lost barriers

Degraded modes of operation arise when a barrier element experiences some kind of reduced performance or reduced/lost ability to perform its intended function. This applies for both technical and organizational barrier elements:

- For technical barriers this may be due to equipment failure (either revealed during testing or by automatic validation / condition monitoring), intentional override, inhibit or disabling, or added uncertainty concerning the barrier performance, e.g. if functional testing and/or inspection has not been performed in due time
- For organisational elements a degradation may result from personnel being disabled (not present or available), personnel being disqualified due to lack of required courses or competence, personnel with degraded qualifications or exercises/drills not being conducted according to schedule

Safety critical procedures, checklists, work descriptions or P&IDs may also be degraded in the sense that they are not available or outdated, or there may be uncertainty concerning their status or validity due to required updates and changes not being implemented.

Degraded modes of operation may cause increased risk and compensating measures must therefore be considered (cf. Management Regulations, Section 5). A simplified process for handling of barrier non-conformances is illustrated in Figure 6.2.

The process is typically initiated by an impaired or lost barrier element, i.e. a non-conformance against the performance standards, the barrier strategy and/or other requirements.

When such a non-conformance arises, the need for compensating measures must be assessed taking into consideration the criticality of the lost or impaired barrier and possibly the overall effect on the risk level. As discussed in Section 5.4.2, it will often be difficult to relate the lost or degraded barrier to changes in the risk level. Nevertheless, when handling non-conformances it is important to perform at least qualitative evaluations related to the criticality of the degraded barrier element, in terms of consequences of failure/ degradation and available redundancy. The process of handling non-conformances should address questions such as:

- Is it possible to implement immediate or temporary measures that can compensate for the lost/ impaired barrier, e.g. reduced production, production with reduced redundancy, immediate repair (e.g. replacement of component), adjustment of activity level, replacement of personnel, etc.?
- Are there absolute (regulatory or corporate) requirements related to availability of the barrier?
- Does the loss/impairment of the barrier represent a violation of assumptions in the basis for operation of the installation, e.g. assumptions in the QRA?
- Is the barrier loss/impairment short-, medium- or long-term? How fast will it be possible to bring the lost/impaired barrier into normal function?
- Is the trend of performance – if any – positive or negative for the relevant barrier (element)?
- Are compensating measures available and/or possible to implement? Is it possible to continue (reduced) production without the barrier?
- Is a modification of systems or changes to procedures required?

Regardless of the need for compensating measures, a notification shall be written in the maintenance system upon equipment failure or malfunction. In case of a degradation of an organisational or operational barrier element, a non-conformance should be reported in the event reporting system.

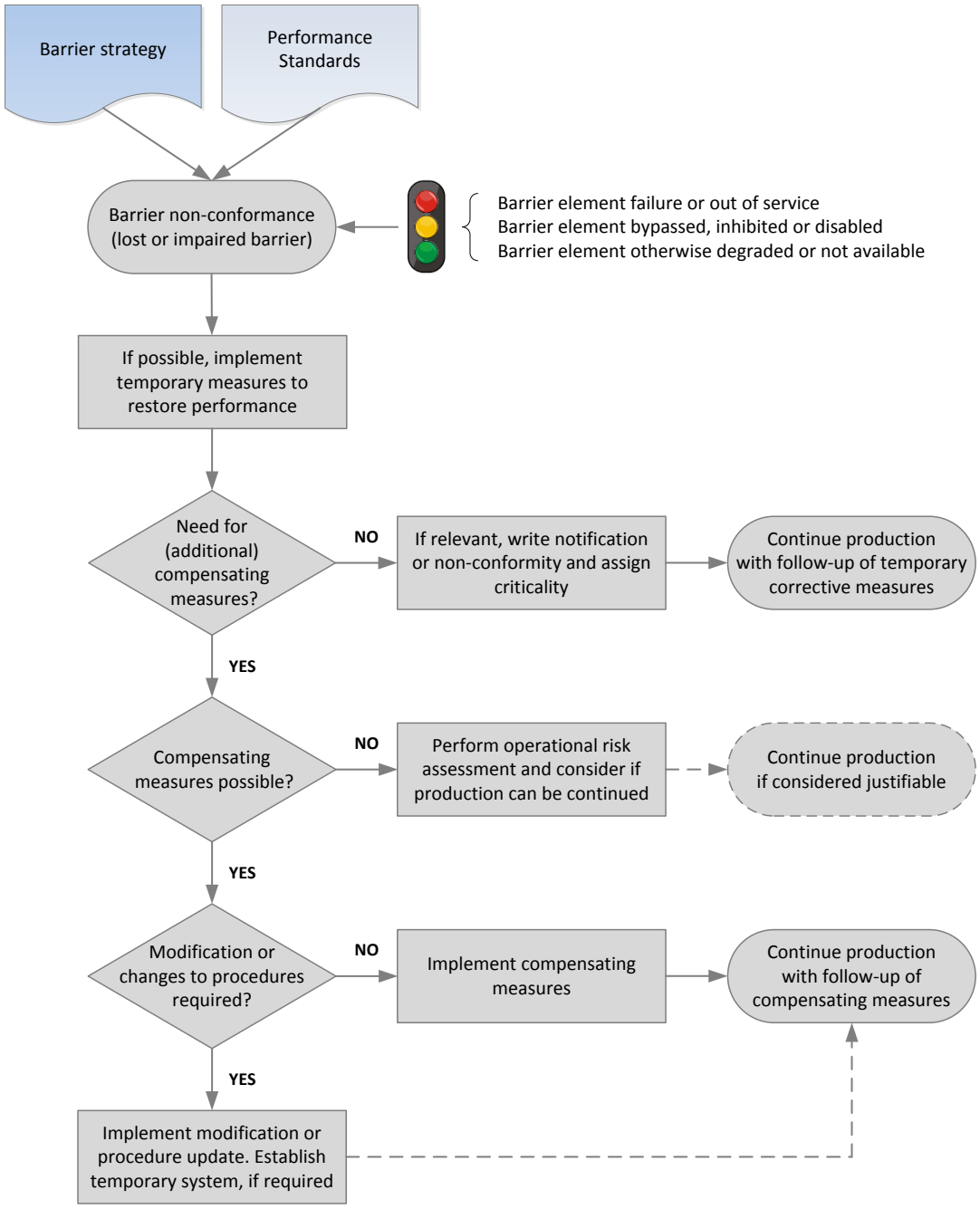


Figure 6.2 Simplified process for handling of barrier non-conformances

6.2 Maintain, verify and evaluate barrier performance

6.2.1 Technical barrier performance

To manage risk during operation, the status of the barriers must be continuously monitored and it must be verified that the barriers perform according to the specifications and assumptions laid down in the design basis. The verification of barrier performance shall be systematic, and directly linked to the identified performance requirements of each barrier element.

Maintaining the performance of the technical barriers is ensured primarily through the facility's *integrity management program*. This will include e.g. condition monitoring, functional testing, scheduled inspections, servicing/checking/calibration, repair, overhaul and replacements. Maintenance may be initiated upon equipment failures (corrective maintenance), scheduled on a regular basis according to calendar time or operating hours (preventive maintenance), or initiated upon request from a condition monitoring system (condition based maintenance).

The technical barrier elements and associated equipment shall be regularly tested in order to ensure that the functional integrity is maintained during the entire lifecycle and if possible have all their activations (demands) - planned and unplanned - automatically validated. The main purpose of a functional test is to reveal critical failures that are not detected during normal operation. The testing shall be performed according to predefined test procedures, which shall be readily available. Test intervals shall be scheduled in the PM programme, and for safety instrumented systems (SIS) they must be consistent with the test intervals given in the safety requirement specification (SRS).

The purpose of automatic validation of planned and unplanned activations is to keep a continuous and validated track of all activations, highlighting in advance any issue (related to performance) between functional tests. Such automatic validation needs to leverage on advanced software solutions for making use of real-time information.

The results from functional tests and any planned/unplanned activations (e.g. from automatic shutdown reports) shall be logged in a traceable manner into the maintenance system. All barrier elements and tags should be traceable in the maintenance system in such a way that failure data can be used to evaluate operational performance and compare it with required performance as specified during design.

As discussed in Section 4.4, performance requirements for technical barrier elements may be classified as shown in Figure 6.3. In Table 6.1, it is indicated how the different types of performance requirements can be verified and evaluated during operation.[11]

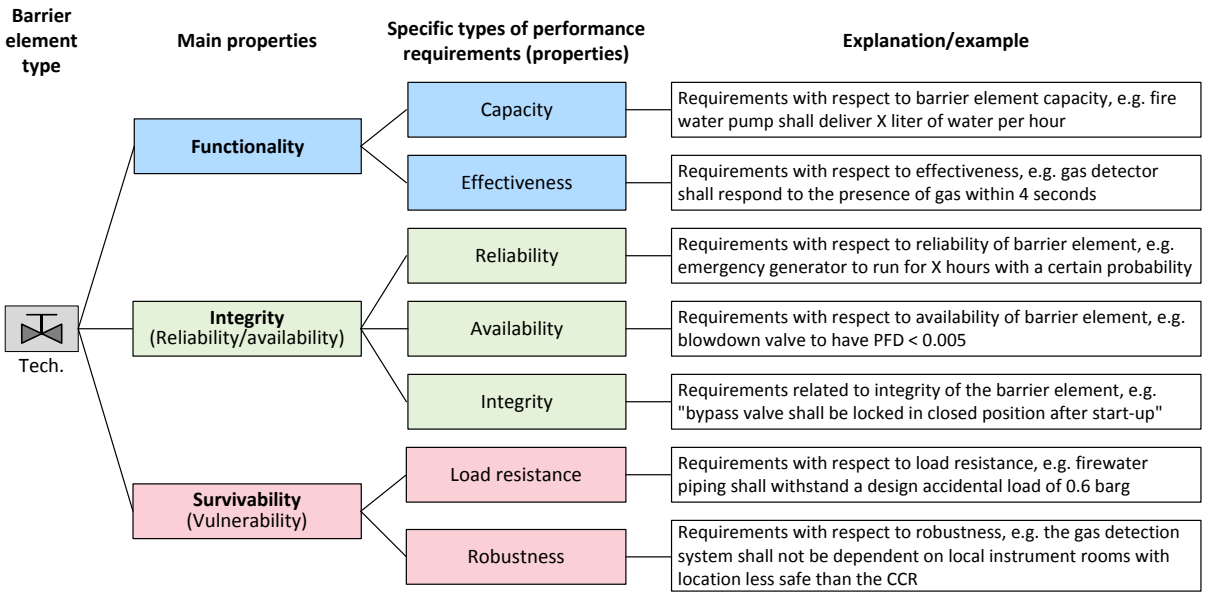


Figure 6.3 Performance requirements for technical barrier elements

[11] Performance requirements and the associated verification activities are largely based on project experience and NORSOK S-001 /18/.

Table 6.1 Verification and evaluation of performance requirements for technical barriers

Type of requirement	Examples of requirements	Verification of requirements during operation
Capacity	- Double acting ESD valves shall have local accumulators with capacity for at least 3 operations (close-open-close)	- Functional testing
	- A mechanical ventilation rate of 12 air changes per hour shall be ensured in all local equipment rooms in hazardous area	- Alarm in CCR upon loss of ventilation / verifications of sufficient ventilation rate
	- Survival suits for 50 % of lifeboat capacity shall be available at the lifeboat and escape chutes	- Regular inspections/verifications
Effectiveness	- The ESD valve shall close on demand and within 30 seconds	- Functional testing / activation during operation
	- The IR detector shall respond to the presence of gas within 4 seconds	- Functional testing
	- Low alarm limit for point gas detector shall be 20 % LEL	- Functional testing / PM calibration
	- HVAC inlet dampers shall close within 6 seconds	- Functional testing / activation during operation
	- The PAHH function for the inlet separator shall have a response time < 12 seconds (end-to-end)	- Functional testing / activation during operation
	- Internal leakage rate for ESD valve shall not exceed x liter per minute	- Leak testing
	- Upon zero voltage on emergency switchboard, emergency power supply shall be established within 45 seconds	- Functional testing
	- The deluge nozzles shall receive water at design pressure not later than 30 seconds after a confirmed fire signal has been given	- Functional testing / calibrations
	- Upon use of temporary equipment that may represent ignition sources, these shall be shut down according to the relevant ignition source groups	- Verification/testing prior to start-up of temporary equipment / automatic validation
Reliability	- The probability of failure of the fire water pumps to run for 18 hours continuously without stop shall be < 2 %	- (Difficult to verify during operation, will typically be verified in design)
	- The probability of failure of the emergency generator to run for 18 hours continuously without stop shall be < 1 %	
Availability	- The maximum number of experienced safety critical failures for the population of 40 ESD valves shall be one per year	- Periodic operational reviews (see Table 6.4) / online SIL validation tools / SIL reports
	- The failure fraction for the lifeboat freefall release function shall be < 0.5 %	
	- The PSD function of preventing high pressure in the inlet separator shall be SIL 1 compatible and have a PFD < 0.02	
Integrity (ability to be present when needed)	- Isolation valves in equalizing lines across ESD valves shall be secured in closed position during normal production	- Daily monitoring / inspection
	- Escape routes shall be available and properly marked incl. signs and florescent arrows	- Daily monitoring / inspection
	- Permanent and/or temporary penetrations shall not reduce the strength or the fire integrity of the fire divisions	- Daily monitoring / Inspections
Load resistance	- Riser ESD valve shall withstand a HC jet fire with duration of 15 minutes	- Visual inspection of passive fire protection
	- The fire detection function for hazardous areas shall be operative after a dimensioning explosion to ensure alarm and that the necessary actions can be realized	- (Difficult to verify during operation, will typically be verified in design)
Robustness	- Logic solver software shall be protected against illegal access from external sources (especially relevant during modifications)	- (TBD)
	- The gas turbine exhaust pipes and channels shall be insulated to prevent exceedance of ignition temperatures	- Visual inspection of insulation material
	- Firewater shall be available at temperatures below 0°C	- Continuous monitoring / functional testing

Note that the classification of type of requirement in Table 6.1 is not always straightforward. E.g., it could be argued that some of the requirements classified as "effectiveness" rather could be classified as "integrity". It can also be argued that for practical purposes, the split between reliability and availability requirements is not required. However, the important point here is that all relevant performance requirements are included. How they are classified is not that critical.

Although Table 6.1 does not represent a complete list of typical performance requirements for technical elements, some observations can be made about the properties:

Functional requirements
Functional requirements, including capacity and effectiveness, are to a large degree verified through functional testing or continuous automatic validation on tag (or loop/function) level. Some functional requirements may be of a different nature that requires other types of verification activities such as regular inspections.

Integrity requirements
Integrity requirements, i.e. reliability and availability, will typically require experience data from an entire population of equipment over a certain observation period to be verified. Collected data / failure reports from functional tests and from online monitoring systems, including automatic shutdown reports, must be regularly reviewed and analysed to obtain e.g. the number of safety critical failures experienced during the last observation period. Based on the sample size and the observation period, the related uncertainty of the estimated reliability/availability can also be assessed.

Integrity can be defined *as the components ability to be present when needed* and can therefore be related to requirements other than only reliability and availability. This can be exemplified by manual interlock valves required to be open for a pressure safety valve to be available, or no obstructions to be present in escape routes. Such requirements are typically verified through daily monitoring and regular inspections.

Survivability requirements
Survivability requirements, including load resistance and robustness, are to a large degree related to inherent design issues, e.g. fire and explosion resistance, impact / mechanical damage resistance, degree of redundancy, segregation of equipment, routing of piping and cables and winterisation aspects. As a result, (re)verification and assessment of many of these requirements may not become relevant until changes or modifications to the design are implemented. Nevertheless, some of the requirements will require regular verification, inspection and follow-up, exemplified e.g. by visual inspection and maintenance of passive fire protection and thermal insulation.

See Table 6.4 for a summary of relevant verification activities.

6.2.2 O&O barrier performance

An important part of barrier management will be follow-up and verification of the operational and organisational barrier elements. Such follow-up are not new to the petroleum industry and has been managed through a number of systems, such as:

- Competency systems / competence matrices / Human Resource (HR) systems
- (Live) manning lists
- Event reporting systems (e.g. Synergi)
- Exercise plans and schedules
- Document handling systems

- Management of change systems

What may be perceived as somewhat "new" related to barrier management, is that the O&O barrier elements shall be explicitly identified and described (cf. Section 4.3), that performance requirements shall be defined for these elements (cf. Section 4.4), and that the performance requirements must be verified and evaluated during operation.

Performance requirements for operational and organizational barrier elements can be classified as shown in Figure 6.4 (cf. Section 4.4 – lower part of Figure 4.10).

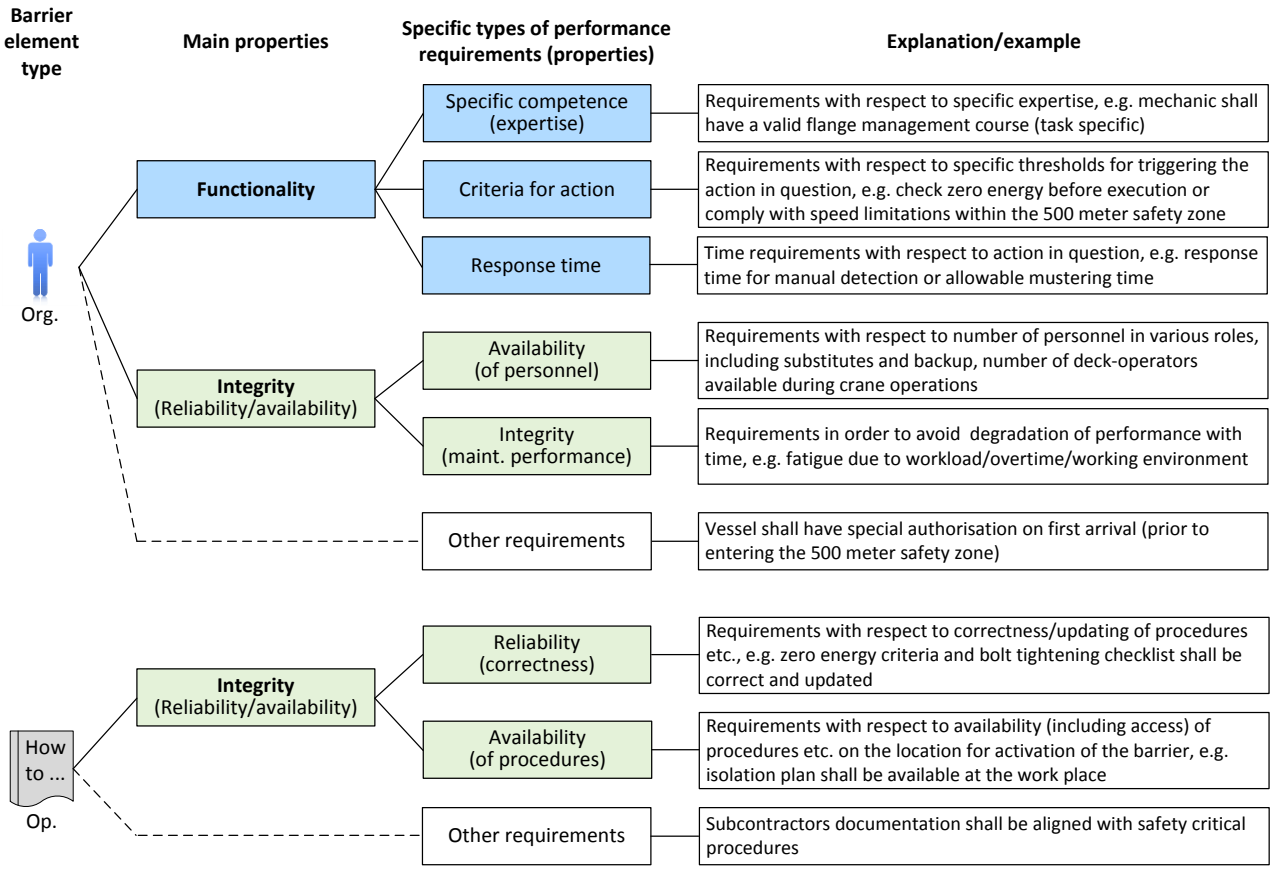


Figure 6.4 Types of performance requirements for O&O barrier elements (and some examples)

In Table 6.2 and 6.3, it has, similar as for the technical barrier elements, been exemplified how different types of performance requirements can be verified and evaluated for organizational and operational barrier elements, respectively. Also for the O&O barrier elements, the important point is that all relevant performance requirements are included, not how they are classified.

Table 6.2 Verification and evaluation of performance requirements for organizational barriers

Type of requirement	Examples of requirements	Verification of requirements
Specific competence (expertise)	- Maintenance personnel must have a valid (and updated) flange tightening course - CCR operators must have a valid and updated alarm response course - Mechanics must have a valid and updated flange management course - Members of the emergency management team must have a valid and updated emergency preparedness management course - Lifeboat crew must have a valid and updated free-fall lifeboat course - Crane operators must have a valid (and updated) crane operation course - Maintenance supervisor must have at least X years of relevant offshore experience	- Regular review of competence matrix / HR system - Possibly automatic warning/alarm through indicators, e.g. in BSP (if data can be automatically collected from relevant systems)
Criteria for action	- Offloading shall be disrupted in case of significant wave heights exceeding X meter - Lifting shall be disrupted by crane operator in case of significant wave heights exceeding Y meter or wind-speed exceeding Z m/s - Captain shall ensure that speed limitations are complied with inside the 500 m safety zone - Blowdown shall be manually initiated by CCR operator in case of confirmed gas detection - Mechanic and area technician shall perform an independent check of barrier setting prior to execution of work	- Exercises/trials/simulations or possible logs from actual operation - Logs from actual operations - Audits and verification of work performance
Response time	- Confirmed situations of hazard and accident shall be alerted by CCR to OIM within 1 minute - In case of confirmed situations of hazard and accidents, the emergency management team shall be established within 5 minutes - The joint rescue coordination centre (JRCC) shall be alerted within 10 minutes after a confirmed situation of hazard and accident - In case of failure of the pipeline overpressure protection system, the ESD inlet valve shall be closed from CCR within 2 minutes	- Scheduled exercises/trials - Simulations/exercises
Availability (of personnel)	- OIM shall ensure that the number of persons on board is known at all time. An overview of persons not accounted for shall be given by name - Two deck-operators shall always be available during offshore crane operations - During lifting operations, two persons shall at any time be able to see the cargo and therefore be able to stop the operation - Captain shall ensure that two bridge officers monitors the operation during supply ship approaching installation	- Monitoring and regular reviews of e.g. live manning lists - Monitoring and review of daily lifting operations - Monitoring and review of daily lifting operations - Monitoring and review of ship approach operations
Integrity (maintain performance)	- Specified rest periods shall not be exceeded with more than X hours per 14 days shift period - The daily time of rest must not be less than 8 hours - The absence rate for offshore workers shall not exceed X %	- Regular reviews of time-sheets or similar

Table 6.3 Verification and evaluation of performance requirements for operational barriers

Type of requirement	Examples of requirements	Verification of requirements
Reliability (correctness)	- Non-conformances concerning safety critical procedures shall be reported in Synergi (event reporting system) - All safety critical procedures shall be updated within 14 days of any approved changes - All safety critical procedures shall be made subject to annual review with respect to correctness and procedures being up-to-date - Zero energy criteria and bolt tightening checklist shall be correct and updated	- Weekly reviews of Synergi (or other event reporting system) - Regular reviews of document handling system - Annual review of all safety critical procedures - Daily monitoring and regular reviews
Availability (of procedures)	- The emergency preparedness plan shall be available at defined locations/offices/control rooms on the facility - Safety critical procedures shall be readily available in paper format in CCR and at the location of barrier activation - Isolation plan shall be available at the work place prior to execution of work - Checklist for start-up of pipelines shall be laminated and always easily available in the CCR	- Daily monitoring and regular reviews

As seen from Table 6.2 and 6.3, verification of operational and organizational barrier performance is either carried out through regular use of performance indicators or through more infrequent audit/review type of verifications. Verification through performance indicators is efficient, and is used to the extent possible, in particular if automatic collection of data for these indicators is feasible. Such data could typically be collected from a wide range of information sources, e.g. competence matrix, manning lists, event reporting systems (e.g. Synergi) and document handling system. Verification activities such as document reviews, surveys and audits may be used as separate methods, and they may provide additional (manual) input to performance indicators.

Manual intervention during actual hazards and accidents is (fortunately) infrequent. Hence, requirements related to criteria for action and response time for personnel/roles (i.e. organisational barrier elements) must often be verified through regular exercises/trials and possibly through simulations.

6.3 Evaluate and decide on measures

Any loss or impairment of one or more barrier elements should continuously be evaluated against the need to implement compensating measures. The handling of impaired or lost barriers, including the need for compensating measures to restore the performance of lost/impaired barriers, is described in Section 6.1.2.

In addition to considering immediate or temporary compensating measures, verification and evaluation of barrier performance may reveal deviations such as:

- A group of technical barrier elements, e.g. ESD valves, have experienced a too high number of safety critical failures, calling for measures to improve their performance
- Water intrusion in junction boxes is a repeated problem that threatens the availability of some types of barrier elements
- The opening time of blowdown valves is generally above the criteria specified in the performance standard
- The competence matrix has not been updated for a year, resulting in uncertainty concerning the personnel's competence and validity of required courses

- There is a sustained use of overtime among control room operators which in the long run can impact their performance
- Safety critical procedures are not easily available and has not been updated for the last two years. P&ID mark-ups are only available in the central control room but not in the electronic document system
- Repeated errors in isolation plans have been revealed in work permit meetings

Such deviations will typically call for the evaluation of more extensive measures such as detailed root cause analyses, additional testing and maintenance, updating of procedures and sometimes modifications in the actual design and operation of technical barriers.

Often it will be necessary to revisit the design basis and the assumptions underlying the performance requirements, and verify whether these assumptions are still valid. In particular, this is relevant for functional requirements to the technical barrier elements, where the basis for response times requirements and capacity requirements may change with time, e.g. due to changed process conditions and process dynamics (cf. Section 6.5).

6.4 Implement measures and modifications

As discussed in the previous section, the evaluation of barrier performance may trigger a need for implementing improvements and/or modifications of a technical, operational or organisational barrier element. This may include:

- Modifications in the actual design of the technical barrier elements, including replacement by improved technical solutions
- Changes and improvements to safety critical procedures or routines
- Improvements and modifications to the supporting systems and tools for barrier management (cf. Chapter 5)
- Modifications to activities and conditions that affect barrier performance, e.g. changes to test intervals, more frequent inspections of particular parts of the process or systems, changes in manning level, increased competence in certain areas, etc.
- Possibly the implementation of new barriers / barrier elements, if the risk picture has changed significantly

For modifications of safety instrumented systems (SIS), a relevant management of change process is proposed by IEC 61511 /16/.

6.5 Keep basis for operation of barriers updated

In case of permanent technical, operational and organisational modifications, as well as changes in internal or external conditions that may significantly influence the performance of the identified barrier functions, the need for updating of the barrier strategy and/or performance requirements shall be evaluated. If updates and changes are made to the basis for operation of barriers, the barrier monitoring and verification systems and tools need to be updated accordingly.

6.6 Summary of barrier management activities during operation

Table 6.4 provides an overview of recommended activities to ensure that the integrity and functionality of the barriers are maintained throughout the operations phase.

The responsible position/role is also (partly) indicated, but will depend on the particular organisation of the facility under consideration. The responsibilities should be specifically defined e.g. in a separate "Barrier Management in Operation" procedure.

The suggested frequencies of the barrier management activities are indications only, and must be adapted to the particular facility and organisation under consideration.

Table 6.4 Overview of barrier management related activities during operation

Type of activity	Description of activities	Responsible position/role	Frequency
Normal (safe) operation	Operation within design envelope, including: • Daily monitoring of the status of TO&O elements (e.g. in a barrier status panel) • Daily monitoring of relevant operation parameters and any deviations from these parameters • Ensure that daily operation of the barriers is performed according to procedures and basis for barrier operation • Ensure that relevant and competent personnel are involved in day-to-day activities, both offshore and onshore	CCR operators / operation responsible/-supervisor	Continuous
	Overview, logging and control of inhibits and overrides	CCR operators	Continuous
	Daily reporting: • Reporting of safety critical failures revealed during activities other than testing (technical equipment) • Reporting of non-conformances related to organisational and operational barriers	Maintenance and operations responsible / -supervisor	Continuous
	Handling of non-conformances such as degraded (lost or impaired) barriers. Initiate actions and compensating measures upon non-normal operating situations	System or PS responsible	Continuous
	Identify and evaluate the need for modifications or changes to procedures based on reported failures, degradations, degradations and non-conformities, process changes, etc.	System or PS responsible	Continuous
Testing and maintenance of technical barriers	Maintenance, testing and inspection according to maintenance programme and test procedures, including: • Reporting of safety critical failures • Reporting of other failures • Repair and replacement of defect and degraded components	Maintenance responsible/-supervisor	Continuous
	Review maintenance/testing back-log and initiate necessary actions as required	Maintenance responsible/-supervisor	Continuous / weekly
Maintenance of organisational and operational barriers	Follow-up of required offshore competence and resources. I.e., having available and maintaining the required competence of the organisational barrier elements (personnel/roles) performing safety critical tasks, including the emergency preparedness organisation	HR responsible	Continuous
	Safety critical procedures must be kept updated at any time to reflect current work practices and any changes or improvements to technical equipment	Procedure responsible	Continuous

Type of activity	Description of activities	Responsible position/role	Frequency
Verification and evaluation of barrier performance	Verify regularly that the performance of all *technical barrier elements and performance standards* are in line with the basis for operation: • Review of backlog on safety critical equipment • Review of reported notifications in the maintenance system. • Review of number of reported failures versus acceptable failure frequencies • Review of trends of performance of barrier elements and PSs • After a shutdown / activation, review relevant reports and system logs to identify possible safety critical failures revealed and, if relevant, prepare corrective work orders	System / PS responsible	Weekly / Monthly As required
	Verify regularly that the performance of all *organisational and operational barrier elements* are in line with the basis for operation: • Review of reported non-conformities in the event reporting system • Review of overdue actions and non-conformities from the event reporting system • Execution of scheduled trials and exercises and review of results from these trials/exercises • Regular review of competence matrix / HR system / live manning lists • Review of safety critical procedures in the light of discrepancies experienced during operation, audits or as a result of non-conformance reports	Responsible personnel	Weekly / monthly As required
	Perform annual performance reviews to ensure that the barrier elements comply with the required performance as stated in the installation specific performance standards and/or the barrier strategy: • For each barrier element type: review failure history from last year, if required perform failure (re)classification and conclude on number of safety critical failures • Evaluate number of safety critical failures for each type of barrier element and compare with installation specific performance requirements • From safety systems, information management system, manual logs, etc.; estimate and verify other relevant follow-up parameters such as demand rates, number of inhibits/ overrides, etc. • Verify that the barriers are operated in line with other assumptions and prerequisites from the basis for operation (e.g. required competence, manning levels, hot-work hours, response times, etc.) • Document annual performance review in suitable format	System, PS and HSE responsible Onshore support personnel	Annually
	Perform audits / inspections / management reviews to ensure that the long term performance of the barriers comply with the required performance as stated in the installation specific performance standards and/or the barrier strategy	System, PS and HSE responsible Onshore support personnel	Bi / Tri-annually
Evaluate, decide and implement measures	Based on the different verification activities, identify performance deviations. Evaluate, decide and implement required improvements and/or modification of the technical, operational or organisational barrier elements	System/PS responsible	As required
Keep basis for barrier operation updated	Update the barrier strategy and/or performance standards accordingly, and implement necessary changes and updates to the barrier monitoring and verification tools	System/PS responsible	As required

7 References

/1/ Øien, K., Hauge, Størseth, F., S., Tinmannsvik, R.K., 2015. Towards a holistic approach for barrier management in the petroleum industry, SINTEF A26845 (ISBN 978-82-14-05947-2)

/2/ Hauge, S., Hoem, Å.S., Hokstad, P., Håbrekke, S., Lundteigen, M.A., 2015. CCFs in Safety Instrumented Systems – Beta Factors and Equipment Specific Checklists based on Operational Experience, October 2014, SINTEF A26922 (ISBN 978-82-14-05953-3)

/3/ Petersen, S., Aakvaag, N., 2015. Wireless Instrumentation for Safety Critical Systems – Technology, Standards, Solutions and Future Trends, SINTEF A26762 (ISBN 978-82-14-05938-0)

/4/ Petroleum Safety Authority Norway, Principles for barrier management in the petroleum industry, 29.01.2013

/5/ The Management Regulations; Regulations Relating to Management and the Duty to Provide Information in the Petroleum Activities and at Certain Onshore Facilities, http://www.psa.no/management/category401.html, December 2015

/6/ Rahim, Y., Barrier management through Technical Integrity Management Programme (TIMP), ESRA seminar, Oslo 2015

/7/ DNV GL / NSA, Barrier Management in Operation for the Rig Industry; "Good practices", March 2014

/8/ Petroleumstilsynet, 2015. Risikonivå i Norsk petroleumsvirksomhet. Hovedrapport, utviklingstrekk 2014, Norsk sokkel. In Norwegian.

/9/ Øien, K., Hauge, S., 2014. Vedlikeholdets plass i barrierestyringen. SINTEF A26001 (ISBN 978-82-14-05676-1). In Norwegian.

/10/ Tinmannsvik, R.K., Albrechtsen, E., Bråtveit, M., Carlsen, I.M., Fylling, L., Hauge, S., Haugen, S., Hynne, H., Lundteigen, M.A., Moen, B.E., Okstad, E., Onshus, T., Sandvik, P., Øien, K., 2011. Deepwater Horizon-ulykken: Årsaker, lærepunkter og forbedringstiltak for norsk sokkel. SINTEF A19148 (ISBN 978-82-14-05088-2). In Norwegian.

/11/ Etterlid, D., I-See, IO Conference 2013, Trondheim

/12/ Reason, J., 1997. Managing the Risks of Organizational Accidents. Burlington: Ashgate Publishing Company

/13/ Norwegian Oil and Gas Association 070 (former OLF 070), Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry, Rev. 03, Draft version, dated 23.02.2016

/14/ Sklet, S., Ringstad, A. J., Steen, S. A., Tronstad, L., Haugen, S., and Seljelid, J., 2010. Monitoring of human and organizational factors influencing risk of major accidents. SPE International Conference on Health, Safety and Environment in Oil and Gas Exploration and Production, Rio de Janeiro, Brazil

/15/ IEC 61508 (2010). Functional Safety of Electrical/Electronic/Programmable Electronic Safety – Related Systems. Part 1-7. International Electrotechnical Commission, Geneva

/16/ IEC 61511 (2016). Functional Safety: Safety Instrumented systems for the Process Industry Sector, Part 1-3. International Electrotechnical Commission, Geneva

/17/ NORSOK Z-013, Risk and emergency preparedness assessment, Ver. 03, October 2010

/18/ NORSOK S-001, Technical Safety, Rev. 4, Feb. 2008

/19/ Petroleum Safety Authority Norway, Guidelines regarding the Management Regulations (29.4.2010), www.ptil.no

/20/ Øien, K., 2005. Barriereendringsanalyse (BEA). SINTEF Teknologi og samfunn, STF38 A04430, ISBN 82-14-02595-8. In Norwegian.

/21/ IO Center report; Handbook for monitoring of barrier status and associated risk in the operational phase - The risk barometer approach. SINTEF Technology and Society, Safety Research, 2015-06-26

/22/ ISO/DIS 17776 (2015), Petroleum and natural gas industries - Offshore production installations – Major accident hazard management during the design of new installations

/23/ Bye, A. et al., Petro-HRA Guideline, Internal version dated 2015-12-29

/24/ Kirwan, B., 1994. A Guide to Practical Human Reliability Assessment, Taylor & Francis

/25/ Lauridsen, O., et al., Barrier Management and the Interaction between Technical, Operational and Organisational Barrier Elements, SPE conference Stavanger 2016

/26/ Statoil internal document, Definitions and guidelines for non-technical barriers, April 2015

/27/ IOGP; Standardization of barrier definitions, April 2016. http://www.iogp.org/pubs/544.pdf

/28/ Offshore technology report- OTO 1999 092; Human factors assessment of safety critical tasks, HSE 1999

Technology for a better society

www.sintef.no