PDS

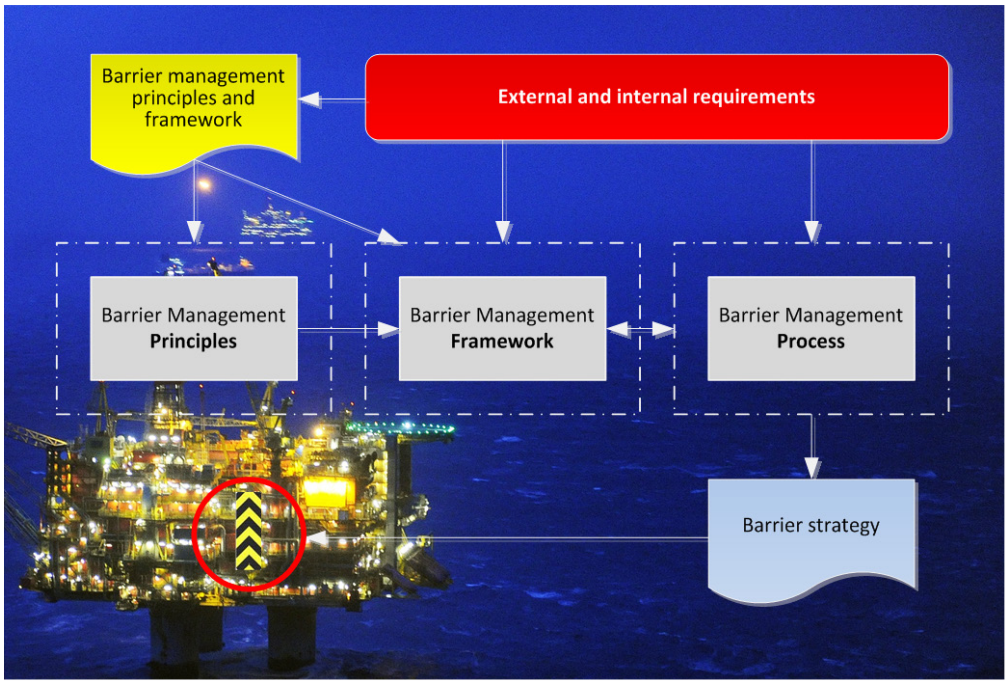
SINTEF

SINTEF A26845 - Unrestricted

Report

Towards a holistic approach for barrier management in the petroleum industry

Authors
Knut Øien, Stein Hauge, Fred Størseth, Ranveig Kviseth Tinmannsvik



SINTEF Technology and Society
Safety Research
2015-04-01

(Empty page)

Background picture on front page of Statfjord A. Photo: Harald Pettersen / Statoil.

SINTEF Technology and Society
Safety Research
2015-04-01

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

Towards a holistic approach for barrier management in the petroleum industry

VERSION
Version 1

DATE
2015-04-01

AUTHOR(S)
Knut Øien, Stein Hauge, Fred Størseth, Ranveig Kviseth Tinmannsvik

CLIENT(S)
Multiclient

CLIENT'S REF.
Håkon S. Mathisen

PROJECT NO.
102001170

NUMBER OF PAGES/APPENDICES:
58 + 2 Appendices

ABSTRACT

The purpose of this report is to elaborate on and discuss important aspects and challenges related to barrier management during different lifecycle phases of an offshore or onshore facility. Challenges and recommendations are based on SINTEF's project experience, review of relevant documents, review of audits performed by the Petroleum Safety Authority and input from a PDS workshop on barrier management. An outline of a holistic approach/method for management of safety critical barriers is presented, which will be used as a foundation for the development of a practical industry guideline for overall barrier management. It may also be used for self-assessment of on-going or established barrier management processes, e.g. checking compliance with the recommendations provided in this report. 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
Knut Øien, Stein Hauge, Fred Størseth, Ranveig Kviseth Tinmannsvik

SIGNATURE

CHECKED BY
Lars Bodsberg

SIGNATURE

APPROVED BY
Stian Antonsen, Research Director

SIGNATURE

REPORT NO.	ISBN	CLASSIFICATION	CLASSIFICATION THIS PAGE
SINTEF A26845	978-82-14-05947-2	Unrestricted	Unrestricted

Document history

VERSION	DATE	VERSION DESCRIPTION
Version No. 01	2014-11-10	Draft for PDS member comments
Version No. 1	2015-04-01	Final

Preface

This report is a deliverable from the research project: "Tools and guidelines for integrated barrier management and reduction of major accident risk in the petroleum industry" (2012-15). The project has been funded by the PETROMAKS2 programme for petroleum research at the Research Council of Norway and industry participants of 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
- 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
Eni Norge AS
GDF SUEZ E&P
Odfjell Drilling & Technology
Marathon Petroleum Company (Norway) LLC
Talisman Energy Norge
Teekay Petrojarl ASA
Statoil 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

Consultants / Engineering companies:

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

http://www.sintef.no/PDS

(Empty page)

SINTEF

Table of contents

Executive Summary

Introduction

This report elaborates on and discusses important aspects and challenges related to barrier management during different lifecycle phases of an offshore or onshore facility. It presents an outline of a holistic approach/method for management of safety critical barriers, and it will be used as a foundation for the development of a practical industry guideline for overall barrier management.

Need for barriers and barrier management

The petroleum industry is facing the risk of major accidents, i.e. accidents with major consequences – typically multiple fatalities and/or massive oil spills. Fortunately, such accidents have low probability of occurrence. The reason for the low probability is due to e.g. layers of protection or what is also called "defense in depth". This is achieved through multiple barriers. 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.

Status, challenges and recommendations

The field of barrier management is rapidly evolving. For several reasons there are many existing barrier management approaches and initiatives that differ quite substantially. Some of the challenges which are leading to differences in approach are exploited in this report, and recommendations are provided. The challenges being discussed are:

General challenges

- Interactions between key management processes and stakeholders
- Multiplicity of approaches including the chaos of terms
- The term "strategy" and the implications of the wider interpretation
- Life cycle perspective and framing
- Multiplicity of methods and tools
- The barrier concept, terms and definitions (including delimitation of the concept)
- Communication and consultation with the sharp end; from theory to practice

Specific challenges

- Quality of data for verification of performance requirements in operation
- Organizational dependency between barriers
- Performance requirements for operational and organizational barrier elements

Challenges have also been identified by authorities and industry. Although they partly overlap with the general and specific challenges, they have led to some additional recommendations.

Recommendations and preliminary outline of approach

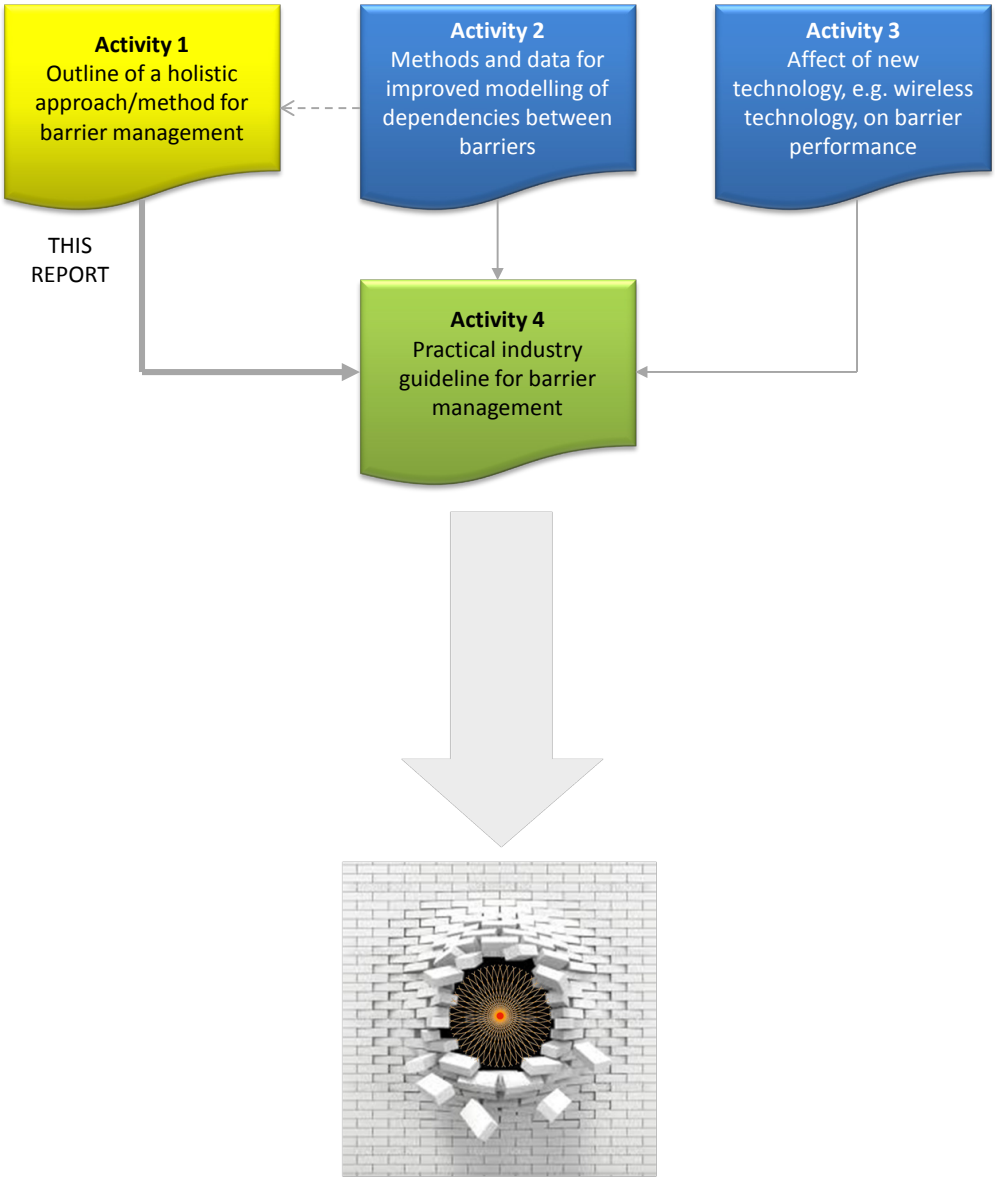
To face the challenges, a total of 18 recommendations have been provided. Challenges and recommendations are based on SINTEF's project experience, review of relevant documents, review of audits performed by PSA and input from a PDS workshop on barrier management.

A preliminary outline of a holistic barrier management approach is presented covering:

1. Barrier management principles and framework
2. Barrier management process and barrier strategy

Further work

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"* (PDS project), funded by the Norwegian Research Council and the members of the PDS forum. The outline of a holistic approach/method for barrier management (Activity 1 in the PDS project) will provide the main foundation for the development of an industry guideline for barrier management (Activity 4 in the project) as illustrated below.



The PDS industry guideline for holistic barrier management aims at contributing to prevent and mitigate holes in the barriers.

1 Introduction

1.1 Background and scope

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[1]. The work has mainly been carried out by SINTEF and may therefore not express the views of all the PDS participants.

The project period is 2012-2015 and it comprises the following five main activities:

1. Development of an overall method for barrier management
2. Development of improved methods and data for modelling of dependencies between barriers and barrier elements, /32/
3. Evaluation of how new technology – and wireless technology in particular – may affect the performance of the barriers, /33/
4. Development of a practical industry guideline for overall barrier management including technical, operational and organisational barrier elements for all relevant lifecycle phases
5. Publication of results

This report documents Activity 1. It elaborates on and discusses important aspects and challenges related to barrier management during different lifecycle phases of an offshore or onshore facility. It presents an outline of a holistic approach/method for management of safety critical barriers.

The report will be used as a foundation for the development of a practical industry guideline for overall barrier management (Activity 4). Thus, Activities 1 and 4 are closely connected.

1.2 Approach

The work is based on experience gained through participation in authority and industry projects on barrier management, review of relevant documents (including e.g. the PSAN "barrier memo" /1/, regulations /2/, 28 PSAN audit reports from 2010-2012 /3/, and industry initiatives such as the DNV GL / NSA "good practices" document /4/), review of barrier performance data (e.g. RNNP data /5/ and company/project specific data in a SINTEF report for PSAN /6/), analyses of accidents with particular emphasis on inadequate barrier management /7/, review of a specific barrier study /8/, discussions with representatives from the industry and a PDS workshop on challenges related to barrier management.

1.3 Limitations

The aim has been to cover the most important aspects and challenges related to barrier management; however, it is obviously not possible to cover all aspects and challenges. There are certainly challenges related to barrier management that is not treated in this report.

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

[1] PDS is a Norwegian acronym for "reliability of safety instrumented systems". For more information about PDS see: www.sintef.no/pds

1.4 Concepts and abbreviations

1.4.1 Barrier and barrier management

One of the key challenges related to barrier management is the concepts, terms and definitions used – or what we have denoted "the chaos of terms". We will return to an elaboration of this in Chapter 3, but we introduce two main concepts in this introductory chapter to enhance the understanding of the topic in question – "barrier management".

The Petroleum Safety Authority Norway (PSAN) has issued a memo; "Principles for barrier management in the petroleum industry" (hereafter referred to as the "Barrier memo") /1/, 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 (/1/, page 1).

The definitions of "barrier" and "barrier management" provided by PSAN /1/ are:

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.*

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

We use the definitions suggested by the authorities as a starting-point. PSAN does not have "monopoly" on what are the most useful definitions; on the other hand it is hardly a disadvantage for operating companies to go along with the regulators.

However, as discussed in Chapter 3, we will challenge some of the existing definitions.

1.4.2 Abbreviations

ATEX	ATmosphere EXplosibles
BM	Barrier Management
BOP	Blowout Preventer
CAP	Critical Action Panel
CMMS	Computerized Maintenance Management System
COSL	China Oilfield Services Limited
C&E	Cause & Effect
D	Design
DFU	See DSHA (Norwegian abbreviation: Definerte Fare- og Ulykkessituasjoner)
DNV GL	Det Norske Veritas Germanischer Lloyd
DSHA	Defined Situations of Hazard and Accident
DU	Dangerous Undetected (failures)
EN	European Norm

EPA	Emergency Preparedness Analysis
ESD	Emergency Shutdown
ESRA	European Safety and Reliability Association
ESV	Emergency Shutdown Valve
FES	Fire and Explosion Strategy
FPSO	Floating Production, Storage and Offloading
HAZID	Hazard Identification
HAZOP	Hazard and Operability Study
HFC	Human Factors in Control
HRA	Human reliability analysis
HSE	Health, Safety and Environment
IEC	International Electrotechnical Committee
ISO	International Standardization Organization
LNG	Liquefied Natural Gas
MR	Management Regulations
NFV	Norw.: Norsk forening for vedlikehold
NORSOK	Norw.: Norsk sokkels konkurranseposisjon
NS	Norsk Standard (Norwegian Standard)
NSA	Norwegian Shipowners' Association
O	Operation
OLF	Norw.: Oljeindustriens landsforening (now: Norwegian Oil and Gas Association)
OCS/OTS	Operational Condition Safety / Operasjonell Tilstand Sikkerhet
PCS	Process Control System
PDS	Norw.: Pålitelighet av Datamaskinbaserte Sikkerhetssystem
PFD	Probability of Failure on Demand
PIF	Performance Influencing Factor
PS	Performance Standards
PSA	Petroleum Safety Authority (= PSAN)
PSAN	Petroleum Safety Authority Norway
PSD	Process Shutdown System
QRA	Quantitative Risk Analysis
RM	Risk Management
RNNP	RisikoNivå i Norsk Petroleumsvirksomhet (Risk Level in the Norw. Petroleum Industry)
SAT	Safety Analysis Tables
SIL	Safety Integrity Level
SINTEF	Stiftelsen SINTEF (full name – no longer an acronym)
SIS	Safety Instrumented Systems
SRS	Safety Requirement Specification
TCS/TTS	Technical Condition Safety / Teknisk Tilstand Sikkerhet
TIMP	Technical Integrity Management Project
λ	Failure rate
λ_{DU}	Failure rate of Dangerous Undetected failures
τ	Test interval

1.5 Report structure

In Chapter 2 we describe the need for and focus on barriers both from the authority and the industry side. Chapter 3 is the main chapter, elaborating on and discussing a range of aspects and challenges related to barrier management. The challenges are grouped in general challenges (Section 3.1), specific challenges (Section 3.2), and challenges identified by authorities and industry (Section 3.3).

Throughout the report we point to some directions or provide recommendations. These recommendations are summarized in Chapter 4, providing a foundation for the development of a practical industry guideline on barrier management. A preliminary outline of an overall approach is presented in Chapter 5, and we end with conclusions and further work in Chapter 6.

2 Need for and focus on barriers

2.1 Need for barriers

The petroleum industry, like the nuclear industry, aviation and others, is facing the risk of major accidents, i.e. accidents with major consequences – typically 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.

The reason for the low probability is due to e.g. layers of protection or what 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" /9/.

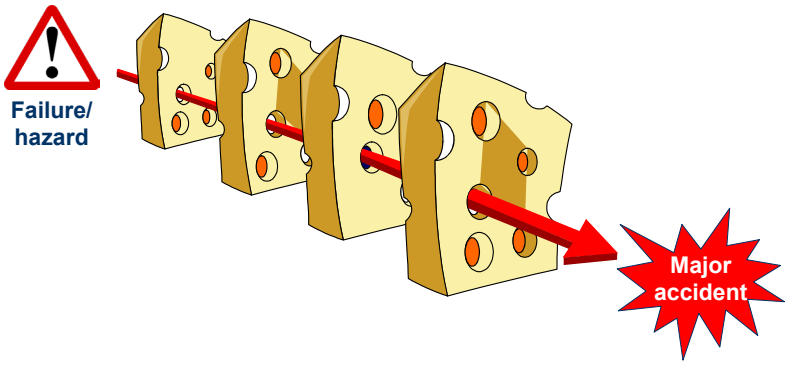


Figure 2.1 Swiss Cheese model (adapted from /9/)

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 /7/.

Copyright: Getty Images

Figure 2.2 The Deepwater Horizon accident in 2010 /7/

To "allow" such events to occur can be seen as an organizational neglect. Investigations of major accidents rarely stop at simple technical failures or human errors, but often identifies multiple weaknesses (e.g. in multiple barriers) with investigations sometimes reaching all the way to the top managers and into the boardrooms (and beyond; e.g. the role of regulations).

2.2 Authority and industry focus on barriers

Top managers' role in major accidents is one reason why PSAN has focused on the top management responsibilities with respect to managing risk of major accidents and also on barriers and barrier management. These two issues have received top priority by the authorities over a period of several years.

Figure 2.3 PSANs four main priorities in 2014 (http://www.psa.no/?lang=en_US) /10/

PSAN has, among other things, issued the before mentioned "barrier memo" /1/, and the industry has responded by a substantial increase in barrier analyses and comprehensive barrier management projects. Also, some collective effort has been made, such as the DNV GL / NSA "Good practices" for barrier management in the rig industry /4/. Finally, some more specialized reports have been produced on the topic of barrier management, such as the SINTEF report on the role of maintenance in barrier management /6/.

Figure 2.4 Examples of barrier management documents within the Norwegian Petroleum Industry /1/, /4/, /6/

3 Status, challenges and recommendations

The existing barrier management approaches differ quite substantially for several reasons[2]. Some of the main challenges that cause these differences are further exploited in this document:

- Interactions between key management processes and stakeholders
- Multiplicity of approaches including the chaos of terms
- The term "strategy" and the implications of the wider interpretation
- Life cycle perspective and framing
- Multiplicity of methods and tools
- The barrier concept, terms and definitions (including delimitation of the concept)
- Communication and consultation with the sharp end; from theory to practice

The term "sharp end" may not be familiar and deserves an explanation; see Fact box 1.

Fact box 1: The sharp end – blunt end dichotomy (from http://patientsafetyed.duhs.duke.edu/module_e/vocabulary.html /11/)

Processes may be referred to as having sharp and blunt ends.

- **Sharp end** – the actualizer of the process – the person actually doing the task (e.g., the nurse administering a medication; the surgeon holding the scalpel).

- **Blunt end** – parts of the process farther away from the action itself. At its extreme, the blunt end is the environment in which we deliver healthcare. Regulators, accreditors, administrators, and designers function at the blunt end.

In between are many other steps and factors influencing the sharp end's operation.

In the petroleum industry the control room operators and maintenance personnel (e.g. mechanics and electricians) are typically at the sharp end, whereas e.g. the maintenance planners are at the blunt end.

[2] The title "Towards a holistic approach for barrier management in the petroleum industry" indicates that we are (still) on the way towards a unified holistic approach. There is a need for convergence and consensus, although some differences will remain and provide flexibility.

In addition to these general challenges which need to be resolved through convergence in the industry, there remain some challenges that are independent of the chosen approach. In this document we will outline such challenges related to:

- Quality of data for verification of performance requirements in operation
- Organizational dependency between barriers
- Performance requirements for operational and organizational barrier elements

Finally, we include challenges identified by authorities and industry leading to additional recommendations:

- Challenges identified in audits performed by the authorities
- Challenges identified in a well control study
- Challenges identified in a PDS workshop

3.1 General challenges and recommendations for barrier management

3.1.1 Interactions between key management processes and stakeholders

Key management processes and associated stakeholders with different interests and views are indicated in Figure 3.1.

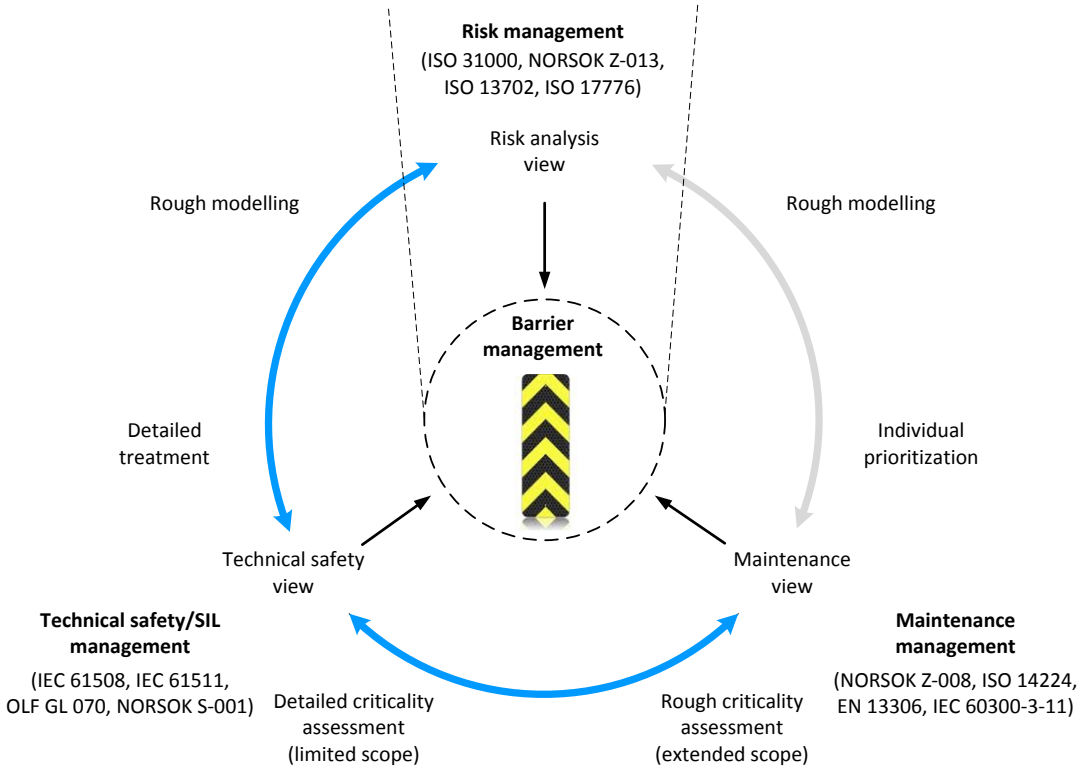


Figure 3.1 Key management processes and associated stakeholders in barrier management

Three key stakeholders are (1) those involved in the risk management process, since barrier management is part of risk management; (2) those working with technical safety, including safety instrumented systems (SIS); and (3) those responsible for maintenance management, in particular the establishment of the maintenance program (maintenance activities and intervals).

We will return to a detailed explanation of Figure 3.1, but first, we introduce the interactions as simplified parallel processes, as shown in Figure 3.2.

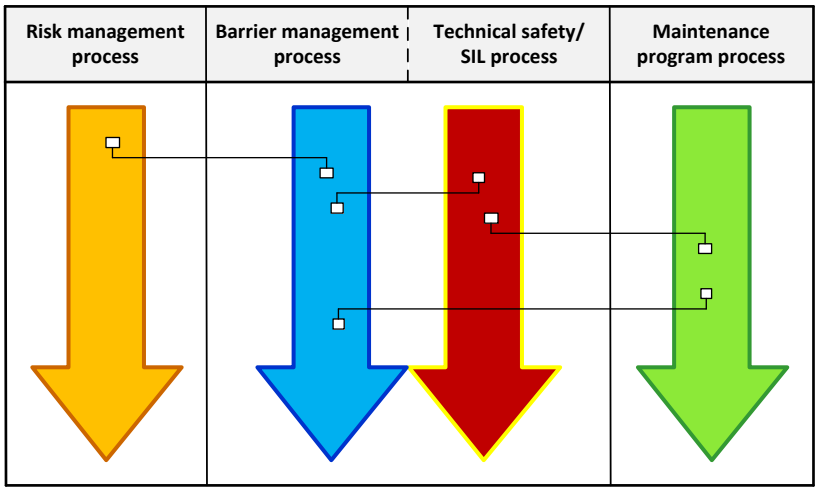


Figure 3.2 The barrier management process link with other interacting processes

Technical safety management, including the "SIL process"[3], is indicated as closely connected with the barrier management process. Safety instrumented systems are an important sub-class of barrier systems. However, it may not be the case in practice that the "SIL process" is carried out as an integral part of the barrier management process. Rather, as we have experienced, the "SIL process" has been run separately and independently from both the barrier management process and the maintenance management process.

Also the barrier management process is run disintegrated from the risk management process and the maintenance management process. In some cases different staff and different consultants are responsible for the risk management process versus the barrier management process.

Recommendation 1

The SIL process should be integrated in the barrier management process, and both processes should be an integral part of the risk management process. These processes also need to be coordinated with the maintenance management process.

The level of detail in the descriptions of the barrier management process varies to a great extent between the various projects/companies, some being overly detailed. If detailed descriptions/illustrations are considered necessary, they should be accompanied with some overview illustrations as well (similar to, but not as "overly simplified" as Figure 3.2) to ease the understanding and avoid getting lost in details. This is also related to life cycle framing (Section 3.1.4) and communication with the sharp end (Section 3.1.7).

Recommendation 2

Comprehensible descriptions of the barrier management process should be provided. Detailed descriptions/ illustrations should be accompanied with overview illustrations.

[3] It may be more correct to use the term "SIS process" and "SIS management". However, we have used "SIL process" throughout this report.

We now return to an explanation of Figure 3.1. Barrier management, the core issue of this report, is as indicated in Figure 3.1 an integral part of risk management. The risk management process, including the identification of hazards and the establishment of the overall risk picture, has an extensive scope in covering all hazards and risks for an entire installation (/12/-/15/).

However, considering the interactions with the safety systems (/16/-/18/, /26/) and the maintenance activities (/19/-/22/), they are (presently) only roughly modelled in the quantitative risk analysis (QRA). Thus, there is a limited integration of safety systems and maintenance activities in the QRA due to insufficient level of details in the risk models.

The safety systems, in particular the safety instrumented systems (SIS), are modelled and analyzed in far more detail than what is captured in the QRA. This includes issues such as configuration/redundancy, voting, etc. Performance requirements such as safety integrity levels (SIL) are established, which implicitly expresses the criticality of the system or element, but (normally) without being reflected in the QRA. However, the scope of analysis is limited compared to the QRA, focusing only on some of the systems on an installation.

All maintainable items on an installation need to be classified based on "criticality", whether or not this includes only consequence classification or also probability assessments (i.e. risk based classification). The importance of the individual items, reflected in the extent of planned maintenance activities and prioritization of corrective maintenance, are established on an individual basis using e.g. simple risk matrices (as prescribed in NORSOK standard Z-008 /19/). The QRA is not detailed enough to be feasible as a basis for classification or prioritization.

Safety instrumented systems with SIL requirements need to be verified during operation through functional testing. The test intervals are established based on the SIL requirements and the anticipated failure rates. Thus, some of the information needed for these systems in the maintenance program can be directly transferred from the technical safety management process (from the safety requirement specification – SRS).

3.1.2 Multiplicity of approaches including the chaos of terms

To describe the barrier management approach terms like barrier management process, framework and strategy are common, but it does not stop here; as indicated in Figure 3.3.

Figure 3.3 The chaos of terms

This jungle of terms certainly represents a challenge in the communication between the blunt and the sharp end (cf. Section 3.1.7); in that they are struggling to understand the differences and connections between these terms. This is also related to the specific challenge of the duality in the meaning of the term "strategy", which is treated separately in Section 3.1.3, and it is related to the barrier concept, terms and definitions (treated in Section 3.1.6).

Throwing all the different barrier related terms together, the picture becomes a real mess, as shown in Figure 3.4 (from /27/).

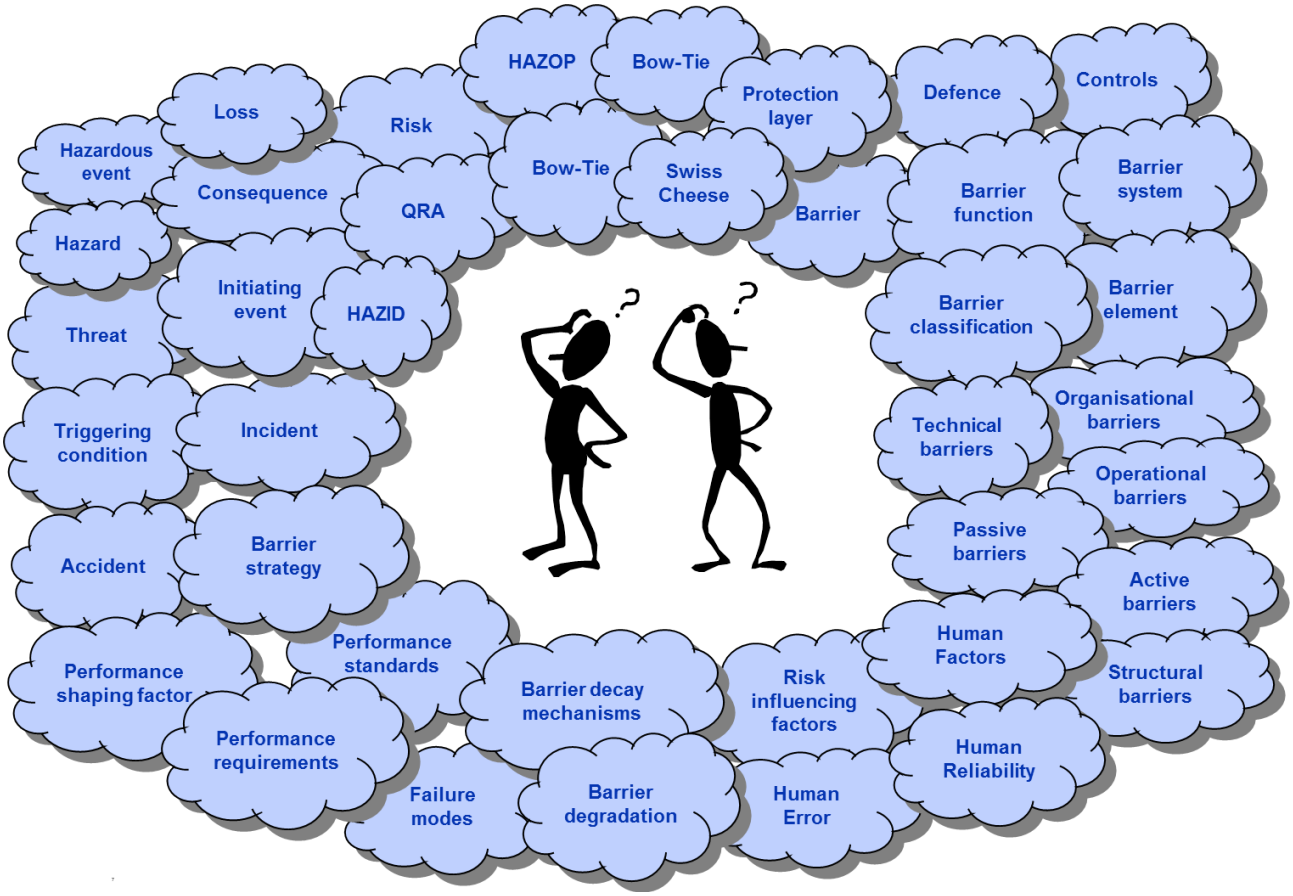


Figure 3.4 Barrier – the "fuzzy" concept (from /27/)

Using different terms may also contribute to a perceived difference of approaches, which is actually more about differences in terms, than genuine differences in approaches. Still, there are also genuine differences in approaches; there is no common approach for barrier management in the petroleum industry, one reason being the range of possible methods and tools for barrier analyses cf. Section 3.1.5.

One single common approach is probably not an achievable goal, but exchange of ideas and experience in conferences, seminars and workshops may support convergence towards a few suitable approaches.

We will return to an outline of a recommended barrier management approach in Chapter 5.

3.1.3 The term "strategy" and the implications of the wider interpretation

The term "strategy", used in *barrier strategy*, has caused profound confusion in the industry, both at the sharp and the blunt end.

In common language "strategy" is thought of as high level plans and principles (cf. Fact box 2), whereas in some areas (such as barrier management and emergency preparedness) the term has a quite different and wider meaning. It refers to "the documentation of the process and results", see Fact box 2.

Fact box 2: Strategy – the dual interpretation (from http://en.wikipedia.org/wiki/Strategy, /23/ and /1/)

> **Strategy** (in general) /23/:
>
> Strategy (from Greek στρατηγία stratēgia, "art of troop leader; office of general, command, generalship") is a high level plan to achieve one or more goals under conditions of uncertainty.
>
> **Barrier strategy** /1/:
>
> 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]
>
> [1] See NS-EN ISO 13702, referenced in the guidelines to section 5 of the management regulations and the way "fire and explosion strategy" (FES) is defined: "Results of the process that uses information from the fire and explosion evaluation to determine the measures required to manage these hazardous events and the role of these measures". In other words, "strategy" is used in a special sense in a barrier context. …

The wider[4] interpretation of the term strategy has implications for the documentation of the barrier management process, as discussed below.

The Management Regulations Section 5 on Barriers states (third and fourth subsection) /2/:

The operator or the party responsible for operation of an offshore or onshore facility, shall stipulate the strategies and principles that form the basis for design, use and maintenance of barriers, so that the barriers' function is safeguarded throughout the offshore or onshore facility's life.

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 technical, operational or organisational elements necessary for the individual barrier to be effective.

The Guidelines regarding the Management Regulations Section 5 on Barriers states (regarding the third and fourth subsection) /24/:

The strategies and principles as mentioned in the third subsection, should e.g. be designed so that they contribute to provide all of the involved parties with a common understanding of the requirements for the

[4] By "wider" is meant that the principles and philosophies, which is normally considered a "strategy", is a short high level document, whereas the strategy document in the wider interpretation – covering the documentation of the process and results – becomes something much more than just a high level plan; it is a voluminous document or documents. (However, some may see it as having a more *specific* meaning, even though it is more extensive).

individual barriers, including the connection between risk and hazard assessments and requirements for and relating to barriers. Barriers can also be measures designed to prevent or limit the spread of acute pollution.

The NS-EN ISO 13702 standard should be used for development and stipulation of strategies for risk reducing measures and functions. IEC 61508 should be used for safety systems. In addition, Norwegian Oil and Gas Association Guideline 070 should be used as a basis for offshore petroleum activity.

The regulations refer to the NS-EN ISO 13702 standard /14/, and this standard introduces the "wider interpretation" of the term strategy. The standard introduces the concept of strategies but states that such strategies do not have to be separately documented, as the relevant information may be included with other HSE information for an installation or may be contained in recognized codes and standards that are relevant to the operating location. Indeed there can be significant overlap between strategies and other HSE information, so that combining this information into one source can enable people on the installation to understand how the various measures are integrated.

This may lead to at least two documents; one on principles (and framework) and one documenting the process and results (which in turn can point to various other documents, i.e. the strategy may not be documented in only one document). Also, it is common to have one document containing the specific requirements, i.e. the performance standard (PS) document(s), which should be e.g. installation and area specific (not just a copy of the NORSOK S-001 standard /18/)[5]. This is illustrated in Figure 3.5.

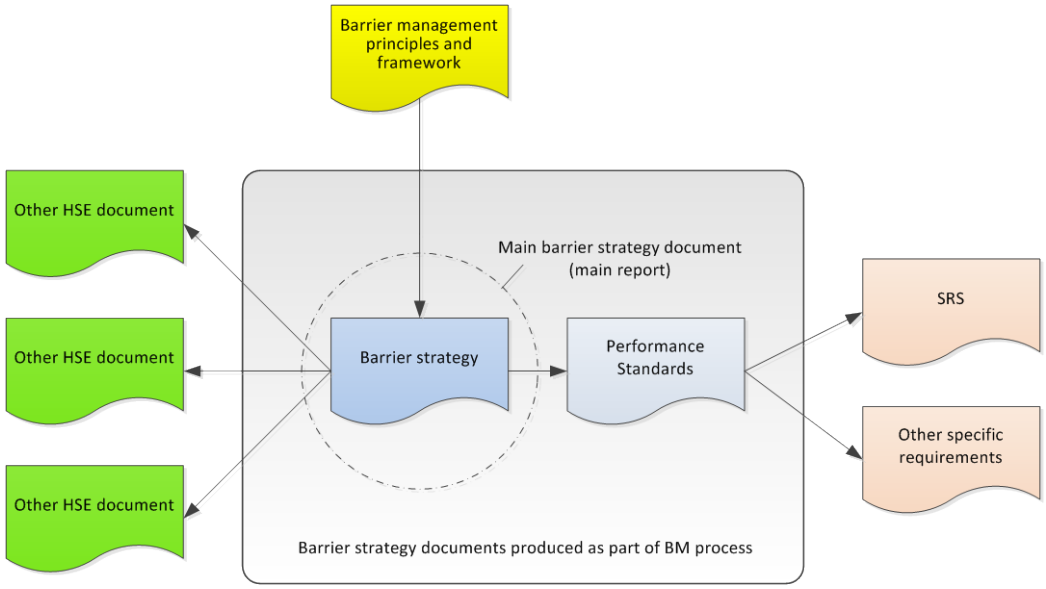


Figure 3.5 The barrier strategy documents

"Strategies and principles" (referred to in the Management Regulations Section 5) should first be divided in two parts; preferably two documents. The first document should cover high level guiding principles and framework, which should be a short document not needing frequent updating. This document could also be termed barrier philosophy, and it could be a separate document on company level applicable for all projects/ installations[6]. The second document should be the main report for the barrier strategy linking all documents, studies and analyses together.

[5] This is stated in the regulations (guideline to the Management Regulations, section 5 on barriers): "*The strategies and principles as mentioned in the third subsection, should be broken down to a convenient level, e.g. area level on the individual offshore or onshore facility …*".

[6] This company level document may also include a description of the barrier management process.

The detailed barrier/barrier element requirements can be quite comprehensive, at least when entering the operations phase, and it will be appropriate to document them in a separate document(s) (Performance Standards) or some kind of register/database.

Figure 3.5 indicates that some of the documents are produced as part of the barrier management (BM) process; whereas other documents are related to the barrier strategy or the performance standards: These other documents, such as the Safety Requirement Specification (SRS) for equipment with SIL requirements, should be referred to and included in the recording of the barrier management process and results.

3.1.4 Life cycle perspective and framing

Barrier management starts from the early design phases and carries on into the operations phase. Some approaches and guides advocate a distinction between establishing/implementing barriers and operating them, i.e. two distinct phases or work processes, whereas others also distinguish between early design and detailed design phases (in establishing/implementing barriers), thus having three main phases.

The life cycle phases or iterations of analyses are sometimes described in loops (as illustrated in Figure 3.6 and emphasized in Figure 3.7), whereas others use vertical or horizontal flowcharts (as illustrated in Figure 3.8). For the illustration of loops/iterations we use the ISO 31000 based PSAN figure (from the "barrier memo" /1/).

Before introducing the PSAN figure with loops/iterations (Figure 3.7), we will show how PSAN describes the barrier management (BM) process as an "integrated extension" of the risk management (RM) process from ISO 31000 /12/. This is shown in Figure 3.6.

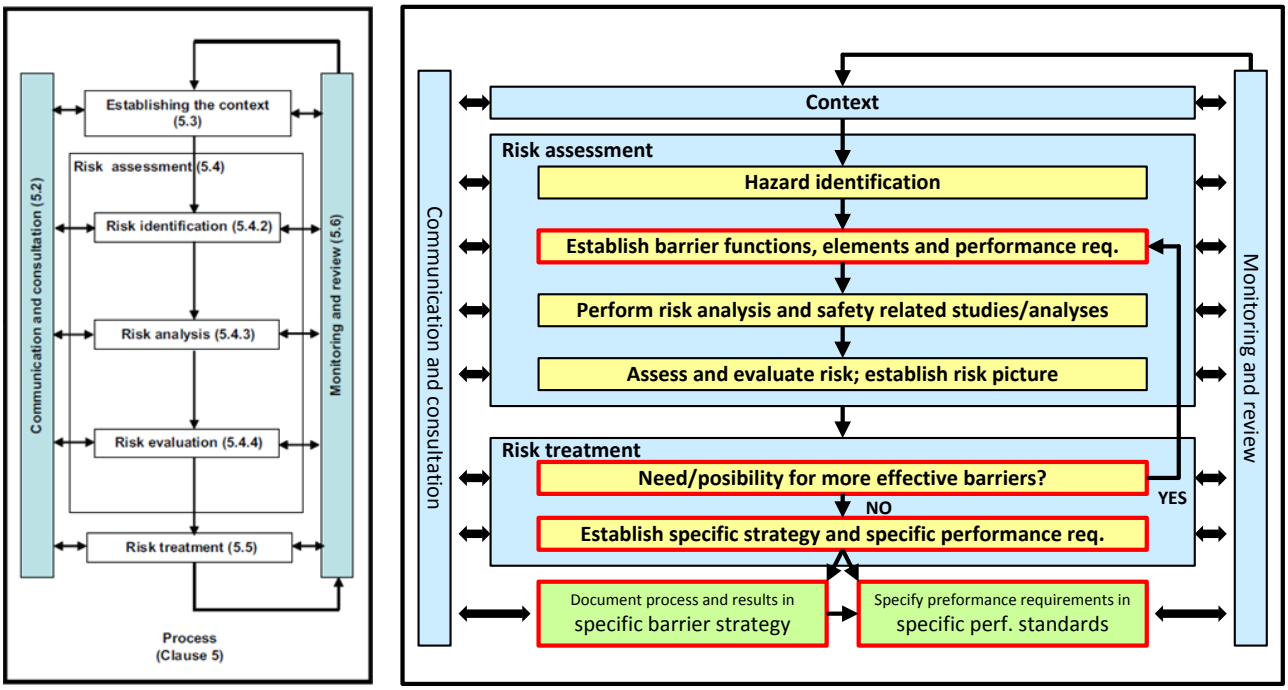


Figure 3.6 RM process from ISO 31000 /12/ versus RM+BM process from PSAN /1/

The steps which explicitly emphasize the barrier management related activities in the PSAN figure are highlighted with red frames. The first step is the second box within risk assessment ("establish barrier functions, barrier elements and performance requirements"). This is inserted in between the two first steps of

risk assessment in ISO 31000. Prior to risk analysis not only hazards need to be identified, also the barriers must be decided on (e.g. in order to model branches in the event trees in the QRA[7]).

In risk treatment, one measure to reduce risk is to provide more effective barriers. The result and process (related to the BM process part) is documented in the specific barrier strategy and specific performance requirements are established and documented in performance standards. These two documents are illustrated as green boxes in the PSAN figure (and as blue boxes/shapes in Figure 3.5).

In Figure 3.7 we have removed the emphasis on the specific BM steps, and rather focused on the loops/ iterations explaining the time development of the BM process during various life cycle phases.

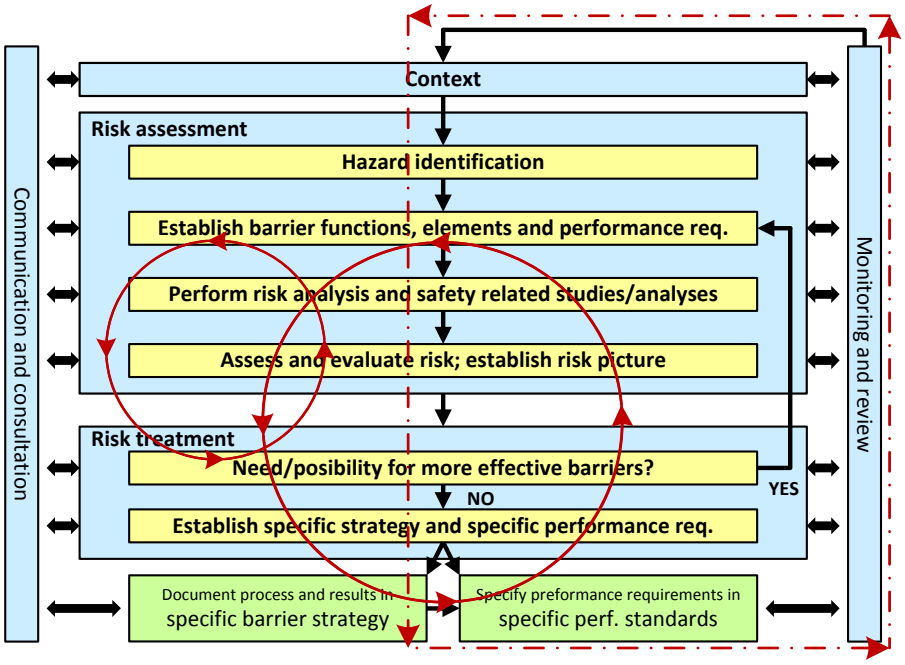


Figure 3.7 Loops indicating iterations throughout various life cycle phases

The small red circular loop includes more effective barriers iteratively until there is no more need for or no possibility for more effective barriers.

The large red circular loop is repeated for each phase and each update of the barrier strategy and the performance standards. The first established barrier strategies and performance standards will typically focus on technical barriers, whereas in later phases (e.g. in preparing for operations) also operational and organizational elements are included.

The red rectangular loop indicates the monitoring and review (and necessary updating) during the operations phase.

When describing the barrier management process, it is useful to use some graphical presentations (similar to what is principally shown in Figure 3.8), but it is a question how comprehensive the interactions with other management processes shall be illustrated/described. In some cases only the BM process is shown, in other cases the RM and BM process, and sometimes even the SIL process is added to the RM and BM processes.

[7] We use the term "QRA" also for risk analyses in early life cycle phases, although other terms are often used.

Also other processes, such as the process of establishing the maintenance program could be included, as shown in Figure 3.8. If not illustrated graphically, there should at least be some short description of the interactions between the BM process and the main interfering processes.

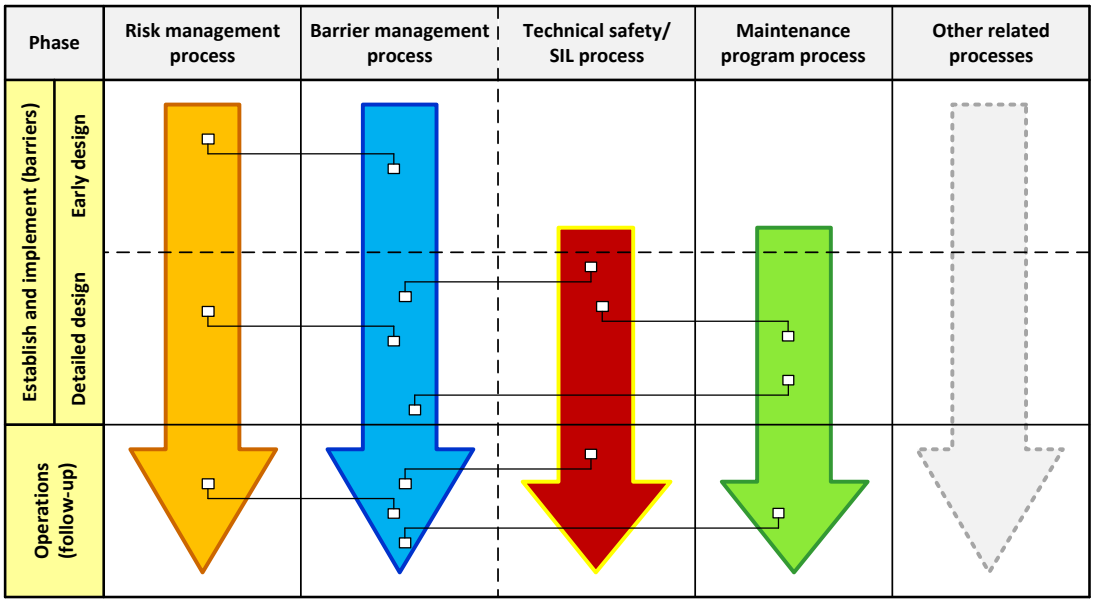


Figure 3.8 "Lanes" passing through various life cycle phases (vertically)

The "lanes" in Figure 3.8 are only illustrated principally, and they could also be turned horizontally (i.e. "swim lanes" as used in work process diagrams) for each process along a horizontal time (life cycle phase) axes.

In Figure 3.8 it is indicated with a dashed vertical line that the SIL process could be seen as part of the BM process, or considered separately. A dashed line is also used for the life cycle phases to indicate that sometimes the design phase is considered as one phase, not distinguishing between early and detailed design.

One challenge with the explicit illustration of phases and processes in vertical or horizontal lanes is the link to other processes such as the risk management process and the impression that analyses, e.g. the QRA, are updated once in each phase concurrently with the barrier analyses. This may lead to a false impression, since the various analyses are updated at different "speed", and not necessarily concurrent.

The loops in Figure 3.7 indicate iterations, but they do not indicate a certain number of updates, which in some sense is more correct. On the other hand, a better alignment between the various interrelated processes should be aimed at, since e.g. PSAN firmly states that BM is an integral part of RM.

Recommendation 3

The links between risk management, barrier management, maintenance management and other interrelated processes should be described and illustrated.

As discussed in Section 3.1.1, the level of detail in the descriptions/illustrations of the processes varies to a great extent. Necessary details should, as already mentioned, be accompanied by some simple overview descriptions/illustrations, i.e. gradually increasing the level of detail.

Relatively detailed process illustrations/descriptions are sometimes termed "work processes". This may be confusing. A barrier management process consist of activities or steps, whereas a work process usually should include much more details, e.g. "who is doing what and when". If it is considered necessary to define work processes for the work carried out as part of the barrier management process, this should be seen as a separate activity to the barrier management process.

A work process description is not a replacement for the barrier management process description, which can be seen as a description of the "overall methodology". Specific methods and tools, which will be described in Section 3.1.5, are means to solve single steps or activities in the process.

ISO 31000 /12/ distinguishes between risk management principles, framework and process. A similar distinction can be made for barrier management. This is illustrated in Figure 3.9.

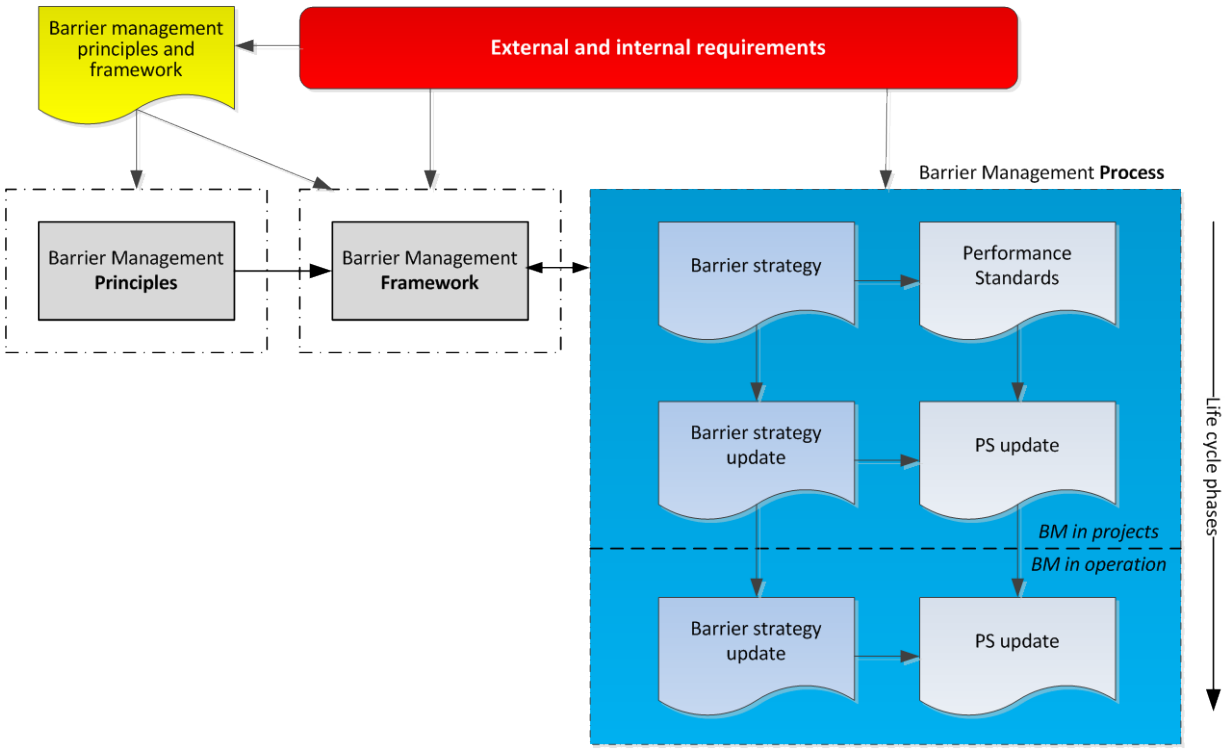


Figure 3.9 Barrier management principles, framework and process

The barrier management principles provide guidance for the establishment and implementation of the barrier management framework as well as the barrier management process. The barrier management process is run for each project establishing and updating the barrier strategy and performance standards in the various life cycle / project phases.

A specific overview (example) of a holistic barrier management framework (from Statoil) is illustrated in Figure 3.10 /28/. This illustration also shows the red thread from the risk picture, through the safety strategy (including the barrier strategy; sometimes termed *safety and barrier strategy* or just *barrier strategy*) and the performance requirements, down to the maintenance and verifications processes. Thus, the TRA (QRA) is highlighted compared to other safety studies and analyses, and it provides the links referred to in recommendation 3 above.

Figure 3.10 Example of (overview of) holistic barrier management /28/

Although the maintenance of technical equipment is important, also "maintaining" operational and organizational barriers should be included, e.g. managing competence and training of personnel.

The barrier management process needs detailing in specific steps or activities for each phase included. An example of this is shown in Figure 3.11, taken from the DNV GL / NSA "Good practices" document /4/.

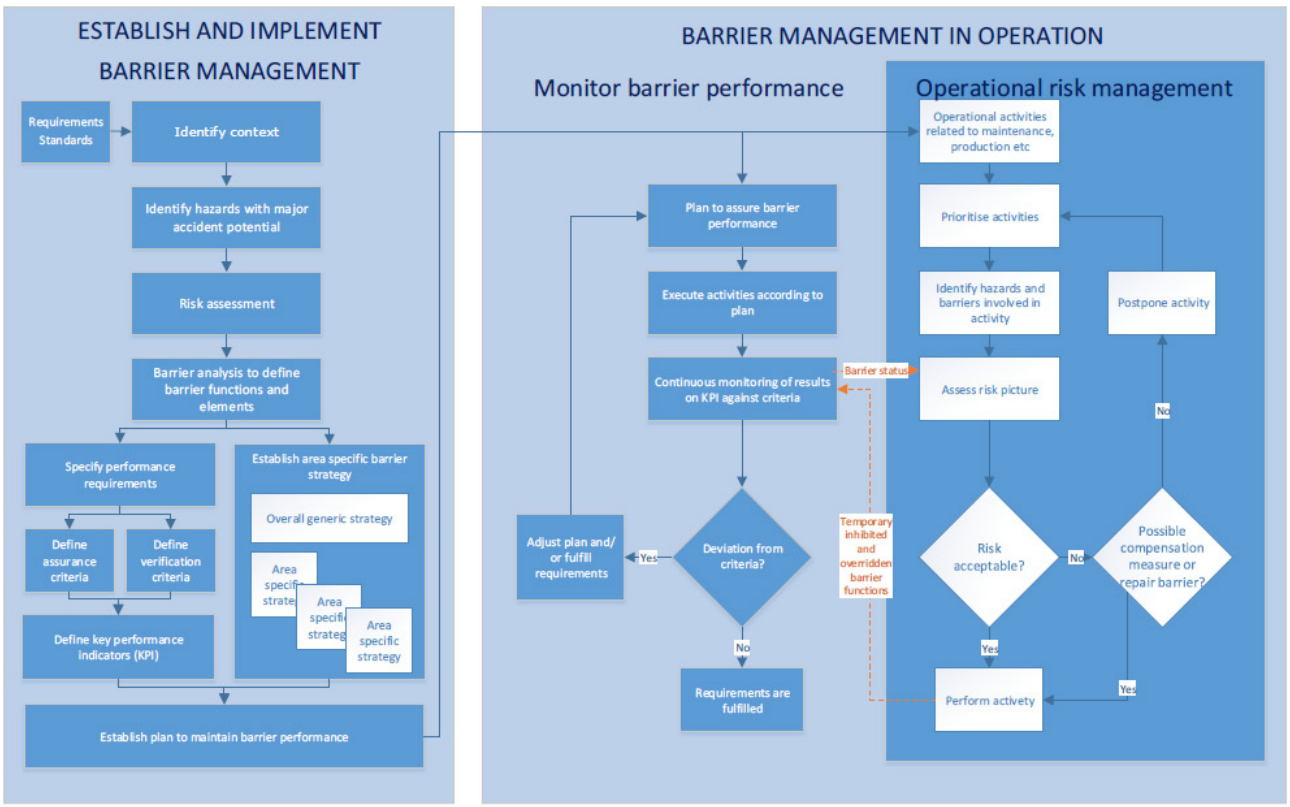


Figure 3.11 Barrier management in the DNV GL / NSA "Good practices" report /4/

This is similar to the way PSAN describes it in the "barrier memo" /1/, where they distinguish between two main phases (establish and implement barrier management versus barrier management in operation), they integrate BM in RM, and they use loops to illustrate the iterations – not timelines.

Another way would be to provide details to Figures 3.8 and 3.9 and either use two or three main phases. This will allow for the inclusion of related studies and documents; however, as stated before (in Section 3.1.1), if the illustration is too detailed, it is recommended to provide an overview figure first.

Following-up and maintaining barriers during operation
Within the operations phase of the life cycle we can have both short term and long term perspectives for the follow-up of barriers. This is illustrated in Figure 3.12.

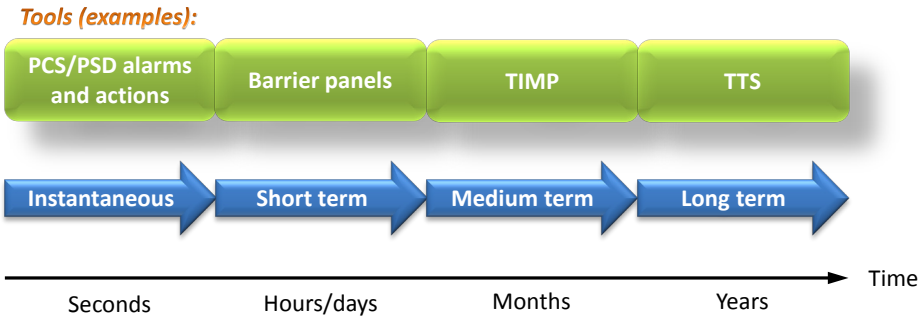


Figure 3.12 Follow-up of barrier status during operation

The status of technical barriers related to process accidents is provided instantaneously through the process control system, if they are needed (demanded). I.e. on a demand (barrier system activation) the control room operators will see whether the barriers are functioning or not (at least for the barrier elements with status feedback).

Such status information from the process control system and from dedicated condition monitoring systems may also be transferred to a barrier panel on-line. In addition, barrier panels extract information from the maintenance management system (CMMS) and other systems (if relevant and available[8]), usually with some short delay.

Some tools collect, combine and assess (quality assures) barrier information in a medium term perspective. One example of this is TIMP (Technical Integrity Management Project) /28/. Information through indicators forms the basis for technical assessment by experts, as illustrated in Figure 3.13.

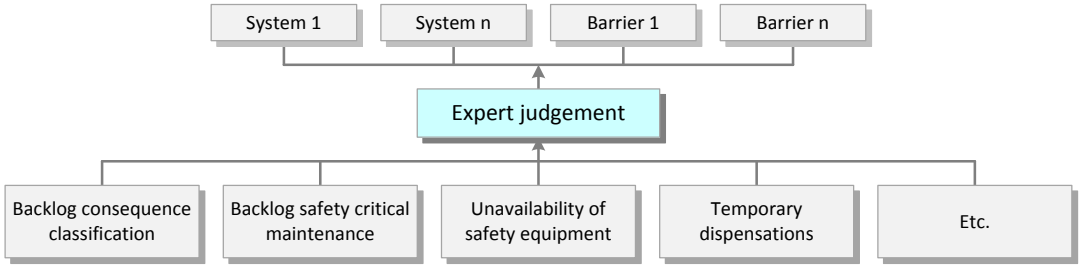


Figure 3.13 Manual/expert assessment of the status of equipment, systems and barriers (based on /28/)

[8] One issue here is the inclusion of non-technical information, i.e. information on the status of operational and organizational barriers from e.g. the competence management system.

The result is presented in a generic bow-tie diagram as illustrated in Figure 3.14 /28/.

Figure 3.14 TIMP visualization of technical barrier status /28/

This information may be updated on a bi-monthly basis (i.e. a medium term perspective).

Finally, detailed verifications of barrier systems are carried out by many companies using a TTS/TCS (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 similar review of defined barrier functions and systems is performed every 2nd year (i.e. a long term perspective). Operational issues can be assessed in a similar manner using e.g. OTS/OCS (Operational Condition Safety) /29/.

Barrier management needs to cover both long term and short perspectives. One perspective does not exclude the other, e.g. TIMP type of medium term perspective does not exclude or cover the need for a barrier panel. A barrier panel provides information that is needed on a daily basis for e.g. planning of work and work order approval, whereas TIMP captures threats to the barriers that may gradually increase over some time. A barrier panel may also provide trends and can therefore also show how the status of the barriers develops over time.

Immediate actions, manually or automatically, are taken care of by the process control system, the process shutdown system, the emergency shutdown system, the fire and gas system and the control room operators, without the need to rely on barrier panels or longer term methods/tools. However, information about the current status of barriers, as presented in a barrier panel, is not only useful for the control room operators. It is also useful information for e.g. maintenance personnel in planning and preparing for maintenance activities.

3.1.5 Multiplicity of methods and tools

There is a whole range of methods and tools used for barrier analyses as part of barrier management (e.g. functional analysis, barrier grids, etc.). In addition there are methods and tools for presenting the results, such as barrier panels.

The choice of methods is mainly a matter of preference, but (unfortunately) also a matter of thorough understanding of the analyst(s). Some relevant requirements related to choice of method are:

1. All major accident types / DSHAs with major accident potential must be identified/included
2. The barrier analyses must cover the entire installation
3. The barrier strategy and performance requirements need to be area specific
4. The barrier analyses should be transparent and traceable

5. The methods and tools or the presentation of them should be easy to communicate/verify
6. The methods and tools should be non-ambiguous

It is particularly important to consider how to communicate the intermediate barrier analyses results with operational and technical experts, such that the analyses can be verified. It is not a good solution to send thousands of lines of results in the form of spreadsheets or databases and expect operating personnel to verify the results.

Recommendation 4

The methods and tools used for barrier analyses should be suitable for communication with operating personnel and technical experts in order to verify the analyses.

It is necessary to ensure not only that the barrier elements identified and their attributes are correct, but also that all relevant barrier elements have been identified, which requires suitable methods/tools. It will often be beneficial to apply two different approaches in order to check for consistency between the results.

Recommendation 5

The methods and tools used for barrier analyses should be suitable for systematic identification of all relevant barrier elements (e.g. by the use of "triangulation" or at least two comparative methods).

It is also important to provide "a red thread" in the analyses starting from the identified hazards in the risk analysis all the way to the individual barrier elements including performance requirements, verification methods and verification intervals[9].

Recommendation 6

The methods and tools used for barrier analysis should ensure that the area specific barrier strategy and the area specific performance standards provide a common thread from the identified hazards and potential major accidents to the individual barrier elements and their attributes (e.g. performance requirements, verification method and test interval).

3.1.6 The barrier concept, terms and definitions (including delimitation of the concept)

Explanations of the barrier concept can be found in the Management Regulations, cf. Fact box 3.

PSAN has also provided definitions in the "barrier memo" /1/ and accompanying documents/presentations. Still, there are some challenges related to the delimitations and categorizations of the barrier concept. More specifically the following questions puzzle the industry:

1. How can we distinguish between barriers/barrier elements and performance influencing factors? (Is e.g. maintenance a barrier or a performance influencing factor?)
2. At what point in an accident sequence do we activate or rely on barriers, compared to the use of control measures as part of normal operation (not being defined as barriers)?

[9] In some cases the term "verification" is used whether this is carried out internally or externally, whereas others distinguish between assurance activities as internal activities and verification activities as external/independent activities, cf. e.g. /4/ and /31/. In this report we have not distinguished between assurance and verification activities.

3. Is it useful to distinguish between operational and organizational barrier elements, or is it sufficient with two categories; technical and non-technical (or human or operational or some other name)?

Fact box 3: Barriers – as described in the regulations /2/[10]

Management Regulations
Section 5
Barriers

Barriers shall be established that:

a) reduce the probability of failures and hazard and accident situations developing,

b) limit possible harm and disadvantages.

Where more than one barrier is necessary, there shall be sufficient independence between barriers.

The operator or the party responsible for operation of an offshore or onshore facility, shall stipulate the strategies and principles that form the basis for design, use and maintenance of barriers, so that the barriers' function is safeguarded throughout the offshore or onshore facility's life.

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 technical, operational or organisational elements necessary for the individual barrier to be effective.

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

The responsible party shall implement the necessary measures to remedy or compensate for missing or impaired barriers.

The two first questions are somewhat influenced by PSAN's desire to restrict the barrier definition and avoid a too wide definition. They state the following in the "barrier memo" /1/:

There is little point in including or considering "everything of importance" as barriers or barrier elements. Such an interpretation will not contribute to more conscious barrier management and follow-up.

Both of the aspects raised in the two first questions will influence the extent of what is considered as barriers.

1. Barrier/barrier elements versus performance influencing factors

As already stated above, PSAN advocates a restriction in what is considered as barriers compared to performance influencing factors. They e.g. explain why maintenance should be considered as a performance influencing factor and not a barrier.

DNV GL / NSA do the same in the "Good practices" document /4/ illustrating this with a bow-tie as shown in Figure 3.15.

[10] The description of barriers in the Management Regulations Section 5 has recently (from 01.01.2015) been changed to a "wider definition". We will return to this.

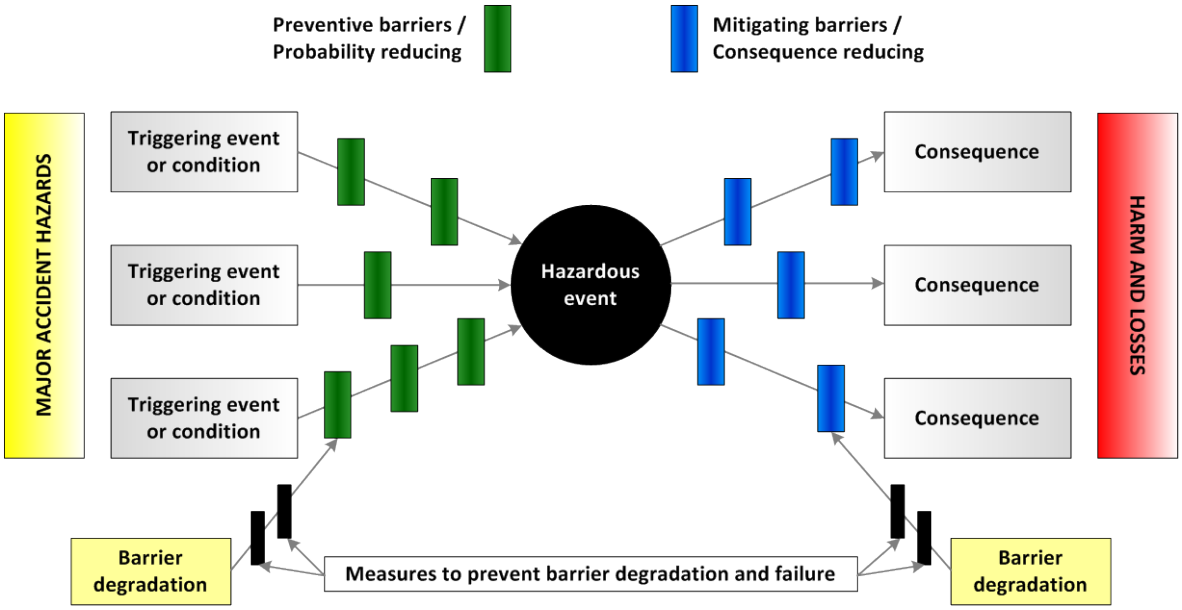


Figure 3.15 Distinction between barriers and performance influencing factors /4/

Figure 3.15 is a generic bow-tie diagram in which a certain hazardous event (placed in the center) can have several causes or triggering events/conditions (to the left) and result in a spectrum of consequences (to the right). The probability or likelihood of the hazardous event depends not only on the triggering events/ conditions, but also on the probability reducing barriers (green barriers). The consequences depend on the consequence reducing barriers in place (blue barriers).[11] The green and blue barriers are (real) *barriers*.

At the bottom of Figure 3.15 there are some "black barrier symbols", which are actually not "real barriers". Rather they are measures to prevent barrier degradation and failure, i.e. they are what PSAN denotes *performance influencing factors;* one example being maintenance, another example being competency.

There is probably agreement about the need to distinguish between barrier/barrier elements and factors that only influence the performance, i.e. performance influencing factors, but there is still some disagreement about "what to put in which basket". If we take the example of maintenance, some will claim that a barrier cannot be realized if it has not been properly maintained, simply because it will not work, which means that maintenance is a necessary prerequisite for the realization of a barrier. This is in a sense true, but *at the time of realization of a barrier*, maintenance should not be carried out "there and then". It must be carried out in advance. There is no time for maintenance actions during realization of a barrier. Thus, maintenance influences the probability of successful realization of the barrier function, e.g. closing a valve, which means that it is a performance influencing factor.

The "disagreement" we mentioned above is probably caused by a belief among some performance influencing factor (PIF) stakeholders that "their" area of responsibility (e.g. maintenance or some organizational factor) will obtain more attention if it is defined as a barrier/barrier function. They fear that

[11] One challenge with the bow-tie diagrams is that they are often taken "too literally", immediately considering a specific event as the hazardous event (center event). In an accident sequence there are a sequence of events (e.g. overpressure, gas leak, fire, and explosion) and which barriers to consider as probability reducing versus consequence reducing depends on the event placed in the center of the diagram. Thus, in general it is too simplistic to just distinguish between probability reducing and consequence reducing barriers. The consequence reducing barriers for one event can be probability reducing barriers for the next event in the sequence.

"their PIF" will be neglected, since PSAN also stresses (in the "barrier memo" /1/) that it is the barrier elements that need to be assigned performance requirements, not the performance influencing factors.

This is probably an unfounded fear, since the PIFs are used indirectly as part of the performance requirements. If for example a SIS element (e.g. an ESV) has a SIL requirement, this is translated to a certain probability of failure on demand (failure fraction) with a corresponding functional test interval. Thus it is required by the maintenance function to carry out functional testing according to the assigned test intervals.

The same is true for e.g. training as a PIF for organizational barrier elements.

However, it is not our intention to give the impression that the distinction between barrier/barrier elements and PIFs is always easy. There may well be cases (and hazards[12]) where it is difficult to decide which basket to put them in, but this should be sought solved logically and pragmatically and not politically (i.e. not because someone think it is strategically smart rather to have their PIF defined as a barrier/barrier element than "simply" as a PIF).

2. Control measures versus barriers

If we consider the descriptions of barriers in the Management Regulations in detail, it is reasonable to claim that barriers come in addition to "something else". The Management Regulations Section 4 on Risk reduction says /2/:

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 probability that harm, errors and hazard and accident situations occur.

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

"Furthermore" (underlined by authors) indicates that barriers comes in addition to what is stated in the first paragraph.

A similar hint can be obtained from the Management Regulations Section 5 on Barriers /2/, which says:

Barriers shall be established that:

a) reduce the probability of failures and hazard and accident situations developing,

b) limit possible harm and disadvantages.

"Developing" (underlined by authors) can be interpreted as "further developing", i.e. from an initial failure or hazard towards an accident.[13]

Based on this we will claim that barriers are something that shall not be used at all hours, but to stop specific accident sequences. Normal operation should not be dependent on realization of barriers[14]. Only when something goes wrong, and we are outside the boundaries of normal operation, barriers should be needed.

[12] Typically apply to hazards where barriers and barrier elements are not so well defined and studied as for e.g. process leaks (e.g. structural failure and ship collisions).

[13] This was the case for the previous versions of the Management Regulations Section 5. Unfortunately, the prevailing regulations (from 01.01.2015) have been changed towards a wider definition of barriers. However, in our argumentation we stick to the previous versions of the regulations.

[14] Special cases are barriers that also have an operational/control function, such as containment and drilling mud; they are needed during normal operation for their operational functions, not for their safety functions. In an abnormal situation, e.g. overpressures in pipe or well, the barriers are realizing their safety functions through extra wall thickness and extra heavy mud weight, respectively. I.e. they have dual functions.

Both inherent safety measures (inherent design solutions) and various control measures ("controls") are in place to handle deviations from normal operation. We use an extended version of the bow-tie from the DNV GL / NSA "Good practices" document /4/ to illustrate this (extended to the left). This is shown in Figure 3.16.

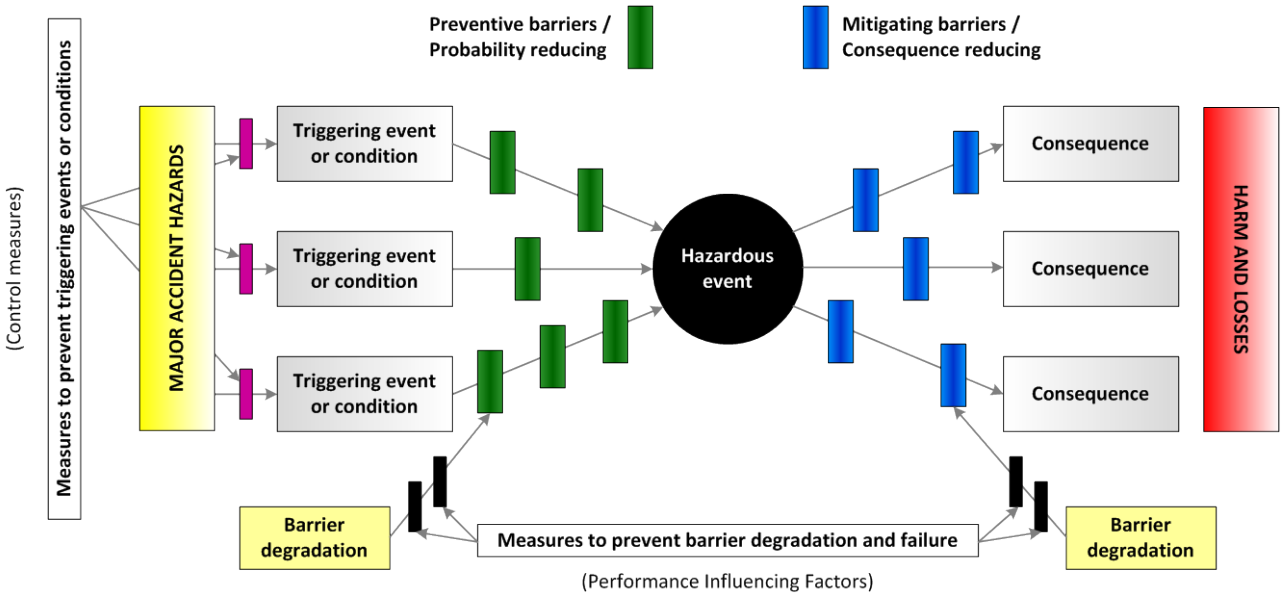


Figure 3.16 Control measures to prevent triggering event/condition and subsequent need for barriers

A triggering event in the case of process accidents can be overpressure. One important means to prevent overpressure is the process control system (PCS). This is clearly not a safety system / barrier system (since we are within the boundaries of normal operation); it is a control system. The PCS is one of the purple symbols to the left of the triggering events. If overpressure is not avoided, then the process shutdown system (PSD) is activated. This happens after the triggering event (loss of control), i.e. it is one of the green barriers to the right of the triggering events. In general we can distinguish between *barriers* (barrier functions/ systems/elements) and *controls* (control functions/systems/elements).

We have a similar challenge in distinguishing between barrier/barrier elements and the technical, operational and organizational solutions that "comes before" the barriers (cf. MR Section 4 /2/), as we have with barrier/barrier elements versus PIFs. There is a need to be somewhat pragmatic when classifying measures as either barriers or "controls", and also take current practice into consideration.

In order to reserve barriers to "abnormal" operations, we suggest a somewhat more precise barrier definition than suggested by PSAN /1/.

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

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.

Recommendation 7

Considerations should be given to restrict the term barriers to measures needed after loss of control and outside the boundaries of normal operation. E.g. the process control system is considered a control measure/system, not a barrier.

3. Distinction between operational and organizational barrier elements

Broadly speaking there are "two schools" when it comes to the classification of barrier elements; one advocating three classes; i.e. technical, operational and organizational barrier elements (such as PSAN does both in the regulations and in the "barrier memo"), and the other advocating two classes; e.g. technical and "non-technical" barrier elements (or some other term such as "operational" or "human"). The latter is advocated by e.g. DNV GL / NSA in the "Good practices" document /4/, where "operational" covers both operational and organizational barrier elements.

There are pros and cons with both "schools" and we will not prescribe one of them. However, we will outline how it can be possible to follow the intensions of PSAN – with some minor adjustments. We will also exemplify the difference between the two schools.

Technical barriers established during design need to be made *operational* (e.g. *how* to operate the barrier systems) and *organizational* responsibility with respect to use and authorization needs to be assigned (e.g. *who* is going to operate the barrier systems and under which conditions). Thus, a barrier may consist of *operational and organizational barrier elements* in addition to *technical barrier elements*.

The barrier elements constitute what is *necessary and sufficient* or *specific prerequisites* to realize a barrier function when needed (at the time of the realization). The three categories of barrier elements represent the solutions or "materializations" of the sub-functions (or sub-sub-functions etc.) necessary to realize a barrier function. The understanding of the technical barrier elements is relatively straight-forward, whereas the operational and organizational barrier elements are somewhat more challenging.

The *organizational barrier element* of a barrier function is constituted by the personnel (roles) directly involved in the realization of the function[15], e.g. the driller who activates the BOP. It also includes authorization to realize a barrier function. Realization of barrier functions is often represented by control room operators and various emergency response roles (emergency response leaders and teams).

How a barrier function should be *manually* realized is covered by the *operational barrier element*. This will typically be operational procedures, check lists, instructions, manuals, handbooks, etc., describing how, when and under which circumstances/conditions the organizational element (e.g. 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.

The action itself is not a materialization or solution of a sub-function. It is still possible to continue to ask how and when to carry out the action/task/sub-sub-function – it is a function until it materializes in a *description* (see example in Table 3.2).

[15] This is different from, and should not be confused with, organizational (causal or performance influencing) factors. These organizational factors are part of the *performance influencing factors*, and not considered as barrier elements by themselves; they only influence the performance of the barrier elements.

This interpretation of operational barrier elements, as the *description* of the required action during manual operation of a barrier function, 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, e.g. in emergency preparedness analyses (referring to e.g. acute medical procedures, helideck manual, the emergency response plan, etc.).

The two versus three classes of barrier elements is illustrated in Tables 3.1 and 3.2 using the barrier function "control kick" as an example. The example using two classes of barrier elements are taken from Øie, 2014 /30/.

Table 3.1 Barrier elements using two classes (control kick example) /30/

Barrier sub-functions	Operational barrier elements	Technical barrier elements
2.1 Detect kick	Detect gain in mud pit volume	Pit volume totalizer
	Perform flow check	Return flow line / CCTV
	Etc.	Etc.
2.2 Shut in well	Space out drill string	Drawworks
	Close upper annular preventer	Blowout preventer
	Etc.	Etc.
Etc.	Etc.	Etc.

Table 3.2 Barrier elements using three classes (control kick example)

Barrier sub-functions	Barrier sub-sub-functions	Technical barrier elements	Operational barrier elements	Organizational barrier elements
2.1 Detect kick	Detect gain in mud pit volume	Pit volume totalizer	Well control handbook Well control response guide	Driller, assistant driller, mudlogger
	Perform flow check	Return flow line / CCTV	Well control handbook Well control response guide	Driller, assistant driller, mudlogger
	Etc.	Etc.	Etc.	Etc.
2.2 Shut in well	Space out drill string	Drawworks	Well control handbook	Driller, ...
	Close upper annular preventer	Blowout preventer	Well control handbook	Driller, toolpusher, ...
	Etc.	Etc.	Etc.	Etc.
Etc.	Etc.	Etc.	Etc.	Etc.

Splitting barrier elements into two classes is "simple", and one argument for this approach is that it is difficult and/or unnecessary to distinguish the person from the action and therefore the operational and the organizational barrier elements are combined into one element. Here this combined element is termed "operational barrier element".

Another argument is that in avoiding using the term "organizational barrier element" there is no danger of confusing this with the "organizational underlying causes" (as mentioned in footnote no. 15).

In using three classes of barrier elements the function has to be broken down until a level is reached where it can be "materialized" as a solution (it answers the question how, and is no longer a function). Thus, the second column, which in using two classes of barrier elements was defined as an operational barrier element and expressed as a task, is now considered as still being a function, i.e. a sub-sub-function, needing further breakdown. This consists of the *description of how* to perform the task (i.e. the operational barrier element – fourth column), the personnel *who* are performing the task (i.e. the organizational barrier element – fifth column), and the technical equipment – the *"with-what"* – used to perform the task (i.e. the technical barrier element – third column); thus realizing the barrier sub-sub-function. There are several arguments for classifying barrier elements into three classes, some of which have already been discussed above.

Identifying the sharp end personnel performing the sub-sub-functions (as organizational barrier elements) is useful. Roles and responsibilities are not always quite clear, and it can be multiple actors involved with different roles and responsibilities. In the kick detection example the driller, assistant driller and the mudlogger shall all monitor the pit volumes and flows, but the mudlogger cannot take any action apart from alerting the driller and assistant driller.

Also for closing of the BOP several persons can be involved, e.g. both the driller and the toolpusher can close the BOP. During the Macondo accident it was the toolpusher who closed the annular preventer. It is important to have an overview of the roles and responsibilities, also with respect to redundancy/robustness.

A description of how the tasks shall be solved/performed (as operational barrier elements) is also necessary. Even if the personnel are trained to perform tasks without the use of procedures during the execution of the tasks, the procedures need to be in place. In the Macondo case it was referred to the Well Control Handbook, but stated that this was made for "normal kicks", not "extreme kicks", and it was neither suitable for End-of-Well operations, which needed a special well control response guide.

It may also be considered necessary to refer to the exact section in the procedure/manual/handbook that applies for the task in question, to facilitate verification. A task can be quite complex requiring an extensive description, for which it will be practical to refer to the procedure/manual/handbook.

If three classes are used, then the following definitions for the barrier elements can be used:

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 play a part in realising a 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.*

Organizational barrier element:

> *Personnel with defined roles or functions playing a part in realising a barrier function.*

The definitions are in line with the definitions proposed by PSAN. One minor deviation is the definition of operational barrier elements. It is suggested that the operational barrier elements are the *description* of actions, and not the actions themselves. The reasons for this are stated above.

When splitting barrier elements into two classes only, the definition of the operational barrier element is the actions (with the actors seemingly covered implicitly).

In this struggle to find useful classifications of barrier elements (being it two classes or three classes), some voices are raised to whether it is adequate at all to define static categories of barrier elements. There is particularly a concern with respect to the treatment of organizational issues, since in the classification schemes described above the sharp end is included in the organizational barrier element, whereas the blunt end is included in the performance influencing factors. The question is whether it is possible or desirable to confine the organizational influences to categorical classification /25/.

3.1.7 Communication and consultation with the sharp end; from theory to practice

Communication and consultation are activities that are running in parallel with all steps in the risk management process. It was explicitly included in the model / process flow diagram in the ISO 31000 standard /12/ (see Figure 3.17), later adopted by NORSOK standard Z-013 /13/ (see Figure 3.18).

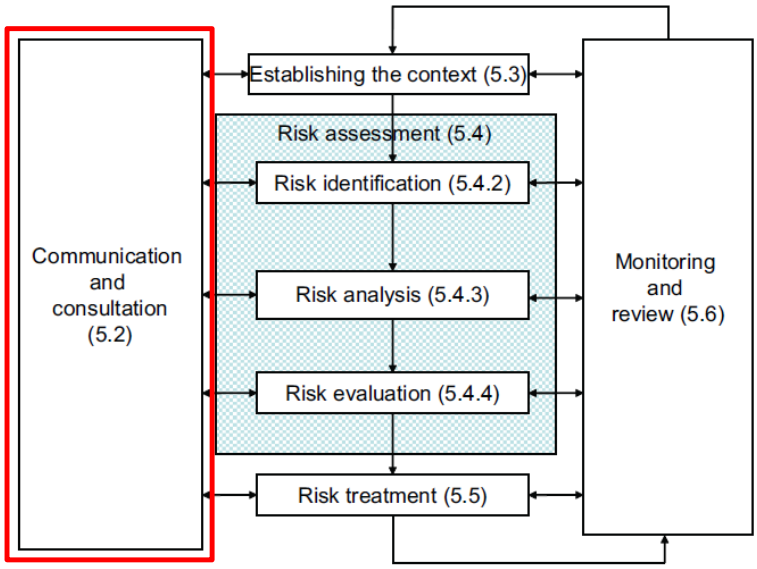


Figure 3.17 Communication and consultation in all steps of the ISO 31000 risk management process /12/

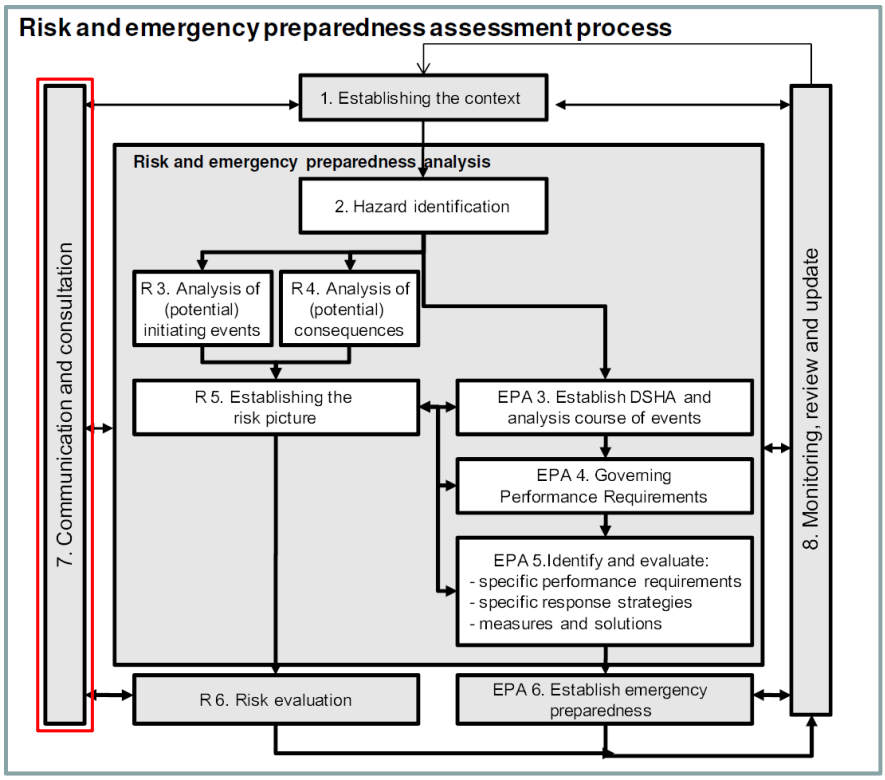


Figure 3.18 Communication and consultation in the NORSOK Z-013 standard /13/

The barrier management process is, as stressed by PSAN, an integral part of risk management; thus, communication and consultation are needed for the barrier management process as well (see Figure 3.19).

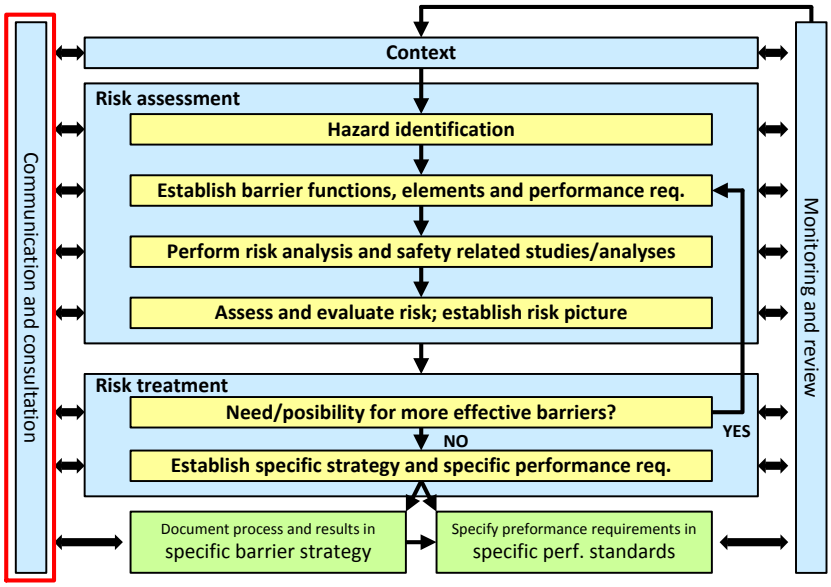


Figure 3.19 Communication and consultation in the PSAN barrier management process /1/

Keeping the barrier management process as a genuinely integral part of the risk management process is easier said (and illustrated) than done in practice. The situation is often that these two processes are run in parallel (as discussed in Section 3.1.4), but they are not as integrated as the PSAN illustration indicates. It is not unusual that the two processes are carried out by two different consulting companies and without coordinated updating of the corresponding documents (i.e. the risk management documents such as the QRA and the barrier strategy).

Recommendation 8

The risk management process (including establishing and updating the risk analysis, e.g. QRA) should be coordinated with the barrier management process. It should even be considered to include one of the QRA analysts to actively participate in the barrier management process team.

The need for consultation with the sharp end personnel in providing input to the barrier analysis is probably greater than in the traditional risk analyses (QRAs). This also requires an ability to communicate the barrier management process to the sharp end personnel, which is a challenge due to "the chaos of terms" as mentioned in Section 3.1.2, including the term "strategy" (cf. Section 3.1.3) and the barrier concept, definitions and terms (cf. Section 3.1.6).

The QRA is seldom actively used in operation by sharp end personnel (unless it is further adapted into easily accessible summaries such as area risk maps[16]); whereas the results of the barrier management process "shall" be used by sharp end personnel through e.g. tools like a barrier panel.

It is also a challenge to make sure that all the "theoretical" work carried out in the barrier management process ends up with practical useful tools and decision support for the sharp end personnel. This requires extensive consultation and communication suitable for the various stakeholders, including sharp end personnel.

Recommendation 9

All relevant stakeholders, including sharp end personnel, should be consulted and participate in the barrier management process to ensure practical useful tools and decision support for the sharp end personnel.

3.2 Specific challenges and recommendations for barrier management

3.2.1 Quality of data for verification of performance requirements in operation

Barriers that are active safety systems will reveal hidden failures either during functional testing or on real demands (i.e. in activating the barriers). We will describe some challenges related to quality of data for verification of performance requirements in operation based on an example illustrated in Fact box 4 /6/.

We assume that the performance requirement determined in the design phase is SIL 2, and we assume that the failure rate is based on data achieved from the vendor. Based on this a required maintenance interval can be calculated/determined. It can also be "verified" by the approximation formula for the PFD that the SIL 2 requirement is met. A first challenge in this "verification" of the performance requirement during design is the accuracy of the vendor data, i.e. how realistic they are in operation.

[16] This is another reason why it should be considered to include one of the QRA analysts in the barrier management process team.

Fact box 4: Safety integrity in design versus safety integrity in operation

EXAMPLE

ESV with SIL 2 requirement for associated loop, i.e. 10^{-3}<PFD<10^{-2}

SIL	PFD
SIL 4	$10^{-5} – 10^{-4}$
SIL 3	$10^{-4} – 10^{-3}$
SIL 2	$10^{-3} – 10^{-2}$
SIL 1	$10^{-2} – 10^{-1}$

DESIGN	OPERATION
Vendor failure data/rate: $\lambda_{DU} = 1 \cdot 10^{-6}$ hr^{-1}	Experienced data/rate: $\lambda_{DU} = 4 \cdot 10^{-6}$ hr^{-1}
Required maintenance interval: τ = 12 mths	Maintenance interval from design: τ = 12 mths
Design safety integrity: PFD = $\lambda_{DU} \cdot \tau/2 = 4.38 \cdot 10^{-3}$ i.e. within SIL 2	Operational safety integrity: PFD = $\lambda_{DU} \cdot \tau/2 = 0.02$ i.e. within SIL 1
	Adjusted maintenance interval: τ = 6 mths
	Adjusted operational safety integrity: PFD = $\lambda_{DU} \cdot \tau/2 = 8.76 \cdot 10^{-3}$ i.e. within SIL 2

PFD = Probability of Failure on Demand
λ_{DU} = failure rate of dangerous undetected failures
τ = test interval

The design failure rate can be translated into expected number of failures per year for each individual barrier element (in this example the ESV) against which operational data can be compared. The second challenge is that for one single barrier element the expected number of failures per year is very low, far below 1 failure per year. It will take many years to verify the design failure rate with operational data / experience data.

If we have a pool of similar barrier elements (e.g. 30 similar ESVs) on the installation, the number of failures per year becomes "meaningful" for a comparison with operational data; although even in this case the expected number of failures per year is typically very few. Thus, a third challenge is that it usually takes some years to collect a meaningful amount of operational data to compare with the design data.

In the example we have assumed that 6 failures (DU-dangerous undetected failures) have been experienced during a period of 3 years, which gives a much higher failure rate compared to the expected 1 failure in 4 years based on the design data. The failure rate used for the adjusted operational safety integrity shown in Fact box 4 is a weighted failure rate also taking the original design failure rate into account. A fourth challenge is how much weight to put on the design failure rate versus the experienced operational failure rate, and as new data is available how to "blur" the old data compared to the new data.

The example shows that with more failures experienced during operation than anticipated in design, the performance requirement to the barrier element is not fulfilled (only SIL 1 is achieved). However, by adjusting the test interval from 12 months to 6 months the associated performance requirement of SIL 2 may (again) be met. A fifth challenge is that it may take several years to unveil that the barrier performance actually are below the required performance; the safety integrity of the barrier element is not as high as anticipated in design, and the risk is higher than calculated.

A sixth challenge is that the adjustment of the test interval may not be enough to compensate for the higher failure rate. It may be necessary to redesign and modify the barrier system or the barrier elements.

In some computerized maintenance management systems (CMMS) "test reports" is automatically generated producing failure fractions for the barrier elements, i.e. number of failures divided by number of tests. This is the numbers used to obtain the operational failure rate, and also the numbers submitted to the PSANs RNNP project. When reviewing all failure reports for the ESVs, including failures during normal use/demand, and comparing the numbers with the automatically generated "test reports", it was found that only approximately half of the failures where included in the "test reports". Equally many failures were discovered during "normal use" as during functional testing. Thus, a seventh challenge is that automatically generated "test reports" may underestimate the experienced failure rate, and a subsequent eight challenge is that the RNNP data may be underestimated. Therefore, it is recommended to conduct manual operational reviews of barrier element failure reports. This is more thoroughly treated in /6/.

Most of the challenges we have mentioned here are well-known and they are being dealt with in some way or another; however, the operational reviews of failure reports are probably not commonplace in all operating companies. Thus, we recommend this to be implemented. It also provides quality assurance of the failure reports covering other aspects, such as wrong classification of both failure reports and equipment.

Recommendation 10

Manual operational reviews of failure data reports for barrier elements should be implemented to ensure that all relevant failures are taken into account; including failures discovered between tests and not only failures discovered during functional testing.

3.2.2 Organizational dependency between barriers

For the "defence in depth" strategy to be as efficient as possible, it is a premise that the barriers ("the cheese slices" cf. Figures 2.1 and 3.20) are independent. This may be difficult to verify in practice, both for technical-, but especially for operational and organizational barrier elements.

Experience from major accidents like Macondo /7/, show that various human/psychological and organizational mechanisms have a potential to disintegrate multiple barriers, as illustrated in Figure 3.20. This undermines the defence-in-depth strategy and therefore needs to be dealt with as part of the barrier management strategy.

Barrier management as of today mainly focuses on single barriers (area and systems thinking) and on sharp end aspects related to technical and 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.

Furthermore, the focus on technical and operational aspects may disregard the organizational dimensions that may act as catalysts for common cause failures (see Størseth et al., 2014[17] /25/ for a thorough discussion).

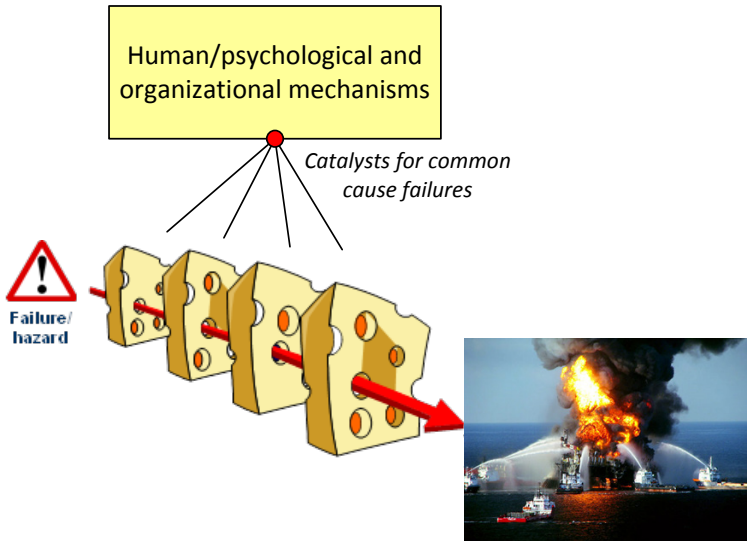


Figure 3.20 Human/psychological and organizational mechanisms causing multiple barrier failure

It is therefore important that barrier management also focuses on the entire barrier system and on organizational issues in particular, in order to avoid potential multiple barrier failures.

Recommendation 11

The potential for "organizational multiple barrier failures" should be considered in the barrier strategy, since it can degrade several individual barriers due to the same cause or mechanism. It may require a separate "search methodology" to identify the potential failures/mechanisms.

There is no straight forward way to deal with the potential for "organizational multiple barrier failures", but some systematic method to search for these failures/mechanisms need to be established and used.

One line of approach, starting in the early nineties, focused on the development of organizational factor frameworks linked to a technical or socio-technical model of risk /34/, whereas another line of approach is to focus on "forces of psychology" acknowledging the impact of psychological mechanisms like consensus-mode decision-making, confirmation bias, normalization of warnings, groupthink as well as social forces of power and persuasion. Such psychological forces may serve as 'transmitters' of organizational principles, strategies and decisions throughout the barrier system. In turn, this may contribute to risk transfer, and dependence between barriers /25/.

For challenges with respect to models and data for modelling of dependencies between barriers and barrier elements in general (not restricted to human/psychological and organizational mechanisms), we refer to Activity 2 in the project, cf. Section 1.1.

[17] This paper "Safety barriers: Organizational potential and forces of psychology" /25/ published in Journal of Loss Prevention in the Process Industries, is a result of this PETROMAKS research project.

3.2.3 Performance requirements for operational and organizational barrier elements

Performance requirements for technical barriers and barrier elements can be found both in regulations, recommended standards and guidelines, and in company specific requirement documents. Whereas there are a large number of requirements defined for the technical barriers and barrier elements, the situation for operational and organizational barriers and barrier elements is the opposite. This is a challenge when verifiable performance requirements shall be established for all barrier elements.

The challenge of establishing verifiable performance requirements for operational and organizational barrier elements is related to i) having necessary time during the barrier analyses/barrier strategy process to consider useful and verifiable requirements, ii) making the requirements both specific enough and also sufficiently comprehensive, iii) having access to personnel with competence on operational and organizational issues and iv) defining objective measurement criteria is in itself often a major challenge, e.g. how to measure competency of an operator or how to measure the quality of a given procedure. How to obtain information and data to verify the requirements also need to be considered.

Recommendation 12

Time and resources (including competency) should be allocated to establish verifiable performance requirements for operational and organizational barrier elements.

3.3 Challenges identified by authorities and industry – additional recommendations

3.3.1 Challenges identified in audits performed by the authorities

We have made a review of audit reports from PSAN in the period 2010 – 2012 /3/ in order to identify challenges (non-conformities and need for improvements) as seen from the authorities' point of view. In total 28 audit reports were reviewed, and each report was analysed in terms of:

- Main issues of the audit (e.g. major accident risk, barrier management)
- Objectives of the audit (e.g. to verify that the company complies with the regulatory requirements related to barrier management)
- Non-conformities / deviations
- Improvement items
- Comments (e.g. details regarding barriers and barrier management from the audit reports)

Scope
The audits covered offshore production facilities and drilling rigs, as well as onshore gas terminals. Both building/construction of facilities, and facilities during production were subject to audits, although there was a predominance of audits of facilities in the production phase.

Approach
Criteria for selecting reports for the review were whether one or more of the following topics were included in the title of the audit report:

- Major accidents
- Barriers
- Barrier management
- Organizational and human factors

Additionally, audit reports concluding with observations, i.e. deviations and/or improvement items, related to barriers or barrier management were included in the sample.

Results
The review is documented in Appendix A. A summary is presented below for the different categories (i.e. installation category, and non-conformities and improvement needs, respectively).

Onshore gas terminals
The non-conformities that were identified in the audits were related to:

- Insufficient determination of strategies and principles that should form the basis for the design, use and maintenance of barriers, so that the barrier function is maintained throughout the facility's lifetime
- Insufficient understanding and knowledge of the barriers that are established, and the functions they must fulfil
- Inadequate knowledge and awareness of the performance requirements to the barrier elements
- Lack of system to ensure that results of the risk analysis, including requirements for barriers and operating conditions and limitations, are forwarded to the emergency preparedness analyses (EPA)
- Inadequate prioritization of barrier management: The work is not sufficiently prioritized, is not given adequate support, and is not clearly rooted in action plans.

Additionally, improvement items were emphasized in relation to:

- Deficient training and understanding of how the facility is divided into different hazard zones, how components and equipment contribute to the risk picture, and what requirements are set for barriers and the impact the most important barriers have on reducing risk.

Offshore installations / operators
Non-conformities identified in the audits were related to:

- Inadequate identification and monitoring of barrier elements
- Unclear or lack of connection between risk analysis and strategy and the specific performance requirements for barrier elements
- Lack of system for monitoring and following up assumptions/conditions in the risk analysis
- Deficiencies related to the establishment and monitoring of barriers (technical and operational) and performance requirements.

Additionally, improvement items were emphasized in relation to:

- Inadequate strategy for follow-up of barriers (e.g. no clear relationship between risk and strategy and the acceptance criteria for barriers)
- Insufficient understanding of how the criteria for barrier performance and testing are based on assumptions from the design, related to regulations, standards and barrier philosophy
- Overview of barrier status; deficient identification and monitoring of barrier impairments
- Functional testing of safety critical valves: Results from the first tests not always reported in the maintenance system
- Description of roles and responsibilities in barrier management.

Drilling rigs / drilling contractors
Non-conformities identified in the audits were related to:

- Inadequate strategies and principles to form the basis for the design, use and maintenance of barriers to ensure that the barrier function is maintained throughout the facility's life
- Performance standards did not reflect the requirements related to barriers, and did not ensure that barriers are effective at any time.

Additionally, improvement items were emphasized in relation to:

- Lack of system to safeguard the overall requirements for follow-up of barriers and performance requirements across the organization
- How safety strategies are to be established and communicated.

Construction / development projects

Non-conformities identified in the audits were related to:

- Incomplete specification and consistency between safety strategy, performance standards and underlying principles, specifications and guidelines to be applied for the design, use and maintenance of barriers
- Inadequate systematic relationship between risk, strategy and the specific performance requirements for barrier elements
- Inadequate documentation of facility-specific performance requirements for barriers
- Performance standards not established in a holistic way that encompassed all requirements for monitoring of barriers to ensure that the barriers are effective at any time
- Established philosophies are characterized by being aimed at the design and construction phase.

No additional improvement items were emphasized in relation to barrier management in construction/ development projects.

Summary

When summarising the above findings and the more detailed audit results referred in Appendix A, some recurring points include:

- Inadequate strategies and principles that should form the basis for the design, use and maintenance of barriers to ensure that the barrier function is maintained throughout the facility's life
- Lack of connection between risk/hazard assessment, the need for barriers and the barriers' role in the individual area (strategies)
- Inadequate or lacking performance requirements and performance standards
- Barriers and associated performance requirements not installation specific
- Inadequate systems for monitoring and following up the status and "health" of barriers during operation.

In relation to the last bullet PSAN has pointed out in the audit reports a need for identifying conditions that could reduce the barriers' performance over time (changed user conditions, degradation mechanisms, aging, incidents, etc.), for establishing indicators for monitoring function and performance, and processes for making barrier function and performance robust enough to handle these conditions.

All the challenges summarized above points to the very need for a holistic and structured approach for barrier management. At the same time, it may be useful to review recent PSAN audit reports related to barrier management, when conducting a barrier management process for a specific project, in order to check (self-assess) that all non-conformities and improvement items identified by PSAN (for other projects as well as own projects) are accounted for in the on-going barrier management project.

Recommendation 13

Recent PSAN audit reports on barrier management (for all projects/companies) should be reviewed to check that identified non-conformances and improvement items are considered.

3.3.2 Challenges identified in a well control study

In 2009-2010 there was an increase in the number of well control incidents on the Norwegian Continental Shelf reported to the Petroleum Safety Authority Norway (PSAN) /5/. This, together with the Deepwater Horizon accident[18] in 2010 /7/, made PSAN initiate a comprehensive investigation into the causes and possible mitigating measures related to well control incidents. The main purpose of the study was to describe key challenges the petroleum industry has to face to reduce the number of well control incidents in the future.

Among the topics addressed in this study were also barrier management and better adapted risk analysis. The study was based on a review of public documentation (e.g. investigation reports) on well control incidents in the period 2003-2010, interviews with 33 drilling and well professionals in the industry, and a review of additional documents and material received from 8 oil companies and 10 drilling contractors operating in Norway /8/.

According to the informants from this study, PSAN's focus on barriers and barrier management has resulted in considerably increased awareness on this topic in the industry over the last couple of years. Based on the interviews, we can see that "barriers" is a familiar term, even if several informants limit themselves to speaking about BOP and drilling mud when speaking about barriers. As regards "barrier management", this is an area with a need for considerable maturation and further industry efforts.

Based on the interviews and the investigations, as well as results from other relevant projects, some main areas for improvement were identified:

- Increased awareness in the companies across the industry as regards what is included in barrier management, e.g. related to which requirements are included in the current regulations.
- Clarifying the term "operational and organizational barrier elements". The industry should convene to clear up the confusion associated with how one should define "operational and organizational barrier elements". The PSAN's recommendation that verifiable performance requirements must be set for the barrier elements, may well be a good point of departure for such a review.
- Stipulating performance requirements for all the barriers and following-up in operation. Performance requirements are lacking (including reliability requirements) for several of the technical barriers during drilling. Systems to detect well kicks, technical systems to ensure a stable mud column and diverter systems are typical examples of some of the systems for which there are currently deficient requirements.

Recommendation 14

The barrier philosophy document should include a chapter on regulations and other references describing and explaining explicitly barrier management requirements. It may also be considered to include this in the barrier strategy document.

For the clarification of the term "operational and organizational barrier elements" we refer to Section 3.1.6.

Similar as for recommendation 12 it must be allocated sufficient time and resources to develop performance requirements also for technical barrier elements where this is currently lacking (as is the case for e.g. drilling operations).

[18] Also referred to as the Macondo accident.

Recommendation 15

Time and resources (including competency) should be allocated to establish verifiable performance requirements for technical barrier elements for which requirements are missing. This is e.g. the case for several barrier elements during drilling operations.

3.3.3 Challenges identified in a PDS workshop

The PDS members were asked to identify important and challenging areas related to barrier management. The results are summarised below:

1. Clarification of concepts is important. In particular related to operational and organizational barrier elements and performance influencing factors. It should be sufficient to make a division between technical and non-technical elements. PSAN's split between operational and organizational elements appears somewhat "artificial".
2. It is challenging to define measurable requirements, especially for organizational and operational elements. It is important to operationalise requirements so they can be applied on the installations.
3. Measuring and quantifying barriers that involve humans; e.g. how to measure competency (experience, courses and training, subjective evaluations). Do we want people that are specialised or people that are resilient?
4. Management commitment; there is still a long way to go and top management need to become more aware of major hazard risks.
5. Operational personnel need to become more aware of how the barriers and the associated performance requirements are defined and how these should be followed up.
6. Increasing complexity is a growing challenge as the safety systems grow larger and larger. Too many tags, too many C&Es and too many shutdown levels. The operators do not always have control of the safety logic themselves and must consult the vendors. As a result none has the complete overview and understanding of the safety systems.
7. Monitoring and following-up requirements to barriers, in particular operational and organizational elements are challenging. They are also difficult to define.
8. Management of change is challenging.
9. The QRA is too often used for verification. The project defines the technical solutions and the QRA is used for verifying these solutions, even though the granularity of the QRA is not sufficient for such verifications.
10. Proving independence between barriers and systems is very challenging.
11. Too little focus on non-instrumented barriers (such as lifeboats and passive fire protection), maybe due to the huge focus on safety instrumented systems (SIS).

Points 1-3 are covered in Section 3.1.6 (the barrier concept, terms and definitions).

Regarding point 4, at least some industry representatives perceive that sufficient management commitment and awareness of major accident risks are not in place. It is necessary to ensure top management commitment to the barrier management projects and to the management of major accident risks (including risk awareness), which is in line with the expectations and prioritizations of the authorities, cf. Section 2.2.

Recommendation 16

Top management commitment to barrier management should be ensured to enable necessary risk awareness to manage major accident risks in line with the expectations of the authorities.

Point 5 is addressed in Section 3.1.7 (communication and consultation with the sharp end; from theory to practice). Point 6 is tricky, but we have touched upon this in Section 3.1.5 (multiplicity of methods and tools) where we recommend that the methods and tools used for barrier analyses should be suitable for systematic identification of all relevant barrier elements (e.g. by the use of "triangulation" or at least two comparative methods). The need for use of more than one method in the barrier analysis is due to e.g. complexity.

For point 7 we refer to Section 3.1.6, 3.2.1 and 3.2.3. Also point 8 is touched upon in Section 3.2.1.

Regarding point 9, it is recommended to be cautious when using the QRA for verification of technical solutions, since the level of detail in the QRA often makes it unsuitable for such verifications.[19]

Recommendation 17

Special care should be taken using the QRA for verification purposes, since the level of detail in the QRA may not be suitable for such verifications.

Point 10 is partly addressed in Section 3.2.2 (organizational dependency between barriers), but we refer to Activity 2 in the project for this issue (cf. Section 1.1).

Finally, regarding point 11, it is recommended to allocate sufficient time and focus on non-instrumented safety systems during the barrier management process. There is a perception that safety instrumented systems are over-focused compared to the non-instrumented safety systems.

Recommendation 18

Time and resources (including competency) should be allocated to non-instrumented safety systems during the barrier management process.

[19] This is not a critique of the QRA as such; it is only a warning against using it for verification purposes when the level of detail in the analysis is insufficient.

4 Summary of recommendations

No	Description	D	O
1	The SIL process should be integrated in the barrier management process, and both processes should be an integral part of the risk management process. These processes also need to be coordinated with the maintenance management process.	✓	✓
2	Comprehensible descriptions of the barrier management process should be provided. Detailed descriptions/illustrations should be accompanied with overview illustrations.	✓	✓
3	The links between risk management, barrier management, maintenance management and other interrelated processes should be described and illustrated.	✓	✓
4	The methods and tools used for barrier analyses should be suitable for communication with operating personnel and technical experts in order to verify the analyses.	✓	
5	The methods and tools used for barrier analyses should be suitable for systematic identification of all relevant barrier elements (e.g. by the use of "triangulation" or at least two comparative methods).	✓	
6	The methods and tools used for barrier analysis should ensure that the area specific barrier strategy and the area specific performance standards provide a common thread from the identified hazards and potential major accidents to the individual barrier elements and their attributes (e.g. performance requirements, verification method and test interval).	✓	
7	Considerations should be given to restrict the term barriers to measures needed after loss of control and outside the boundaries of normal operation. E.g. the process control system is considered a control measure/system, not a barrier.	✓	✓
8	The risk management process (including establishing and updating the risk analysis, e.g. QRA) should be coordinated with the barrier management process. It should even be considered to include one of the QRA analysts to actively participate in the barrier management process team.	✓	✓
9	All relevant stakeholders, including sharp end personnel, should be consulted and participate in the barrier management process to ensure practical useful tools and decision support for the sharp end personnel.	✓	
10	Manual operational reviews of failure data reports for barrier elements should be implemented to ensure that all relevant failures are taken into account; including failures discovered between tests and not only failures discovered during functional testing.		✓
11	The potential for "organizational multiple barrier failures" should be considered in the barrier strategy, since it can degrade several individual barriers due to the same cause or mechanism. It may require a separate "search methodology" to identify the potential failures/ mechanisms.	✓	✓
12	Time and resources (including competency) should be allocated to establish verifiable performance requirements for operational and organizational barrier elements.	✓	✓
13	Recent PSAN audit reports on barrier management (for all projects/companies) should be reviewed to check that identified non-conformances and improvement items are considered.	✓	
14	The barrier philosophy document should include a chapter on regulations and other references describing and explaining explicitly barrier management requirements. It may also be considered to include this in the barrier strategy document.	✓	
15	Time and resources (including competency) should be allocated to establish verifiable performance requirements for technical barrier elements for which requirements are missing. This is e.g. the case for several barrier elements during drilling operations.	✓	✓
16	Top management commitment to barrier management should be ensured to enable necessary risk awareness to manage major accident risks in line with the expectations of the authorities.	✓	✓
17	Special care should be taken using the QRA for verification purposes, since the level of detail in the QRA may not be suitable for such verifications.	✓	✓
18	Time and resources (including competency) should be allocated to non-instrumented safety systems during the barrier management process.	✓	✓

D = relevant for the Design phase; O = relevant for the Operations phase

(Empty page)

5 Overall approach – preliminary outline

This chapter provides a preliminary outline of an overall approach for barrier management. It includes:

1. Barrier management principles and framework
2. Barrier management process and barrier strategy

5.1 Barrier management principles and framework

We recommend having this document at company level with the purpose of presenting overall principles and framework for barrier management of major accident risk at any installation or project. A barrier management principles and framework document at company level 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

The barrier management principles and framework is illustrated in Figure 5.1.

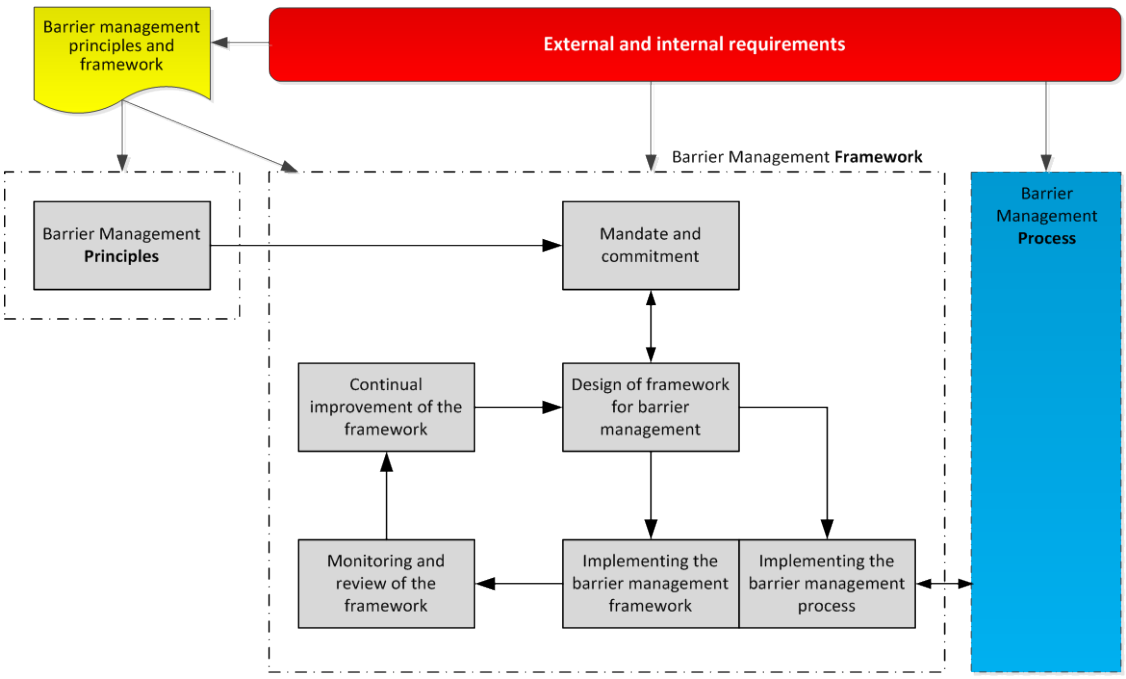


Figure 5.1 The barrier management principles and framework

This content is further discussed below.

Rules and regulations, codes, standards and guidelines
The following standards and guidelines provide guidance to the process of barrier management:

- PSA Principles for barrier management in the petroleum industry /1/
- NORSOK Z-013 Risk and emergency preparedness assessment /13/
- NORSOK S-001 Technical safety /18/
- NORSOK Z-008 Risk based maintenance and consequence classification /19/
- ISO 31000 Risk management – Principles and guidelines /12/
- ISO 13702 Petroleum and natural gas industries: Control and mitigation of fires and explosions on offshore production installations - Requirements and guidelines /14/
- IEC 61508 Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems /16/
- IEC 61511 Functional Safety: Safety Instrumented systems for the Process Industry Sector /26/
- Norwegian Oil and Gas Association, Guideline 070; Application of IEC 61508 and IEC 61511 in the Norwegian petroleum industry /17/
- DNV-GL / NSA Barrier management in operation for the rig industry. Good practices /4/

Company internal documents and requirements
To limit the scope and size of the barrier management philosophy, references can be made to company internal documents that shall be part of the barrier management process in the company. The following aspects may typically be dealt with in internal company documents:

- Management of major accident risk / risk reduction principles
- Technical safety standards/documents
- Operational safety standards/documents
- Barrier management in design and engineering
- Barrier management in operation
- Management of change

Definitions and abbreviations
In order to ensure standardisation and a common understanding across the company, it is advantageous to provide a set of definitions and abbreviations that shall be applied for all development projects and facilities in operation. Reference is made to Section 3.1.6 in this report.

High level guiding principles
This is one of the central parts of the document. It may consist of principles such as:

- The barrier management shall be based on facility specific risk, as identified through safety studies and specified and detailed in the design of the installation
- Barrier management shall as a minimum be in accordance with current regulations, overall company policy, as well as facility specific conditions and design premises.

Description of the barrier management framework
This is another central part of the document. The framework shall ensure complete implementation of the barrier management process when developing local barrier strategies for a specific installation.

An outline of the barrier management process to be followed
This includes references to some of the company specific documents described above and particularly (work) processes related to:

- Establishing the barrier strategy in accordance with the barrier management philosophy
- Monitoring and maintaining the performance of the barrier to ensure safe operation
- Managing changes (i.e. modifications of technical as well as non-technical barriers).

5.2 Barrier management process and barrier strategy

The barrier management (BM) process is outlined in Table 5.1.

Table 5.1 Main barrier management activities in various life cycle phases

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

The barrier strategy (document) is one of the outcomes of the barrier management process. As described in Section 3.1.3, barrier strategy is defined 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/.

A barrier strategy shall be established for each facility and shall be based on the barrier management principles and the unique characteristics of the facility. The purpose of the strategy is thus 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.

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. Detailed descriptions of identified barrier systems and 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 systems and 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, are often included in a separate document (denoted Performance Standards, Barrier Function Performance Standards, or something similar).

6 Conclusions and further work

We have in this report discussed important aspects and challenges related to barrier management, and also presented an outline of a holistic approach/method for barrier management as part of Activity 1 in the PETROMAKS project *"Tools and guidelines for overall barrier management and reduction of major accident risk in the petroleum industry"*.

This will provide the main foundation for the development of the industry guideline for barrier management in Activity 4 (cf. Figure 6.1). It may also be used for self-assessment of (comparison with) on-going or established barrier management processes, e.g. checking compliance with the recommendations.

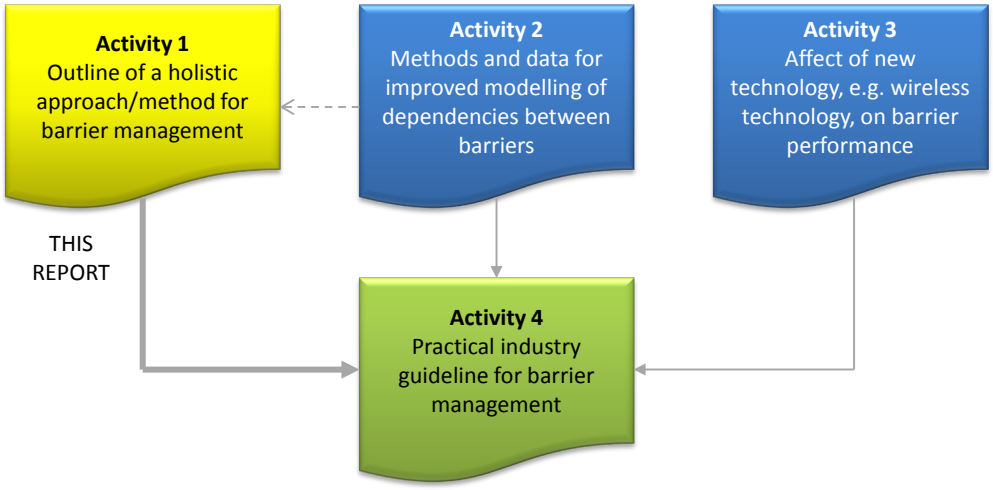
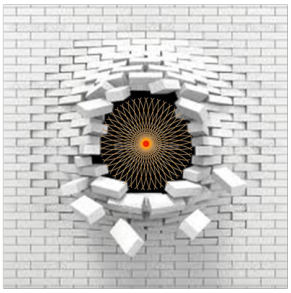


Figure 6.1 Link between the various project reports

The outline, described in Chapter 5, covers barrier management principles and framework, the barrier management process, and barrier management strategy. The industry guideline will also take into account the 18 recommendations developed and described in Chapter 3 and summarized in Chapter 4.

The more specific issues treated in Activity 2 and 3 will be incorporated in the industry guideline if relevant, and other issues identified during the development of the industry guideline (in Activity 4) may also be included.



The PDS industry guideline for holistic barrier management aims at contributing to prevent and mitigate holes in the barriers.

(Empty page)

7 References

/1/ Petroleum Safety Authority Norway, Principles for barrier management in the petroleum industry, 29.01.2013

/2/ The Management Regulations; Regulations Relating to Management and the Duty to Provide Information in the Petroleum Activities and at Certain Onshore Facilities, 1 January 2011

/3/ PSAN audit reports (2010-2012), see Appendix A

/4/ DNV GL / NSA, Barrier Management in Operation for the Rig Industry; "Good practices", March 2014

/5/ Petroleumstilsynet, 2012. Risikonivå i norsk petroleumsvirksomhet. Hovedrapport, utviklingstrekk 2011, norsk sokkel. In Norw.

/6/ Øien, K., Hauge, S., 2014. Vedlikeholdets plass i barrierestyringen. SINTEF A26001 (ISBN 978-82-14-05676-1). In Norw.

/7/ 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 Norw.

/8/ Tinmannsvik, R.K., Hauge, S., Okstad, E.H., Carlsen, I.M., 2011. Brønnkontrollhendelser i norsk petroleumsvirksomhet – årsaksforhold og tiltak. SINTEF A22981 (ISBN 978-82-14-05478-1). In Norw. (This study is chapter 10 in the RNNP 2011 Main report, published on ww.ptil.no 25th of April 2012: Causes and measures related to well control incidents in Norwegian petroleum activities)

/9/ Reason, J., 1997. Managing the Risks of Organizational Accidents. Burlington: Ashgate Publishing Company

/10/ PSAN web page – main priorities, http://www.psa.no/?lang=en_US

/11/ Fact box 1 web, http://patientsafetyed.duhs.duke.edu/module_e/vocabulary.html

/12/ ISO 31000:2009, Risk management – Principles and guidelines

/13/ NORSOK Z-013, Risk and emergency preparedness assessment, ver. 03, October 2010

/14/ ISO 13702:1999 Petroleum and natural gas industries – Control and mitigation of fires and explosions on offshore production installations – Requirements and guidelines

/15/ ISO 17776:2000, Petroleum and natural gas industries – Offshore production installations – Guidelines on tools and techniques for hazard identification and risk assessment

/16/ IEC 61508 (2010). Functional Safety of Electrical/Electronic/Programmable Electronic Safety – Related Systems. Part 1-7. International Electrotechnical Commission, Geneva

/17/ Norwegian Oil and Gas Association 070 (former OLF 070), Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry, Rev. 02, 29.10.2004

/18/ NORSOK S-001 Technical Safety, Rev. 3, Jan. 2000

/19/ NORSOK Z-008, Risk based maintenance and consequence classification, Edition 3, June 2011

/20/ ISO 14224:2006 Petroleum, petrochemical and natural gas industries -- Collection and exchange of reliability and maintenance data for equipment

/21/ NS-EN 13306: Maintenance and maintenance terminology. Lysaker: Standards Norway

/22/ IEC 60300-3-11 (2009). Dependability management - Part 3-11: Application guide - Reliability centred maintenance. International Electrotechnical Commission, Geneva

/23/ Fact box 2 web, http://en.wikipedia.org/wiki/Strategy

/24/ Petroleum Safety Authority Norway, Guidelines regarding the Management Regulations (29.4.2010), www.ptil.no

/25/ Størseth, F., Hauge, S., Tinmannsvik, R.K., 2014. Safety barriers: Organizational potential and forces of psychology. Journal of Loss Prevention in the Process Industries 31(2014) 50-55

/26/ IEC 61511 (2003). Functional Safety: Safety Instrumented systems for the Process Industry Sector, Part 1-3. International Electrotechnical Commission, Geneva

/27/ Øie, S., 2013. Defining and operationalizing the barrier concept; The human contribution, ESRA-seminar, 30 April 2013
/28/ Rugsveen, N.M., 2014. Tilstandsoppfølging av Sikkerhetsbarrierer. NFV seminar, 14.10.2014
/29/ 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
/30/ Øie, S., 2014. Operational barrier elements. Good practices. HFC Forum, 16.10.2014, www.sintef.no/Projectweb/HFC/
/31/ Step Change in Safety (unknown). Assurance & verification practitioner's guide. www.stepchangeinsafety.net
/32/ Draft SINTEF report; CCFs in Safety Instrumented Systems – Beta Factors and Equipment Specific Checklists based on Operational Experience, October 2014
/33/ Draft SINTEF report; Wireless Instrumentation for Safety Critical Systems – Technology, Standards, Solutions and Future Trends, October 2014
/34/ Øien, K., 2001a. A framework for the establishment of organizational risk indicators. Reliability Engineering and System Safety 74, 147–167.

Appendix A: Review of audit reports from PSA (2010 – 2012)

Main issues (year)	Objectives	Non-conformities	Improvement items	Comments
Major accident risk, ***barrier management***, registration and follow-up of incidents (2011)	• Verify compliance with applicable regulations • Ensure that certain *safety-critical barriers* are safeguarded in a comprehensive and consistent manner • Verify the company's control of incidents, registration, follow-up and how corrective measures are handled	None	None	(Esso - Slagentangen) The audit questioned the systems for the management of selected safety critical *barrier elements* as emergency shutdown valves, pressure relief, process safety, gas detection, fire detection, passive fire protection and alarm systems.
Major accident risk (2010)	• Audit how the operator handles its duty to ensure that regulatory requirements related to management of major accident risk and maintenance management is safeguarded • Audit how the safety report for the facility has been followed up	None	• Management of improvements in the maintenance program • Access to spare parts for safety-critical equipment • Handling of nonconformities	(Norske Shell - Nyhamna) In addition, the following issues were commented in the audit report: • Skills management and resources • Organization chart • Work permits • Bridging document between Shell and Statnett • Safety report • Major Accident Regulation and a new Planning an Building Act
Major accident risk, technical and operational ***barriers,*** learning from incidents (2010)	• Verify compliance with the requirements in the Major Accident Regulations • Verify that *selected safety-critical barriers* are managed in a compre-hensive and consistent manner • Verify that management is	None	• Deficient training and understanding for how the facility is divided into different hazard zones, how components and equipment contribute to the risk picture, and *what requirements are set for barriers and the impact that*	(Statoil - Hammerfest LNG) PSA claims that it is important that *technical and operational barriers* are safeguarded in a comprehensive and consistent manner so that the risk of major accidents is reduced as far as possible, and that knowledge on how to safeguard and improve technical and operational barriers is further developed.

Main issues (year)	Objectives	Non-conformities	Improvement items	Comments
	involved in and contributes to systematic work aimed at learning from and preventing incidents		*the most important barriers have on reducing risk.* • Lack of interest in and understanding of the importance of the TCS[20] work in order to achieve good control over the *condition of barriers*, and the significance this work has for improving safety. Other improvement items were related to: • Backlog of maintenance of safety-critical equipment • Learning and implementation of measures following incidents in other organizations.	Within those areas where individuals had a direct responsibility, PSA's impression was that competence was good. <u>Regarding the TCS-report:</u> Topics in the report that PSA asked questions about were: • Firewater coverage at different height levels on the barge • Possible gas penetration in electrical rooms • Too much use of jumpers (overrides) • Quality and confidence in blow down valves to achieve rapid pressure reduction and to avoid damage to process equipment All these factors are said to be important elements in barrier control.
Electrical and safety-critical barriers (2011)	To verify that the company satisfies the regulatory requirements related to *electrical and barrier management*	Four non-conformities in relation to the regulations were identified: • Ignition source control • *Barrier management* • *Barrier performance requirements* • Depressurization valves	Two improvement items were identified in connection with: • Firewater • Risk analyses	(Statoil - Hammerfest LNG) *Barrier management:* There was insufficient determination of strategies and principles that should form the basis for the design, use and maintenance of barriers, so that the barrier function is maintained throughout the facility or land plant life. *Barrier performance requirements:* There was insufficient understanding and knowledge of the barriers that are established, and the functions

[20] TCS: Technical Condition Safety.

Main issues (year)	Objectives	Non-conformities	Improvement items	Comments
				they must fulfill, as well as of the performance requirements that are set at the technical, operational and /or organizational elements necessary for the individual barrier to be effective.
Major accident risk management, ***barrier handling*** (2010)	• Evaluate the company's understanding, knowledge and competence in connection with major accident risk and *barrier thinking* • *Evaluate strategies and principles for management, design, use and maintenance of barriers* – especially as regards major accident scenarios	• The personnel transport basket was set up as the primary rescue appliance during evacuation. • Deficient plan for training the fire team.	• Major accidents – *follow-up of barriers and performance requirements*: ○ A system was not established to safeguard the overall requirements for follow-up of barriers and performance requirements across the organization. Other improvement items: • The emergency preparedness plan did not appear to be user friendly, and was not updated. • A permanent fire fighting system had not been installed in the machine room to fight larger fires in the room in a quick and efficient manner. • Unclear procedures for evacuation with lifeboats in a major accident situation. • Deficiencies in training and drills. • Deficient battery-operated	(Odfjell Drilling)

Main issues (year)	Objectives	Non-conformities	Improvement items	Comments
			emergency lighting in rooms for CO2 containers.	
Major accident risk and ***handling of barriers*** (2010)	To evaluate the company's understanding, knowledge and competence as regards major accident risk and *barrier mindset*, on the part of both management and employees. Furthermore, to evaluate strategies and principles for *management, design, use and maintenance of barriers* – particularly with regard to major accident scenarios.	Six non-conformities were identified, including: • *Follow-up of barriers and performance requirements:* Comprehensive strategies and principles were not established for the design, use and maintenance of barriers. • Maintenance management and *barrier follow-up*	Eight improvement items, no one related to barrier management.	(Transocean – Transocean Leader) Excerpt from PSA's presentation of the audit report (09.12.10): Transocean's main management has defined which DFUs can primarily trigger major accidents. Currently there is not a complete overview of the appurtenant operational and organizational barrier systems, and the company lacks a systematic approach in the area. The implementation of the "bow-tie" methodology is intended to maintain and visualize the connection between hazardous situations and barriers. The PSA views the methodology as a useful tool that has a good potential for practical application through further development in the company. The methodology has recently been introduced, and has not yet been prepared for all major accident scenarios. The PSA found little familiarity with the bow-tie methodology and little knowledge of how this methodology was supposed to be used among the personnel on board Transocean Leader. The PSA found varying degrees of knowledge and understanding of which DFUs have major accident potential. It was not clear to the audit team that training and exercises focused on major accident risk were awarded special attention.

Main issues (year)	Objectives	Non-conformities	Improvement items	Comments
Organizational and human factors in handling well control (2012)	The companies should demonstrate vis-à-vis the PSA that a functional management system and associated work processes that contributed to safeguarding of well control had been established.	• Lack of compliance between Statoil's and Transocean's governing documents for handling well control • Using manual valves in drilling fluid systems	• Lack of performance requirements for volume control in connection with the drilling operation • Uncertainty regarding responsibility for communicating assessments and performance requirements to a third party • Deficient experience transfer from training and exercises • Overlapping systems for identification, assessment and management of risk • Inadequate presentation of information from the screens of the well service company	(Statoil and Transocean) The interviews stated that volume control (mud) is an *operational barrier element* that should be a subject for performance requirements. The audit revealed that the facility had not identified common performance requirements for volume control and that there was no requirement for alarm limits (margin) of volume expansion of the fluid system during operation. The informants claimed that supporting information for volume control (e.g. calculations of "kick tolerance") was communicated to the driller, but not to the mud logger. It appeared unclear how Statoil and / or Transocean ensured that drillers and mud logger (3rd party) had common supporting information, and who was responsible for communicating such information to the 3rd party.
Major accident risk, ***barrier management*** – light well intervention (2012)	• Evaluate the companies' understanding, knowledge and expertise related to major accident risk and *managing barriers* • Evaluate *strategies and principles that form the basis for design, use and maintenance of barriers* • Verify that performance requirements are established and implemented	• Deficient analysis of defined situations of hazard and accident (DSHA) • Deficient layout of kill and stimulation lines • Deficient basis for and documentation of maintenance	• Incompatible duties in emergency response organization • Blind zones and noise to radio communications • Responsible person for radiation on the facility was not clearly defined • Lack of employee involvement in the evaluation process of the required staffing	(Island Offshore , on contract for Statoil) An objective of the audit were also to develop PSA's own competence: • Develop the PSA's expertise in following up management's work to reduce major accident risk, and clarify the need to develop a framework and supervision methods • Contribute to the PSA development of their own methods that will form the basis for more effective barrier supervision

Main issues (year)	Objectives	Non-conformities	Improvement items	Comments
Process integrity; electrical systems, instrumentation and technical safety (2012)	Special emphasis on how Statoil, in collaboration with Aibel, ensures better understanding of: • The interaction between operator, development project, suppliers and operations preparations • The connection between the quantitative risk analysis, design accident loads, safety strategies and *the barrier elements' condition* and performance in a lifetime perspective.	• Inadequate documentation of facility-specific *performance requirements for barriers* • Inadequate protection against electrical power supply failure.	Improvement items identified within: • Flame detection • Command structure in the emergency shutdown system.	(Statoil/Aibel – Gudrun)
Technical and operational barriers (2012)	Special emphasis on how Eni, in cooperation with the building yard Hyundai Heavy Industries, ensures better understanding of: • The collaboration between the operator, development project, suppliers and operations preparations • The relationship between the quantitative risk analysis, dimensioning accident loads, design loads, safety strategies and the *barrier elements' performance requirements* in a lifetime perspective	• Incomplete specification and consistency between safety strategy and performance standards and underlying principles, specifications and guidelines to be applied for *the design, use and maintenance of barriers, so that the barrier function is maintained throughout the life of the facility*. Other nonconformities in relation to: • Risk reduction • Process securing system • Qualification and use of	Improvement items were identified in the following areas: • Quantitative risk analysis – purpose, application, definitions and timely updates in the engineering phase • Implementation and verification of "Safety Integrity Level" requirements (SIL requirements) • Gas emission system – documentation of chosen solution • Performance requirements for the emergency shutdown valves	(Eni Norge – Goliat FPSO) <u>Excerpt from PSA's presentation of the audit report (15.05.12):</u> Barriers are one of the PSA's four main priorities in 2012. Experience shows that the players have implemented the regulatory barrier requirements to varying degrees. Making barriers resilient in the different phases of a facility's life cycle has developed in different directions with varying maturity. Faults and inadequacies in one or more barrier elements' performance is a pervasive causal factor of incidents. This requires greater attention and closer follow-up, both from the players and authorities, to ensure continuous improvement.

Main issues (year)	Objectives	Non-conformities	Improvement items	Comments
		new technology	• "Cargo pump room" gas spread analyses based on mechanical ventilation and potential gas leaks • ATEX[21] implementation – non-electrical equipment • Emergency generator unit – independence and vulnerability	The audit was a follow-up and continuation of the PSA's previously conducted barrier audits of Goliat FPSO within the process integrity discipline in 2010 and 2011.
Commissioning of a drilling facility (2012)	The systems used for follow-up, testing and commissioning of the facility. Another intention was to verify compliance with regulatory requirements for selected solutions in electrical and safety systems, as well as how maintenance management and preservation work are safeguarded in relation to the company's own compliance measurements and reporting.	Non-conformities in relation to: • Procedure for commissioning activities • Maintenance program • Marking of equipment and components	Improvement items in relation to: • Risk and *barrier management*, with regard to how safety strategies are to be prepared and communicated • Document control system • Compliance with own preservation procedure • Certification and calibration of instruments • Frost protection of fire water line	(COSL Drilling Europe – COSL Promoter)
Maintenance management, electrical and safety systems – drilling facility (2012)	Technical and management aspects on the installation.	• The Company has not established a final strategies and principles that should form the basis for the *design, use and maintenance of barriers* to ensure that the *barrier*	Several improvement items in relation to electrical and safety systems on board.	(Saipem – Scarabeo 8)

[21] ATEX: Equipment and systems for use in hazardous areas.

Main issues (year)	Objectives	Non-conformities	Improvement items	Comments
		function maintained throughout the facility's life. Work on the development of *performance standards to ensure that barriers* are effective at any time was not completed. Other nonconformities included: • Maintenance management • Maintenance program • Certificates for equipment • Marking of equipment		
Electrical systems, incl. system for mapping and monitoring of ***electrical related barriers*** (2012)	Special emphasis on management system that comprise the person responsible for the electrical system's role, responsibility and tasks during engineering, operations, modification and maintenance of electrical systems.	• Deficiencies related to the *establishment and monitoring of electrical related barriers and performance requirements*.	Several improvement items in relation to organisation of the electrical discipline, onshore/offshore, quality assurance of minor modifications in electrical systems and routines for updating important operations documents.	(Norske Shell)
Safety-critical barriers (2011)	To verify that Statoil has followed up and further *developed performance requirements for barriers*. Emphasis was placed on reviewing requirements and implementation methodology for the preventive maintenance work that will *verify a barrier's performance*. The audit also looked *at how management has implemented and followed up the barrier requirements*.	None	One improvement item was proven, related to implementation of measures following TCS review.	(Statoil – Sture-terminal)

Main issues (year)	Objectives	Non-conformities	Improvement items	Comments
Technical barrier design (2011)	To assess how Eni Norge ensures *compliance with safety-critical barriers* in a comprehensive and consistent manner, as well as how Eni Norge follows up to ensure that the design solutions on Goliat FPSO fulfil the regulatory requirements and preconditions in the plan for development and operation.	• Deficiencies in the stated strategies and principles that should form the basis for the *design, use and maintenance of barriers* in the area of technical safety at Goliat FPSO. Inadequate systematic relationship between risk, strategy and the specific *performance requirements for barrier elements*.	Improvement items were identified in connection with: • Experience knowledge • Emergency shutdown system • CAP (Critical Action Panel)	(Eni Norge – Goliat FPSO)
Technical and management factors (2011)	To verify that the quality of performed compliance measurements of technical and management factors was satisfactory; To verify and follow up that the facility has been designed and built according to applicable requirements in the petroleum regulations.	One non-conformity related to barrier management: • The Company has not established policies and principles that should form the basis for *the design, use and maintenance of barriers.* It is not established *performance standards* to ensure that the barriers are effective at any time. Established philosophies are characterized by being aimed at the design and construction phase.	No improvement items related to barrier management.	(COSL Drilling Europe – COSL Pioneer)
Electrical systems and process safety (2011)	To gain an overview of systems and work processes for *management of technical and operational barriers* related to	• Deficiencies as regards hydraulics in the emergency shutdown system (ESD) • Deficiencies related to the	Improvement items were related to: • Internal audit of safety instrumented systems	(ConocoPhillips – Ekofisk)

Main issues (year)	Objectives	Non-conformities	Improvement items	Comments
	electrical systems and process safety, and to evaluate this in relation to applicable regulatory requirements within the audit's technical areas.	documentation of the ESD system.	• Documentation of process safety • Information about deviations • Maintenance of electrical equipment	
Technical and operational barriers (2011)	To assess how Statoil at Statfjord B safeguards *barrier management.*	None	Improvement items were related to: • *Inadequate strategy for follow-up of barriers* (i.e. no clear relationship between risk and strategy and the acceptance criteria for barriers). • Inadequate *overview of barrier status* • Inadequate description of roles	(Statoil – Statfjord B) Excerpt from PSA's presentation of the audit report (01.04.11): The industry must be able to describe and implement work processes, and the individual elements in these processes, for barrier management in a lifetime perspective through: • Describing and highlighting the connection between risk and hazard assessment, the need for barriers and the barriers' role in the individual area (strategies) • Identifying, describing and implementing performance standards for defined barriers and risk-influencing factors • Identifying conditions that could reduce the barriers' performance over time (changed user conditions, degradation mechanisms, aging, incidents, etc.), establishing indicators for monitoring function and performance, and processes for making barrier function and performance robust enough to handle these conditions • Continuously improving the barriers and the system for barrier management

Main issues (year)	Objectives	Non-conformities	Improvement items	Comments
				Safety-critical barriers must be maintained in a comprehensive and consistent manner so the risk of major accidents is reduced as much as possible. A barrier can be considered a function which prevents or influences a concrete course of events in a deliberate direction by limiting damage and/or loss. The term function refers to the barrier's task or role, for example, preventing leaks or preventing spread.
Work processes for ***barrier management*** (2012)	To follow up how ExxonMobil satisfies regulatory requirements for *risk reduction and barriers* in a lifetime perspective.	Non-conformity was identified in relation to robustness in the emergency preparedness organization.	Improvement items were identified in relation to: • *Barrier management:* Deficient anchoring of the performance requirements for barrier testing in the design requirements • Capacity in the organization • Labeling of facilities, systems and equipment	(ExxonMobil – Balder FPSO) The organization does not have sufficient understanding of how the criteria for *barrier performance* and testing are based on assumptions for the design, related to regulations, standards and *barrier philosophy*.
Barrier management (2011)	To verify that the company complies with the regulatory requirements related to own follow-up and *barrier management.*	Two non-conformities in relation to: • Inadequate prioritization of *barrier management.* • Inadequate technical risk reduction		(Statoil – Mongstad) *Barrier management:* Efforts to systematize barrier management to satisfy regulatory requirements. The work is not sufficiently prioritized and is not given adequate support. The work was not clearly rooted in action plans.
Operational and organizational barriers with a main focus on preparedness (2012)	To verify that certain *operational and organizational barriers* are safeguarded in a comprehensive and consistent manner, so the risk of major accidents is reduced as much as	Non-conformity was identified in relation to the basis for updating emergency preparedness analyses (EPA): • Lack of system to ensure that results of the risk	Improvement items were identified in relation to: • Execution of the preparedness analysis • Preparation of a new	(Statoil – Mongstad)

Main issues (year)	Objectives	Non-conformities	Improvement items	Comments
	possible. Furthermore, that the residual risk is handled in a good manner through well-planned preparedness and a robust preparedness organization.	analysis, *including requirements for barriers* and operating conditions and limitations, are forwarded to the EPA.	preparedness plan	
Management systems and work processes for managing risk (2012)	To follow up how A/S Norske Shell satisfies regulatory requirements for *risk reduction and barriers* in a lifetime perspective.	None	One improvement item was identified in relation to the description for testing ESD valves.	(Norske Shell – Nyhamna)
Risk management – drilling company and drilling facility (2012)	To evaluate emergency preparedness management on Mærsk Inspirer, including the company's emergency preparedness philosophy, how this is incorporated into analysis, governing documentation and procedures, *management and follow-up of barriers* in relation to emergency preparedness.	Eleven non-conformities, included: • Deficiency in risk management • Deficiency in *barrier strategy* • Performance standards do not reflect the *requirements related to barriers*	Four improvement items, but none of them related to barrier management.	(Maersk Drilling Norge – Maersk Inspirer)
Barrier management (2011)	To ensure that Teekay Petrojarl has a management system in place that safeguards the regulatory requirements for *barrier management* in a lifecycle perspective. Furthermore, the audit followed up how the different parts of the	Non-conformities were identified in connection with: ***Barrier management in the base organization:*** • It was not established adequate requirements and policies that in a compre-hensive manner take care of regulatory requirements for	Improvement items were identified in relation to: • Use of regulations and standards • Use of titles and preparation of documents • Preservation during the project period	(Teekay Petrojarl – Knarr FPSO) The activity identified that the barrier management regulatory requirements was not adequately safeguarded by the company. Procedures and guidelines in the company did not comprehensively safeguard all of the regulatory risk and barrier management requirements. However, work was ongoing to further develop some of the processes and

Main issues (year)	Objectives	Non-conformities	Improvement items	Comments
	management system were implemented in the Knarr project.	risk and barrier management. Some existing requirements were not implemented on their installations on the Norwegian continental shelf. ***Barrier management in the Knarr project:*** • The strategy document did not encompass all relevant requirements for determining strategies and principles that should form the basis for design of barriers. • Performance requirements for barrier elements necessary for the individual barrier to be efficient was not highlighted and collated. The process of determining the requirements were not described. Other non-conformities were related to: • Implementation of analyses and safety studies • Verification and follow-up plans in the project		systems the company would use.

Main issues (year)	Objectives	Non-conformities	Improvement items	Comments
Major accident risk and ***barrier management*** (2011)	To evaluate the company's understanding, knowledge and expertise related to major accident risk and *barrier system mindset*. Another objective was to evaluate strategies and *performance standards* that are to form the basis for *the design, use and maintenance of barriers* so that the barriers' function is safeguarded throughout the lifetime of the facility.	Non-conformities were identified in relation to: ***Follow-up of barriers and performance requirements*** • It was not established strategies and performance standards in a holistic way encompassed all require-ments for monitoring of barriers. Other non-conformities were related to: • Fire risk in the engine room • Maintenance routines for equipment • Battery emergency lights • Gas detection • Stretcher transport of persons in the stairwell in the living quarters • Signposting and marking of escape routes	Improvement items were identified in relation to: • Fire-fighting using fixed CO_2 extinguishing systems • Preparedness • Notification of the joint rescue coordination centre	(Dolphin Drilling) It was observed that the company did not fulfill all the requirements for barrier management, but that an internal project had been initiated to ensure compliance with regulatory requirements.

Main issues (year)	Objectives	Non-conformities	Improvement items	Comments
Management of the working environment and ***safety-critical barriers*** (2011)	To evaluate: 1. Management of working environment risk 2. Management of *technical and operational barriers*: • Systems for management of barriers • Preventive work to ensure quality of important barriers • Systems and equipment that will prevent ignition of hydrocarbon leaks • The management's involvement, particularly in relation to implementation and follow-up of barrier requirements in the new regulations.	No non-conformities in relation to barrier management.	Two improvement items in relation to safety-critical barriers: • *Missing or incomplete strategy to design, use and maintenance of barriers to reduce risk* • Hooking up and disconnecting heating cables in connection with winterization	(Statoil – Tjeldbergodden)
Major accident risk ***and safety-critical barriers*** (2011)	To verify that the company safeguards the regulatory requirements related to the selected topics within major accident risk and *barrier management*	None	One non-conformity in relation to management of safety-critical barriers: • *Inadequate strategies and principles for barrier management*	(Statoil – Kårstø) Determining the strategies and principles that should form the basis for the design, use and maintenance of barriers, so that the barrier function is maintained throughout the life of the country is not complete. Performance requirements for barriers are known only within a small academic community.

Main issues (year)	Objectives	Non-conformities	Improvement items	Comments
Barrier management (2011)	To assess the company's planning, implementation and follow-up of activity on Sleipner in relation to relevant regulatory requirements.	Non-conformities in relation to: • Inadequate *identification and monitoring of barrier elements.* • Unclear proven connection between risk analysis and strategy and the specific *performance requirements for barrier elements*. • Lack of system for monitoring conditions in the risk analysis. Other non-conformities in relation to: • Testing of valves critical to safety • Fire division in fire pump room • Evacuation	Improvement items included: • *Testing of barrier elements:* Related to the function test of the safety critical valves not always the results of the first test are reported in the maintenance system. • Deficient *identification and monitoring of barrier impairments*.	(Statoil – Sleipner A, T and R) <u>Excerpt from PSA's presentation of the audit report (23.06.11):</u> One of the PSA's main priorities is maintaining barriers. PSA is aware that the players have implemented regulatory requirements relating to barriers to varying degrees in accordance with the intention. Errors and deficiencies in one or more barrier elements' performance are general causal factors of incidents. Strategies and processes for making barriers robust in the different phases of a facility's life cycle have developed in different directions and have varying degrees of maturity. There is a need to highlight common denominators and complementary properties between the barrier elements' condition and performance, operation and maintenance management and risk management.

(Empty page)

Appendix B: Paper on Safety Barriers: Organizational potential and forces of psychology

(Empty page)

Journal of Loss Prevention in the Process Industries 31 (2014) 50–55

Contents lists available at ScienceDirect

Journal of Loss Prevention in the Process Industries

journal homepage: www.elsevier.com/locate/jlp

Safety barriers: Organizational potential and forces of psychology

Fred Størseth*, Stein Hauge, Ranveig Kviseth Tinmannsvik

SINTEF Technology and Society, Safety Research, NO-7465, Trondheim, Norway

ARTICLE INFO

Article history:
Received 20 May 2014
Received in revised form
27 June 2014
Accepted 29 June 2014
Available online 10 July 2014

Keywords:
Macondo
Safety barriers
Organization
Psychology

ABSTRACT

Safety barriers are often described as a safety function realized in terms of technical, operational and organizational barrier elements. These elements, in some shape or configuration are established to ensure that the barrier works as intended.

While technical and operational barrier elements appear fairly definable, the organizational barrier element often remains elusive. An appealing solution oriented strategy is probably to urge for a clear-cut categorization of what applies as 'organization'. This tactic may contribute to a tidy method with respect to barrier categorization. However, the question remains whether it is possible or desirable to confine the organizational influences to categorical classifications?

The aim of this paper is to address this question by examining the run-up to the Macondo blowout from a barrier element perspective.

Hopkins' (2012) analysis of the Macondo blowout is applied to identify patterns of organizational impact in three of the pre-blowout defenses: The cement job, the well integrity test, and the kick monitoring.

By re-analyzing Hopkins' study from a barrier element perspective we argue that the organizational impact may morph and change in nature, be contagious and spread across barriers, and travel long distances. The implication is a need to rethink the impact of organizational barrier elements. Part of this rethinking involves acknowledging the impact of psychological mechanisms like consensus-mode decision-making, confirmation bias, normalization of warnings, groupthink as well as social forces of power and persuasion. It is shown how such psychological forces may serve as 'transmitters' of organizational principles, strategies and decisions throughout the barrier system. In turn, this may contribute to risk transfer, and dependence between barriers.

1. Introduction

Safety barriers are part of orthodoxy in safety science and management. Represented by the classic Swiss cheese metaphor, this is the idea of a string of defenses, or barriers – aligned so that if any of the preceding barriers fails, the subsequent defense in line will do its job of preventing the occurrence of hazardous events or limiting their consequences. The safety philosophy forming the basis for barrier management is often denoted 'defense in depth' (Reason, 1997) (referring to the deep layers of defenses or barriers established to prevent harm). Defending 'in depth' may also trigger associations along the lines of 'going deep into the complexities' and so on. In terms of accident causation and explanation, 'further back' is often related issues of organization. Current efforts to understand the organizational impact is a lucid reflection of the acknowledgment that organization matters (see e.g. Weick & Sutcliffe, 2007). Organizational issues may be a forceful contributor to maintain safety; but also in the development of major accidents. Connections between organization and safety are compellingly addressed and revealed in the literature (e.g. Hopkins, 2008; Reason, 1997; Vaughan, 2005).

A barrier is often described by referring to its function. That is, barrier x is established in order to implement function y (e.g. the flare system is installed to relief the process pressure). The barrier function may here be realized and maintained by barrier elements. These barrier elements are typically classified as technical, operational, or organizational. In this approach, a barrier can be defined as *'…technical, operational and organizational elements which are intended individually or collectively to reduce the possibility for a specific error, hazard or accident to occur, or which limit its harm/disadvantages'* (PSA, 2013, page 3).

While technical and operational barrier elements appear fairly definable, the organizational barrier element often remains elusive. An appealing solution oriented strategy is probably to urge for a

* Corresponding author.
E-mail addresses: fred.storseth@sintef.no, fredstoe@online.no (F. Størseth).

http://dx.doi.org/10.1016/j.jlp.2014.06.006
0950-4230/

clear-cut categorization of what applies as 'organization'. This tactic may contribute to a tidy method with barrier elements of unambiguous character. But, will a categorical classification of organization solve the challenges related to acknowledging the actual influences on safety? The aim of this article is to address this question by examining the run-up to the Macondo blowout from a barrier element perspective.

2. Conceptual framework

A rendition of Hopkins' (2012) analysis of the Macondo blowout is used as source and conceptual framework.

The following presents selected elements of Hopkins' (2012) analysis of the Macondo accident. This presentation is limited to looking at episodes related to three of the defenses before the blowout: the cement job, the well integrity test, and the kick monitoring.

A simple chronology of the run-up to the Macondo accident: at 5.45 am, 16 h before the blowout, the cement job was declared a success; at 8 pm the well integrity test was affirmed as ok; in the hour before the blowout there were indications that something was wrong. These signals passed unnoticed as no one was monitoring the well; at 9.45 pm drilling mud were churning out – the catastrophe was a fact.

See also the reports from the National Commission to the President (National Commission, 2011a, 2011b as well as Tinmannsvik et al., 2011). Fig. 1 depicts the pre-blowout defenses.

2.1. Cement job

The rig was about to move and begin its next job. In order to leave the well in a safe state, the bottom had to be plugged with cement. This was a case of a 'temporary abandonment' as the well would later be converted to a producing well. This would involve drilling the cement out for oil and gas to flow into the well. The Macondo engineers planned and executed the cement job. And on completion, they declared it a success; a textbook job (Hopkins, 2012). According to Hopkins, this declaration of triumph was based on indications of full returns of fluid and thereby no signs of losses into oil and gas sands. Full returns denote the process when cement is pumped down into position; equal amount of fluid should be coming out on top of the annulus as is going down the casing. This particular well design demanded high pressure on the cement near the well bottom. This increased the possibility of a loss into oil and gas sands. As noted by Hopkins however, this error mode was only one of at least four plausible error modes. The three others were: (i) instable cement (due to the light weight foam cement that was needed in this particular well design); (ii) channeling (i.e. that the cement leaves mud channels behind it during cement placement), (iii) contamination (i.e. that mud is blended into the cement, leaving a less than optimal cement consistency) (Hopkins, 2012).

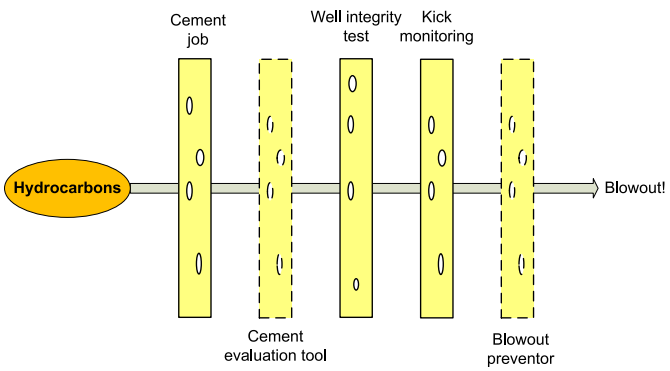


Fig. 1. Pre-blowout defenses in the Macondo accident (based on Fig. 4.1 in Hopkins, 2012, page 54).

Hopkins' point is that a fallacy was made. By concluding that the cement job was successful (due to signs of full returns) the job was affirmed as completed. The declared success rendered the cement evaluation (cement bond log, CBL) unnecessary. The crew that was ready to perform the CBL was brought home by helicopter. By declaring the job a success, corners could be cut by omitting the cement evaluation test, and thereby save money. By the time of the blowout the operation was 38 days delayed and an estimated $58 million above budget (Chief Counsel's Report, National Commission, 2011b). The presumption being, that any needed mitigation regarding cement instability could be done at a later stage. In this way, progression of an already delayed job was ensured. Hopkins (2012) shows how tunnel vision and a consensus mode of operandi contributed to the declaration of a successful cement job.

2.1.1. Tunnel vision engineering

Hopkins argues that the Macondo engineers displayed tunnel vision engineering. Their eyes were fixated on one objective: a well design that was cheaper and would enable easier production when that time came. It was as if peripheral risk awareness was virtually eliminated. Hopkins traces this tunnel vision back to a 'management of change' (MoC) document that had been previously designed to give formal authorization for the well design. Here, the potential of loss of mud into surrounding sands was emphasized specifically. This hazard was in other words primed in the engineers' minds. From the beginning (design approval stage), only one of at least four possible failure modes was addressed (Hopkins, 2012).

2.1.2. Decisions in consensus-mode

Decisions were made in a consensus-mode, effectively made in settings where no one could be held accountable later on. This is according to Hopkins illustrated by (1) decisions that were made in meetings intended to collect information; with the implication of making all – and in effect no one actually responsible; and (2) the management of change documents that were reviewed and approved by a long string of signatures. These signatures often belonged to the same people as those being involved in the plan. In other words, there was no independence, and the system of assurance served only to undermine the process. The MoC process, in reality, was a consensus decision-making process; with the disturbing effect that responsibility was diluted (Hopkins, 2012).

2.2. Well integrity test

Before moving the rig to the next location, the integrity of the well had to be tested (this is part of the temporary abandonment procedure). Removing riser and mud leaves the well underbalanced, meaning that the cement seal must function. In order to test the sealing, a temporary reduction in well pressure is administered. The logic of this test is: a pressure rise indicates that oil and gas flows into the well bottom, meaning that the seal is not working. If the seal does work, the pressure remains steady. The test involves pumping sea water down the drill pipe under high pressure; this, in order to force the mud upwards, thereby creating a water cavity. When the mud level is positioned above the blowout preventer, this is closed with a rubber seal. The cavity (between well bottom and rubber seal) now simulates a situation of no other defense than the cement being in place. Having created this space,

the valve on the drill pipe on the rig is opened in order to drop the pressure. The key point is thus that, if the cement sealing worked – the pressure at the top of the drill pipe would remain at zero. The team opened the valve to reduce pressure; but as soon as they closed it, pressure began to rise. The same thing happened in a second attempt. The pressure increased. Still, the team would not accept this result (Hopkins, 2012).

Hopkins shows how the following social psychological processes contributed to this 'denial': confirmation bias, normalization of deviation, inadequate situational awareness and groupthink.

2.2.1. Confirmation bias

In psychology, confirmation bias refers to the unconscious tendency of preferring information that confirms ones beliefs; a tendency of selective use of information. Hopkins (2012) points to several features that contributed to confirmation bias in relation to the well integrity test. First, the rarity of the phenomenon is in itself a dimension here. As a well integrity test rarely fails, this is itself a bias towards viewing the test as a way to confirm that the well was ok, rather than to test if it was ok. Second, it was not only those carrying out the test that executed confirmation bias. The engineers had just days earlier designed a decision tree, at which the well integrity test was defined as a point in a sequence – as opposed to a decision-process. Put differently, the diagram presupposed that the test would be fine. Third, the first draft of the work plan for the day of the blowout did not refer to the well integrity test. According to Hopkins, this demonstrates that it was not seen as a critical operation. Fourth, the cement job that had been completed just hours previously had been declared a textbook operation (Hopkins, 2012). Taken together these are forces pushing to create a strong confirmation bias for those making the decisions.

2.2.2. Normalization of warnings

This is a variation of what Diane Vaughan called normalization of deviance related to the space shuttle Challenger. It refers to a reconceptualization and normalization of a partial malfunction, until it at some point became assessed as an acceptable risk (Vaughan, 2005). Hopkins (2012) shows how a similar normalization took place during the well integrity testing at the Macondo well. The pressure readings were normalized by reference to a 'bladder effect' theory; a suggested explanation for the change of pressure. '*The 'bladder effect' explanation contends that heavy fluids (mud and spacer) displaced to the riser were exerting force on the annular preventer from above, which in turn communicated pressure into the well*' (Chief Counsel's Report, National Commission, 2011b, page 157).

When the riser is pressure tested, the mud in the riser is supported by a rubber seal that is closed around the drill pipe. The intention of this seal is to '*…isolate the water in the cavity below the seal from any downward pressure exerted by the mud*' (Hopkins, 2012, page 43). The bladder theory provided an explanation ("normalization") of the exerted pressure by claiming that this seal is somewhat flexible, so that the mud above exerted pressure on it. This would create added pressure on top of the drill pipe. This was advocated by some. Others had never heard of it, but became persuaded by the concept. According to Hopkins, the bladder effect has no credibility in comfortable hindsight. It was the normalization of an unambiguous warning (Hopkins, 2012). The bladder theory provided a needed explanation of the pressure readings. Still, they needed some evidence to be able to establish that the well was safe. Thus, a decision was made to use the 'kill-line' to perform the pressure test. They filled the kill pipe with water, opened the valve to reduce the pressure, and closed it. This time, the pressure remained at zero in the cavity (the wanted result), but the pressure remained high on top of the kill pipe. The difference in pressure was ignored. It was decided to go with the pressure reading from the kill pipe (showing a steady zero). Hopkins links this with mental models and situational awareness. He draws attention to the fact that if the kill pipe was in contact with cavity, a difference in pressure would not be possible. Therefore, if the team understood the picture, they could not have accepted the pressure difference (Hopkins, 2012).

2.2.3. Groupthink

According to Hopkins, a vital point is to understand the composition of the group. The formal decision-maker was the BP company man. On any shift a company man would be on duty. The well integrity decision was however taken in a shift transfer – meaning that there were actually two BP company men present. In this case then, the decision group consisted of: Two BP company men accompanied by a trainee. From Transocean, there were two long-serving drillers and an assistant driller. Within this group, Hopkins advocates that the psychological process of groupthink took place; a process that deters questioning the wisdom of the dominant view. Groupthink and group decision-making may be affected by 'risky shift', where groups are often more inclined to make risky decisions than individual group members (Shaw, 1976). Hopkins argues that group decision-making tends to absolve individuals of responsibility. Groupthink involves a presumption (within the group) that it will be unanimous. In principle, any doubting group members would be in a powerful position here, as they may well block consensus. However, the pressure exerted on them (from the other group members) is to accomplish consensus (Hopkins, 2012).

Hopkins' point is that, to understand the decision, it is necessary to identify the actual power of the group. This demands looking at the culture on the rig, with a tight rig crew (from Transocean). Hopkins describes the driller culture as a group of highly skilled, opinionated technicians taking personal interest in every well. They take on leadership. Also, the complexity of the operations (drilling) is typically reflected in an esoteric language with extensive use of slang expressions and acronyms. What is more, peer pressure is extensive, with widespread use of teasing and humor. "Unintelligent" questions are heavily sanctioned. This was the culture that the BP company men had to resist. At first, the company men were skeptical to the bladder theory; but one of them found it acceptable leaving one person outside the "good company of agreement". During later interviews, he has told that his reluctance to accept the bladder explanation was found humorous by the drillers. The dominant view triumphed in the end, the test was declared as passed. This is groupthink in action. According to Hopkins, the social processes made it "virtually impossible for them to act independently" (Hopkins, 2012, page 49).

2.3. Kick monitoring

'A kick is an unwanted influx of fluid or gas into the wellbore. The influx enters the wellbore because a barrier, such as cement or mud, has failed to control fluid pressure in the formation. In order to control the kick, personnel on the rig must first detect it, then stop it from progressing by adding one or more barriers' (Chief Counsel's Report, National Commission, 2011b, page 165). As kicks are considered blowout precursors, monitoring the circulation of fluids is important. The well monitoring instrumentation and the training of the operators on Deepwater Horizon were however inadequate to effectively detect a kick (Chief Counsel's Report, National Commission, 2011b, page 182).

Drilling involves constant circulation of fluids in and out of the well. If oil and gas enters the well bottom, the outflow will exceed the inflow; the result being that the well is 'flowing'. The fluids

going into the well are normally drawn from the pit (input tank) – while fluids coming out of the well go into the outflow pit. The comparison of these pits serves as an instrument to control (monitor) for well flowing. The monitoring responsibility on the rig was shared by the Transocean drillers and assistants, and a mudlogger from the company Sperry Sun. The well was in a critical stage; seawater had replaced the mud, leaving the well underbalanced. In other words, the only defense in place was the cement plug. Still, the Transocean crew had effectively made flow monitoring impossible by running outflow directly to a supply vessel (as opposed to the outflow pit, to save time). The mudlogger made a complaint to the drillers that this prevented monitoring. This complaint was disregarded. (Hopkins also points to a second fluid discharge, something that prevented the second mudlogger (due to shift change) from monitoring). The point is; the drilling crew prevented the monitoring capacity for the mudloggers as well as for themselves (Hopkins, 2012).

2.3.1. State of mind = finish up

Hopkins (2012) suggests that the practice of bypassing the outflow pit was a norm on the rig. In any case, the puzzling question is why they did not acknowledge the criticality of what they were doing. Why did the drillers act with so little concern? Hopkins' point is that they acted in a state of mind where the job was defined as over. Drilling was finished, the well had been declared safe twice (cement job, well integrity test). Their modus operandi was now simply to finish up and to move on to the next job. Also, they were short on time. Tank cleaning personnel were arriving, ready to start their work.

In the next section, we present a re-examination of Hopkins' analysis, with the specific aim to identify constellations and patterns of barrier elements.

3. Re-analyzing Hopkins'

We must begin by pointing out that the Deepwater Horizon drilling rig was not subject to a strict 'barrier management regime' with specified barrier elements. Our re-analysis is thus an attempt to identify how barrier elements could look like and interact within the Macondo run-up.

Hopkins emphasizes that contextualization is the key to understand the decisions and actions taken in the *cement job.* He traces the engineers' tunnel vision back to the MoC-document, a document that from the onset established only one error possibility (loss of mud into sands). Also, the possibility of accountability was effectively pulverized by consensus mode decisions (cf. decisions made in information meetings and the long string of approval signatures from people that lacked necessary independence).

This contextualization has an organizational flavor. But, are these features organizational barrier elements?

If we pursue the possibility that they are, this suggests a long distance link between operational and organizational barrier elements. Put differently, we catch a glimpse of a barrier element constellation with operational elements in close vicinity to the actual barrier function, but with an organizational contribution that travels a considerable distance, from managerial echelons straight into the heart of the barrier.

On the other side, what if this kind of influence is rejected as a barrier element? In conventional barrier approaches, a barrier element is defined as a measure or solution playing a direct part in realizing a barrier function. This definition suggests that long distance impact will be an outlier by definition. Even if rejection is the case, we argue that Hopkins' contextualization points demonstrate the crucial importance of identifying paths from further back in the organizational echelons and straight in to the operational core. If this impact falls outside of the conventional definition of barrier element, it is still an active organizational impact; meaning that it affects the performance of the barrier. The challenge is thus for barrier management approaches to find ways to acknowledge and handle this long distance organizational impacts.

The implication by this is that although proximity to hazard may remain a critical criterion when considering barriers and barrier elements, it should not be the only criterion. The scope should be expanded.

Risk transfer is another aspect that is brought to the fore by opening for long distance coupling of barrier elements. In the cement job, the organizational issues acted as a trigger for the operational barrier element actions (declared success) further down the line of defenses. In turn, this declaration of success acted both to transfer of risk and to undermine the defense in depth principle of maximizing each barrier.

Risk transfer is also the case in the *well integrity test*. A relevant approach here is to look at how decisions made in the previous defense (cement job), served to diminish the search for hazards. By declaring the cement job a success, all risk handling was effectively transferred to 'the next in line', in this case, the well integrity test.

What was the declaration of success? Was it just another operational failure; that in turn contributed to a subsequent operational failure (in the well integrity defense)? We argue that the declaration of success can be seen as transforming in character. That is, that it morphs from operational to organizational; it becomes an organizational premise that plays a key role in the subsequent well-integrity test. In this way, the organizational impact stretches out and travels across barrier functions.

The way that the organizational impact stretches across barriers is further demonstrated in the *kick monitoring*. By the time of the kick monitoring, the state of mind was to 'wrap up'. When the defenses are seen in coherence, what springs forward is a total lack of barrier independence. From the onset (cement job), each defense were relying on the subsequent defense in terms of risk handling, creating a systematic transfer of risk throughout. In effect, the principle of barrier independence appeared as completely undermined.

4. Discussion

The key implication in terms of barrier element categorization is that the organizational contribution may come from 'somewhere else'. Put differently, the organizational impact travels long distances. Opening up for long distance organizational influences creates sensitivity towards possibilities of risk transfer and barrier dependence. These are possibilities that must be actively sought prevented in defense in depth strategies.

As per today, barrier element categorization has a strong focus on front end personnel and technical systems. Based on our paraphrasing of Hopkins' analysis, we argue for a need to broaden the scope of barrier management. This involves rethinking the organizational potential and acknowledging the potential impact of psychological mechanisms. Although Hopkins' analysis is saturated with organizational impact, another core issue is psychology.

4.1. Forces of psychology

Hopkins points to specific psychological mechanisms as contributors to the barrier breakdowns leading to the Macondo blowout:

- Tunnel vision (inadequate risk awareness)
- Decision-making in consensus-mode
- Confirmation bias

- Normalization of warnings
- Groupthink

A common denominator of these mechanisms is that they are permeated with 'the social'. There are strong social psychological forces at play here. In fact, we are confronted with the powerful potential of social psychological group dynamics and interaction. These forces of psychology can thus be defined as '*dynamics of social interaction*'. For our purposes then, in terms of safety barrier thinking – this strongly suggests paying attention to what happens *between* people.

People affect each other. This is well recognized by Hopkins (2012) as his analysis addresses the impact of broad ranging social psychological forces related to persuasion, pressure, and power. The 'bladder effect' dilemma is a vivid example of the triad of persuasion, pressure and power in action. The social forces in the group effectively defused any attempt to think differently.

But, this triad of persuasion, pressure and power can be said to cut across and be part of all the defenses considered here (cement job, well integrity test, and kick monitoring). In this vein of thought, we argue that the dynamics of social interaction have an additional role in terms of barrier elements. Hopkins' study put emphasis to a critical link between organization and people. Of course, at some point any organization can be said to be the people in it. However, Hopkins' analysis illuminates an additional point: That the organizational impact may be *channeled* by psychological mechanisms. In this way, organizational principles, strategies or decisions are potentially transmitted or carried forward throughout a line of barriers by forces of psychology.

As shown in this article, the forces of psychology that needs attention, is very much part of what psychology denotes *group dynamics*. Groups can be both efficient and important, in terms of trying to ensure safe and adequate decisions. But, the potential negative side effects of group dynamics should be considered seriously. As noted by Forsythe: '*Wh*en a group sacrifices rationality in its pursuit of unity, the decisions it makes can yield calamitous consequence' (Forsythe, 2009, page 313). The potential impact of how the people interact and affect each other in their efforts to realize a barrier function cannot be ignored.

The impact of psychological mechanisms and social forces are important issues that currently receive little attention in safety barrier approaches. More focus on including these mechanisms as an active part of barrier management therefore seems important.

4.2. Rethinking the organizational potential

We argue for a need to acknowledge that organizational elements may:

1. *Morph and change in nature* (e.g. from management strategy to operational decision).
2. *Be contagious* (in the way that organizational structures or principles may represent 'default' solutions that travels unquestioned across barrier functions).
3. *Travel long distances* (the unquestioned 'free-passing' (cf. point 2) is a force that potentially propels the organizational influence over long distances).
4. *Be channeled and transmitted* by forces of psychology (dynamics of social interaction).

These points emphasize the value of broadening the scope of organizational issues as part of barrier management. It may also suggest how: A broadening of scope should involve loosening up the categorical approach dictating a finite and static formula to define and establish organizational barrier elements. Alternatively or additionally, these organizational elements must be incorporated in the analysis as part of the risk influencing conditions that may influence several barrier elements (and thus contribute to risk transfer, and dependence between barriers). The 'forces of psychology' are critical here, and should permeate any of these broadening efforts.

This broadening of scope can in a sense be seen as a rethinking of the organizational potential; from organizational impact as a static proportion – towards a sensitivity of organizational elements or influences that in nature may be transient, changeable and context dependent.

5. Conclusions

- The scope of organizational influences should be broadened. One way to widen the scope could involve loosening up the categorical approach dictating a finite and static formula to define and establish organizational barrier elements. Alternatively or additionally, the organizational elements must be incorporated in the analysis as part of the risk influencing conditions that may influence several barrier elements. The approach to establish the organizational potential must be flexible, sensitive to context and open for changes.
- The impact of psychology must be incorporated into safety barrier approaches. Training is frequently emphasized as the curative way to go. People must be trained – to become capable, proficient and effective. The advantages of various training programs are pushed out and promoted by the safety experts. What often lacks is a focus on social forces and mechanisms that may well permeate the suggested measures and methods. In terms of safety barriers, there is a need to acknowledge how forces of psychology may affect the barrier system. A specific action that should be considered is to systematically examine barrier functions in terms of forces of psychology ('dynamics of social interaction'). A parallel critical action in these respects is to thoroughly consider the potential for risks to spread across barrier functions via these types of 'dynamics of social interaction'.
- The organizational and psychological mechanisms discussed in this article by nature influences several barriers and barrier elements and thus contribute to risk transfer, and dependence between barriers. Future barrier management should therefore emphasize more on incorporating these mechanisms when defining barriers and barrier elements, and when establishing performance requirements and indicators for measuring the performance.

Acknowledgments

This study has been performed as part of the research project "Tools and guidelines for overall barrier management and reduction of major accident risk in the petroleum industry", and has been funded by the Research Council of Norway (220841) and the PDS forum participants (PDS is a Norwegian acronym for reliability of safety instrumented systems. For more information about PDS and the PDS forum see: www.sintef.no/pds). We will also like to thank everyone who has provided comments and input to this work.

References

Hopkins, A. (2008). *Failure to learn. The BP Texas City Refinery Disaster*. CCH Australia.
Hopkins, A. (2012). *Disastrous decisions. The human and organisational causes of the Gulf of Mexico blowout*. CCH Australia Limited.
Forsythe, D. R. (2009). *Group dynamics* (5th ed.). Belmont, USA: Wadsworth, Cengage Learning.

National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling. (2011a). *Deepwater – The Gulf Oil Disaster and the Future of Offshore Drilling*. Report to the President.

National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling. (2011b). *The Chief Councel's report. Macondo – The Gulf Oil Disaster*. A supplement to the report to the President.

Reason, J. T. (1997). *Managing the risks of organizational accidents*. Ashgate Publishing Company.

Tinmannsvik, R. K., Albrechtsen, E., Bråtveit, M., Carlsen, I. M., Fylling, I., Hauge, S., et al. (2011). *The Deepwater Horizon accident: Causes, lessons learned and recommendations for the Norwegian petroleum activity*. SINTEF report A19148, Trondheim, Norway. (in Norwegian; executive summary in English).

PSA. (2013). *Principles for barrier management in the petroleum industry* [*Prinsipper for barrierstyring i petroleumsvirksomheten*]. Petroleum Safety Authority Norway.

Shaw, M. E. (1976). *Group dynamics: The Psychology of Small Group Behaviour*. New York: McGraw-Hill.

Vaughan, D. (2005). System effects: on slippery slopes, repeating negative patterns, and learning from mistake? In W. H. Starbuck, & M. Farjoun (Eds.), *Organization at the limit. Lessons from the Columbia Disaster* (pp. 41–59) Blackwell Publishing.

Weick, K. E., & Sutcliffe, K. M. (2007). *Managing the Unexpected: Resilient performance in an age of uncertainty*. Jossey-Bass.

Technology for a better society

www.sintef.no