



Faculty of Science and Technology

MASTER'S THESIS

Study program/ Specialization:

Offshore Technology

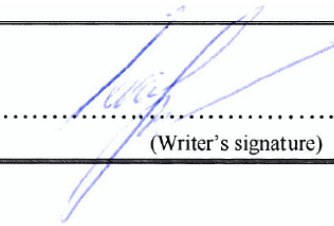
Industrial Asset Management

Spring semester, 2014

~~Open~~/ Restricted access

Writer:

Aleksandras Sevcik


.....
(Writer's signature)

Faculty supervisor: **Ove Tobias Gudmestad**

External supervisor(s): **Egil Hope - Aker Solutions AS**

Thesis title:

Control of safety barriers through maintenance system

Credits (ECTS): **30**

Key words:

Safety, barrier, control, maintenance

Pages: ...**34**.....

+ Enclosure: ...**128**.....

Stavanger, 2014

Abstract

Measures used to reduce the likelihood of hazardous events and limit the consequences of major accidents are generally referred to the term ‘safety barriers’. There are challenging to identify due to the wide variability of work processes and complex interactions between technical systems. In addition, the question is whether safety barriers are the only measures for risk reduction. A holistic view is required in order to foster adequate comprehension.

There is much discussion about safety barriers and the interactions between them in the offshore industry on the Norwegian Continental Shelf (NCS). This discussion is fostered to a large extent by the Norwegian Petroleum Safety Authority’s (PSA) emphasis on safety barriers. The PSA focuses on maintaining a high level of health, environment, and safety awareness within the petroleum activities on the NCS. The application of safety barriers has been a key safety principle in the PSA regulations for more than 10 years to guide the Norwegian oil and gas industry. The PSA constantly emphasizes the necessity for the risk picture to be clear and understandable with links and relations between associated elements.

This thesis will present (1) the process model of an accident and discuss risk-reducing measures following ISO 17776 and national regulations such as the Management Regulations from the PSA and (2) the incorporation of risk-reducing elements into the maintenance system to assure that maintenance routines cover their functional requirements. The paper intends to systemize existing knowledge and connect separate work processes into a unified system that will present risk-reducing measures in a structured way, thus enabling adequate maintenance and follow-up of the barriers during their lifecycle.

Acknowledgements

I would like to express my gratitude to all those who aided me during the research of my thesis work. A special thanks to my university supervisor, prof. Ove T. Gudmestad, whose encouragement and guidance helped me to write this report.

I would also like to acknowledge with much appreciation the role of the external supervisor, specialist engineer Egil Hope who facilitated and supported me during the whole work as well as shared his valuable ideas.

Last but not least, many thanks go to all my colleagues in Aker Solutions and BP whose support helped me to achieve a good understanding of the maintenance processes in the industry.

Table of Contents

ABSTRACT	2
ACKNOWLEDGEMENTS	3
TABLE OF CONTENTS	4
1 INTRODUCTION	5
1.1 BACKGROUND	5
1.2 OBJECTIVES	5
1.3 STRUCTURE OF THE THESIS	6
2 RISK REDUCING MEASURES	8
2.1 INTRODUCTION	8
2.2 RISK-REDUCING MEASURES IN AN ACCIDENT MODEL	9
2.3 RISK-REDUCING MEASURES AS SYSTEMS	10
2.4 SAFETY-RELATED ORGANIZATIONAL MEASURES	12
2.5 TECHNICAL SOLUTIONS AND BARRIERS	13
2.6 MAINTENANCE SYSTEM.....	13
2.7 OPERATIONAL SOLUTIONS AND BARRIERS	14
2.8 PERFORMANCE-SHAPING FACTORS (PSF)	14
2.9 SUMMARY.....	15
3 MAINTENANCE OF RISK REDUCING MEASURES	16
3.1 INTRODUCTION. BASICS OF RELIABILITY-CENTERED MAINTENANCE (RCM).....	16
3.2 PRACTICAL ADAPTATION OF RCM PROCESS FOR RISK REDUCING MEASURES	17
3.3 CHALLENGES IN THE LINKS BETWEEN TECHNICAL SAFETY AND MAINTENANCE.....	18
3.4 DISCUSSION FOR SOLUTIONS	19
3.5 PERFORMANCE STANDARD (PS) AND SAFETY REQUIREMENT SPECIFICATION (SRS)	21
3.6 MAINTENANCE ACTIVITIES FOR SCE/SBE	22
3.7 SUMMARY.....	24
4 CASE STUDY	25
4.1 DESCRIPTION	25
4.2 PROCESS	26
4.3 SUMMARY.....	30
5 SUMMARY AND CONCLUSIONS	31
6 ACRONYMS	32
7 REFERENCES	33
PAPERS	35
PAPER 1 SYSTEMATIC APPROACH TO RISK REDUCTION MEASURES IN THE NORWEGIAN OFFSHORE OIL AND GAS INDUSTRY	35
PAPER 2 SOLUTIONS AND SAFETY BARRIERS: THE HOLISTIC APPROACH TO RISK-REDUCING MEASURES	54
APPENDIX A. MAIN ANALYSIS TABLE FOR CASE STUDY	64
APPENDIX B. THE MAIN TABLE OF THE RESULTS	120
APPENDIX C. THE PILOT LIST OF STANDARDIZED PM ROUTINES	131
APPENDIX D. BRIEF PRESENTATION OF MASTER THESIS “CONTROL OF SAFETY BARRIERS THROUGH MAINTENANCE SYSTEM”	133

1 Introduction

1.1 Background

The Petroleum Safety Authority Norway (PSA) focuses on maintaining a high level of health, environment, and safety awareness within the petroleum activities on the Norwegian Continental Shelf (NCS). The implementation of safety barriers has been a key safety principle in the PSA regulations for more than 10 years to guide the Norwegian oil and gas industry. The PSA constantly underlines the need for the risk picture to be clear and understandable with links and connections between related elements.

Sklet (2006) writes that although PSA has developed requirements to safety barriers, they did not give a clear definition of the concept, and discussions have begun on what is a safety barrier within the Norwegian offshore industry. It is also created challenges within the maintenance field due to the requirement to insure that correct maintenance activities are performed for safety barriers.

The extensive literature survey presented by Sklet (2006) reveals that a wide variety of different approaches and definitions are used to describe safety barriers as risk-reducing measures. The author says that “different terms with similar meanings (barrier, defense, protection layer, safety critical element, safety function, etc.) have been used crosswise between industries, sectors, and countries” and claims that “it is also difficult for the PSA to manage the regulations without a clear definition and delimitation of the concept”. The importance of communication is highlighted by Kaplan (1997):

[...] 50% of the problems in the world result from people using the same words with different meanings. The other 50% come from people using different words with the same meaning.

However, the question is whether safety barriers are the only measures of risk reduction. This thesis will describe the process model of an accident and discuss risk-reducing measures following ISO 17776 and national regulations such as the Management Regulations from the PSA (2014). Two main groups of risk-reducing measures are distinguished: (1) technical, operational and organizational solutions applied to the critical systems and (2) safety barriers

Furthermore the challenges of the maintenance management are on focus with respect to risk-reducing measures. Therefore a well-defined process is required to integrating the barriers into the currently existing maintenance systems. Such integration must be seen as a continuous process, rather than one-time workshop. It must embrace the identification of risk-reducing elements, incorporation into a Computerized Maintenance Management System, selection of preventive & functional maintenance routines, work order preparation and feedback of actual operator performing the task and verification phase of the whole process, insuring that a continuous improvement can be implemented. A practice-oriented system should be clearly described that would be linked with the relevant performance standards to ensure that proper maintenance routines are established.

1.2 Objectives

The thesis project will have an extensive practical approach through case study in accordance with PSA regulations, IEC61511, ISO 13702, ISO 17776 and relevant NORSOK standards.

Special focus will be placed on Safety Instrumented Systems maintenance to ensure IEC61511 standard is followed and constant update of proof test intervals is performed thus ensuring pre-designed risk reduction during the whole operational lifetime of the facility.

The main objective of the Master thesis project is to describe the risk-reducing elements including safety barriers and to create a maintenance process workflow that would allow controlling the safety-related equipment in the operational phase of offshore oil and gas production platforms. The intention is to systematize the existing knowledge and connect the currently separate work processes and elements to the unified system that allows closing gaps between various parties involved in the operational phase.

General question arose:

- What is a safety barrier?
- How to maintain a safety barrier?

Based on these questions and the main objective, the following objectives are stated:

- Describe the process model of an accident and discuss risk-reducing measures following ISO 17776 and national regulations such as the Management Regulations from the Petroleum Safety Authority Norway (PSA). Redefine the concept of safety barrier.
- Describe the maintenance process and create the linkage to technical safety in order to integrate risk-reducing measures in a clear and consistent way. The process should be practically applicable and seek to optimize the current maintenance practice in general.
- Use currently existing BP maintenance process and alter it according the model proposed to demonstrate the practical applicability of the proposed method (case study).

1.3 Structure of the thesis

The thesis comprises four main parts:

- ‘Risk reducing measures’ part describes the process model of an accident and discusses risk-reducing measures following ISO 17776 and the Management Regulations from the PSA. Two main groups of risk-reducing measures are distinguished: (1) technical, operational and organizational solutions applied to the critical systems and (2) safety barriers. This part is based on the two conference papers written by the author of this report and prof. O.T. Gudmestad during the development of the thesis.
- ‘Maintenance of risk reducing measures’ part describes the operational maintenance process with clearly defined links between other disciplines with focus on the risk reducing measures.
- ‘Case study’ part presents the application of proposed maintenance model to an existing BP facility.

- 'Papers' part includes two scientific papers with regards to the first part. They have been accepted for oral presentation at the conferences and included in the conference proceedings. These papers have been written during the development of Master thesis with respect to the discussion of 'safety barrier' concept and should be seen as an integral part of the thesis.

Paper 1:

Sevcik, A. & Gudmestad, O.T. 2014. Systematic Approach to Risk Reduction Measures in the Norwegian Offshore Oil and Gas Industry. In: *9th International Conference on Risk Analysis and Hazard Mitigation, Wessex Institute, 4 - 6 June*. New Forest, UK.

Paper 2:

Sevcik, A. & Gudmestad, O.T. 2014. Solutions and safety barriers: the holistic approach to risk-reducing measures. In: *ESREL 2014*.

2 Risk reducing measures

This part is a shortened version of the paper “Solutions and safety barriers: the holistic approach to risk-reducing measures” presented in the fourth part and written by the author of this thesis and university supervisor prof. O.T. Gudmestad. This paper has been written during the development of Master thesis with respect to the discussion of ‘safety barrier’ concept and should be treated as an integral part of the thesis.

2.1 Introduction

Currently in the offshore industry on the Norwegian Continental Shelf (NCS), there is a lot of discussion about barriers and the interactions between them that are greatly fostered by the Norwegian Petroleum Safety Authority’s (PSA) emphasis on safety barriers. However, the question is whether safety barriers are the only measures of risk reduction. In order to start a discussion, it is necessary to have an overview of the main steps in the risk reduction process.

Generally, risk treatment may be seen as a process which ensures that an acceptable risk level is achieved and maintained. To align with the Norwegian Petroleum Safety Authority regulations, Sections 4 & 5 of the Management Regulations are followed (PSA 2014a & PSA 2014b):

In reducing risk [...] the responsible party shall select technical, operational and organizational solutions that reduce the probability that harm, errors and hazard and accident situations occur.

Furthermore, barriers as mentioned in Section 5 shall be established. The solutions and barriers that have the greatest risk-reducing effect shall be chosen [...].

Barriers shall be established that:

- a) reduce the probability of failures and hazard and accident situations developing,
- b) limit possible harm and disadvantages.

Two main groups of risk-reducing measures are named: risk-reducing solutions and safety barriers (Sevcik & Gudmestad 2014).

On further assessment of the definitions provided, it may be stated that risk-reducing solutions are the measures to reduce the likelihood of errors, hazards and accident situations occurring, i.e. preventing hazards (potential source of harm) from being realized. In other words, the solutions are used to reduce the likelihood of such deviations which could initiate (trigger) an unwanted chain of events. Systems that are primary targets of these solutions may be seen as Safety Critical Systems (SCS) and will be discussed further in the paper.

Safety barriers are the measures which are selected after the risk-reducing solutions have been established, with the purpose of reducing the likelihood of failures and hazards, preventing accident situations from developing and limiting the possible harm caused by an unwanted chain of events. Safety barriers are established to reduce the likelihood of the development of an unwanted chain of events when an initiating (triggering) event has already occurred, i.e. a hazard scenario has already started. The main and only function of a barrier is a safety function that is required on demand.

While we make a distinction between the risk-reducing solutions and safety barriers, it is important to see both of them as one entity designed to reduce the risk within performed activities.

2.2 Risk-reducing measures in an accident model

In line with ISO 17776 (2000) and its general hierarchy of risk-reducing measures, this work will propose the following risk-reducing phases as generic safety functions: Prevention, Detection, Control, Mitigation and Emergency Response. These functionalities act in the same sequence when placed on the chain of accident development (Fig. 1).

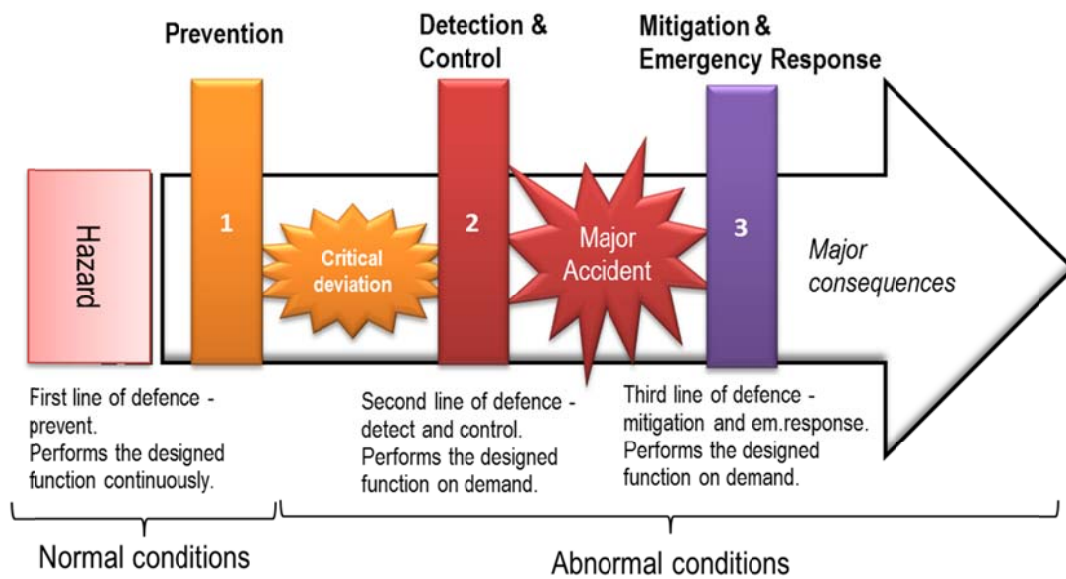


Figure 1 General accident model with safety functions

In line with ISO 13702 (1999), prevention means a reduction of the likelihood of a hazardous event, and a further specified definition is used in this thesis: to prevent means *to reduce the likelihood that a critical deviation occurs*, where critical deviation is seen as an initiating event of an unwanted chain of events.

ISO 13702 defines control as the limitation of the extent and/or duration of a hazardous event. In this thesis we further specify the term and state that control means *to reduce the likelihood that a critical deviation will develop into a major accident once it occurs*, i.e. to stop the unwanted chain of events when critical deviation occurs.

A major accident is the result of the failure of the safety-related solutions (prevention) and detecting/controlling barrier systems. In order *to limit or reduce the consequences of an accident*, mitigating barrier systems are established together with emergency response measures. The successful functioning of these systems will ensure the lowest feasible harm by stopping the accident escalation as soon as possible.

2.3 Risk-reducing measures as systems

Currently the industry uses the term ‘SCE’ to define all the elements that are “such parts of the installation [...] which could cause and contribute substantially to a major accident or a purpose of which is to prevent or limit the effect of a major accident” (Dhar 2011). According to the concept presented in this work, the boundaries of the SCE would only embrace parts of the installation which could cause or contribute to a major accident (Fig. 2).

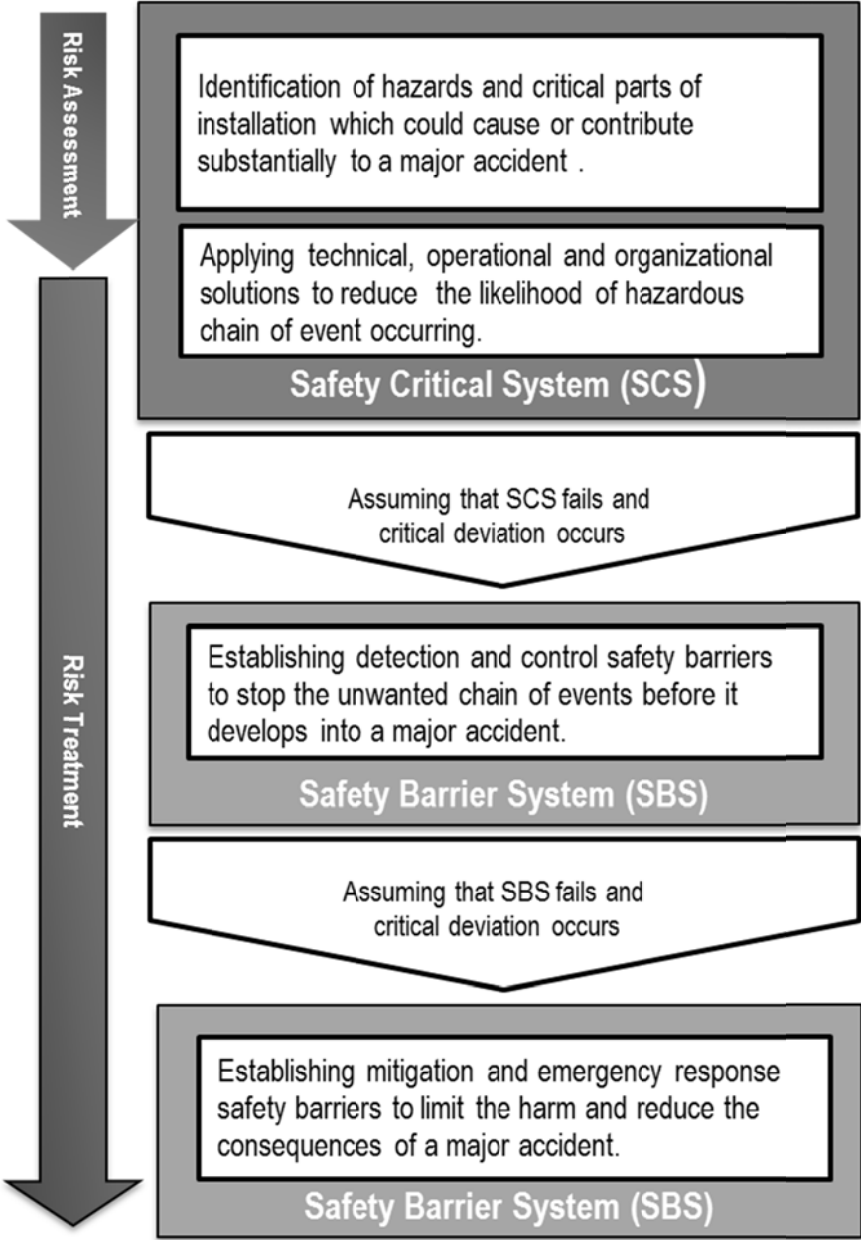


Figure 2 Establishing SCS and SBS of an installation

A Safety Critical System (SCS) is described as a system with applied technical, operational and organizational solutions designed to prevent the realization of a potential source of harm inherent in the activities. The requirement to perform is constant. In the case of a system failure, a critical deviation will occur and start the development of an unwanted

chain of events. The Safety Barrier System – SBS – will embrace the elements of independent safety systems that are installed only for the safety function and in the case of failure will stop the accident’s development or limit the effect of an accident (Fig. 3).

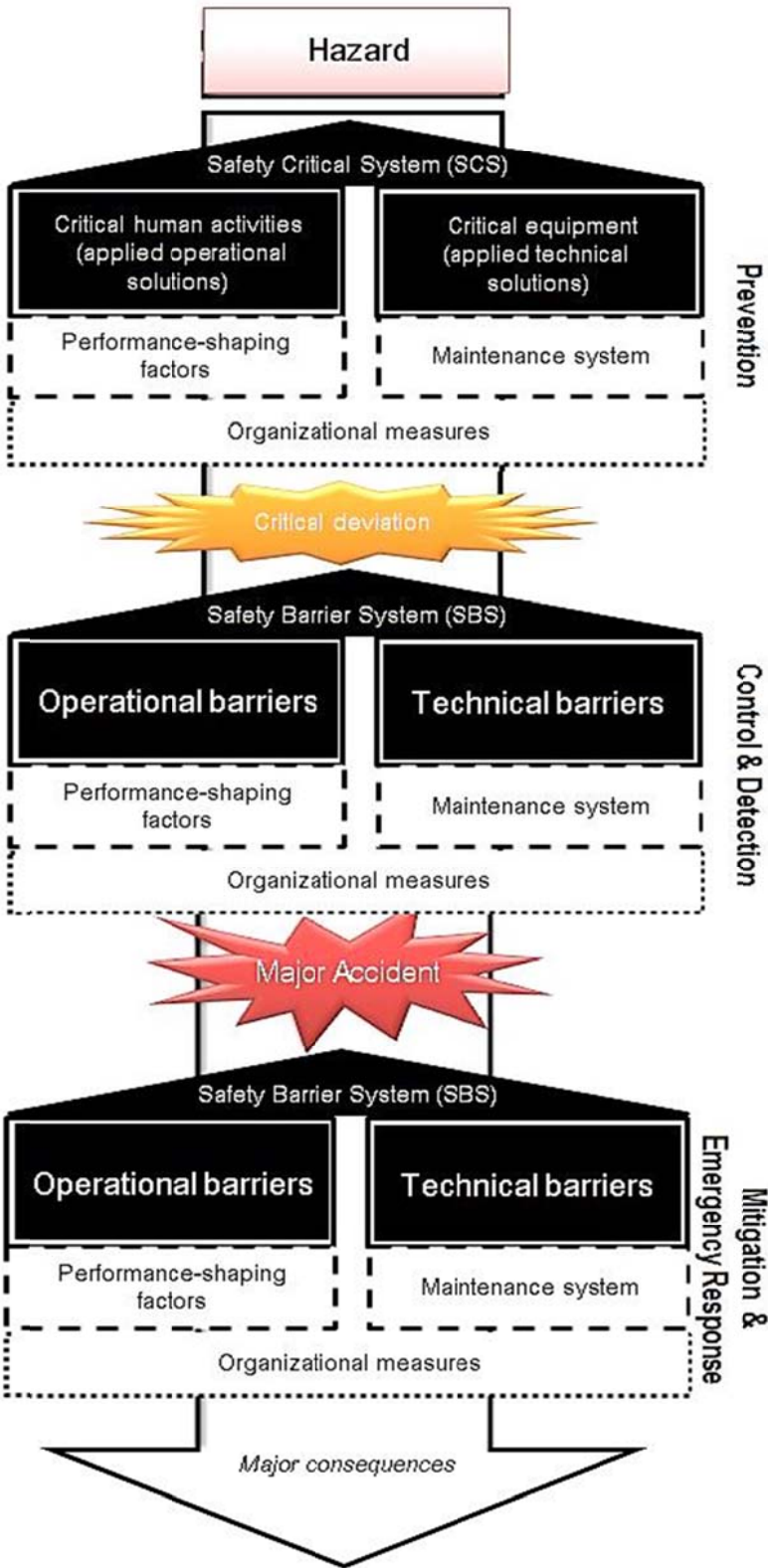


Figure 3 SCS for prevention, SBS for detection and control, SBS for mitigation and emergency response

It is important to see a barrier as an actually established measure that is able to prevent or stop the unwanted chain of events once the initiating event is triggered. Safety principles for nuclear power plants distinguish barriers as physical measures only, while other types of protection are recognized but not defined as barriers (IAEA 1999). Organizational safety measures, such as procedures, strategies, guidelines, requirements, etc., can be seen as part of a regulatory basis that is used to establish the barriers, but they are not barriers in themselves. There is considerable eagerness are a lot of intentions to name them as organizational barriers; however, they cannot be seen as actual barriers that would be able to perform in the case of need. Either physical equipment – a technical barrier – or human actions – an operational barrier – can actually stop the unwanted chain of events that has already started due to the specific critical deviation or mitigate the consequences of it. The differences between SCS and SBS are summarized in Table 1.

Table 1 SCS and SBS comparison

Safety Critical System (SCS)	Safety Barrier System (SBS)
Technical, operational and org. solutions applied to process, utilities, structural, etc. elements to reduce risk.	Independent system designed only for risk-reducing functions.
Reduces the likelihood of critical conditions occurring.	Reduces the likelihood of critical conditions developing and limits the harm.
Requirement to perform – constant (normal conditions).	Requirement to perform – on demand (abnormal conditions).
Cannot be removed without affecting process.	Can be removed without affecting process.

2.4 Safety-related organizational measures

Safety-related organizational measures embrace the application of principles that ensure inherent Health, Safety and Environment (HSE) qualities related to the design and technical basis of the facility. The examples of such principles could be the principle of an Inherently Safer Design (ISD) (Mannan 2014), that involves the concept of reducing (avoiding, eliminating) rather than preventing or controlling hazards. The ISD principles should be applied during the general design and layout of the facility. Best Available Techniques (BAT) is another principle, which states that technology and the way it is used in the installations should be “most effective in achieving a high general level of protection of the environment as a whole” (EU Directive 1996); it is similar to the As Low as Reasonably Practicable (ALARP) principle that adapts a best common practice for judgment of the balance of risk and benefit (HSE 2014). Furthermore, Samarakoon and Gudmestad (2011) have extended the BAT principle to include Qualification: Best Available Qualified Technology (BAQT).

In general, safety-related organizational measures may be seen as a foundational basis for safety-related systems including the design, technology and operational activities.

2.5 Technical solutions and barriers

Technical solutions are applied to the main process and related auxiliary equipment as a derivation of the safety-related principles mentioned in the third section above. The purpose of these solutions is to prevent a critical deviation from occurring and to sustain the normal designed conditions. For example, the thickness of a particular pipeline could be 10 mm if process-needs alone (i.e. pressure or flow rate) are taken into the account, but for safety reasons (i.e. estimated corrosion allowance, etc.) the pipeline is designed with 15 mm walls. Another example could be the selection of process control equipment, preferring modern technology to an obsolete version. The idea of technical safety-related solutions is to decrease the risk within the associated equipment and so it differs from the general design of the facility, which is focused on the process needs. Once applied, technical solutions cannot be removed from the installation without interrupting the functions of the facility for which the solutions were designed.

A technical barrier is a physical element that is established to perform safety functions related to stopping the unwanted chain of events once it has started: detection, control, mitigation or emergency response. It is designed to perform once prevention fails and abnormal conditions occur and to stop the development of a chain of unwanted events, or to limit the harm of these unwanted events. Examples of technical barriers are: a firewall that is designed to perform if fire breaks out; an Emergency Shutdown (ESD) system that is activated if process control is lost; the fire detection and deluge systems installed to fight the fire. Technical barriers do not perform constantly and may be removed from the installation without interrupting the main process functions for which the facility was designed.

2.6 Maintenance system

To ensure the required functionality of critical equipment and technical barriers, maintenance and follow-up activities should be performed by establishing a maintenance system (PSA 2014c). For example, the automatic safety system is one of the main technical barriers; therefore function testing and demand monitoring should be established (IEC:61511-1 2004). Technical barriers should be analyzed, the criticality and failure/fault modes of their elements determined and appropriate maintenance activities undertaken. All critical equipment and technical barrier elements should be tagged and marked accordingly in the general maintenance system of the facilities. In addition, the maintenance system should incorporate an analysis of the human factors and the performance-shaping factors of the operational maintenance activities. Industry examples show that a maintenance system may be enabled through the creation of performance standards – the functional requirement list of each barrier system (Firing et al. 2011). The performance standards may serve as a link between technical safety and maintenance disciplines (Fig. 4).

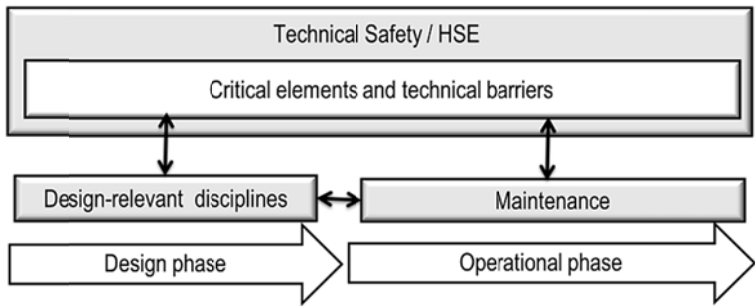


Figure 4 Links between design-relevant disciplines and maintenance

The importance of a well-performing maintenance system is recognized, but industry examples show that implementation often struggles in practice. For example, the accident report on the *Deepwater Horizon* case concludes that “maintenance was inadequate”, work orders issued by the maintenance system were “disorganized, erroneous, or irrelevant to individual rig crews” and the “maintenance system was not understood by the crew” (Chief Counsels Report 2011). The challenges facing the maintenance management are indicated in the report on trends in risk level in the petroleum activity (RNNP) process prepared by the Petroleum Safety Authority (PSA) Norway (PSA 2012), which describes the existing difficulties fulfilling regulatory requirements for maintenance management: “tagging and classification of equipment, backlogs of preventive maintenance and outstanding corrective maintenance, including HSE-critical maintenance”.

The authors of this paper believe that one of the main reasons for such a situation is the missing links between the maintenance discipline and other disciplines, especially technical safety. The various analyses done by safety and maintenance engineers often do not have clear linkage and can hardly be implemented in the practical sense. Moreover, a general inconsistency in Computerized Maintenance Management Systems (CMMS) may often be observed due to the overlapping data of maintenance criticality analysis and technical safety analysis.

2.7 Operational solutions and barriers

Similarly to technical solutions, operational solutions are derived from safety-related organizational principles and are applied to the main operational activities. For example, an operator could do his job in a very cost-efficient way, but, after a risk analysis is performed, a safety-related operational solution – the way the technology is used – will be applied to the job in order to reduce the risk. A safety checklist before an activity may also be seen as an operational solution, as it is an additional activity with a focus on preventing any abnormalities during the operation. The safety checklist may be seen as a part of safety-critical activities, but it is not a barrier by itself.

An operational barrier can be seen as a determined specific action that shall be carried out in the case of critical deviation to prevent or to stop the development of an unwanted chain of events. A manual shutdown valve is often treated as a technical barrier element; however, it will not perform the barrier function unless somebody activates it on demand. This action is an operational barrier element.

Operational barriers are the part of the Safety Barrier System (SBS) that involves specific human actions related to the barrier function: detection, control, mitigation or emergency shutdown. Examples of operational barriers could be a manual activation of emergency shutdown systems, firefighting and evacuation. A specific lookout or visual check of an operator that is performed only for safety reasons may be seen as an operational detecting barrier.

2.8 Performance-shaping factors (PSF)

The UK Health and Safety Executive defines human factors as “environmental, organizational and job factors, and human and individual characteristics which influence behavior at work in a way which can affect health and safety” (HSG48 2009). Explicitly defined, human factors

may be seen as Performance-Shaping Factors (PSF) and are used to model human behavior as the underlying causes of abnormal performance (El-Ladan and Turan 2012). It must be noted that PSF are explicitly used to describe the influence on human performance (Musharraf *et al.* 2013) and should not be directly referred to as the performance of technical equipment. Technical equipment is affected by maintenance actions which are again influenced by PSF (Toriizuka 2001). However, the PSF of maintenance activities should be seen as an integral part of the maintenance system, and maintenance activities should be distinguished from the operational safety barrier concept that embraces specified safety actions in the case of abnormal situations.

PSF may be characterized as internal and external (Boring *et al.* 2007). Internal PSF influence individual attributes such as mood, fitness, stress level, etc. External PSF exert influence in the situation or environment that affects the individual, such as temperature, noise, work practices, etc. The performance of operational activities is directly affected by PSF, so they must be taken into consideration when SCS or SBS are designed.

2.9 Summary

Based on the synthesis of ISO 17776, the PSA regulations and common features of the terms found in the scientific literature, the concepts of Safety-Critical Systems (SCS) and Safety Barrier Systems (SBS) are proposed as a basis for further discussion of risk-reducing measures in industrial activities.

Correspondingly, prevention, detection/control, and mitigation/emergency response systems have been introduced and described. Aligning with the PSA regulations, safety-related solutions and corresponding critical systems have been separated from safety barriers and described. Links between technical, operational and organizational elements have been suggested, incorporating maintenance activities and performance-shaping factors. The presented accident chain model (Fig. 1) may be used as a tool for a broader communication about the safety barriers and their role in arresting the accident's escalation.

This may be valuable in risk communication, where the model's simplicity could be well-accepted by non-technical safety personnel.

3 Maintenance of risk reducing measures

The intention of this part is to find practical solutions for the current challenges in the industrial maintenance of offshore facilities rather than discuss maintenance theories and fundamental concepts.

3.1 Introduction. Basics of Reliability-Centered Maintenance (RCM)

Reliability-Centered Maintenance (RCM) is a systematic engineering methodology to identify preventive maintenance (PM) requirement for complex systems that has been recognized in many industrial fields, such as aviation, railway network or industrial plant maintenance (Cheng et al. 2008).

ABS Guidance Notes on Reliability-Centered Maintenance (2004) defines Reliability-Centered Maintenance (RCM) as a process of systematically evaluating a system to understand:

- 1) Its functions;
- 2) The failure modes of its equipment that performs these functions;
- 3) How to select an optimal maintenance program to prevent these failures;
- 4) How to determine spare parts requirements;
- 5) How to monitor and improve existing maintenance system over time.

The purpose of RCM is to achieve reliability for all of the operating modes of a system.

An RCM analysis, when properly conducted, should answer the following seven questions:

- 1) What are the system functions and associated performance standards?
- 2) How can the system fail to fulfill these functions?
- 3) What can cause a functional failure?
- 4) What happens when a failure occurs?
- 5) What might the consequence be when the failure occurs?
- 6) What can be done to detect and prevent the failure?
- 7) What should be done if a maintenance task cannot be found?

The basic elements of an RCM analysis process are as follows:

- 1) Identify operating modes and corresponding operating contexts
- 2) Define plant systems
- 3) Develop system block diagrams and identify functions
- 4) Identify functional failures
- 5) Conduct a failure modes, effects and criticality analysis (FMECA)
- 6) Select a failure management strategy
- 7) Determine spare parts holdings
- 8) Document the analysis

Once implemented, the RCM process will be an effective way to ensure reliable and safe operation of an engineered system. Such a maintenance management system is called an RCM system.

3.2 Practical adaptation of RCM process for risk reducing measures

Yet maintenance does its own criticality analyses, the second part of the thesis states that Technical Safety (TS) discipline shall be and is involved in the determination of critical elements and safety barriers. Most oil operators on the NCS have determined groups of critical equipment and prepared the performance standards for these groups (Statoil 2012 & BP 2013). It is common to refer to these groups of equipment as ‘safety barriers’ and elements of these groups as Safety-Critical Element (SCE). Following the second part of the thesis, such terminology was redefined to better reflect the various functionalities and maintenance needs of the system (fig. 5).

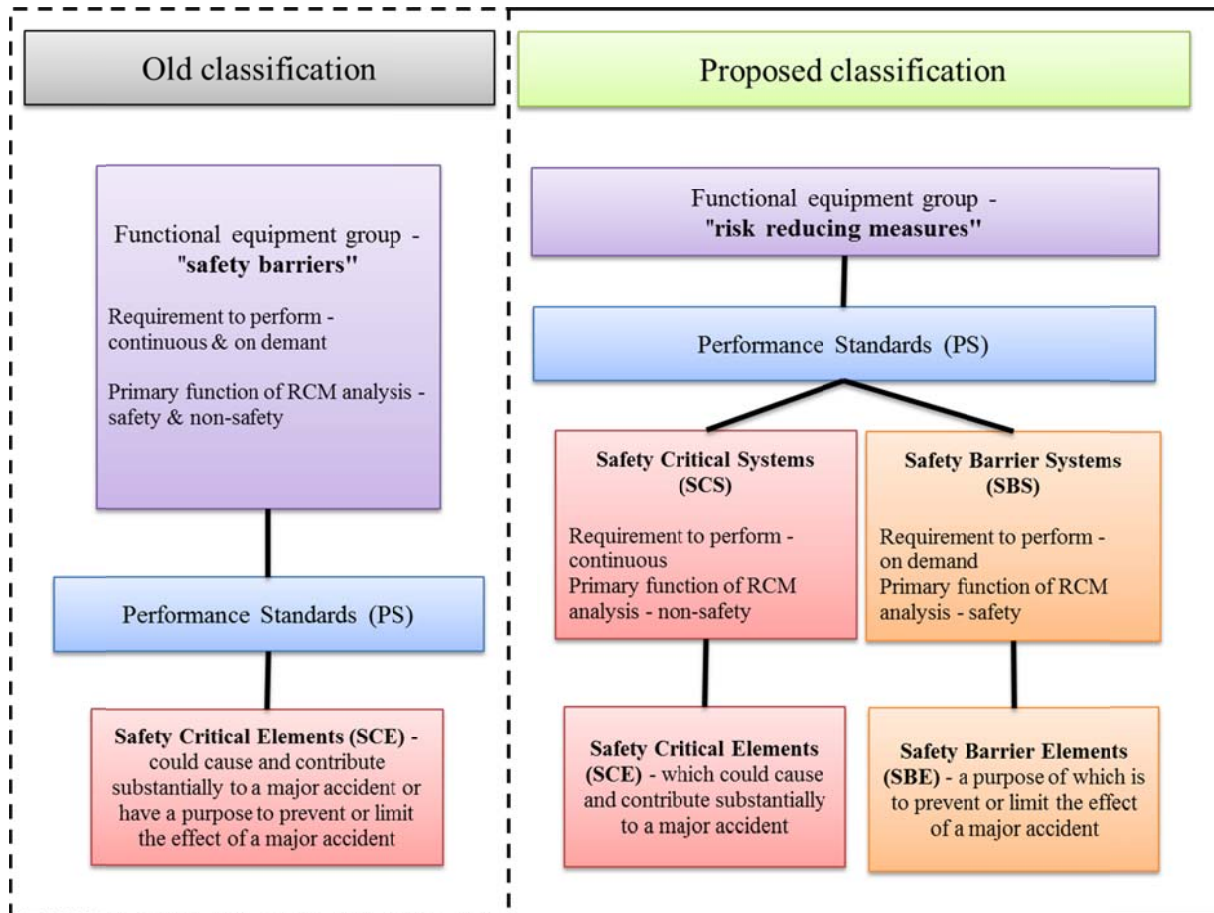


Figure 5 Proposed classification and terminology

Performance Standards (PS) are derived from the risk management processes and may be seen as a final document – output link – produces by technical safety / risk management disciplines (fig. 6). The shown risk management process embraces hazard evaluation & risk assessments (HAZID/HAZOP) and a register of the Safety Critical / Barrier Equipment. It also requires that clear links are shown from the identified hazards and risk assessment to SCE/SBE equipment.

So first part of RCM process – identification of systems and functions – is covered by technical safety / risk management disciplines. However, an issue here is how this information shall be transferred to the operational / maintenance activities. It cannot be just a huge list of

identified tag/locations that soon would become obsolete due to dynamic and constant changes in the facilities, and this connection is discussed further in the paper.

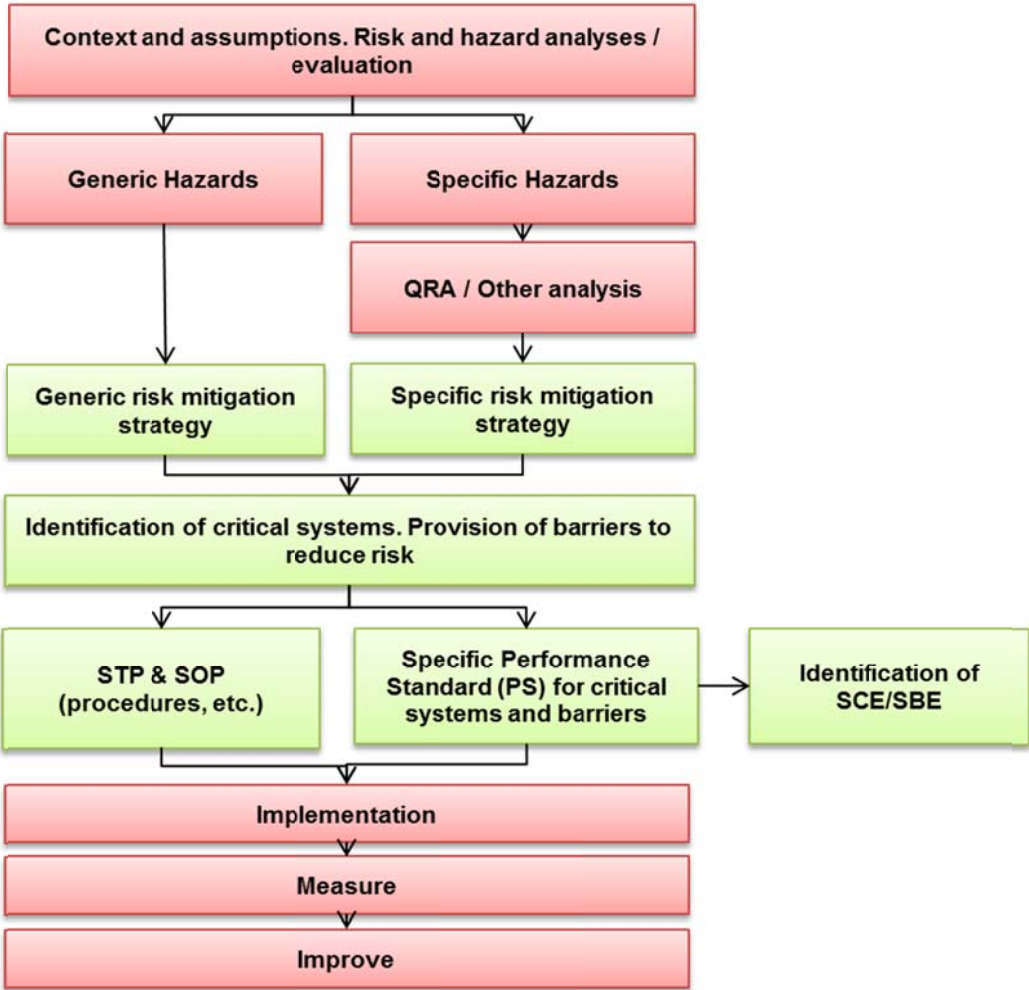


Figure 6 The integrity management strategy (adapted from BP 2013)

3.3 Challenges in the links between technical safety and maintenance

Challenges are basically the links and data transfer between involved parties: technical safety and maintenance disciplines (Fig. 7). The simple approach – one-time workshop that would produce a list of identified safety critical tags – is not an efficient and effective way due to huge (it is possible that hundreds of thousands / several millions and more tags may exist in the systems) and dynamic (due to large number of modifications) nature of the facilities. Such produced lists soon will become obsolete, it is hard to maintain and update when required, and it is time-consuming to use such approach. Therefore the first challenge can be defined as a necessity to find a method to transfer the safety data to the maintenance discipline in the efficient way, thus optimizing and ensuring that safety critical equipment will be covered by maintenance programs.

The second challenge is the back relation from maintenance to the safety discipline. The actual function test results and performance of safety critical equipment shall be evaluated by the responsible safety engineers as it is not in the scope of maintenance engineer to evaluate the changes of the risk level. Therefore the function test /performance test / historical maintenance results with appropriate comment from maintenance engineer shall be transferred back to the responsible safety / risk engineers to make necessary adjustments or changes in the procedures or guidelines, or initiate other necessary actions if required.

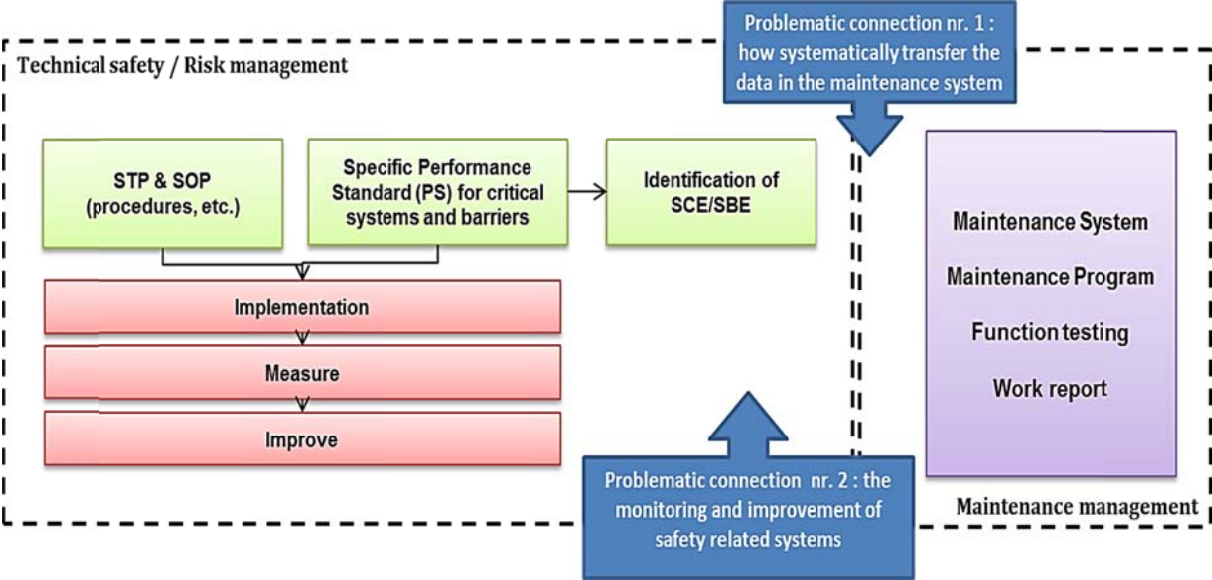


Figure 7 The challenges in connections between technical safety and maintenance

3.4 Discussion for solutions

The actual and practical solutions are not so easily determined. It can be just stated that technical safety discipline should be actively involved and need to provide the requested information to the maintenance management. The actual question is how to do this in the most efficient and optimized way. It is also obvious that it can't be one-time workshop but rather the continuous process with clearly defined inputs and outputs see conceptual workflow in Figure 8.

The obligatory Performance Standards (PS) required by the PSA may be seen as a potential data link between safety and maintenance disciplines. In addition to specific requirements for safety critical and barrier functions, the PS should have a clear description of equipment groups that are considered as part of the SCS/SBS. A properly created PS will allow the correct identification of critical equipment tags and the implementation of data into the CMMS. In addition, the equipment tags of the Safety Instrumented Systems (SIS) and required full function (proof) test intervals should be specified in the Safety Requirement Specification (SRS), a live document made specifically for every installation (GL-070 2004 & IEC:61508 2010). Both these two documents can be a basis for required data link between technical safety and maintenance disciplines.

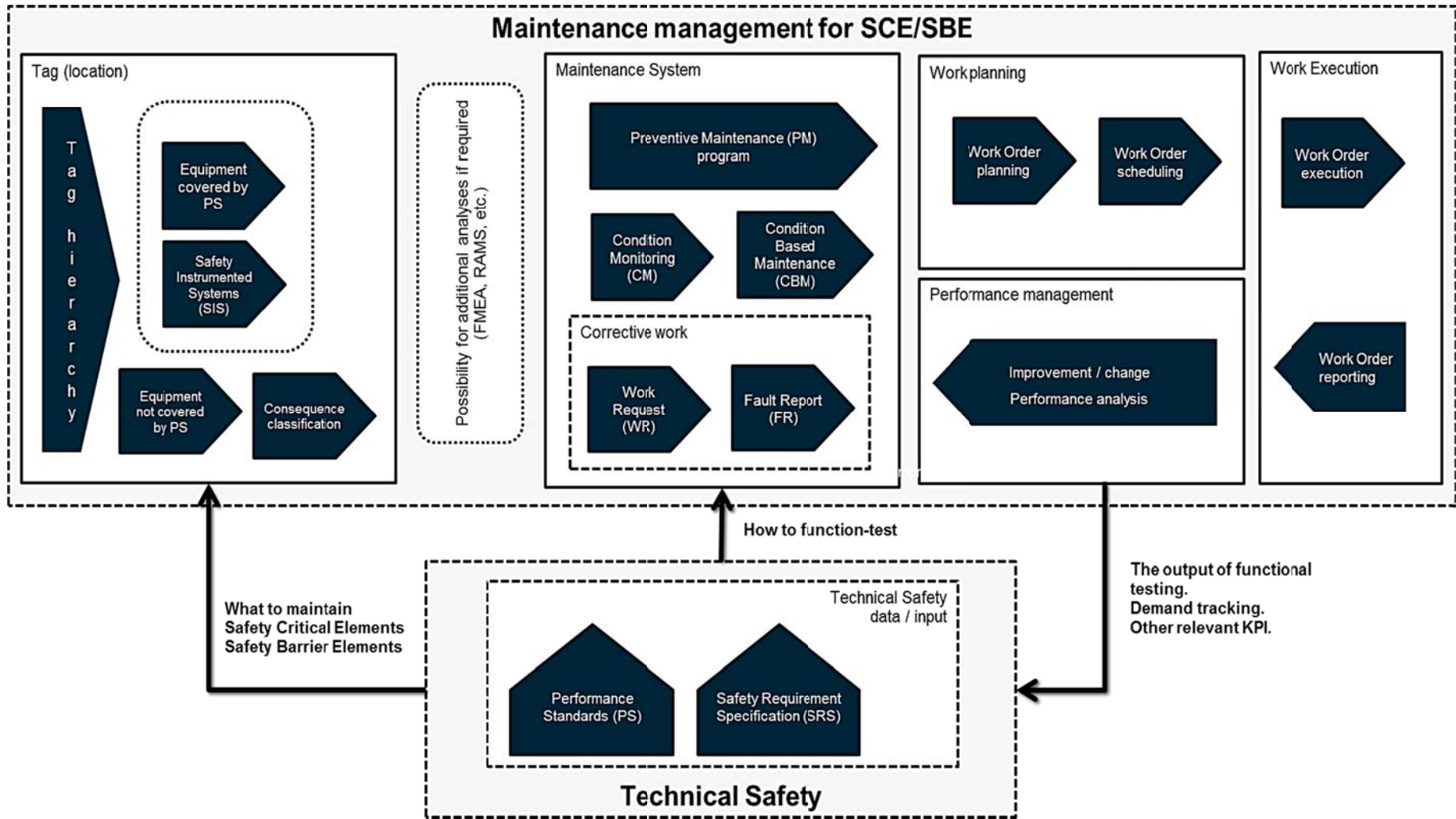


Figure 8 Conceptual workflow of maintenance management for SCE/SBE

The results of functional testing as well as relevant maintenance data (for example, a number of corrective work orders issued for safety equipment) may be a part of the maintenance performance management system. Required data for technical safety should be delivered in structured and continuous way thus ensuring that responsible safety engineers will be informed about actual performance of critical systems and established barriers. In that way, the continuous follow-up can be assured and required actions can be initiated if performance of critical systems / safety barriers is not satisfactory. It is not in the scope of this thesis to discuss this link explicitly.

3.5 Performance Standard (PS) and Safety Requirement Specification (SRS)

Hereby PS and SRS documents will be introduced according the example of BP operating company. Additionally it must be noted that SCE in BP embraces both SCE and SBE discussed in this thesis.

Performance Standards

PSA Management regulations require “identifying specific performance requirements of barrier functions and barrier element”, and the operating companies shall create such accordingly. The Performance Standard in BP is a document that combines regulatory requirements in Norway, BP best practices, standards and industry recommended practices, results and assumptions from various risk analyses, etc.(BP 2013). It is an engineering knowledge collection that includes the requirements for each of the safety critical systems required to manage possible hazardous events on the installation. Performance Standards are describing functionality, integrity and survivability requirements for currently 27 safety critical systems

Typical PS for one system can take up to 25 pages, so the whole list of PS for the facility can be quite extensive. Every PS will contain:

1. Scope of Performance Standard
2. Objectives
3. Dependency and interfaces
4. Performance Standard Details on Functionality
5. Performance Standard Details on Integrity
6. Performance Standard Details on Survivability
7. IM related data and documentation for performance standard
8. Identification of Safety Critical Equipment (SCE)
9. Test, inspection and maintenance requirements
10. Deviations from performance requirements

The numbers 8 and 9 are the most relevant for the maintenance engineer and should serve as basic input data for the maintenance of safety critical / safety barrier systems. GL 070 (2004), former OLF – 070, is an adaptation of the IEC 61508 / 61511 standards for the use in the Norwegian petroleum industry.

Safety Requirement Specification

Safety Requirement Specification (SRS) is a document for requirements stated in the IEC 61508 (2010) standard. A SRS is developed during the design of Safety Instrumented System (SIS) and contains the essential data required for successful performance and maintenance of the system. It is a “live” document, meaning that the document shall be further developed and maintained through all lifecycle phases of the SIS. Generally, the SRS shall contain the relevant key information for use in specifying and operating the instrumented safety functions. The most relevant for the maintenance is:

- 1) The boundaries and location (tag) of the SIS
- 2) Functional requirements like capacities and response times
- 3) Requirement of proof test intervals

It may contain other relevant data:

- 4) Minimum worst-case repair time, which is feasible for the SIS, taking into account the travel time, location, spares holding, service contracts, environmental constraints, etc.

3.6 Maintenance activities for SCE/SBE

The generalized maintenance process for SCE/SBE is shown in the figure 9.

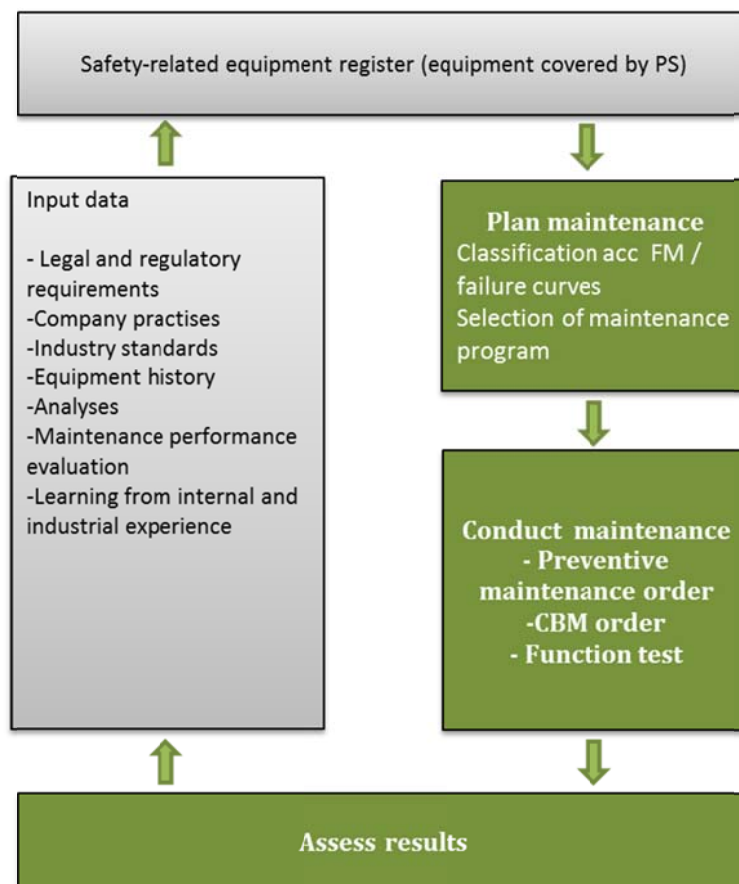


Figure 9 Principal schematics of the result table

Failure of equipment should be systematically prevented through a maintenance programme. It is usually based on the failure modes and include activities for monitoring performance and technical condition to ensure identification and correction of failure modes that developing or have occurred. The maintenance programme can consist of several activities for inspection, testing, preventive maintenance,

The hidden failures are of the biggest threats in the maintenance of SCE/SBE that usual cannot be efficiently found by general maintenance activities. Therefore appropriate function tests must be included in the maintenance program for safety critical / safety barrier elements (Fig. 10). The most “tricky” one is full function test which is applicable mostly for only Safety Instrumented Systems (SIS) with predefined Safety Integrity Level (SIL). The interval and job planning of full functional test is in the scope of technical safety discipline while partial function tests for non-SIS equipment and generic PM task activities are in the scope of maintenance discipline.

Summarizing with the example of valve:

- Generic PM task for valve. The equipment type (construction) is important here, for example, ball valve or butterfly valve may have different PM tasks due to different construction of the valve itself.
- Partial function test for valve, i.e. valve testing. It can be based on ISO14224 (2006) or other relevant ISO/NORSOK standards, dependent on the functionality of the equipment. Valve can be tested for closing/opening on the signal, closing/opening time, or leakage rate.
- Full function (proof) test is usually applicable for the whole Safety Instrumented Function (SIF) with SIL requirements. Generally it has a specific order, can have various methods (like partial stroke testing, etc.), defined intervals that should be re-updated time to time based on the actual demand rate of the function in the facility, etc. So if the valve is a part of any SIF, it is subjected to full function testing as well.

It must be noted that *standard PM task* embraces inspection and CM / CBM scope as well, if applicable (for example, piping, rotating machinery, etc.) in this context.

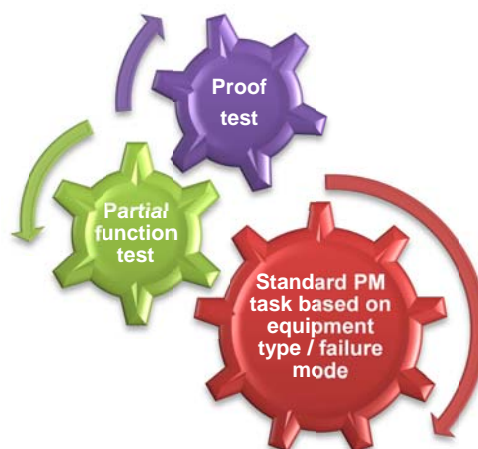


Figure 10 Different types of activities for SBE maintenance

3.7 Summary

The second part of thesis analyzed the practical approach to the maintenance of SCE/SBE, offering to use the relevant input from the technical safety discipline as a basis for identification of safety-related equipment and its functional requirements that are required to be maintained during the operational phase of the system lifecycle.

The connections and touch points of data input & output between the disciplines have been described and possible solutions have been discussed. Generic examples of conceptual workflow have been proposed. Further studies are required to enable a synergy of separate work processes and that would ensure adequate maintenance and follow-up of risk-reducing measures during their lifecycle.

4 Case study

4.1 Description

The scope of case study is the Skarv floating production storage and offloading (FPSO) vessel which is the biggest ever built for deployment on the Norwegian Continental Shelf (NCS). It serves the Skarv and Idun fields, located just below the Arctic circle in the northern Norwegian Sea.

Currently there are 27 PS issued for this installation, and specific functionalities for the scope of every PS has been established by DNV. These functionalities have links, dependencies and interconnections between them; all together they represent a lot of requirements that may be extensive to manage and follow-up continuously.

The scope of this case study is SBE only, i.e. elements that functional requirement is on demand. Also only technical barrier elements will be analyzed as only they are subject to the maintenance.

The major objective of this case study is to group and connect the safety functions to particular equipment through the established functionalities of relevant PS. The final result should present the particular equipment group, its connection to relevant safety function as well as corresponding functionalities of relevant PS and the incorporation of ISO:14224 (2006) that would enable further connections with relevant maintenance data. Additionally the list of generic maintenance routines required for SBE may be created that would facilitate to optimize the maintenance system by having standardized routines for the same type of equipment. The summary result should be able to ensure to create a required PM program in the structured and consistent way among the maintenance engineers (Fig. 11).

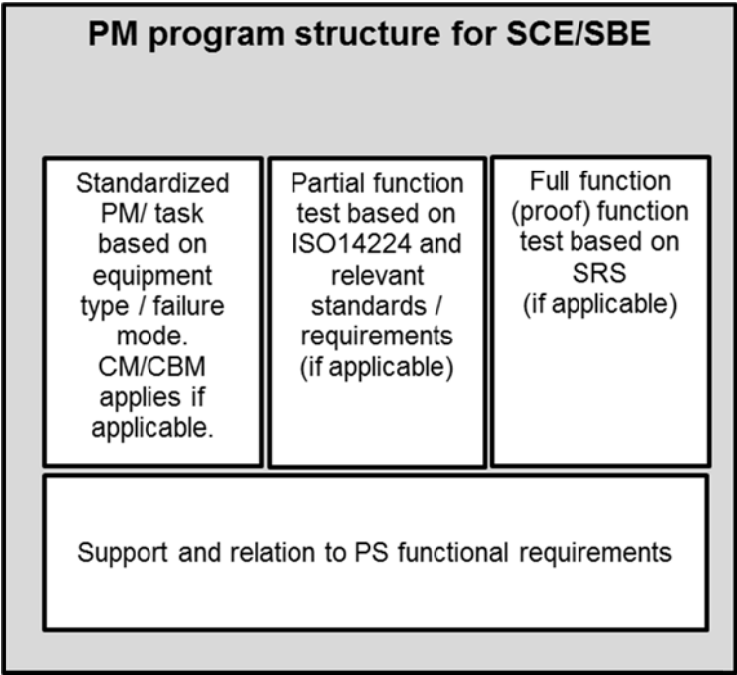


Figure 11 Parts of PM program required for SBE maintenance

4.2 Process

1. Establishment of the list of safety functions based on the regulatory requirements and general company's PS according the framework of SCS / SBS concept described in the thesis.

Starting from safety functions defined in PSA Guidelines, The Facilities Regulations:

- Sectioning of the process
- Fire detection
- Gas detection
- Isolation of sources of ignition
- Maintaining overpressure in unclassified areas
- Starting and stopping fire pumps, both manually and
- Active fire fighting
- Process safety
- Well safety
- Isolation of riser
- Subsea ESD isolation
- Topside and subsea HIPPS protection
- Depressurization
- General alarm and evacuation alarm
- Emergency power
- Emergency lighting
- Ballasting for floating facilities
- Maintenance of correct pressure, humidity, temperature and gas composition in diving facilities
- Prevention of blowouts and prevention of well leaks during drilling operations

PS for FPSO Skarv:

- PS 1 Layout and Arrangement
- PS 2 Structural Integrity
- PS 3 Fire & Gas Detection
- PS 4 Emergency Shutdown
- PS 5 Ignition Source Control
- PS 6 HVAC
- PS 7 Control of Spills
- PS 8 Active Fire Protection
- PS 9 Passive Fire Protection
- PS 10 Emergency Power and Emerg
- PS 11 PA Alarm and Emergency Cc
- PS 12 Escape and Evacuation
- PS 13 Blow down
- PS 14 Process Safety
- PS 15 Loss of Containment
- PS 16 Barriers to prevent ship collisions
- PS 17 Well
- PS 17c Drilling Lifting System
- PS 18 Rescue and Safety equipment
- PS 24 Lifting Equipment
- PS 30 Green Sea Barrier
- PS 31 Bilge and Ballast System
- PS 32 Station keeping
- PS 33 Dynamic Risers
- PS 34 Subsea dropped object protection
- PS 35 Subsea Loss of Containment
- PS 36 Offloading Operation

Prevention of well leaks during drilling operations / well intervention operations are not in the scope of this case study (Skarv does not have drilling facilities).

Framework:

PREVENT - function on constant use - Safety Critical System (SCS)
(functions are required during normal conditions)

DETECT & CONTROL - function on demand - Safety Barrier System (SBS)
(functions are required during critical deviations / accidents)

MITIGATION & EMERGENCY RESPOND - function on demand - Safety Barrier System (SBS) (functions are required during critical deviations / accidents)

Result:

Table 2 Risk reducing function groups

Nr	Risk-reducing function group (technical only)	Role
1	PREVENT - Loadbearing structures / structural integrity	SCS P1
2	PREVENT - Dynamic Risers	SCS P10
3	PREVENT - Offloading operations	SCS P11
4	PREVENT - Ignition prevention	SCS P2
5	PREVENT - HVAC	SCS P3
6	PREVENT - Containment, piping and static process equipment	SCS P4
7	PREVENT - Subsea containment	SCS P5
8	PREVENT - Collision	SCS P6
9	PREVENT - Lifting equipment	SCS P7
10	PREVENT - Bilge & Ballast (normal mode)	SCS P8
11	PREVENT - Station keeping	SCS P9
12	DETECT - gas detection	SBS D1
13	DETECT - fire detection	SBS D2
14	DETECT - F&G logic	SBS D3
15	DETECT - MCP /Alarm	SBS D4
16	CONTROL - process safety	SBS C1
17	CONTROL - ignition source disconnection	SBS C2
18	CONTROL - well isolation	SBS C3
19	CONTROL - emergency shutdown	SBS C4
20	CONTROL - blowdown	SBS C5
21	MITIGATE - impact protection	SBS M1
22	MITIGATE - CO2/Inergen system	SBS M10
23	MITIGATE - Water mist system	SBS M11
24	MITIGATE - Open drain	SBS M12
25	MITIGATE - Passive fire protection	SBS M2
26	MITIGATE - FW supply	SBS M3
27	MITIGATE - FW pumps	SBS M4
28	MITIGATE - Deluge	SBS M5
29	MITIGATE - FW input	SBS M6
30	MITIGATE - AFFF	SBS M7
31	MITIGATE - Manual firefighting	SBS M8
32	MITIGATE - Helideck firefighting	SBS M9
33	MITIGATE - Emergency ballast	SBS M13
34	EM RESPONSE - Emergency power	SBS E1
35	EM RESPONSE - Emergency communication	SBS E2
36	EM RESPONSE - Rescue	SBS E3
37	EM RESPONSE - Evacuation	SBS E4
38	EM RESPONSE - Lifeboats & Rafts w/escape chutes	SBS E5

2. Analyze PS for every system using the DNV predefined functionalities

This part is intended to define relevant equipment group and its function group for every functionality evaluated as safety critical by DNV. The established worktable is used for this analysis, see table 3.

Table 3 The established worktable for case study

PS	Function	PS No.	Functionality	Related Assurance Activities	Work Scope	Equipment group	Risk-reducing function group (technical only)	Code
Nr of PS	The required functionality scope of the system	Nr of functionality	Description of functional requirement	Related activities	Defined activity scope	Assigned equipment group	Assigned function group according table 2	Assigned function group code

Legend:

	Data from PS sheets
	Data from DNV defined functionalities
	Relation to equipment group / risk reducing function group

The full worktable with the analysis data can be found in appendix A.

3. Connect defined equipment group with relevant groups from GL-070 and ISO14224. Establish standardized PM routines.

Further only SBE will be analyzed due to time constraints. The established worktable is used for this analysis, see tables 4-5 as an example for PSD system. The full worktable with the analysis data can be found in appendix B.

GL 070 (2004), former OLF – 070, is an adaptation of the IEC 61508 / 61511 standards for the NCS which contains the SIS-scope functionalities and predefined minimal SIL for them. If functionality falls under GL-070 then related equipment is subject to full function (proof) testing and relevant data from corresponding SRS should be used.

ISO14224 annex F “Classification and definition of safety-critical failures” contains some typical dangerous failures for some common safety systems/components. It states that “use by operators of the standard definitions would facilitate comparison and benchmarking to enhance safety levels in the industry”. However, it must be noted that just a part of required functionalities are covered by the mentioned standard (“not defined” where it doesn’t, see table 4). It is believed that PS functionalities could be used to expand the standardized functionalities, but this is not in the scope of this study.

Finally, the list of standardized PM routines is established. This would help to optimize the maintenance activities as the same PM routine for equipment can be used without referring to its safety function, i.e. same type level transmitter will have the same standardized PM routine. But if the level transmitter is a part of SIS, then it is subjected to proof testing and corresponding routine will be attached to it. The predefined list of the standardized routines can be found in the appendix C.

Table 4 First part of the results table

Technical barriers			PS		Proof testing
Role	Risk-reducing function group	Equipment group	PS	PS No.	SIL min req (GL-070)
SBS C1	CONTROL - process safety	PSD (incl HIPPS & IOPPS) system - initiator	PS14	2, 5, 6, 7, 8	SIL1-3, SRS scope
SBS C1	CONTROL - process safety	PSD system - logic	PS14	2, 5, 6, 7, 8	SIL1-3, SRS scope
SBS C1	CONTROL - process safety	PSD system - final element	PS14	2, 5, 6, 7, 8	SIL1-3, SRS scope

Table 5 Second part of the results table

Functional testing (partial)			Periodic maintenance
Equipment class ISO14224	Failure definitions ISO14224	Applicable failure modes ISO14224	Generic periodic maintenance activities
Input devices	Function Sensor does not give signal or gives erroneous signal (exceeding predefined acceptance limits).	NOO, ERO	Instrumentation, Transmitter, Pressure Instrumentation, Transmitter, Level Instrumentation, Transmitter, Temperature
Control units	Not defined	Not defined	Instrumentation, Controller, Standard industrial PLC Instrumentation, Controller, Programmable safety system Instrumentation, Controller, Hardwired safety system
Valves	Function Valve fails to close upon signal or within a specified time.	FTC, DOP, LCP, INL	Mechanical, Valve, PSD incl. actuator Valve, Solenoid/pilot

4.3 Summary

The twenty seven PSs have been studied for the Skarv floating production storage and offloading (FPSO) together with pre-defined functional requirements. The goal was to connect the barrier functionalities and maintenance equipment groups into the unified system thus allowing establishing standardized approach to the efficient maintenance program for the safety critical / barrier equipment. Due to the time limitation and extent scope of the study, only technical SBEs have been taken into account. It also may be noticed that presented ideas are highly related to the actual practical problems therefore implementable solutions have been proposed.

The final result is an excel table in the appendix B. The principal idea of the table is shown in the figure 12. Additionally the list of generic maintenance routines required for SBE have been created as a pilot and presented in the appendix C thus believing that standardization is major objective in order to facilitate the maintenance optimization.

Further studies should focus on how to transfer the established connection into the work systems, i.e. CMMS. In order to have a success, the continuous process should be created through all involved parties. Maintenance engineers should be available to see if the SCS/SBS functions and performance requirements are being updated by technical safety personnel. Moreover, the involved disciplines should be able to mark a newly created tag with the relevant barrier function thus ensuring that all equipment is properly marked. The multi-disciplinary approach and system thinking is a must in order to implement such process and follow the philosophy of continuous improvement.

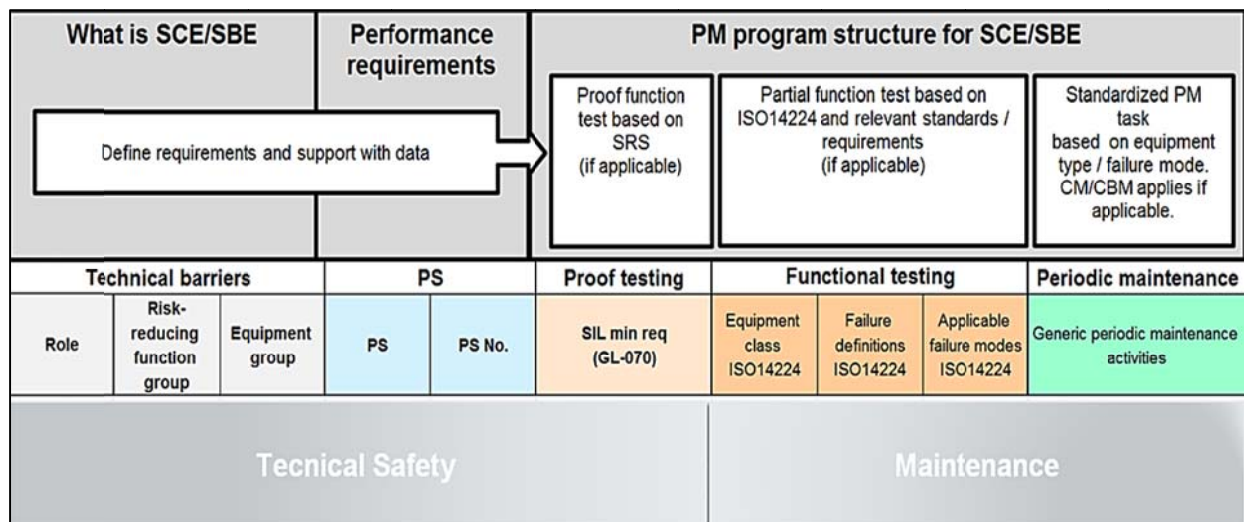


Figure 12 Principal schematics of the result table

5 Summary and conclusions

This thesis has been started with the idea of describing and standardizing the maintenance process for the safety barriers. However, due to the absence of standard definitions and accepted common interpretation of what is a safety barrier in the industry, the thesis has been expanded to the larger scope – from the beginning of risk analysis, where barriers are “born”, to the operational maintenance activities of the barrier follow-up.

Safety barriers and the interactions between them has been a key safety principle in the PSA regulations for more than 10 years to guide the Norwegian oil and gas industry. However, Sklet (2006) concludes that there is a large variety of different interpretations and terms which are used to define safety barriers and claims that it is “difficult for the PSA to manage the regulations without a clear definition and delimitation of the concept”. Therefore the first part of thesis redefined the concept of a safety barrier and provided new definitions to improve the risk communication between involved parties.

The new framework for the safety barrier concept based on the accident modelling and recognized industry standards have been introduced and thoroughly described. A conceptual structure of safety critical and safety barrier systems consisting of technical and operational elements has been developed and presented in the thesis as practically applicable.

The second part of thesis focused on the practical challenges in the maintenance management of safety-related equipment. As safety barrier as such comes from the definitions of risk management and technical safety, the analysis of work processes between technical safety and maintenance disciplines have been conducted based on the actual work experience in the relevant industry projects. Yet the processes within the boundaries of the disciplines are well defined, the connections between them are vague and not clearly identified. The output data from technical safety that should serve as input data for maintenance to confirm that proper maintenance is executed on identified critical equipment is barely used in the practice. Also there is no systemized process which would ensure the back relation from the actual maintenance records to the technical safety to follow-up the critical equipment performance.

The link *technical safety-to-maintenance* was on focus in the second part. The new practical model of maintenance program for SCE/SBE was proposed with the high focus on standardization of activities to facilitate the optimization of maintenance system. As the verification of the proposed model, the actual case study has been conducted to show the possibility of practical application of it. The result table was able to summarize and connect all required data sources with relevant equipment group thus ensuring that safety critical equipment is covered by required maintenance routines and function testing is performed as required.

The *maintenance-to-technical* safety connection should be established to allow continuous check and improvement of the critical elements/barriers performance. It is essential to understand that continuous process should be created rather the one-time workshops. Further studies are required to facilitate a synergy of separate work processes that would ensure adequate maintenance and follow-up of risk-reducing measures during their lifecycle

6 Acronyms

ABS	American Bureau of Shipping
ALARP	As Low As Reasonably Practicable
BAQT	Best Available Qualified Technology
BAT	Best Available Technology
CBM	Condition Based Maintenance
CMMS	Computerized Maintenance Management System
DNV	Det Norske Veritas
ESD	Emergency Shutdown
FMECA	Failure Mode, Effects and Criticality Analysis
FPSO	Floating Production, Storage and Offloading unit
HAZID	Hazard Identification study
HAZOP	Hazard and Operability study
HIPPS	High-integrity Pressure Protection System
HSE	Health, Safety, Environment
HVAC	Heating, Ventilation, and Air Conditioning
IAEA	International Atomic Energy Agency
IEC	International Electro technical Commission
IOPPS	Inlet Overpressure Protection System
ISD	Inherently Safer Design
ISO	International Organization for Standardization
NCS	Norwegian Continental Shelf
NORSOK	Norsk Sokkels Konkuransesepisjon (<i>Norwegian organization for standardization</i>)
OLF	Oljearbeidernes Fellessammenslutning (<i>Norwegian Oil Industry Association</i>)
PLC	Programmable Logic Controller
PSA	Petroleum Safety Authority
PSD	Process Shutdown
PSF	Performance Shaping Factor
RCM	Reliability Centered Maintenance
RNNP	Risikonivå i norsk petroleumsvirksomhet (<i>The trends in risk level in the petroleum activity</i>)
SBE	Safety Barrier Element
SBS	Safety Barrier System
SCE	Safety Critical Element
SCS	Safety Critical System
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SRS	Safety Requirement Specification

7 References

- ABS. 2004. "Guidance Notes on Reliability-Centered Maintenance", rev. 1. Houston: American Bureau of Shipping.
- Boring, R.L., Griffith, C.D. & Joe, J.C. 2007. The Measure of Human Error: Direct and Indirect Performance Shaping Factors (ed.). In *Human Factors and Power Plants and HPRCT 13th Annual Meeting*. IEEE, 170-176.
- BP. 2013. General safety strategy and performance standards for technical barriers, ed: Governing document of company.
- Cheng, Z., Jia, X., Gao, P., Wu, S., & Wang, J. 2008. A framework for intelligent reliability centered maintenance analysis. *Reliability Engineering & System Safety*, 93(6), 806-814.
- Chief Counsels Report: Chapter 4.10: Maintenance. 2011. <http://cybercemetery.unt.edu/archive/oilspill/20121210200431/http://www.oilspillcommission.gov/final-report,p.221-224>. [Accessed 2014]
- Dhar, R. 2011. Performance Standards For Safety Critical Elements – Are We Doing Enough! In *SPE European Health Safety and Environmental Conference in Oil and Gas Exploration and Production*. Society of Petroleum Engineers.
- El-Ladan, S.B. & Turan, O. 2012. Human reliability analysis—Taxonomy and praxes of human entropy boundary conditions for marine and offshore applications. In *Reliability Engineering & System Safety*, 98, 43-54.
- EU Council Directive 96/61/EC of 24 September 1996 concerning integrated pollution prevention and control. 1996. <http://eur-ex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996L0061:en:HTML>. [Accessed 2014].
- Firing, F.L., Ostby, E., Ingvarson, J. & Strom, O. 2011. TTS-The Systematic and Efficient Approach to Define Maintain and Demonstrate Safety Performance on Complex Hydrocarbon Processing Facilities (ed.). In *Offshore Technology Conference*.
- GL-070. 2004. "Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry", rev. 2. The Norwegian Oil Industry Association.
- HSE. 2014. UK Health and Safety Executive. <http://www.hse.gov.uk/risk>. [Accessed 2014].
- HSG48. 2009. "Reducing error and influencing behaviour". UK Health and Safety Executive.
- IAEA. 1999. "Basic safety principles for nuclear power plants: 75-INSAG-3", rev. 1. Vienna: The International Atomic Energy Agency.
- IEC:61508. 2010. "Part 1–7 Functional safety of electrical/electronic/programmable electronic safety-related systems". Geneva: International Electrotechnical Commission.
- IEC:61511-1. 2004. "Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements". Geneva: International Electrotechnical Commission.
- ISO:13702. 1999. "Petroleum and natural gas industries — Control and mitigation of fires and explosions on offshore production installations". Geneva: International Organization for Standardization.
- ISO:14224. 2006. "Petroleum, petrochemical and natural gas industries — Collection and exchange of reliability and maintenance data for equipment". Geneva: International Organization for Standardization.
- ISO:17776. 2000. "Petroleum and natural gas industries. Offshore production installations. Guidance on tools and techniques for hazard identification and risk assessment". Geneva: International Organization for Standardization.
- ISO:31000. 2009. "Risk management. Principles and guidelines on implementation". Geneva: International Organization for Standardization.
- Johansen, J.A. & Toennesen, N. 2002. Maintenance Management of Essential Safety Systems (ed.). In *SPE International Conference on Health Safety and Environment in Oil and Gas Exploration and Production*. Society of Petroleum Engineers.
- Mannan, S. 2014. Chapter 21 - Inherently Safer Design. In S. Mannan (ed.), *Lees' Process Safety Essentials*. Oxford: Butterworth-Heinemann, 403-407.
- Musharraf, M., Hassan, J., Khan, F., Veitch, B., Mackinnon, S. & Imtiaz, S. 2013. Human reliability assessment during offshore emergency conditions. *Safety Science*, 59, 19-27.
- PSA. 2012. "The trends in risk level in the petroleum activity (RNNP)". Norway, Stavanger: Petroleum Safety Authority.
- PSA. 2014a. "Regulations relating to management in the petroleum activities (The Management Regulations)". Norway, Stavanger: Petroleum Safety Authority.
- PSA. 2014b. "Guidelines to regulations relating to management in the petroleum activities (The Management Regulations)". Norway, Stavanger: Petroleum Safety Authority.
- PSA. 2014c. "Regulations relating to conducting petroleum activities (The Activities Regulations)". Norway, Stavanger: Petroleum Safety Authority.

- Ratnayake, R.M.C., Singh, S.P. & Raza, J. 2012. Development of a Barrier Management System for Continuous Monitoring and Maintenance of Safety Barriers (ed). In *Proceedings of the IEEE International Conference on Industrial Engineering and Engineering Management*. IEEE.
- Samarakoon, S.M.S.M.K & Gudmestad, O.T. 2011. Qualification of offshore facilities prior to application in a new field. *Journal of Cleaner Production*, 19, 13-20.
- Sevcik, A. & Gudmestad, O.T. 2014. Systematic Approach to Risk Reduction Measures in the Norwegian Offshore Oil and Gas Industry. Accepted for publication in *9th International Conference on Risk Analysis and Hazard Mitigation, Wessex Institute, 4 - 6 June*. New Forest, UK.
- Sklet, S. "Safety barriers: Definition, classification, and performance," *Journal of loss prevention in the process industries*, vol. 19, pp. 494-506, 2006.
- Statoil. 2012. Performance standards for safety systems and barriers - offshore. Technical and professional requirement, TR1055, Final Ver. 4.02, valid from 2012-02-09, ed: Governing document of company.
- Toriizuka, T. 2001. Application of performance shaping factor (PSF) for work improvement in industrial plant maintenance tasks. *International Journal of Industrial Ergonomics*, 28, 225-236.
- Wong, W. & Ceng, F. 2002. *How did that happen?: engineering safety and reliability*. Professional Engineering.

Papers

Paper 1 Systematic approach to risk reduction measures in the Norwegian offshore oil and gas industry

The paper has been accepted for the presentation in 9th International Conference on Risk Analysis and Hazard Mitigation, Wessex Institute, 4 - 6 June. New Forest, UK.

Risk Analysis 2014 is the ninth international conference on risk analysis and hazard mitigation. The conference covers a series of important topics of current research interests and many practical applications. It is concerned with all aspects of risk management and hazard mitigation, associated with both natural and anthropogenic hazards.

Papers presented at Risk Analysis 2014 will appear in a volume of WIT Transactions on Information and Communication Technologies (ISSN: 1746-4463, Digital ISSN: 1743-3517).

All conference papers are archived online at <http://library.witpress.com> where they are immediately and permanently available to the international scientific community.

Papers presented at Wessex Institute conferences are referenced by CrossRef and regularly appear in notable reviews, publications and databases, including referencing and abstract services such as SCOPUS, Compendex, ISI Web of Knowledge, Index to Scientific and Technical Proceedings, ProQuest and Scitech Book News. All conference books are archived in the British Library and American Library of Congress.

Systematic approach to risk reduction measures in the Norwegian offshore oil and gas industry

A. Sevcik, O.T. Gudmestad
University of Stavanger, Norway

Abstract

The term 'safety barriers' refers to the measures used in the various risk-assessment methods to reduce the likelihood and limit the consequences of hazardous events. An industry consensus is yet to be reached with regard to the boundaries and classification of safety barriers. The wide variability of work processes and physical systems that can be classified as barriers and the complex interactions between them means that they are challenging to identify. As such, a holistic view is required in order to foster adequate comprehension. The Petroleum Safety Authority Norway (PSA) focuses on maintaining a high level of health, environment, and safety awareness within the petroleum activities on the Norwegian Continental Shelf (NCS). The implementation of safety barriers has been a key safety principle in the PSA regulations for more than 10 years to guide the Norwegian oil and gas industry. The PSA constantly underlines the need for the risk picture to be clear and understandable with links and connections between related elements. This paper intends to provide some practical thoughts on how the boundaries for terms such as 'barrier', 'barrier element', 'barrier system' and 'function' can be determined. We will systemize existing knowledge and connect separate work processes into a unified system that will present barriers in a structured way, thus enabling adequate maintenance and follow-up of the barriers during their lifecycle. We intend to provide clarifications such that companies can manage and meet PSA regulations more precisely and efficiently.

Keywords: safety barrier, safety critical element, defence-in-depth, risk measure, safety management, offshore safety

1 Introduction

The broad literature survey presented by Sklet [1] reveals that a wide variety of different approaches and terms are used to describe and systemize barriers as risk-reducing measures. The author states that “different terms with similar meanings (barrier, defence, protection layer, safety critical element, safety function, etc.) have been used crosswise between industries, sectors, and countries” and claims that “it is also difficult for the PSA to manage the regulations without a clear definition and delimitation of the concept”. The importance of communication is highlighted by S. Kaplan [2]:

[...] 50% of the problems in the world result from people using the same words with different meanings. The other 50% come from people using different words with the same meaning.

For clarification of the discussion, several basic definitions of common terms used in this paper are presented below:

- Hazard - potential source of harm.
- Critical deviation - initiating (triggering) event of unwanted chain of events.
- Near-accident (incident) - event or chain of events which could have caused the unwanted (major) consequences once critical deviation occurred.
- Accident - event or chain of events which caused (major) consequences once critical deviation had occurred.

The main focus in this paper is on demands from the Norwegian offshore industry for clarification of the term ‘safety barrier’ and to present a new view of risk-reducing functions, as an interpretation of national regulations such as the Management Regulations from the Petroleum Safety Authority Norway (PSA). The topic is also relevant for other industries (e.g., the process industry) and application areas. The risk of major accidents is the focus.

2 Risk reduction measures: solutions and safety barriers

Currently in the offshore industry on the Norwegian Continental Shelf (NCS), there is a lot of discussion about barriers and the interactions between them that are greatly fostered by the Norwegian Petroleum Safety Authority’s (PSA) emphasis on safety barriers. However, the question is whether safety barriers are the only measures of risk reduction. In order to start a discussion, it is necessary to have an overview of the main steps in the risk reduction process.

ISO 31000’s definition [3] of risk as the “effect of uncertainty on objects” differs considerably from conventional understanding of risk in the engineering world, where it is seen as a product of probability and consequence in line with ISO 17776 [4]. It is not an objective of this paper to contribute to the understanding of risk essence; however, it may be assumed that barrier management cannot be seen as a substitute for risk management in the organization, but rather as a part of it.

Barrier management is a part of risk management in the organization that focuses on the reduction of the likelihood of negative consequences within activities performed. An interpretation of ISO 31000 and PSA's Management Regulations sections 4 & 5 [5] would propose the following view of the barrier management process (fig. 1).

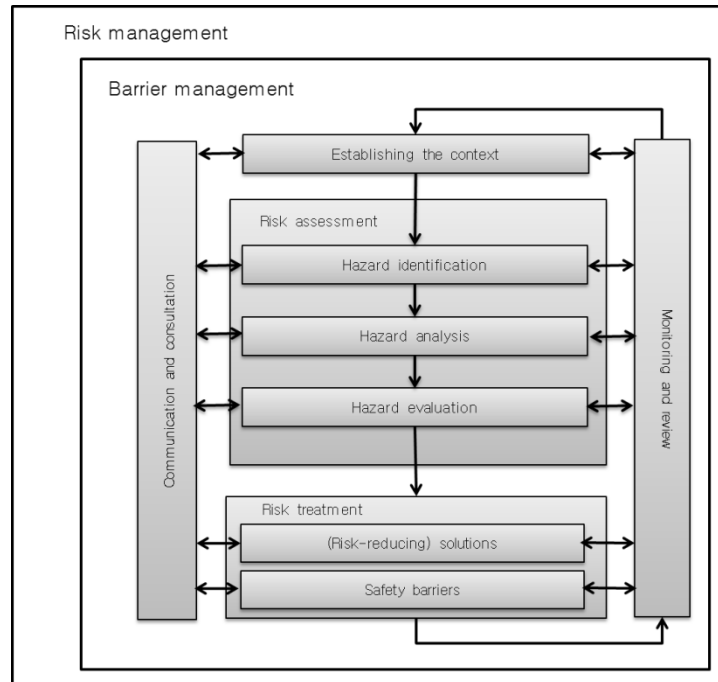


Figure 1: Barrier management process (an interpretation of ISO31000 and national regulations such as the management regulation from the Petroleum Safety Authority Norway)

The context is seen directly or indirectly as acting factors that may be important in the risk-reduction process. It includes not only requirements, standards, guidelines, acting regulations and policies, but also general experience, expert knowledge, engineering judgment, etc.

The risk assessment is intended to identify, analyse and evaluate the hazards in the activities performed. By understanding the nature of the hazard, the possible scenarios can be laid out and corresponding safety measures can be discussed accordingly. Required safety solutions and barrier functions should be derived as a result of this process.

Generally, risk treatment may be seen as a process which ensures that an acceptable risk level is achieved and maintained. To align with Petroleum Safety Authority regulations, Sections 4 & 5 of the Management Regulations [5] are incorporated:

In reducing risk [...] 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. The solutions and barriers that have the greatest risk-reducing effect shall be chosen [...]

Barriers shall be established that:

- a) reduce the probability of failures and hazard and accident situations developing,
- b) limit possible harm and disadvantages.

Two main groups of risk-reducing measures are stated: risk-reducing solutions and safety barriers.

Further assessing the definitions provided, it may be stated that solutions are the measures to reduce the likelihood of errors and hazards and accident situations occurring, i.e. preventing hazards (potential source of harm) from being realized. In other words, the solutions are used to reduce the likelihood of deviation which could initiate (trigger) an unwanted chain of events. Systems that are primary targets of these solutions may be seen as Safety Critical Systems (SCS) and will be discussed further in the paper.

Safety barriers are the measures which are selected after the risk-reducing solutions have been established and their purpose is to reduce the likelihood of failures and hazards and accident situations developing and limit the possible harm caused by an unwanted chain of events. Safety barriers are established to reduce the likelihood of the development of an unwanted chain of events when an initiating (triggering) event has already occurred, i.e. a hazard scenario has already started. The main and only function of a barrier is a safety function that is required on demand. Kecklund et al. [6] also describe safety barriers as “subsystems which can arrest the evolution of an accident through the execution of barrier functions”.

While we make a distinction between the solutions and safety barriers, it is important to see both of them as one entity designed to reduce the risk within performed activities.

3 Risk-reducing functions

3.1 Hierarchy of risk-reducing measures

In line with ISO17776 [4] and its general hierarchy of risk-reducing measures, this work will propose the following risk-reducing phases as generic safety functions (fig. 2): Prevention, Detection, Control, Mitigation, Emergency Response. These functionalities act in the same sequence when placed on the chain of accident development (fig. 3).

As presented in the introduction, Norwegian Petroleum Safety Authority (PSA) regulations [5] distinguish between the solutions and barriers. Following the interpretation of the regulations, it is hereby proposed that the prevention function is performed by solutions in the Safety Critical Systems (SCS) while other risk-reducing functions are performed by the Safety Barrier Systems (SBS).

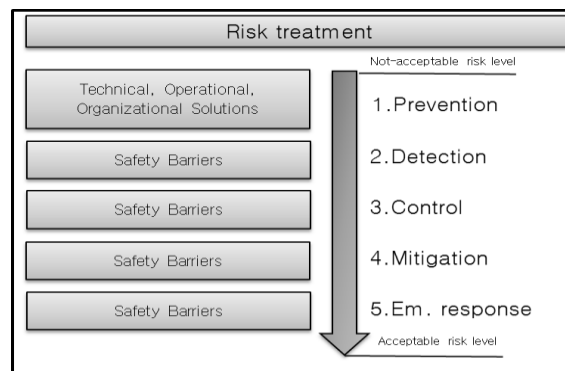


Figure 2: Risk treatment by solutions and safety barriers

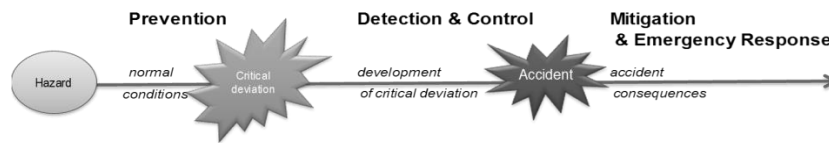


Figure 3: Accident event chain

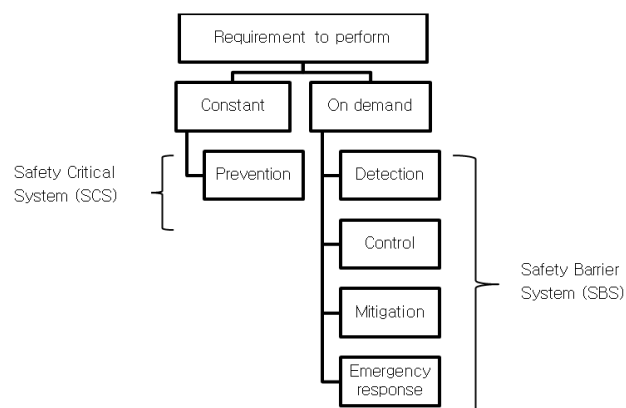


Figure 4: Requirement to perform

The requirement to perform indicates the actual need for the function and can be split between systems that perform the designed function continuously or at the pre-determined time intervals, and systems that are established to act on demand, where demand is seen as a critical deviation (fig. 4).

The requirement to perform should not be confused with the functionality or availability of the system. For example, the availability of a gas detector and firewall may differ, but the requirement to perform is on demand for both. A requirement to perform continuously is necessary for the measures that are directly engaged with hazards by ensuring that critical deviation will not occur. For example, a hydrocarbon-containing pipeline, pressure vessels and main process control systems are required to perform as designed continuously, because, in the case of failure, a critical deviation will immediately or subsequently occur.

3.2 Prevention

The prevention part embraces the inherent safety design (ISD) and process control activities by selecting such technical, operational and organizational solutions that would ensure the lowest risk level according to the ALARP principles.

The term 'prevention' can be used with several meanings. In line with ISO 13702 [7], prevention means a reduction of the likelihood of a hazardous event, and a further specified definition is used in this paper: *to prevent means to reduce the likelihood that critical deviation occurs*, where critical deviation is seen as an initiating event of an unwanted chain of events (hazardous event).

The practical meaning of prevention measures embraces the wide range of physical and non-physical elements, from Inherent Safe Design (ISD) and Best Available Technology (BAT) principles to main process equipment, containment vessels, piping including process-related operational actions, etc. Avoidance of a hazard is seen as a part of the ISD principles and is therefore embraced by the prevention definition used in this paper, because the likelihood of a hazardous event will be reduced if the hazard is removed (avoided).

The main function of safety critical (solution-targeted) equipment or activities is a process-, or utility-related function. These solutions may be:

- Organizational: process design principles, equipment selection guidelines, HSE strategies, etc.
- Operational: selection and improvement of operational process activities with a focus on risk-reduction.
- Technical: selection of technical equipment that shall ensure that designed process or utility functions will be performed safely and associated hazards will be prevented, i.e. the likelihood of a triggering event is reduced.) This prevention function is required to perform constantly to keep a hazard from its realization.

The prevention measures cannot be removed from the system without affecting the main process functions, i.e. they are inherent in the main process functions and have an effect constantly. If they function as designed, the

abnormal conditions will not occur. A typical example of safety critical equipment with an applied technical solution would be hydrocarbon process piping designed to prevent leakage by adding a corrosion allowance.

Theoretically, the applied solutions would be sufficient to ensure the required safety if errors and overall uncertainty could be avoided. In the real world, however, they fail and cause the critical deviation and hazard realization to lead to an accident. Once the unwanted chain of events starts, the safety barriers are mobilized to stop its development or to limit the consequences if an accident occurs.

3.3 Detection and control

Detection and control systems are the safety barriers that are designed to perform the safety function only when an unwanted chain of events starts to develop. They act on demand when the prevention measures – safety-related solutions – fail. A detection function ascertains the existence, presence, or appearance of critical deviation as soon as possible and serves as further input to other barrier systems as well as being necessary to activate operational barriers, i.e. human actions. The detection function itself will not stop the unwanted chain of events, but it is essential in order to enable the function of controlling barrier systems. ‘To control’ refers to stopping the unwanted chain of events before it develops into a major accident, and emergency shutdown or depressurization functions are the examples of such functions. While the term ‘detection function’ is commonly understood, the term ‘control function’ has several different interpretations. ISO 13702 [7] defines control as the limitation of the extent and/or duration of a hazardous event. In this paper we further specify the term and state that *control means to reduce the likelihood that critical deviation will develop into a major accident once it occurs*, i.e. to stop the unwanted chain of events when critical deviation occurs.

It is important to distinguish between a process control function that is a part of the safety-related solutions and one that is a function of the control barriers. Most of the process control systems are activated constantly or on a regular basis. The control function of barrier systems is activated on demand when the process or activity control is lost and the critical deviation occurs. If the barrier function to control succeeds, the development of an unwanted chain of events is stopped, i.e. the control is regained, and the near-accident event is reported. If these barriers fail, the major accident occurs, and then barriers to limit the consequences of the accident are activated.

3.4 Mitigation and emergency response

The definition of a major accident is not standardized, but can be seen as an escalation of an unwanted chain of events that has already caused certain consequences. It may be referred as Defined Hazard and Accident Situations (Norwegian: *Definerte Fare og Ulykkessituasjoner, DFU*). Generally, a major accident is defined as an acute incident such as a major spill, fire or explosion that immediately or subsequently causes multiple serious personal injuries and/or

loss of human lives, serious harm to the environment and/or loss of major financial assets [8].

A major accident is the result of the failure of safety-related solutions (prevention) and detection/control barrier systems. In order to limit or reduce these consequences, mitigating barrier systems are established together with emergency response measures. The successful functioning of these systems will ensure the lowest harm possible by stopping the accident escalation as soon as possible. If the mitigation and emergency response barrier systems function poorly, the accident may develop to its full potential and cause maximal damage.

Mitigation and emergency response barrier functions are designed to perform on demand, when an accident occurs and the operational control is lost. A well-known example of a mitigation system is a deluge system.

4 Risk-reducing systems

4.1 Functional equipment groups

Most oil operators on the NCS have determined groups of critical equipment and prepared the performance standards for these groups [9, 10]. It is common to refer to these groups of equipment as barrier elements. It is well-understood that these equipment groups are tightly linked together; however, the attention to these links is often not clearly expressed. It should be stressed that a risk-reducing function can be ensured just by a fully-functioning safety system, which usually consists of various elements from different equipment groups, so the links between them are very important.

The need to know the boundaries of a system is well-expressed when the system's independence is analysed. The independence requirement is also stated in the Management Regulations of the PSA [8]. A good example of system independence could be a fire-fighting system that has its own firewater pumps designed to use just for the system in case of demand. Older installations sometimes have their firewater supply system connected to a general seawater utility used to supply seawater for the process needs. In this case, the independence requirement is not fulfilled, as the fire-fighting system's critical element – a pump – is not specifically designed for the safety-function only. The actual safety system should not be seen as only the equipment group based on its functionality, but more as the combination of these acting in defence against hazard realization.

4.2 Hazard and three lines of defence

Hazard identification is the first step of the process to identify existing or establish new barriers and should be the integral part of the barrier management system. It is important to note that hazard identification activities should be continuously performed and existing hazard lists should be updated. The HAZID process is a good example used in the industry for hazard identification. It is

important to select a proper scale of hazard analysis, for example: Hydrocarbon leak in area no. xxx, Dropped objects, Collision with ship, etc. Once site-specific hazard scenarios have been laid out, each of them can be looked at from the time perspective (fig. 5). It is possible to distinguish between three major phases when looking at the timeline of any hazard scenario: normal conditions, abnormal condition such as the result of critical deviation, and the accident phase. Some systems can perform more than one main function, depending on the hazard scenario.

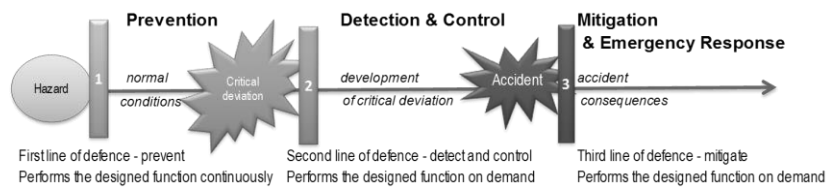


Figure 5: Three lines of defence

4.3 First line of defence – Safety Critical System (SCS) as prevention system

A Safety Critical System (SCS) is a system with applied technical, operational and organizational solutions designed to prevent the realization of a potential source of harm inherent in the activities. The requirement to perform is constant. In the case of a system's failure, a critical deviation will occur and start the development of an unwanted chain of events.

The SCS can be composed just of the technical solutions part, or just of operational solutions, or of a combination of both (fig. 6). A possible example of an SCS could be a system to prevent the loss of containment, a system to prevent process deviations (process safety), or a system to prevent the loss of structural integrity.

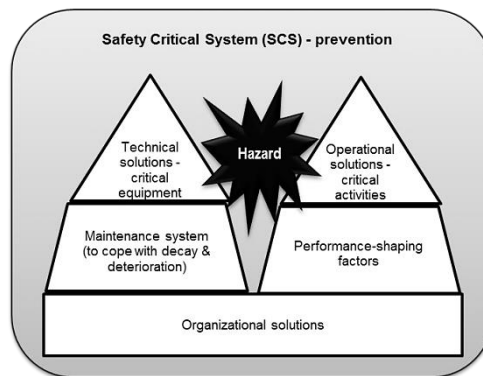


Figure 6: Safety Critical System (SCS)

- Organizational: strategies and principles under which the system is built.
- Operational: operational process activities performed by the operator. Performance-shaping factors should be known in order to estimate the likelihood of human error.
- Technical: process equipment and related auxiliary equipment that is subjected to a specific hazard scenario and should be designed or/and selected according to ALARP principles. The maintenance system is established to ensure the functional and safety requirements over the asset's lifetime. Performance-shaped factors related to operational maintenance activities are treated as a part of the maintenance system.

The SCS and associated elements cannot be removed from the facility or process system without affecting that process imminently or subsequently.

4.4 Second and third lines of defences - Safety Barrier Systems (SBS)

It is important to see a barrier as an actually established measure that is able to prevent or stop the unwanted chain of events once the initiating event is triggered. Safety principles for nuclear power plants distinguish barriers as physical measures only, while other types of protection are recognized but not defined as barriers [11]. Organizational safety measures such as procedures, strategies, guidelines, requirements, etc. can be seen as a regulatory basis that is used to establish the barriers, but they are not barriers in themselves. There are a lot of intentions to name them as organizational barriers; however, they cannot be seen as actual barriers that would be able to perform in the case of need. Either physical equipment – a technical barrier – or human actions – an operational barrier – can actually stop the unwanted chain of events that has already started due to the specific critical deviation or mitigate the consequences of it.

A Safety Barrier System (SBS) is comprised of technical and operational barriers (figs. 7, 8). Some of the automatized system will only have the technical barrier part, while manually-activated or manually-operated systems will require appropriate human actions – an operational barrier. There can also be systems based only on operational barriers.

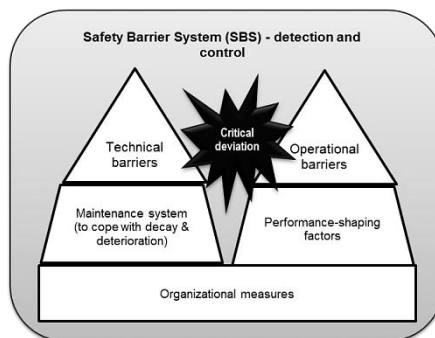


Figure 7: Safety Barrier System – detection and control

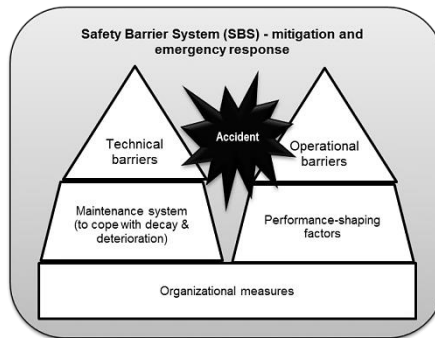


Figure 8: Safety Barrier System – mitigation and emergency response

The technical part of a Safety Barrier System (SBS) is comprised of a technical barrier, the maintenance system, and organizational measures that are used as a basis for the establishment and follow-up of the barrier system. A technical barrier is a physical element that is established to perform safety functions related to stopping the unwanted chain of events when it has been started: detection, control, mitigation or emergency response.

The Safety Barrier System (SBS) can theoretically be removed from the facility as it functions on demand after the critical deviation has occurred. Then process activities could theoretically still be carried out, assuming that no critical deviations would happen; however, in the case where they did occur, the potential consequences would be extreme.

To ensure the required functionality of technical barriers, the maintenance and follow-up activities should be performed by establishing a maintenance programme. For example, the automatic safety system is one of the main technical barriers; therefore function testing and demand monitoring should be established. This refers to the field of functional safety and is governed by IEC61511 [12] and IEC61508 standards [13]. Other technical barriers should be analysed, the criticality and failure/fault modes of their elements shall be determined and appropriate maintenance activities should be undertaken. All technical barrier elements should be tagged and marked accordingly in the general maintenance system of the facilities. In addition, the maintenance system should incorporate the analysis of human factors and the performance-shaping factors of operational maintenance activities. Industry examples show that maintenance system and barrier follow-up is enabled through the creation of performance standards – the functional requirement list of each barrier system [14, 15]. It must be noted, however, that the boundaries of barrier definition used in most companies differ from those presented in this paper.

The operational part of a Safety Barrier System (SBS) consists of an operational barrier, the performance-shaping factors and organizational measures that are used as a basis to establish the system itself. An operational barrier can be seen as determined specific actions that shall be carried out in the case of

critical deviation to prevent or to stop the development of an unwanted chain of events, for example, a manual activation of an evacuation alarm, etc.

An operational barrier is defined as the specific safety activities performed by human operator therefore human factors affect it. The UK Health and Safety Executive defines human factors as “environmental, organizational and job factors, and human and individual characteristics which influence behaviour at work in a way which can affect health and safety” [16]. Explicitly defined human factors may be seen as Performance-Shaping Factors (PSF) and are used to model human behaviour as the underlying causes of abnormal performance [17]. It must be noted that PSF are explicitly used to describe the influence on human performance [18] and should not be directly referred to as the performance of technical equipment. Technical equipment is affected by maintenance actions which are again influenced by PSF [19]. However, the PSF of maintenance activities should be seen as an integral part of the maintenance system, and maintenance activities should be distinguished from the operational safety barrier concept that embraces specified safety actions in the case of abnormal situations.

4.5 Generic work flow diagram

The generic work flow diagram given in fig. 9 embraces the concept of solutions and safety barriers presented in this paper.

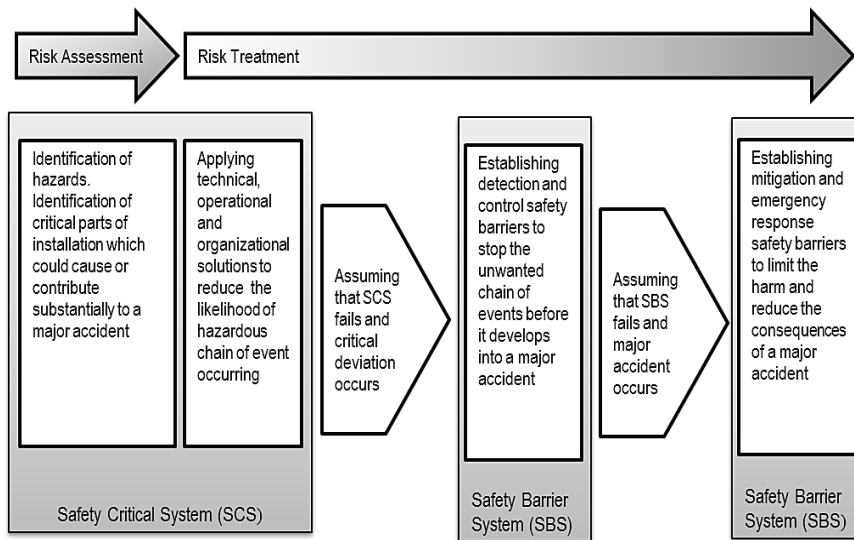


Figure 9: Generic work flow

It presents the general scheme of hazard identification and the treatment process. A facility-specific Barrier Map can be derived to show risk-reducing measures – solutions and barriers – as put in place to manage the hazards (fig. 10).

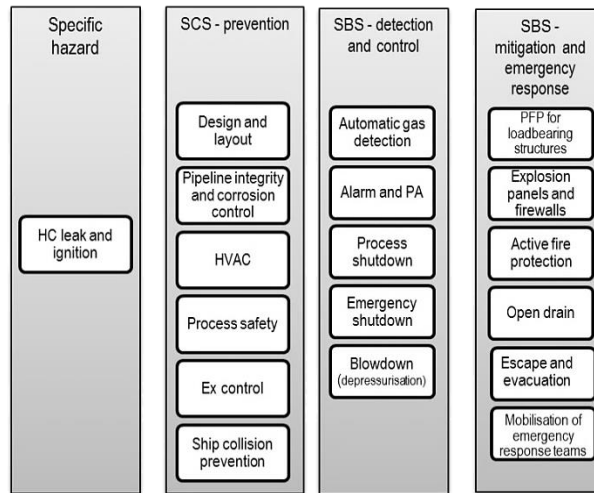


Figure 10: Example of Barrier Map of facility

4.6 Comparison between SCS and SBS

The components of these systems may be named Safety Critical Elements (SCE) and Safety Barrier Elements (SBE). Currently the industry uses the term ‘SCE’ to define all the elements that are “such parts of the installation [...] which could cause and contribute substantially to a major accident or a purpose of which is to prevent or limit the effect of a major accident” [20]. According to the concept presented in this paper, the new boundaries of the SCE would embrace parts of the installation which could cause or contribute to a major accident. Safety Barrier Elements – SBE – would embrace the elements of independent safety systems that are installed only for the safety function and in the case of failure will stop the accident development or limit the effect of an accident as a Safety Barrier System (SBS). Table 1 below summarizes the main differences between Safety Critical System (SCS) and Safety Barrier Systems (SBS).

Table 1: SCS and SBS comparison

Safety Critical System (SCS)	Safety Barrier System (SBS)
Technical, operational and org. solutions applied to process, utilities, structural, etc. elements to reduce risk within them	Independent system designed only for risk-reducing functions
Reduces the likelihood of critical conditions occurring	Reduces the likelihood of critical conditions developing and limits the harm
Requirement to perform – constant (normal conditions)	Requirement to perform – on demand (abnormal conditions)
Cannot be removed without affecting process	Can be removed without affecting process

4.7 Comparison between generic safety functions

Sklet [1] uses the Occupational Accident Research Unit (OARU) process model [21]. The accident is divided into three phases: the initial phase, the concluding phase, and the injury phase. The generic safety functions are intended to stop the chain of events before it develops into the next phase. A comparison reveals the different meanings for the same terms used by researchers and standards (fig. 10). For example, in the classification of Hollnagel [22], both ‘control’ and ‘mitigation’ are treated as protection, while ‘prevention’ also embraces the control measures. In the classification suggested in the ARAMIS-project [23], both functions ‘avoid’ and ‘prevent’ correspond to the function prevention according to [1]. The last row in the figure presents the boundaries of definitions used in this paper (in line with ISO 17776, [4]).

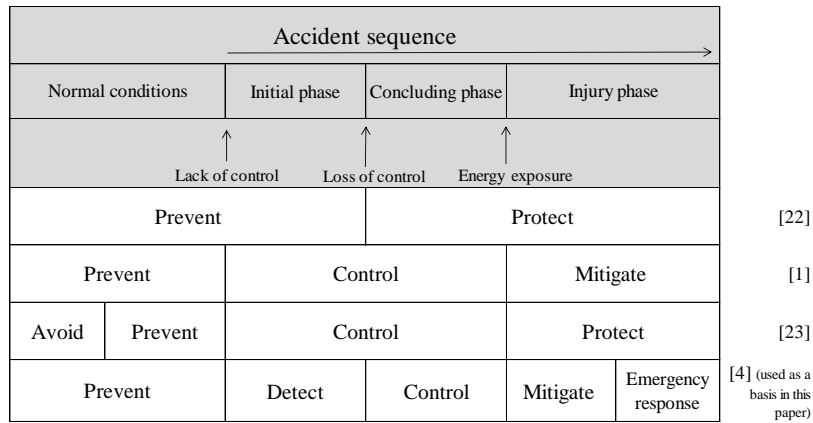


Figure 11: Generic safety functions in a process model, adapted from [1]

4.8 Three lines of defence as a model for risk communication

A typical process model approach divides the accident sequence into several phases, and analyses the defence elements that may stop the unwanted chain of events. A qualitative process model is presented by combining the accident timeline and the proposed risk-reducing systems (fig. 12). It allows the actual established measures to be seen against the specific hazard scenario in the various phases of the potential accident timeline.

Such a sequential accident model may also be used as a basis to analyse particular risk-reducing functions in detail, for example, incorporating fault or event trees [24, 25]. In the generic example, the event tree model could be used to lay down the systems used in the specific hazard scenario, and then a fault tree analysis could be performed for each part (fig. 13).

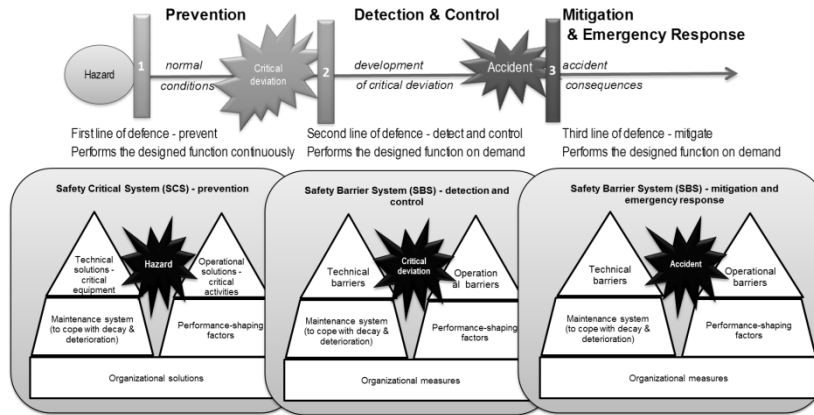


Figure 12: Three lines of defence model

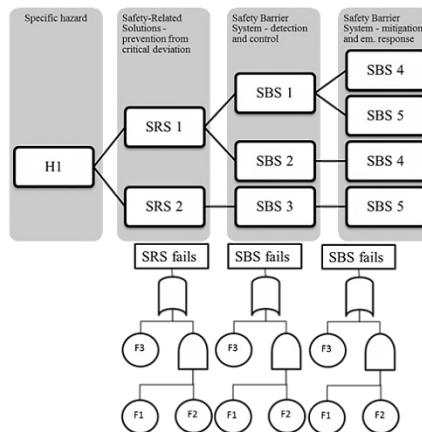


Figure 13: Generic example of using event and fault trees

In [8] it is stated that “personnel shall be aware of what barriers have been established and which function they are intended to fulfil”, and such a model may be used as a first step for broader communication about the safety barriers and their role in arresting the accident’s escalation. Therefore such a model may be valuable in risk communication, where its simplicity could be well-accepted by non-technical safety personnel without the requirement for special knowledge.

5 Defence-in-depth

5.1 Defence-in-depth conception

The concept of defence-in-depth was developed within the nuclear industry and constitutes the basis for the discussion of safety barriers. IAEA (1999: 17), [11], describes the defence-in-depth principle in the following way:

To compensate for potential human and mechanical failures, a defence in depth concept is implemented, centred on several levels of protection including successive barriers preventing the release of radioactive material to the environment. The concept includes protection of the barriers by averting damage to the plant and to the barriers themselves. It includes further measures to protect the public and the environment from harm in case these barriers are not fully effective.

All safety activities within the nuclear industry are subjected to overlapping layers of protection, so that if an error occurs it will be altered or escalation will be stopped without causing harm. The idea of multiple levels of protection is the core principle of defence-in-depth and it aligns with Swiss cheese model [26], where an organization's defences against error are modelled as a series of layers. Following these concepts, Safety Critical Systems (SCS) and Safety Barrier Systems (SBS) are shown as generic safety layers (fig. 14).

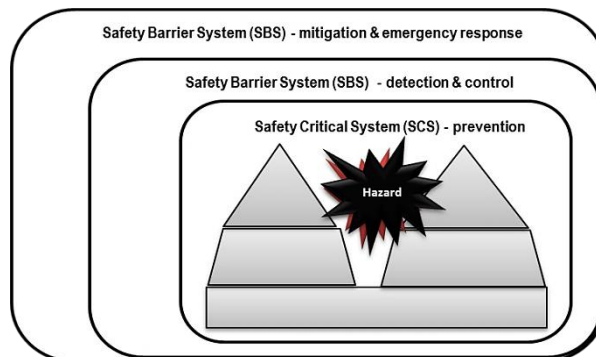


Figure 14: SCS and SBS as generic safety layers

Based on the multiple levels of protection concept, known risk assessment methods such as Layer of Protection Analysis (LOPA) are widely used [27, 28]. Although a layer of protection is currently seen as a synonym to a barrier, it is different according to the re-defined concept of barrier boundaries presented in this paper. Both Safety Critical Systems (SCS) and Safety Barrier Systems (SBS) create layers of protection but are distinguished according to the requirement to perform and the nature of the system. The SCS embrace the layers of protection that are required to perform constantly and have a process-related main function,

while the SBS are treated as additional layers of protection that perform on demand and are established only for safety functions (fig. 15).

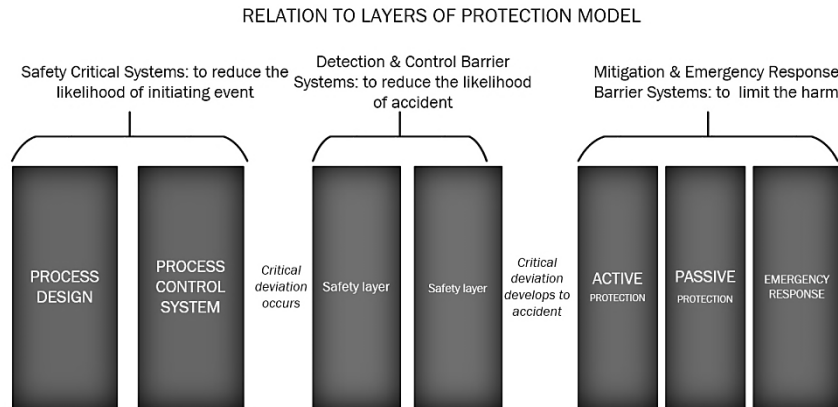


Figure 15: SCS and SBS as layers of protection

6 Conclusions

S. Kaplan [2] describes a case where risk analysts worked for four years trying to define the word 'risk'. They finally gave up, saying that maybe "it is better not to define risk". It was proposed that each author be allowed to define it in his own way, only being asked to clarify what way that is. Accordingly, in order to improve risk communication among the involved parties, it is important to focus more on the clarity than the verbal interpretations of the safety barrier concept.

"Finally, making the decision is not the end of the job. It's necessary to get the decision accepted and implemented. For that we need the support of the people affected by it. That means risk communication, and decision communication. For that to take place, it's crucial that we have words that we all understand and use in the same way"[2].

Based on the synthesis of [4], the PSA regulations and common features of the terms found in the scientific literature, the concepts of Safety-Related Solutions (SRS) and Safety Barrier Systems (SBS) are proposed as a basis for further discussion of risk-reducing measures in the industrial activities.

Sklet [1] notes that "such a broad definition undermines the concept of barrier as some claim that almost everything may be considered as a barrier" and suggests to distinguish between the measures "that may prevent, control, or mitigate the event sequence or accident scenario directly".

Correspondingly, prevention, detection/control, and mitigation/emergency response systems have been introduced and described. Aligning with the PSA regulations, the safety-related solutions have been separated from safety barriers and systematically described. Links between technical, operational and

organizational elements have been proposed incorporating maintenance activities and human factors, such as performance-shaping factors.

In addition, the paper proposes a model for communication about risk-reducing measures: safety solutions and barriers. The results may be useful for the Norwegian oil industry in its effort to fulfil the requirements of the PSA.

References

- [1] S. Sklet, "Safety barriers: Definition, classification, and performance," *Journal of loss prevention in the process industries*, vol. 19, pp. 494-506, 2006.
- [2] S. Kaplan, "The words of risk analysis," *Risk analysis*, vol. 17, pp. 407-417, 1997.
- [3] ISO:31000, Risk management. Principles and guidelines on implementation, ed: Geneva: International Organization for Standardization, 2009.
- [4] ISO:17776, Petroleum and natural gas industries. Offshore production installations. Guidance on tools and techniques for hazard identification and risk assessment, ed: Geneva: International Organization for Standardization, 2000.
- [5] PSA, Regulations relating to management in the petroleum activities (The Management Regulations), ed: Norway, Stavanger: Petroleum Safety Authority, 2014.
- [6] L. J. Kecklund, A. Edland, P. Wedin, and O. Svenson, "Safety barrier function analysis in a process industry: a nuclear power application," *International journal of industrial ergonomics*, vol. 17, pp. 275-284, 1996.
- [7] ISO:13702, Petroleum and natural gas industries. Control and mitigation of fires and explosions on offshore production installations, ed: Geneva: International Organization for Standardization, 1999.
- [8] PSA, Guidelines to regulations relating to management in the petroleum activities (The management regulations), ed: Norway, Stavanger: Petroleum Safety Authority, 2014.
- [9] Statoil, Performance standards for safety systems and barriers - offshore. Technical and professional requirement, TR1055, Final Ver. 4.02, valid from 2012-02-09, ed: Governing document of company, 2012.
- [10] BP, General safety strategy and performance standards for technical barriers, ed: Governing document of company, 2013.
- [11] IAEA, Basic safety principles for nuclear power plants: 75-INSAG-3, rev.1, ed: Vienna: The International Atomic Energy Agency, 1999.
- [12] IEC:61511-1, Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements, ed: Geneva: International Electrotechnical Commission, 2004.
- [13] IEC:61508, in Part 1–7 Functional safety of electrical/electronic / programmable electronic safety-related systems, ed: Geneva: International Electrotechnical Commission, 2010.

- [14] F. L. Firing, E. Ostby, J. Ingvarson, and O. Strom, "TTS-the systematic and efficient approach to define maintain and demonstrate safety performance on complex hydrocarbon processing facilities," in *Offshore Technology Conference*, 2011.
- [15] O. Thomassen and M. Sørum, "Mapping and monitoring the technical safety level," in *SPE International Conference on Health Safety and Environment in Oil and Gas Exploration and Production*, 2002.
- [16] HSG48, *Reducing error and influencing behaviour*, ed: UK Health and Safety Executive, 2009.
- [17] S. B. El-Ladan and O. Turan, "Human reliability analysis—Taxonomy and praxes of human entropy boundary conditions for marine and offshore applications," *Reliability Engineering & System Safety*, vol. 98, pp. 43-54, 2// 2012.
- [18] M. Musharraf, J. Hassan, F. Khan, B. Veitch, S. MacKinnon, and S. Imtiaz, "Human reliability assessment during offshore emergency conditions," *Safety Science*, vol. 59, pp. 19-27, 11// 2013.
- [19] T. Toriizuka, "Application of performance shaping factor (PSF) for work improvement in industrial plant maintenance tasks," *International journal of industrial ergonomics*, vol. 28, pp. 225-236, 2001.
- [20] R. Dhar, "Performance standards for safety critical elements – are we doing enough!," in *SPE European Health Safety and Environmental Conference in Oil and Gas Exploration and Production*, 2011.
- [21] U. Kjellen and T. J. Larsson, "Investigating accidents and reducing risks—a dynamic approach," *Journal of occupational accidents*, vol. 3, pp. 129-140, 1981.
- [22] E. Hollnagel, *Barriers and accident prevention*: Ashgate Publishing, Ltd., 2004.
- [23] N. Duijm, M. Madsen, H. Andersen, A. Hale, L. Goossens, H. Londiche, et al., "Assessing the effect of safety management efficiency on industrial risk," in *European Safety and Reliability Conference (ESREL 2003)*, 2003, pp. 575-581.
- [24] L. Xue, J. Fan, M. Rausand, and L. Zhang, "A safety barrier-based accident model for offshore drilling blowouts," *Journal of loss prevention in the process industries*, vol. 26, pp. 164-171, 2013.
- [25] M. Kujath, P. Amyotte, and F. Khan, "A conceptual offshore oil and gas process accident model," *Journal of loss prevention in the process industries*, vol. 23, pp. 323-330, 2010.
- [26] J. Reason, "The contribution of latent human failures to the breakdown of complex systems," *Philosophical transactions of the Royal Society of London. B, Biological sciences*, vol. 327, pp. 475-484, 1990.
- [27] R. Gowland, "The accidental risk assessment methodology for industries (ARAMIS)/layer of protection analysis (LOPA) methodology: A step forward towards convergent practices in risk assessment?," *Journal of hazardous materials*, vol. 130, pp. 307-310, 2006.
- [28] A. E. Summers, "Introduction to layers of protection analysis," *Journal of hazardous materials*, vol. 104, pp. 163-168, 2003.

Paper 2 Solutions and safety barriers: the holistic approach to risk-reducing measures

The paper has been accepted for the presentation at the 24th ESREL conference, ESREL 2014, 14-18 September 2014, Wroclaw, Poland.

The annual European Safety and Reliability Conference ESREL stems from a European initiative merging several national Conferences into a major yearly conference under the auspices of the European Safety and Reliability Association (ESRA).

The XXIV edition of the conference, ESREL 2014 will provide a forum for presentation and discussion of scientific works covering theories and methods in the field of risk, safety and reliability, and their application to a wide range of industrial, civil and social sectors and problem areas.

The conference proceedings will be published by CRC Balkema and it will have a double form:

- full-length papers will be published on the electronic drive (CD-ROM) with ISBN number, indexed in Scopus and Thomson Reuters Conference Proceedings Citation Index (Web of Science),
- the paper book containing one-paged extended abstracts.

Papers selected by the Technical Committee will be published in Reliability Engineering and System Safety or Journal of Risk and Reliability.

Solutions and safety barriers: the holistic approach to risk-reducing measures

A. Sevcik & O.T. Gudmestad

University of Stavanger, Norway

ABSTRACT: Currently in the offshore industry on the Norwegian Continental Shelf (NCS), there is much discussion about barriers and the interactions between them. This discussion is fostered to a large extent by the Norwegian Petroleum Safety Authority's (PSA) emphasis on safety barriers. The term 'safety barriers' refers to the measures used to reduce the likelihood and limit the consequences of major accidents. However, the question is whether safety barriers are the only measures for risk reduction. This paper will describe the process model of an accident and discuss risk-reducing measures following ISO 17776 and national regulations such as the Management Regulations from the Petroleum Safety Authority Norway (PSA). Two main groups of risk-reducing measures are distinguished: (1) technical, operational and organizational solutions applied to the critical systems and (2) safety barriers. The main focus in this paper is the demand from the Norwegian offshore industry for clarification of the term 'safety barrier'.

1 INTRODUCTION

Generally, risk treatment may be seen as a process which ensures that an acceptable risk level is achieved and maintained. To align with the Norwegian Petroleum Safety Authority regulations, Sections 4 & 5 of the Management Regulations are followed (PSA 2014a & PSA 2014b):

In reducing risk [...] the responsible party shall select technical, operational and organizational solutions that reduce the probability that harm, errors and hazard and accident situations occur.

Furthermore, barriers as mentioned in Section 5 shall be established. The solutions and barriers that have the greatest risk-reducing effect shall be chosen [...].

Barriers shall be established that:

- a) reduce the probability of failures and hazard and accident situations developing,
- b) limit possible harm and disadvantages.

Two main groups of risk-reducing measures are named: risk-reducing solutions and safety barriers (Sevcik & Gudmestad 2014).

On further assessment of the definitions provided, it may be stated that risk-reducing solutions are the measures to reduce the likelihood of errors, hazards and accident situations occurring, i.e. pre-

venting hazards (potential source of harm) from being realized. In other words, the solutions are used to reduce the likelihood of such deviations which could initiate (trigger) an unwanted chain of events. Systems that are primary targets of these solutions may be seen as Safety Critical Systems (SCS) and will be discussed further in the paper.

Safety barriers are the measures which are selected after the risk-reducing solutions have been established, with the purpose of reducing the likelihood of failures and hazards, preventing accident situations from developing and limiting the possible harm caused by an unwanted chain of events. Safety barriers are established to reduce the likelihood of the development of an unwanted chain of events when an initiating (triggering) event has already occurred, i.e. a hazard scenario has already started. The main and only function of a barrier is a safety function that is required on demand.

While we make a distinction between the risk-reducing solutions and safety barriers, it is important to see both of them as one entity designed to reduce the risk within performed activities.

2 RISK-REDUCING MEASURES IN AN ACCIDENT MODEL

2.1 Generic accident model

In line with ISO 17776 (2000) and its general hierarchy of risk-reducing measures, this work will propose the following risk-reducing phases as generic safety functions: Prevention, Detection, Control, Mitigation and Emergency Response. These functionalities act in the same sequence when placed on the chain of accident development (Fig. 1).

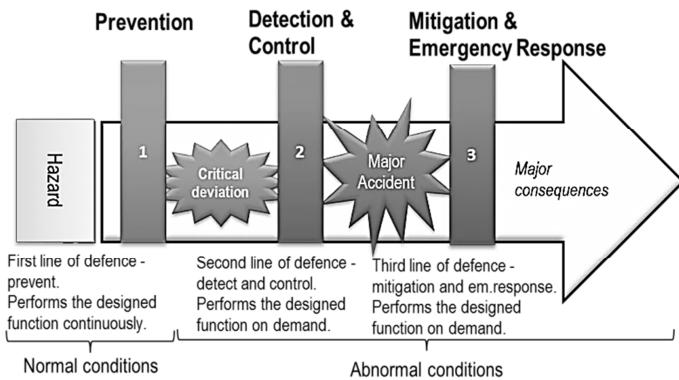


Figure 1. General accident model with safety functions

The term ‘prevention’ can be used with several meanings. In line with ISO 13702 (1999), prevention means a reduction of the likelihood of a hazardous event, and a further specified definition is used in this paper: to prevent means *to reduce the likelihood that a critical deviation occurs*, where critical deviation is seen as an initiating event of an unwanted chain of events.

While the term ‘detection function’ is commonly understood, the term ‘control function’ has several different interpretations. ISO 13702 defines control as the limitation of the extent and/or duration of a hazardous event. In this paper we further specify the term and state that control means *to reduce the likelihood that a critical deviation will develop into a major accident once it occurs*, i.e. to stop the unwanted chain of events when critical deviation occurs.

A major accident is the result of the failure of the safety-related solutions (prevention) and detecting/controlling barrier systems. In order to limit or reduce the consequences of an accident, mitigating barrier systems are established together with emergency response measures. The successful functioning of these systems will ensure the lowest feasible harm by stopping the accident escalation as soon as possible. If the mitigation and emergency response barrier systems function poorly, the accident may develop to its full potential and cause maximal damage.

2.2 Risk reducing measures as systems

Currently the industry uses the term ‘Safety Critical Element (SCE)’ to define all the elements that are “such parts of the installation [...] which could cause and contribute substantially to a major accident or a purpose of which is to prevent or limit the effect of a major accident” (Dhar 2011). According to the concept presented in this paper, the boundaries of the SCE would embrace parts of the installation which could cause or contribute to a major accident (Fig. 2).

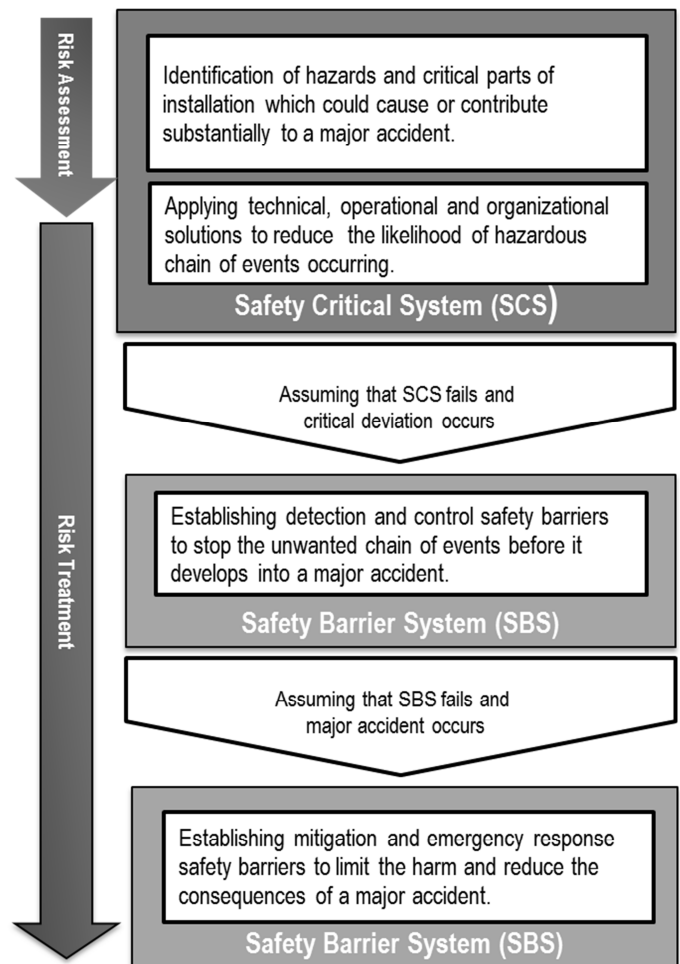


Figure 2. Establishing SCS and SBS of an installation

A Safety Critical System (SCS) is described as a system with applied technical, operational and organizational solutions designed to prevent the realization of a potential source of harm inherent in the activities. The requirement to perform is constant. In the case of a system failure, a critical deviation will occur and start the development of an unwanted chain of events (Fig. 3).

The Safety Barrier System – SBS – will embrace the elements of independent safety systems that are installed only for the safety function and in the case of failure will stop the accident’s development or limit the effect of an accident (Figs. 4-5).

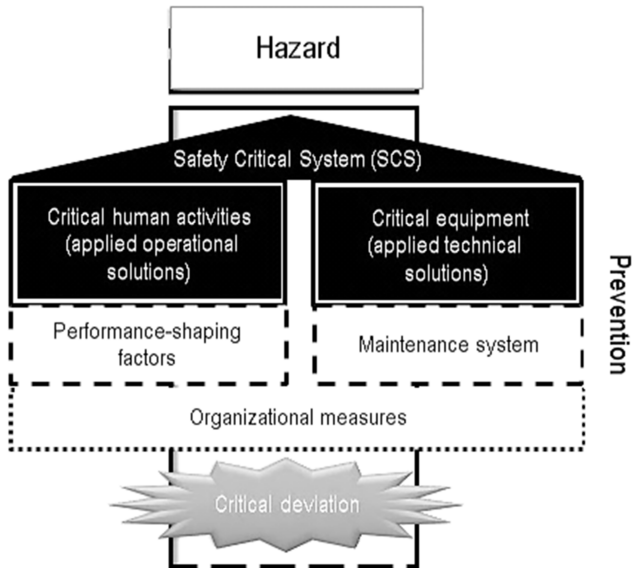


Figure 3. SCS for prevention

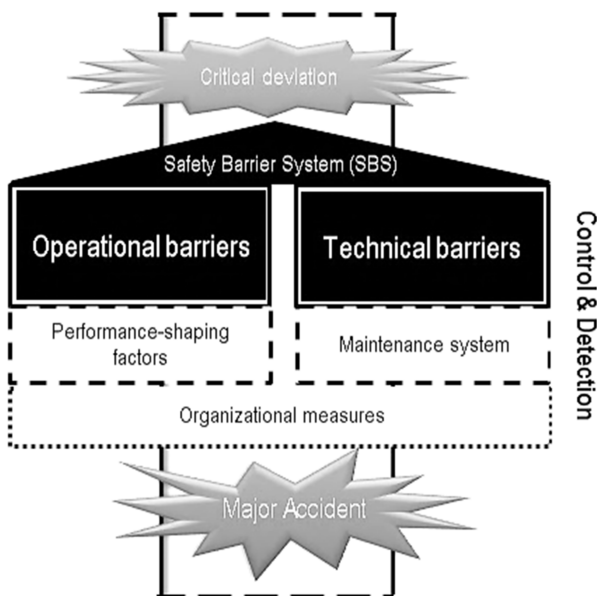


Figure 4. SBS for detection and control

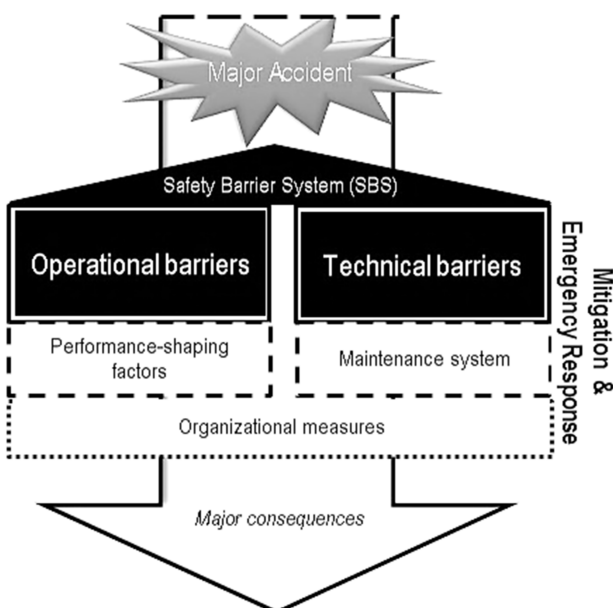


Figure 5. SBS for mitigation and emergency response

It is important to see a barrier as an actually established measure that is able to prevent or stop the unwanted chain of events once the initiating event is triggered. Safety principles for nuclear power plants distinguish barriers as physical measures only, while other types of protection are recognized but not defined as barriers (IAEA 1999). Organizational safety measures, such as procedures, strategies, guidelines, requirements, etc., can be seen as part of a regulatory basis that is used to establish the barriers, but they are not barriers in themselves. There is considerable eagerness are a lot of intentions to name them as organizational barriers; however, they cannot be seen as actual barriers that would be able to perform in the case of need. Either physical equipment – a technical barrier – or human actions – an operational barrier – can actually stop the unwanted chain of events that has already started due to the specific critical deviation or mitigate the consequences of it.

The differences between SCS and SBS are summarized in Table 1 and Figure 6.

Table 1. SCS and SBS comparison

Safety Critical System (SCS)	Safety Barrier System (SBS)
Technical, operational and org. solutions applied to process, utilities, structural, etc. elements to reduce risk.	Independent system designed only for risk-reducing functions.
Reduces the likelihood of critical conditions occurring.	Reduces the likelihood of critical conditions developing and limits the harm.
Requirement to perform – constant (normal conditions).	Requirement to perform – on demand (abnormal conditions).
Cannot be removed without affecting process.	Can be removed without affecting process.

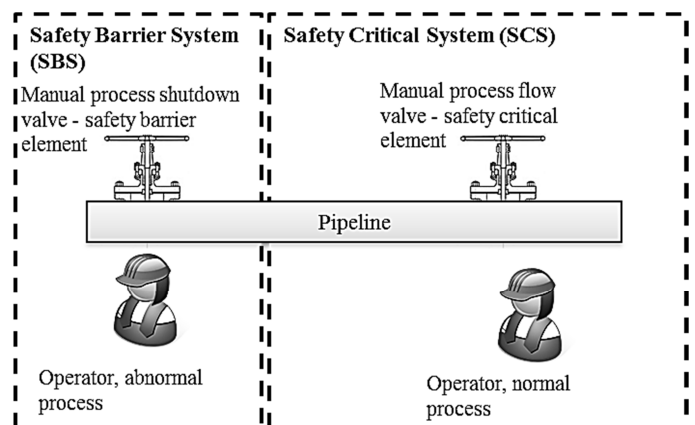


Figure 6. SCS and SBS comparison – generic example

3 SAFETY-RELATED ORGANIZATIONAL MEASURES

Safety-related organizational measures embrace the application of principles that ensure inherent Health, Safety and Environment (HSE) qualities related to the design and technical basis of the facility. The examples of such principles could be the principle of an Inherently Safer Design (ISD) (Mannan 2014), that involves the concept of reducing (avoiding, eliminating) rather than preventing or controlling hazards. The ISD principles should be applied during the general design and layout of the facility. Best Available Techniques (BAT) is another principle, which states that technology and the way it is used in the installations should be “most effective in achieving a high general level of protection of the environment as a whole” (EU Directive 1996); it is similar to the As Low as Reasonably Practicable (ALARP) principle that adapts a best common practice for judgment of the balance of risk and benefit (HSE 2014). Furthermore, Samarakoon and Gudmestad (2011) have extended the BAT principle to include Qualification: Best Available Qualified Technology (BAQT).

In general, safety-related organizational measures may be seen as a foundational basis for safety-related systems including the design, technology and operational activities.

4 TECHNICAL SOLUTIONS AND BARRIERS

4.1 Technical solutions

Technical solutions are applied to the main process and related auxiliary equipment as a derivation of the safety-related principles mentioned in the third section above. The purpose of these solutions is to prevent a critical deviation from occurring and to sustain the normal designed conditions. For example, the thickness of a particular pipeline could be 10 mm if process-needs alone (i.e. pressure or flow rate) are taken into the account, but for safety reasons (i.e. estimated corrosion allowance, etc.) the pipeline is designed with 15 mm walls. Another example could be the selection of process control equipment, preferring modern technology to an obsolete version. The idea of technical safety-related solutions is to decrease the risk within the associated equipment and so it differs from the general design of the facility, which is focused on the process needs. Once applied, technical solutions cannot be removed from the installation without interrupting the functions of the facility for which the solutions were designed.

4.2 Technical barriers

A technical barrier is a physical element that is established to perform safety functions related to stopping the unwanted chain of events once it has started: detection, control, mitigation or emergency response. It is designed to perform once prevention fails and abnormal conditions occur and to stop the development of a chain of unwanted events, or to limit the harm of these unwanted events. Examples of technical barriers are: a firewall that is designed to perform if fire breaks out; an Emergency Shutdown (ESD) system that is activated if process control is lost; the fire detection and deluge systems installed to fight the fire. Technical barriers do not perform constantly and may be removed from the installation without interrupting the main process functions for which the facility was designed.

4.3 Maintenance system

To ensure the required functionality of critical equipment and technical barriers, maintenance and follow-up activities should be performed by establishing a maintenance system (PSA 2014c). For example, the automatic safety system is one of the main technical barriers; therefore function testing and demand monitoring should be established (IEC:61511-1 2004). Technical barriers should be analyzed, the criticality and failure/fault modes of their elements determined and appropriate maintenance activities undertaken. All critical equipment and technical barrier elements should be tagged and marked accordingly in the general maintenance system of the facilities. In addition, the maintenance system should incorporate an analysis of the human factors and the performance-shaping factors of the operational maintenance activities. Industry examples show that a maintenance system may be enabled through the creation of performance standards – the functional requirement list of each barrier system (Firing *et al.* 2011). The performance standards may serve as a link between technical safety and maintenance disciplines (Fig. 7).

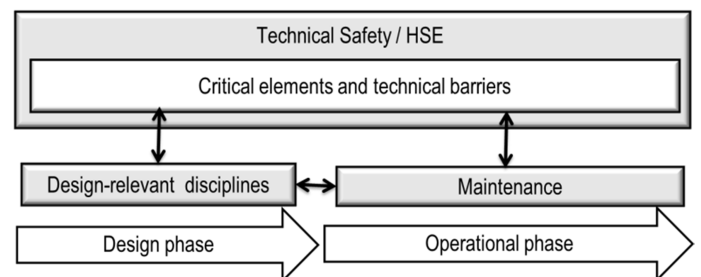


Figure 7. Links between design-relevant disciplines and maintenance

The importance of a well-performing maintenance system is recognized, but industry examples show that implementation often struggles in practice. For example, the accident report on the *Deepwater*

Horizon case concludes that “maintenance was inadequate”, work orders issued by the maintenance system were “disorganized, erroneous, or irrelevant to individual rig crews” and the “maintenance system was not understood by the crew” (Chief Counsels Report 2011). The challenges facing the maintenance management are indicated in the report on trends in risk level in the petroleum activity (RNNP) process prepared by the Petroleum Safety Authority (PSA) Norway (PSA 2012), which describes the existing difficulties fulfilling regulatory requirements for maintenance management: “tagging and classification of equipment, backlogs of preventive maintenance and outstanding corrective maintenance, including HSE-critical maintenance”.

The authors of this paper believe that one of the main reasons for such a situation is the missing links between the maintenance discipline and other disciplines, especially technical safety. The various analyses done by safety and maintenance engineers often do not have clear linkage and can hardly be implemented in the practical sense. Moreover, a general inconsistency in Computerized Maintenance Management Systems (CMMS) may often be observed due to the overlapping data of maintenance criticality analysis and technical safety analysis.

5 OPERATIONAL SOLUTIONS AND BARRIERS

5.1 *Operational solutions*

Similarly to technical solutions, operational solutions are derived from safety-related organizational principles and are applied to the main operational activities. For example, an operator could do his job in a very cost-efficient way, but, after a risk analysis is performed, a safety-related operational solution – the way the technology is used – will be applied to the job in order to reduce the risk. A safety checklist before an activity may also be seen as an operational solution, as it is an additional activity with a focus on preventing any abnormalities during the operation. The safety checklist may be seen as a part of safety-critical activities, but it is not a barrier by itself.

5.2 *Operational barriers*

An operational barrier can be seen as a determined specific action that shall be carried out in the case of critical deviation to prevent or to stop the development of an unwanted chain of events. A manual shutdown valve is often treated as a technical barrier element; however, it will not perform the barrier function unless somebody activates it on demand. This action is an operational barrier element.

Operational barriers are the part of the Safety Barrier System (SBS) that involves specific human actions related to the barrier function: detection, control, mitigation or emergency shutdown. Examples of operational barriers could be a manual activation of emergency shutdown systems, firefighting and evacuation. A specific lookout or visual check of an operator that is performed only for safety reasons may be seen as an operational detecting barrier.

5.3 *Performance-Shaping Factors (PSF)*

The UK Health and Safety Executive defines human factors as “environmental, organizational and job factors, and human and individual characteristics which influence behavior at work in a way which can affect health and safety” (HSG48 2009). Explicitly defined, human factors may be seen as Performance-Shaping Factors (PSF) and are used to model human behavior as the underlying causes of abnormal performance (El-Ladan and Turan 2012). It must be noted that PSF are explicitly used to describe the influence on human performance (Musharraf *et al.* 2013) and should not be directly referred to as the performance of technical equipment. Technical equipment is affected by maintenance actions which are again influenced by PSF (Toriizuka 2001). However, the PSF of maintenance activities should be seen as an integral part of the maintenance system, and maintenance activities should be distinguished from the operational safety barrier concept that embraces specified safety actions in the case of abnormal situations.

PSF may be characterized as internal and external (Boring *et al.* 2007). Internal PSF influence individual attributes such as mood, fitness, stress level, etc. External PSF exert influence in the situation or environment that affects the individual, such as temperature, noise, work practices, etc. The performance of operational activities is directly affected by PSF, so they must be taken into consideration when SCS or SBS are designed.

6 MANAGEMENT SYSTEM

6.1 *Workflow*

The general steps for establishing the management system for risk-reducing measures is shown in Figure 8. It may be seen as an interpretation of ISO31000 (2009) and the PSA regulations, Section 17 of the Management Regulations (PSA 2014a).

The context is seen directly or indirectly as acting factors that may be important in the risk-reduction process. It includes not only requirements, standards, guidelines, acting regulations and policies, but also general experience, expert knowledge, engineering judgment, etc. The risk analysis is intended to iden-

tify, analyze and evaluate the hazards in the activities performed. By understanding the nature of the hazard, the possible scenarios can be laid out and the corresponding safety measures can be discussed accordingly. The required safety-related solutions and barrier functions should be derived as a result of this process. Further steps are the actual identification of system functions and corresponding systems up to the equipment tag level to include them into the maintenance system. Finally, visualization and monitoring tool should be created specifically for SCS & SBS.

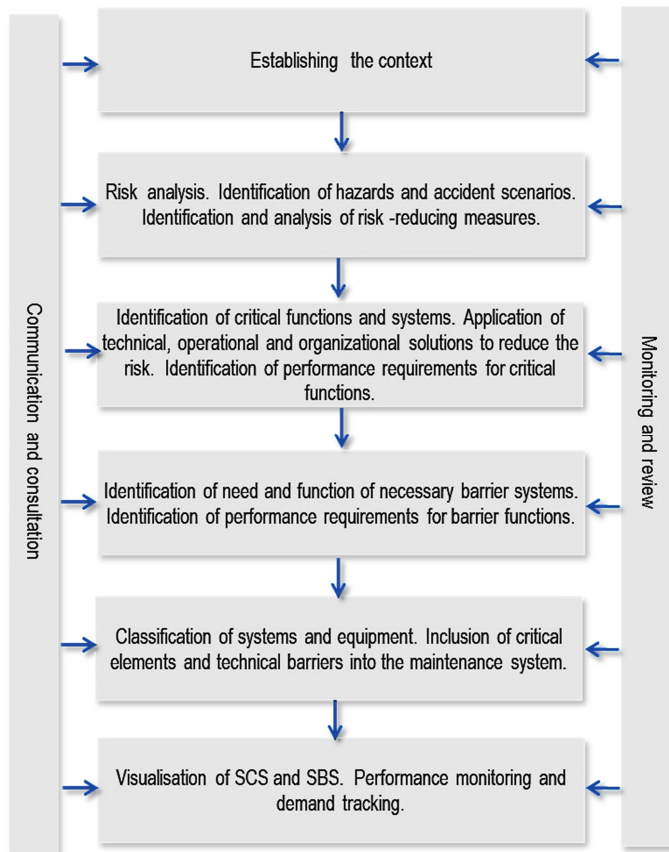


Figure 8. Managing the risk-reducing measures

6.2 Challenges facing maintenance management

The audit activities often find deficiencies in the completion of maintenance activities and missing links between equipment and the safety barriers (Ratnayake *et al.* 2012). It is essential to know the links and interconnections between maintenance and technical safety disciplines. The safety analyses and identification of safety functions should be transferred to the maintenance engineers in order to classify specific equipment accordingly. Results of safety-related analyses performed by technical safety engineers should be prioritized over results of maintenance criticality analyses. Clear links should be established in order to ensure that one discipline's output can be used as input for other disciplines. The mandatory Performance Standards (PS) required by the PSA may be seen as a potential major link between safety and maintenance disciplines (Fig. 9).

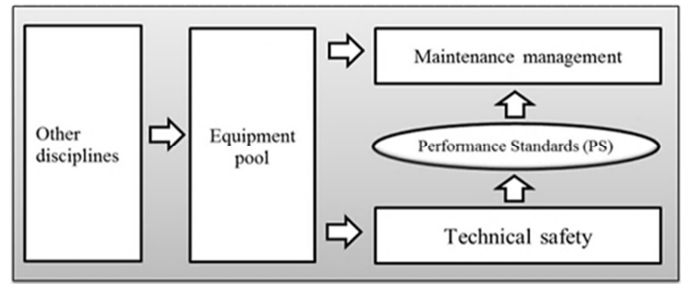


Figure 9. PS as a link between technical safety and maintenance

For example, the equipment tags of the Safety Instrumented Systems (SIS) should be specified in the Safety Requirement Specification (SRS), a live document made specifically for every installation (GL-070 2004 & IEC:61508 2010). The PS should contain links to such relevant documentation. In addition to specific requirements for safety critical and barrier functions, the PS should have a clear description of equipment groups that are considered as part of the SCS/SBS. A properly created PS will allow the correct identification of critical equipment tags and the implementation of data into the CMMS.

6.3 Visualization of system

The integrity status of SCS/SBS should be visualized. From the point of view of ergonomics and human factors, it is important that only the required data and information should be provided; it should not overflow, but be sufficient, unambiguous and non-misleading (Wong and Ceng 2002). Industry examples show how the visualization of safety systems is being implemented (Johansen and Toennessen 2002 & Firing *et al.* 2011). The purpose of this paper is not to evaluate the current achievement but to provide additional insights to the discussions and further development of these systems.

The visualization system should not only show the integrity status of technical parts of the SCE/SBS, but contain the names and duties of responsible personnel in the case of abnormal process conditions. Specific human activities are seen as operational barriers and as an integral part of the safety system. Automatic systems such as Safety Instrumented Systems (SIS) are an exception and may be seen as an SBS without an operational barrier element. The proposed concept of the visualization system is based on the generic accident model shown in Figure 1 and separates SCS and SBS (Fig.10).

A status color code can be used as an indication of the general status. There may be various selections, for example, three levels of status: green, yellow, and red. The green would indicate that SCS/SBS integrity meets performance requirements, the yellow would demand attention and possible actions to be taken, while a red status would mean that the SCS/SBS is not performing and the risk is

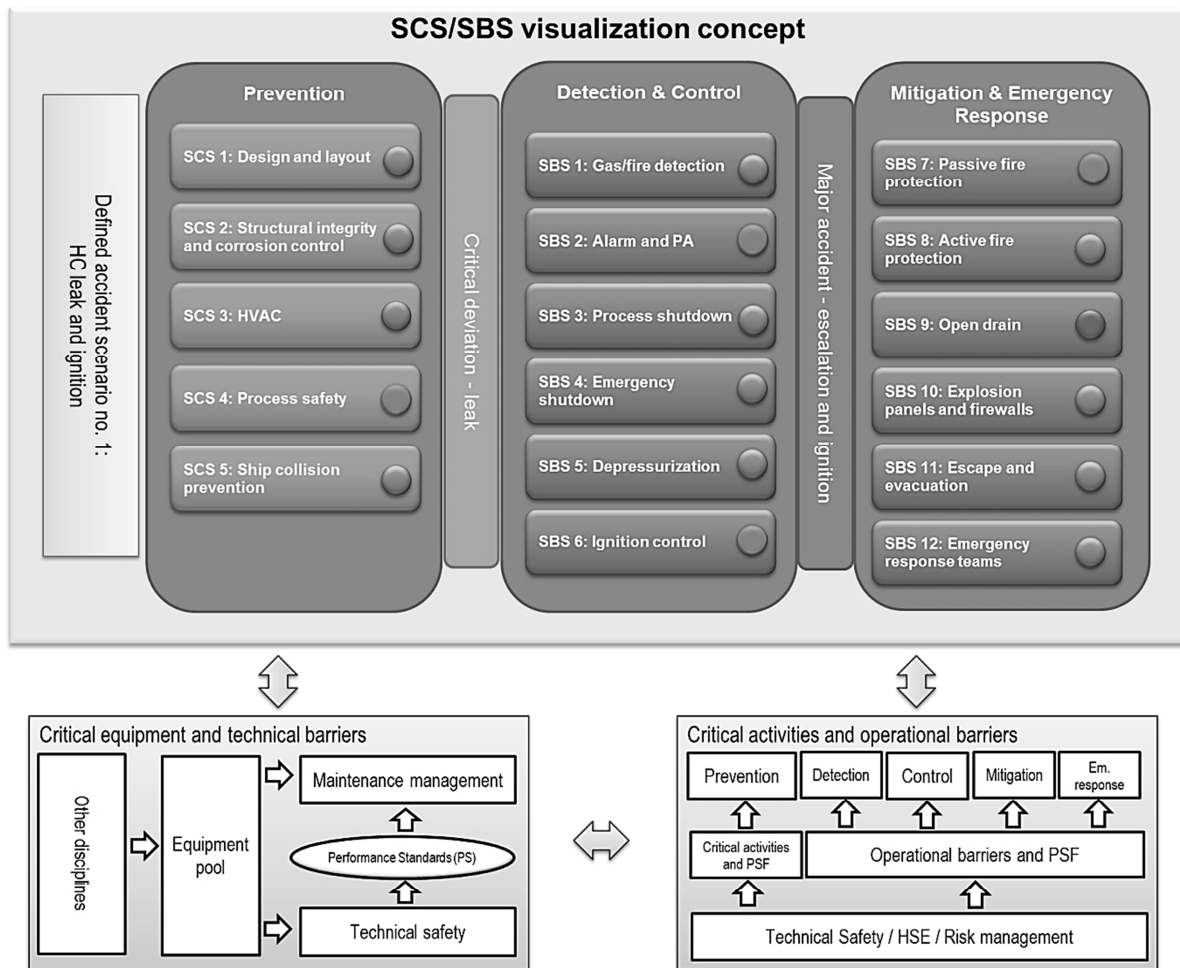


Figure 10. Generic example of visualization of SCS/SBS

increased. The integrity status may be derived from the results of a system function test, preventive/corrective maintenance reports, etc.

By visualizing the status of the safety-related systems, an overview of the integrity status can be made available for operators and managers. This information is essential when evaluating work permits, the bypass of safety systems for maintenance, and increased levels of activities. Easy and user-friendly access to the information would facilitate good practices of safety management (Johansen and Toennesen 2002).

7 SUMMARY

Based on the synthesis of ISO 17776, the PSA regulations and common features of the terms found in the scientific literature, the concepts of Safety-Critical Systems (SCS) and Safety Barrier Systems (SBS) are proposed as a basis for further discussion of risk-reducing measures in industrial activities.

Correspondingly, prevention, detection/control, and mitigation/emergency response systems have been introduced and described. Aligning with the PSA regulations, safety-related solutions and corresponding critical systems have been separated from

safety barriers and described. Links between technical, operational and organizational elements have been suggested, incorporating maintenance activities and performance-shaping factors. The presented accident chain model (Fig. 1) may be used as a tool for a broader communication about the safety barriers and their role in arresting the accident's escalation. This may be valuable in risk communication, where the model's simplicity could be well-accepted by non-technical safety personnel.

Furthermore, some important issues regarding the management of safety systems have been discussed with a focus on maintenance and its links with other disciplines. Generic examples of conceptual workflow and system visualization have been proposed and described.

Today the industry has a challenge to link technical and operational elements into a united system. A conceptual framework of systems consisting of technical and operational elements has been discussed in the manuscript.

Further studies are required to enable a synergy of separate work processes that would ensure adequate maintenance and follow-up of risk-reducing measures during their lifecycle.

REFERENCES

- Boring, R.L., Griffith, C.D. & Joe, J.C. 2007. The Measure of Human Error: Direct and Indirect Performance Shaping Factors (ed.). In *Human Factors and Power Plants and HPRCT 13th Annual Meeting*. IEEE, 170-176.
- Dhar, R. 2011. Performance Standards For Safety Critical Elements – Are We Doing Enough! In *SPE European Health Safety and Environmental Conference in Oil and Gas Exploration and Production*. Society of Petroleum Engineers.
- Chief Counsels Report: Chapter 4.10: Maintenance. 2011. http://cybercemetery.unt.edu/archive/oilspill/20121210200431/http://www.oilspillcommission.gov/final-report_p.221-224. [Accessed 2014]
- El-Ladan, S.B. & Turan, O. 2012. Human reliability analysis—Taxonomy and praxes of human entropy boundary conditions for marine and offshore applications. In *Reliability Engineering & System Safety*, 98, 43-54.
- EU Council Directive 96/61/EC of 24 September 1996 concerning integrated pollution prevention and control. 1996. <http://eur-ex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31996L0061:en:HTML>. [Accessed 2014].
- Firing, F.L., Ostby, E., Ingvarson, J. & Strom, O. 2011. TTS-The Systematic and Efficient Approach to Define Maintain and Demonstrate Safety Performance on Complex Hydrocarbon Processing Facilities (ed.). In *Offshore Technology Conference*.
- GL-070. 2004. "Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry", rev. 2. The Norwegian Oil Industry Association.
- HSE. 2014. UK Health and Safety Executive. <http://www.hse.gov.uk/risk>. [Accessed 2014].
- HSG48. 2009. "Reducing error and influencing behaviour". UK Health and Safety Executive.
- IAEA. 1999. "Basic safety principles for nuclear power plants: 75-INSAG-3", rev. 1. Vienna: The International Atomic Energy Agency.
- IEC:61508. 2010. "Part 1–7 Functional safety of electrical/electronic/programmable electronic safety-related systems". Geneva: International Electrotechnical Commission.
- IEC:61511-1. 2004. "Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements". Geneva: International Electrotechnical Commission.
- ISO:13702. 1999. "Petroleum and natural gas industries — Control and mitigation of fires and explosions on offshore production installations". Geneva: International Organization for Standardization.
- ISO:17776. 2000. "Petroleum and natural gas industries. Offshore production installations. Guidance on tools and techniques for hazard identification and risk assessment". Geneva: International Organization for Standardization.
- ISO:31000. 2009. "Risk management. Principles and guidelines on implementation". Geneva: International Organization for Standardization.
- Johansen, J.A. & Toennesen, N. 2002. Maintenance Management of Essential Safety Systems (ed.). In *SPE International Conference on Health Safety and Environment in Oil and Gas Exploration and Production*. Society of Petroleum Engineers.
- Mannan, S. 2014. Chapter 21 - Inherently Safer Design. In S. Mannan (ed.), *Lees' Process Safety Essentials*. Oxford: Butterworth-Heinemann, 403-407.
- Musharraf, M., Hassan, J., Khan, F., Veitch, B., Mackinnon, S. & Imtiaz, S. 2013. Human reliability assessment during offshore emergency conditions. *Safety Science*, 59, 19-27.
- PSA. 2012. "The trends in risk level in the petroleum activity (RNNP)". Norway, Stavanger: Petroleum Safety Authority.
- PSA. 2014a. "Regulations relating to management in the petroleum activities (The Management Regulations)". Norway, Stavanger: Petroleum Safety Authority.
- PSA. 2014b. "Guidelines to regulations relating to management in the petroleum activities (The Management Regulations)". Norway, Stavanger: Petroleum Safety Authority.
- PSA. 2014c. "Regulations relating to conducting petroleum activities (The Activities Regulations)". Norway, Stavanger: Petroleum Safety Authority.
- Ratnayake, R.M.C., Singh, S.P. & Raza, J. 2012. Development of a Barrier Management System for Continuous Monitoring and Maintenance of Safety Barriers (ed). In *Proceedings of the IEEE International Conference on Industrial Engineering and Engineering Management*. IEEE.
- Samarakoon, S.M.S.M.K & Gudmestad, O.T. 2011. Qualification of offshore facilities prior to application in a new field. *Journal of Cleaner Production*, 19, 13-20.
- Sevcik, A. & Gudmestad, O.T. 2014. Systematic Approach to Risk Reduction Measures in the Norwegian Offshore Oil and Gas Industry. Accepted for publication in *9th International Conference on Risk Analysis and Hazard Mitigation, Wessex Institute, 4 - 6 June*. New Forest, UK.
- Toriizuka, T. 2001. Application of performance shaping factor (PSF) for work improvement in industrial plant maintenance tasks. *International Journal of Industrial Ergonomics*, 28, 225-236.
- Wong, W. & Ceng, F. 2002. *How did that happen?: engineering safety and reliability*. Professional Engineering.

Appendix A. Main analysis table for case study

This part is intended to define relevant equipment group and its function group for every functionality evaluated as safety critical by DNV. The established worktable is used for this analysis, see below. All 27 PS for Skarv is covered, and every functional requirement is determined if it is related to technical or operational elements. If technical, then general equipment group as target of a functional requirement is defined. Finally, functionality is connected to risk reducing function group and differentiated between SCS and SBS.

In the end of the table an abbreviation list can be found.

Legend:

	Data from PS sheets
	Data from DNV pre-defined functionalities
	Relation to equipment group / risk reducing function group

PS	Function	PS No.	Functionality	Related Assurance Activities	Work Scope	Equipment group	Risk-reducing function group (technical only)	Role
PS1 Layout and Arrangement	The layout and arrangement shall reduce probability and the consequences of accidents through location, separation and orientation of areas, equipment and functions.	1	The condition of the blast walls (and decks) and explosion relief (panels) shall show no significant sign of damage or deterioration. Significant is defined as preventing performance of the design intent.	Ensure that visual inspection have been completed	Inspection	Structural: fire walls, blast panels	MITIGATE - Passive fire protection	SBS M2

		2	Equipment storage shall have no negative effects on technical barriers on explosion risk and explosion relief (panels). This includes consideration of: - explosion vent path - natural ventilation - F&G detectors - firewater system (nozzles)	Ensure that visual inspections have been completed. Checklist - Storage of equipment - part of PS 1	Operational	Checklist or service routine may be established. This is a part of assurance of fire/blast walls functionality.	-	-
PS	Function	PS No.	Functionality	Related Assurance Activities	Work Scope	Equipment group	Risk-reducing function group (technical only)	Role
PS2 Structural Integrity	To provide structural support for all operational loading situations and provide stability under defined accidental load conditions in order to prevent catastrophic structural failure. The goal is further to ensure the integrity of the supporting structures of the installation, and integrity support for the risers, J-tubes, conductor and caissons.	1	The hull structure shall have no significant signs of degradation, damage or deformation that could affect the structural integrity.	Inspection according to Long Term Inspection Programmed/SIMS.	Inspection	Structural	PREVENT - Loadbearing structures / structural integrity	SCS P1
		2	The coating shall provide the structure with protection from corrosion.	Inspection	Inspection	Structural	PREVENT - Loadbearing structures / structural integrity	SCS P1
		3	The cathode protection system shall provide adequate protection against corrosion and growth of the structure below water level.	Cathode protection readings and extent of depletion of anodes shall be monitored in accordance with the Long Term Inspection Program.	Inspection	Structural	PREVENT - Loadbearing structures / structural integrity	SCS P1
		4	The seabed area around the installation shall be inspected at intervals for erosion, fallen debris and build-up of drill cuttings. Signs of leakage of fluids or gas to be checked.	ROV inspection in accordance with the Long Term Inspection Program.	Inspection	Structural	PREVENT - Loadbearing structures / structural integrity	SCS P1

		5	An up-to-date model of the load bearing structure including topside shall be available for necessary structural integrity assessments.	Review of inspection data Continuous assessment of the model. Annual summary reports give status of the model.	Operational	-	-	-
		6	Additional inspections shall be carried out on special occasions (e.g. after accident/environmental event)	Structural Incident Procedure	Operational	-	-	-
		7	Topsides structural elements shall have no significant signs of degradation, damage or deformation that could affect the integrity of the topsides structure.	Inspection in accordance with the Long Term Inspection Program. Annual inspection summary report.	Inspection	Structural	PREVENT - Loadbearing structures / structural integrity	SCS P1
		8	The weight database shall be updated and reflect all permanent changes. Permanent loading shall be managed through the weight control procedure and verified by structural analysis. A system of calculating and recording the net permanent topside weight and centre of gravity shall be maintained.	Monthly reports on as-built documentation from AFA. Contractor audits every 3 yrs. (ref. SIMS).	Operational	-	-	-
		9	Temporary loading on laydown areas shall be controlled using deck loading charts. Exceptional temporary loads shall be subject to specific review. Maximum loads per lay down areas, as indicated locally, shall be strictly adhered to.	Updated and relevant load charts available offshore.	Operational	-	-	-
		10	The helideck and its support shall be free from signs of significant degradation, damage or deformation which could compromise their ability to support helicopter operations including emergency and heavy landing.	Inspection according to Long Term Inspection Program.	Inspection	Structural	PREVENT - Loadbearing structures / structural integrity	SCS P1

		11	The crane pedestals shall be free from signs of degradation, damage or deformation which could compromise their ability to support working loads in all design operating modes.	Inspection according to Long Term Inspection Program.	Inspection	Structural	PREVENT - Loadbearing structures / structural integrity	SCS P1
		12	The flare structure and its associated platforms and access ladders shall be free from signs of degradation, damage or deformation of primary and secondary members which could impair their ability to provide structural support to the flare and vent pipework.	Inspection according to Long Term Inspection Program.	Inspection	Structural	PREVENT - Loadbearing structures / structural integrity	SCS P1
		13	The module supports shall work as intended from the design.	Inspection in accordance with the Long Term Inspection Program.	Inspection	Structural	PREVENT - Loadbearing structures / structural integrity	SCS P1
		14	Upon visual inspection of topsides dropped and swinging object protection, there shall be no signs of degradation, damage or deformation that could affect their integrity.	Inspection according to Long Term Inspection Program.	Inspection	Structural	PREVENT - Loadbearing structures / structural integrity	SCS P1
		15	Structural bolts shall be in a sound condition and tight within the specified torque tolerances.	Inspection according to Long Term Inspection Program. (Torque tests)	Inspection	Structural	PREVENT - Loadbearing structures / structural integrity	SCS P1
PS	Function	PS No.	Functionality	Related Assurance Activities	Work Scope	Equipment group	Risk-reducing function group (technical only)	Role

PS3a Gas Detection	The goal is to continuously monitor designated areas of the installation and upon detection of a gas to annunciate alarms and provide output signals to field devices which initiate a rapid and appropriate response in accordance with the fire and gas cause & effect charts.	1, 7	<p>Reliable and fast gas detection shall be provided</p> <p>Point detectors: <ul style="list-style-type: none"> •Failure definition: F&G logic does not receive correct alarm level signal from gas detector upon test •Failure frequency target for one detector: max 1% </p> <p>Open path/Line detectors: <ul style="list-style-type: none"> •Failure definition: F&G logic does not receive correct alarm level signal from gas detector when tested with prescribed test filter (or gas cell). •Failure frequency target for one detector: max 1% </p> <p>The testing shall be verified on the HMI , hence, including F&G node as part of the loop test.</p>	<p>Functional test of gas detectors, low and high gas alarm limits - yearly on line detectors - every 4th on IR point - H2 and H2S 6 monthly</p> <p>Scope of function are gas detectors</p>	PM	Gas detectors	DETECT - gas detection	SBS D1
		2	All gas detectors shall be in good working order and clear from obstructions.	Annual maintenance and inspection (ensuring e.g. free sight in detection pathway, physical protection if installed and if required recalibration)	PM	Gas detectors	DETECT - gas detection	SBS D1
		3	Gas detection system shall provide reliable signal interface between field devices and the CCR.	Functional test of gas detectors. (detection range including low and alarms through CCR HMI such as Operator Stations and Safety Matrix)	PM	Gas detectors	DETECT - gas detection	SBS D1
		4	Gas detection system shall activate all actions (gas detector functions) according to C&E charts	Functional test of C&E fire area logic (direct actions, and provision by the Gas detection system of initiation signals to other safety system such as ESD and PAGA)	PM	F&G logic	DETECT - F&G logic	SBS D3

		5	Gas detection system shall upon general platform gas alarms, provide reliable alarm annunciation to strategic locations, additional to CCR, such as crane cabins and drilling locations.	Functional test of gas detectors (all gas alarms also provided through locally installed F&G panels)	PM	Detection alarm	DETECT - alarm	SBS D4
		6	The logic solver shall permit adequate testing through e.g. inhibit/override functionality, of gas detection functions.	Check with CCR that SORA is established for all fire areas (common with fire detection)	Operational	-	-	-
		7	Safety critical equipment shall be tested and maintained to meet specified requirements for probability of failure on demand;	Summarize half yearly RNNP reports	Operational	-	-	-
		8	The duration and compensating measures shall be defined for situations where safety functions are inaccessible (planned or unplanned)	Check the block log that the duration of the last ten inhibits overrides does not exceed the maximum accepted time, as stated in SORA Task is part of operating procedure Completed SORA forms for all areas will be existing in CCR	Operational	-	-	-
PS3b Fire Detection	The goal is to continuously monitor designated areas of the installation and upon detection of a gas to annunciate alarms and provide output signals to field devices which initiate a rapid and appropriate response in accordance with the fire and gas cause & effect charts.	1	Reliable and fast fire detection shall be provided Fire detectors(Heat, Flam & Smoke): •Failure definition: F&G logic does not receive signal from fire detector upon test •Failure frequency target for one detector: max 1%	Functional test of fire detectors and MAC's Scope Flame, Manuel call point, Smoke and heat detectors	PM	Fire detectors	DETECT - fire detection	SBS D2
		2	All fire detectors (including MAC) shall be in good working order and clear from obstructions.	Maintenance and inspection routines (physical checks such as lens cleaning, ensuring free sight/pathway (flame detectors), physical protection if required/installed) - MAC (every 24 month) - Smoke - Flame	PM	Fire detectors	DETECT - fire detection	SBS D2

		3	Fire detection system shall provide reliable signal interface between field devices and the CCR.	Check for corrective work orders regarding loss of status/control of the fire detection system caused by unavailability of operator stations and/or check event log (system alarms) for similar situations Function is covered by PM point 1	PM	Fire detectors	DETECT - fire detection	SBS D2
		4	Fire detection system shall activate all actions according to C&E charts	Functional test of C&E fire area logic (direct actions, and provision by the Fire detection system of initiation signals to other safety system such as ESD and PAGA) No found PM in Workmate	PM	F&G logic	DETECT - F&G logic	SBS D3
		5,8	Fire detection system shall upon general platform fire alarms, provide reliable alarm annunciation to strategic locations additional to CCR, such as crane cabins and drilling locations upon fire detection Manual Call Point: •Failure definition: F&G logic does not receive signal from MCP upon test. •Failure frequency target for one push button: max 1%	Functional test of fire detectors and MAC's. (all fire alarms also are provided through locally installed F&G panels) Function is covered by PM point 1	PM	Manual Call Points	DETECT - alarm	SBS D4
		6	The logic solver shall permit adequate testing, through e.g. inhibit /override functionality, of fire detection functions for fire and gas detectors.	Check with CCR that SORA is established for all fire areas (common with gas detection) Completed SORA forms for all areas will be existing in CCR	Operational	-	-	-
		7	Safety critical equipment shall be tested and maintained to meet specified requirements for probability of failure on demand;	Summarize half yearly RNNP reports Summarize half yearly RNNP reports to PTIL	Operational	-	-	-

		8	The duration and compensating measures shall be defined for situations where safety functions are inaccessible (planned or unplanned)	Check the block log that last ten inhibits overrides does not exceed the accepted time, as stated in SAFETY DOCUMENTATION Task is part of operating procedure Completed SAFETY DOCUMENTATION forms for all areas will be existing in CCR	Operational	-	-	-
PS	Function	PS No.	Functionality	Related Assurance Activities	Work Scope	Equipment group	Risk-reducing function group (technical only)	Role
4a & 4b Emergency Shutdown	The purpose of Emergency Shutdown is to limit the extent and duration of a major accident hazard, after the event has occurred, by initiating and controlling the following actions: <ul style="list-style-type: none"> · Stop flow of hydrocarbons onto facilities · Shutdown process equipment · Trip all relevant parts of the main electrical supply and isolate electrical equipment 	1,2,3 for RESDVs	RESDVs shall be available at all times. RESDVs shall have defined criteria for leakage rates based on safety criticality The maximum allowable leakage rate for the SSIV shall be 0.1 kg/s The RESDVs shall fully close on demand and the closing time shall be maximum 2 sec/inch if safety critical closing time has not been defined	Maintenance routines and testing -yearly function test - Availability and trending from data log	PM	ESD Riser valves	CONTROL - emergency shutdown	SBS C4
		1,2,3 for SSIV	SSIVs shall be available at all times. SSIVs shall have defined criteria for leakage rates based on safety criticality The maximum allowable leakage rate for the SSIV shall be 0.1 kg/s The SSIVs shall fully close on demand and the closing time shall be maximum 2 sec/inch if safety critical closing time has not been defined For SSIV the closure time is set to 120 sec	Maintenance routines and testing - Acoustic measurements	PM	SSIV valves	CONTROL - emergency shutdown	SBS C4

		4	RESRVs and SSIVs shall be continuously available in CCR and the system shall raise alarms in CCR for operator awareness or actions	Check trend on position transmitter (Data log (availability)) Check event log for valve associated tags	Operational	-	-	-
		1	Valves in equalizing lines across ESD valves shall be secured closed during normal production	1) Review locked open/locked closed register 2) Spot check if inspection activities have been conducted on relevant valves (workmate). LO/LC register and PM are not found in WM	Operational	LO/LC valve register control	-	-
		2	Manual valves in safety control circuits (e.g. hydraulic return and accumulator supply, means for valve travel time adjustment) shall be secured in correct position	1)Review that there is a locked open/locked close register in place 2)Review that there is an active log in place for changes in valve position	Operational	LO/LC valve register control	-	-
		3	ESRVs and Well isolation valves shall be available at all times.	Maintenance routines and functional testing (e.g. acoustic measurement).	PM	ESD Topside valves	CONTROL - emergency shutdown	SBS C4
		4	ESD valves shall be in line with defined criteria for maximum internal leakage rates based on safety criticality	Maintenance routines and testing - Acoustic measurement	PM	ESD Topside valves	CONTROL - emergency shutdown	SBS C4
		5	The ESD valves shall fully close on demand and closing time shall be maximum 2 sec/inch if safety critical closing time has not been defined	Maintenance routines and data log associated with closures	PM	ESD Topside valves	CONTROL - emergency shutdown	SBS C4
		6	Activation of a main ESD level shall initiate automatic alarm (GPA) to warn personnel	Maintenance and testing routines (under planned shutdown)	PM	ESD logic	CONTROL - emergency shutdown	SBS C4
		7	ESD system shall be continuously available in CCR and the system shall raise alarms in CCR for operator awareness or actions	Check for corrective work orders regarding loss of status/control of the ESD system caused by unavailability of operator stations	Operational	-	-	-
		8	In the event of a failure of the offloading hose during offloading, the offloading pumps shall cause automatic shutdown and isolation within 60 sec from	Maintenance routines and testing - Test log	PM	ESD offloading valve	CONTROL - emergency shutdown	SBS C4

			detection of an event					
		9	The logic solver shall function in accordance with the cause and effect charts	Function test of red and yellow shutdown levels. PMRs: ESD Logic Proof Test ESD Logic Test Note	PM	ESD logic	CONTROL - emergency shutdown	SBS C4
		10	The reliability of manually initiated safety functions shall be ensured through periodic function testing	Initiator function test for manual pushbuttons during planned shutdowns (input only test) Note: not found	PM	ESD - input (manual buttons)	CONTROL - emergency shutdown	SBS C4
		11	Maximum response time of the ESD function loop from detection to valve closure for all topsides ESD valves shall not exceed 60 seconds, if not otherwise specified.	Check incident/trend report for the maximum response time of the ESD function for any ESD against response times in SRS	Operational	Provides performance input to ESD system testing	-	-
		12	SIS Logic Solver Overrides – any inhibits or overrides shall be logged.	Check that the last ten inhibits overrides recorded in the log book does not exceed the maximum duration as defined in SAFETY DOCUMENTATION.	Operational	-	-	-
		13	Safety critical equipment shall be tested and maintained to meet specified requirements for probability of failure on demand.	Summarize half yearly RNNP reports (report from the workmate off equipment historical log)	Operational	-	-	-
PS	Function	PS No.	Functionality	Related Assurance Activities	Work Scope	Equipment group	Risk-reducing function group (technical only)	Role

PS5 Ignition Source Control	To minimize the probability of ignition of flammable liquids and gases following a loss of containment	1	All certified EX-electrical equipment shall be in good working condition, free from major degradation that would impair its certification and validity for use in that classified area.	Verify that regular PM routines followed and no major issues identified	PM	ATEX strategy for EX rated equipment. It has a broad scope of equipment range. EX capability should be treated not as separate safety function but as safety critical part of equipment integrity	PREVENT - Ignition prevention	SCS P2
		2	The spark arrestors shall be in good condition, free from major degradation that would impair it's functionality of containing sparks and preventing flame formation	Mechanical PM program Included in programs for generators, essential generator, emergency generator and fire water pumps.	PM	Spark arrestors	PREVENT - Ignition prevention	SCS P2
		3	The flame arrestors shall be in good condition, free from major degradation that would impair it's functionality of containing sparks and preventing flame formation	Mechanical PM program Included in programs for generators, essential generator, emergency generator and fire water pumps.	PM	Flame arrestors	PREVENT - Ignition prevention	SCS P2
		4	The temperature of hot surfaces such as exhaust pipes and ducts shall not exceed auto-ignition temperatures (AIT) as relevant to the exposure of flammable mediums that can be present upon accidental leaks.	Verify completion of maintenance procedure for temperature inspection and mechanical insulation inspection	Inspection	Insulation inspection	PREVENT - Ignition prevention	SCS P2
		5	Temporary equipment shall fulfil requirements in accordance with the hazardous area where it is located and shall not be a potential ignition source.	Spot check Temporary equipment register and that requirements are followed	Operational	-	-	-
		6	All earthing and bonding shall be tightly secure and free from major degradation that would impair its functionality during earth fault and static discharge	Check completion of PM routine	PM	Earthing / Bonding	PREVENT - Ignition prevention	SCS P2
		7	Hot work activities shall be controlled through the permit to work system in compliance with PSA and BPN regulations and	Check that hot work log, class A, are properly completed (spreadsheet from offshore)	Operational	-	-	-

PS	Function	PS No.	Functionality	Related Assurance Activities	Work Scope	Equipment group	Risk-reducing function group (technical only)	Role
			guidance.					
PS6 HVAC	To maintain a positive pressurization to prevent hydrocarbons from entering enclosed non-hazardous areas as well as maintaining a habitable and breathable atmosphere within the Temporary Refuge (TR) during normal operating conditions and in the event of a major fire/explosion generating smoke or a gas release.	1	Rooms "safe by ventilation", shall have a positive minimum pressure of 50 pa relative to surrounding classified areas. In mechanical ventilated unclassified areas, alarm shall be given in CCR either upon low overpressures relative to surrounding classified areas, or upon low airflow corresponding to 25 Pa overpressure or time delayed indication of open door	Test of over pressure. Visual inspection (no obstructions for natural ventilation) Function test of alarm	PM	Overpressure system / sensor Ventilation monitoring systems	PREVENT - HVAC	SCS P3
		2	Mechanical ventilation in classified areas, In the event of an internal gas leak, ventilation shall be maintained, and if practical increased.	Function test (by simulating gas leak)	PM	HVAC supply & extract systems powered from Emergency Generator /UPS	PREVENT - HVAC	SCS P3
		3	Ventilation (supply air and extract air) shall continue upon internal fire in low risk areas	Function test (by simulating internal fire situation)	PM	HVAC supply & extract systems powered from Emergency Generator /UPS	PREVENT - HVAC	SCS P3
		4	Ventilation shall continue in case of gas detection within mechanical ventilated zone 2 areas.	Maintenance and test routines for gas detectors (simulate gas in zone 2 areas)	PM	HVAC supply & extract systems powered from Emergency Generator /UPS	PREVENT - HVAC	SCS P3
		5	Uncertified equipment in an area safe by ventilation shall be automatically isolated in the event of loss of overpressure and/or gas detection in the area	Function test (by simulating loss of ventilation). Check according to C&E	PM	Ignition source disconnection system (Circuit breakers (F&G)	CONTROL - ignition source disconnection	SBS C2
		6	Manual means of initiating closure of dampers and HVAC shutdown from the CCR shall be available.	Function test	PM	Fire dampers	MITIGATE - Passive fire protection	SBS M2
		8	All dampers must operate correctly, including solenoid valves and limit switches	Function test of alarm (the response in accordance with the cause and effect chart)	PM	Fire dampers	MITIGATE - Passive fire protection	SBS M2

		9	Total response time for closing of HVAC inlet dampers in rooms where all ignition sources are shut down upon gas detection in the inlet shall meet specified requirements. (total 3 sec, damper 1 sec)	Function test (by simulating gas leak)	PM	Fire dampers	MITIGATE - Passive fire protection	SBS M2
		10	Boost charging in battery rooms shall be stopped automatically on low or missing airflow.	Function test (simulate low or missing air flow)	PM	Ventilation monitoring systems	PREVENT - HVAC	SCS P3
		11	A loss of mechanical ventilation shall be alarmed locally and in the CCR	Function test of alarm (response is in accordance with the cause and effect chart)	PM	Ventilation monitoring systems	PREVENT - HVAC	SCS P3
		12	All inlet and outlet fans shall have shut off dampers that shall be closed when the fans are stopped.	Function test	PM	Fire dampers	MITIGATE - Passive fire protection	SBS M2
PS	Function	PS No.	Functionality	Related Assurance Activities	Work Scope	Equipment group	Risk-reducing function group (technical only)	Role
PS7 Control of Spills	Control of spills is fulfilled through the open hazardous and non-hazardous drain system. The purpose of the drains is to provide measures for containment and proper disposal of hazardous and non-hazardous liquids.	1	Blockage of drain boxes because of temporary equipment etc. shall be avoided.	Inspection routines, regular inspection	PM	Open drain boxes, drip trays	MITIGATE - Open drain	SBS M12
		2	Ensure that the drain systems are not clogged	Maintenance routines	PM	Open drain boxes, drip trays	MITIGATE - Open drain	SBS M12
		3	Ensure that drip trays do not contain spillage	Daily inspection, area inspection	PM	Open drain boxes, drip trays	MITIGATE - Open drain	SBS M12
		4	Ensure that liquid seals are functioning	Inspection to check liquid level and refill (monthly/bi-weekly)	PM	Open drain liquid seals	MITIGATE - Open drain	SBS M12
		5	Inspection of open drain piping shall be performed to prevent pipe rupture and gas leakage (including vacuum breakers)	Piping inspection program	Inspection	Open drain piping	MITIGATE - Open drain	SBS M12
		6	Inspection of open drain pipes inside drain collection tanks shall be performed to prevent pipe rupture and gas leakage	Mechanical/static equipment inspection Intervals need to be specified in PS and updated in WorkMate accordingly Criticality to be re-evaluated as some of the drain	Inspection	Open drain piping	MITIGATE - Open drain	SBS M12

				collection tanks are missing SCE code				
		7	Level transmitter (low and high) must be maintained	Maintenance routines (incl. level transmitters)	PM	Open drain level instruments	MITIGATE - Open drain	SBS M12
		8	The nitrogen purging facilities must be functional to prevent entrance of oxygen. Including to ensure that flow meter is working correctly and is available	Systematic errors in maintenance records	PM	Open drain nitrogen	MITIGATE - Open drain	SBS M12
		9	To inhibit escalation of fires and hydrocarbon liquid spillage, provision shall be made to inhibit flow of hydrocarbon liquid from one deluge fire area to another.	Deluge test	PM	Deluge	MITIGATE - Deluge	SBS M5
		10	It shall be ensured that functionality of the drain system is maintained during cold periods	Maintenance routines for heaters	PM	Heaters, drain system	MITIGATE - Open drain	SBS M12
PS	Function	PS No.	Functionality	Related Assurance Activities	Work Scope	Equipment group	Risk-reducing function group (technical only)	Role
PS8 Active Fire Protection	The purpose of the active firefighting systems is to provide reliable means for fighting fires and mitigate explosions.	1	Pressure peak reducing measures (vacuum breaker/active hydrophore tank/start up sequence of FW pumps and deluge release) shall be in place	Testing and inspection/ maintenance program	PM	Pressure peak reducing measures	MITIGATE - Deluge	SBS M5
		2	The firewater ring main shall be functioning on demand.	Inspection of ring main, including flanges and supports Corrosion monitoring	Inspection	FW piping	MITIGATE - FW supply	SBS M3
		3	All strainers and screens in firewater system shall be regularly inspected to avoid clogging.	Video inspection of caisson and screen Visual inspection of strainers	Inspection	FW strainers, screens	MITIGATE - FW supply	SBS M3

		4	A system to inhibit marine growth shall be intact.	<p>1. Maintenance routines for chemical injection skid.</p> <p>2. Regular check of hypochlorite concentration in fire water distribution system</p> <p>3. check the existence of batch injection procedures to prevent marine growth in pump inlets</p>	PM	FW chlorination	MITIGATE - FW supply	SBS M3
		5, 14	<p>The frost protection measures, i.e. min flow / insulation / heat tracing shall be fully functioning in cold periods.</p> <p>The freeze protection by heating elements (deluge valve station, monitors, hydrants etc.) shall be functioning without introducing too high water temperatures (corrosion).</p>	<p>Operational procedure to bleed off minimum flow according to requirements.</p> <p>Maintenance routine for heating elements.</p> <p>Test and inspection of heat tracing Inspection program for insulation Related PM</p>	PM	FW heaters and heat tracing	MITIGATE - FW supply	SBS M3
		6	Firewater distribution, pump system and ring main sectioning valves shall be car sealed open, clearly marked and functioning on demand.	<p>Inspection of sectioning valves (car seals, position)</p> <p>Function testing (open/close) of sectioning valves</p> <p>Leak test of sectioning valves</p>	PM	FW supply valves	MITIGATE - FW supply	SBS M3
		7	Safety critical Instruments shall be tested/calibrated regularly	Inspection and test routines as per safety critical instrument	PM	FW instrumentation	MITIGATE - FW input	SBS M6

		8,9, 31	<p>Rated capacity of each firewater pumps on the installation shall be within predefined limits. Firewater pumps need to be repaired upon 15% reduction in performance.</p> <p>Fire water pump</p> <p>Failure definition: Firewater pump does not start upon signal. Failure frequency target for one pump: max 1% Failure definition capacity: Firewater pump delivers less than 85% of the original capacity.</p> <p>The starting sequence logic for the start-up of the firewater pumps shall be in accordance with NFPA 20</p>	<p>1. Weekly test run of individual pumps to 100% of rated capacity. 2. Individual pump capacity test (yearly) - (Pump capacity measured by means of flow and outlet pressure from 0 – 150% of rated capacity shall be registered and compared to pump curve.</p> <p>Test of executive actions from logic (fire water pump controller) Test of Fire pump start logic (duty and stand-by) from ISC (instrumented safety control system)</p>	PM	FW pumps	MITIGATE - FW pumps	SBS M4
		10	The fuel supply valve shall be secured in open position.	Inspection of fuel supply valve (secured open)	PM	FW pumps	MITIGATE - FW pumps	SBS M4
		11	A manual isolation switch/valve between the starter motor and the start battery/air bank shall be car sealed.	Inspection of valve position and car sealing	PM	FW pumps	MITIGATE - FW pumps	SBS M4
		12	The FW Pump engine cooling water and/or oil preheat function for diesel drivers shall be functioning as intended.	Pump capacity test (yearly) - (Pump capacity measured by means of flow and outlet pressure from 0 – 150% of rated capacity shall be registered and compared to pump curve.)	PM	FW pumps	MITIGATE - FW pumps	SBS M4

		13,15, 31	<p>The deluge system shall provide adequate coverage with respect to both volume and area coverage, horizontal and vertical surfaces.</p> <p>Deluge valve Failure definition: Deluge valve does not open upon test to ensure that deluge nozzles will receive water at design pressure not later than 30 seconds after a confirmed fire signal has been given. Failure frequency target for one valve: max 1 % Deluge Nozzles: Failure definition: Clogged nozzles Failure frequency target per skid: max 3% clogged nozzles or 3 nozzles on one branch</p> <p>Deluge shall be automatically released upon confirmed gas detection where documented effective for explosion mitigation.</p>	<p>Video Inspection of deluge system (dry area) Function testing of deluge valves (open/close function) - every 3rd/6th month Inspection/testing of deluge system including foam injection system. Full scale testing (clogged nozzles, readings of flow and pressure upstream and downstream deluge valve and min. 1 deluge nozzle (most remote nozzle). The readings shall be verified against updated hydraulic calculations).</p> <p>Testing of executive actions from logic to deluge valves.</p>	PM	Deluge	MITIGATE - Deluge	SBS M5
		16, 31	<p>Foam supply shall be provided as intended.</p> <p>Foam system (not helideck): Failure definition: Foam not delivered into system upon test Failure frequency target for system: max 2 %</p>	Test of foam supply centralized pump system	PM	AFFF	MITIGATE - AFFF	SBS M7
		17	The foam (concentrate) quality shall be as intended.	Yearly foam (concentrate) quality check	PM	AFFF	MITIGATE - AFFF	SBS M7
		18	Block-valves in foam supply lines shall be secured open (e.g. car sealing).	Inspection of block valves in foam supply	PM	AFFF	MITIGATE - AFFF	SBS M7
		19	Foam systems shall have a total foam concentrate capacity sufficient for minimum 30 minutes supply to the largest fire area and the largest neighboring	Verification of injection rates for injectors in deluge skids to ensure correct injection rate	PM	AFFF	MITIGATE - AFFF	SBS M7

			area requiring foam.					
		20	When in operation the centralized foam system shall have an operation pressure of at least 2 bars above the firewater pressure to prevent reverse flow.	Inspection/testing of pressure transmitters and pressure regulators regulating the pressure 2 bar above ring main pressure covered by function 7	PM	FW pressure instr.	MITIGATE - FW input	SBS M6
		21--1	Manual firefighting appliances shall provide a reliable and effective tool for firefighting by manual intervention.	Inspection & testing of fire water hydrants	PM	FW hydrants	MITIGATE - Manual firefighting	SBS M8
		21--2	Manual firefighting appliances shall provide a reliable and effective tool for firefighting by manual intervention.	Inspection & testing of fire water hose, nozzle & reels	PM	FW hoses	MITIGATE - Manual firefighting	SBS M8
		21--3	Manual firefighting appliances shall provide a reliable and effective tool for firefighting by manual intervention.	Inspection & testing of fire water monitors	PM	FW monitors	MITIGATE - Manual firefighting	SBS M8
		22	Portable extinguisher shall be available and ready for use.	Inspection/recertification of mobile/ portable extinguishers (incl. expiring date, availability)	PM	FW portable extinguishers	MITIGATE - Manual firefighting	SBS M8
		23,24,26	Helideck: A deck integrated firefighting system (DIFFS) shall comply with: •The water density shall be minimum 6 l/ (m2·min). •Full water supply shall be available within 15 seconds from time of activation. •Pop-up nozzles shall be tested Helideck firefighting system: Failure definition: Water/Foam not delivered to area upon test Failure frequency target for system: max 1 %	Inspection/function testing of flow rate/response time and application height	PM	DIFFS	MITIGATE - Helideck	SBS M9

		24	The foam supply to helicopter deck foam users shall comply with: •The foam monitor concentrate consumption - the foam consumption to the Pop-up	Inspection & testing of foam monitors on helideck and foam supply (capacity)	PM	FW monitors	MITIGATE - Helideck	SBS M9
		25	•dual agent hose reels (combined water/foam and dry chemical hose reel) shall be provided and have: •Sufficient powder for discharge at a rate of 2-3 kg/s for minimum 100 seconds •Sufficient foam for minimum 10 minutes full discharge.	Inspection & testing of hose reels, foam injector and dry chemical storage on helideck	PM	FW hoses	MITIGATE - Helideck	SBS M9
		26	Helicopter deck: Minimum 3x 10kg CO2 fire extinguisher with extension lance and nozzle shall be functional and ready for use.	Inspection of Mobile/portable extinguishers (incl. expiring date, availability)	PM	FW portable extinguishers	MITIGATE - Helideck	SBS M9
		27, 31	The room where the gaseous agent is released shall be sufficiently tight to maintain the prescribed concentration for the pre-determined time period of minimum 10 min. Failure definition: Release valve does not open upon test. Failure frequency target for system: max 2 %	Function test of gaseous systems Inspection of gaseous rooms (mass/pressure and tightness)	PM	CO2/Inergen	MITIGATE - CO2/Inergen system	SBS M10
		28	The bottles (e.g. N2) for system pressurization shall be refilled or replaced if the pressure drops below the required minimum.	Inspection and register of gaseous medium bottles Inspection of their dedicated water tanks (volume, freeze)	PM	CO2/Inergen	MITIGATE - CO2/Inergen system	SBS M10
		29, 31	Water mist systems shall be automatically released on fire detection. Failure definition: Release valve does not open upon test. Failure frequency target for system: max 2 %	Executive actions from logic to mist system	PM	Water mist system	MITIGATE - Water mist system	SBS M11

		30	Manual release of AFP systems (deluge, gaseous and Water mist systems)	Electrical push buttons: Function testing of individual PB's + logic test as part of F&G system test. Manual valves (air release): Function testing as part of PM for AFP system function testing.	PM	FW manual release	MITIGATE - FW input	SBS M6
PS	Function	PS No.	Functionality	Related Assurance Activities	Work Scope	Equipment group	Risk-reducing function group (technical only)	Role
PS9 Passive Fire Protection	The passive fire protection (PFP) shall ensure that relevant structures and/or equipment/components have adequate protection during a dimensioning fire. It shall contribute to reducing the consequence (escalation risk) in general. Fire divisions fire resistance with regard to stability (load bearing properties) 1), integrity 2), and insulation properties 3) shall ensure that a dimensioning fire does not escalate into surrounding areas.	1	All PFP on loadbearing structures shall be free from significant defects which would impair its ability to perform to the specified standard and/or causes corrosion under insulation.	Inspection program (Surface Protection) of Structure, Decks, Flare tower, etc. Monitoring of corrosion under PFP	Inspection	PFP	MITIGATE - Passive fire protection	SBS M2
		2	All Fire Divisions (insulated) shall be free from significant defects which would impair its ability to perform to the specified standard and/or causes corrosion under insulation.	Inspection program (Fire and Blast walls)	Inspection	Structural: fire walls, blast panels	MITIGATE - Passive fire protection	SBS M2
		3	Fire division penetrations shall maintain the rating of the division.	Inspection program (piping penetrations, cables and ducts)	Inspection	Structural: fire walls, blast panels	MITIGATE - Passive fire protection	SBS M2
		4	The condition of fire rated windows shall be in a suitable condition, free from significant defects.	Inspection program (LQ; Fire and Blast walls; etc.)	Inspection	Structural: fire walls, blast panels	MITIGATE - Passive fire protection	SBS M2
		5, 8	The condition of fire rated doors and frames shall be in a suitable condition. Fire doors shall be tested and maintained to meet specified requirements for probability of failure on demand; •Failure definition: Fire door does not close on demand (automatically) upon test •Failure frequency target for one fire door: max 1%	Inspection/testing: 6m/12m according to vendors recommendation Test sealing properties and self-closing function Test of function (self-closing fire doors)	PM	Fire doors/self-closing doors	MITIGATE - Passive fire protection	SBS M2

		6	All PFP on piping, valves and equipment in pressurized systems shall be free from significant defects which would impair its ability to perform to the specified standard and/or causes corrosion under insulation.	Inspection program (insulation) Monitoring of corrosion under PFP	Inspection	PFP	MITIGATE - Passive fire protection	SBS M2
		7	All PFP at Important cables and cable trays (including suspension) shall be free from significant defects which would impair its ability to perform to the specified standard.	Inspection program	Inspection	PFP	MITIGATE - Passive fire protection	SBS M2
		9	Passive Fire Protection shall be available at all times during normal operation and therefor temporary removal of PFP is only acceptable when subject to MOC.		Operational	-	-	-
PS	Function	PS No.	Functionality	Related Assurance Activities	Work Scope	Equipment group	Risk-reducing function group (technical only)	Role
PS10 Emergency Power	The goal for Emergency Power is to provide reliable and secure power supplies to all critical and essential systems required to function in the event of an emergency. The goal for Emergency Lighting is to provide an adequate minimum level of illumination to enable emergency response activities to be undertaken in the event that normal lighting is lost and ensure that the escape routes are readily identifiable by all personnel in any emergency.	1, 4	The emergency generator rated for a capacity of 1 x 100%, shall be capable of supplying all emergency loads on loss of main power supply.	Emergency generator performance test Emergency generator function test Calculate the sum of the emergency loads and compare with the actual effect of the emergency generator	PM	Emergency generator	EM RESPONSE - Emergency power	SBS E1
		2	The electrical integrity of the emergency switchboard and distribution that feed emergency loads shall have adequate fault protection to avoid harm to personnel and limit loss of	Switchboard maintenance and inspection	PM	Emergency switchboards	EM RESPONSE - Emergency power	SBS E1

			supply and equipment damage under fault conditions.					
		3	The diesel tank shall contain sufficient fuel to ensure the emergency generator is capable of running for a minimum of 18 hours.	Operator watch keeping checks Visual inspection of level indicator and condition of diesel tank.	Operational	Checklist or service routine may be established. This is a part of assurance of emergency power functionality.	-	-
		4	The prime mover for emergency generators shall be stopped in the event of: a)gas detection in ventilation air inlet b)over speeding, c)loss of lubricating oil pressure (this does not apply to emergency generators supplying fire pumps.)	Function test of emergency generator	PM	Emergency generator	EM RESPONSE - Emergency power	SBS E1
		5	The emergency generator shall start automatically and be connected to the emergency switchboard within 45 seconds following loss of main power supply. In cases where a standby unit is installed and the duty emergency generator fails to start, the standby unit shall start and connect to the emergency bus within a further 45 seconds.	Function test of emergency generator Emergency Generator automatic start test (on zero voltage on Emergency Switchboard)	PM	Emergency generator	EM RESPONSE - Emergency power	SBS E1
		6	Exhaust pipes from prime movers of emergency equipment shall not emit sparks or have a surface temperature which exceeds the ignition temperature of the gas mixture which is produced or stored on the installation (water cooled).	Maintenance routines for check of spark arrestors and visual check of insulation.	PM	Spark arrestors	PREVENT - Ignition prevention	SCS P2

		7	UPS shall ensure continuous power supply to all emergency equipment and systems in all situations where main and emergency power generator is not available.	UPS function test performed as part of preventive maintenance.	PM	Emergency UPS	EM RESPONSE - Emergency power	SBS E1
		8	The emergency lighting provision shall be able to provide illumination in the event of main power failure. Emergency/escape light fittings shall be free from dirt, salt deposits or physical obstructions.	Maintenance routines. - Function test (failure to activate on demand). - Inspection and maintenance of light fittings.	PM	Emergency lighting	EM RESPONSE - Emergency power	SBS E1
		9	Emergency lighting shall remain lit upon loss of main power and be supplied from emergency distribution system.	Maintenance program - Function test	PM	Emergency lighting	EM RESPONSE - Emergency power	SBS E1
		10	Emergency lighting or other critical lights (e.g. flood lights) shall be provided with self-contained batteries or UPS, both with a minimum capacity of 30 minutes.	UPS function test or function tests of emergency lighting with self-contained batteries.	PM	Emergency lighting	EM RESPONSE - Emergency power	SBS E1
		11	The UPS system shall be sufficient to power all safety critical loads and shall provide the following minimum power supply duration: UPS time requirements: •ICS including F&G and ESD system) – 60 minutes •Escape Lighting including Helideck lighting – 60 minutes in accordance with NMD MOU Regulation 856/87 §12 •Loading Computer, 60 minutes •PA and status lights, 360 minutes •SOLAS communication equipment, 360 minutes in accordance with NMD MOU Regulation 1200/93 §9 •Navigation aids, 96 hours in accordance with NMD MOU Regulation 856/87 §13	UPS capacity test of the battery bank, as part of maintenance program. Battery discharge test For UPS systems:	PM	Emergency UPS	EM RESPONSE - Emergency power	SBS E1

		12	The UPS system internal supervision facilities shall be operational and monitored.	Function test of the UPS internal supervision facilities. Use of input from the fault supervision facilities to ensure the function of the UPS system (trend monitoring and corrective maintenance).	PM	Emergency UPS	EM RESPONSE - Emergency power	SBS E1
		13	The emergency generator shall be available at all times and ready to start on demand. The emergency generator shall achieve greater than 90%* successful start on demand.	Emergency generator function test (failure to start on demand) Emergency generator performance test Emergency generator maintenance	PM	Emergency generator	EM RESPONSE - Emergency power	SBS E1
		14	The UPS batteries shall be fully charged and ready to provide power on demand. The UPS systems shall have availability figure of greater than *95% on demand.	UPS function test Maintenance of UPS batteries	PM	Emergency UPS	EM RESPONSE - Emergency power	SBS E1
		15	Battery test shall be performed to control that battery capacity has sufficient capacity to meet load requirements.	Battery test (every 12 months) Minimum every 4 years a full capacity test shall be done. This test shall include a written report over each battery capacity and evaluation of reliability of battery minimum next 12 month	PM	Emergency UPS	EM RESPONSE - Emergency power	SBS E1
PS	Function	PS No.	Functionality	Related Assurance Activities	Work Scope	Equipment group	Risk-reducing function group (technical only)	Role
PS11 Emergency Alarm and Communication	The goal for the internal communication systems is to provide visual and audible warning to personnel that an emergency condition has been identified, and the means to communicate with	1	The PAGA system shall issue clear and unambiguous verbal instructions and alarms to all personnel in all areas of the installation. Amplifier output levels shall met design parameters.	Function tests and reference measurements on PA-amplifiers and speakers. Corrective and preventive maintenance activities	PM	PA system	EM RESPONSE - Emergency communication	SBS E2

<p>personnel on the status, mustering, and if necessary, abandonment during an emergency.</p> <p>The goal for the external communication systems is to provide essential communications to external parties particularly during emergency situations.</p>	2	Flashing yellow alarm lights in high noise areas, i.e. above 85 dB, shall ensure that personnel observe the alarm signals and messages. The alarm lights shall be clearly visible and not obstructed.	Function tests of the flashing yellow lights Corrective and preventive maintenance activities	PM	PA system	EM RESPONSE - Emergency communication	SBS E2
	3	PA and alarm equipment shall remain powered after loss of main power generation and have dedicated UPS battery power suitable for 6 hours operation (based on 15% alarm, 85% standby) on event of loss of emergency power.	Battery test. Check that all batteries have been tested according to planned maintenance - and at least once every year. (It is common to test the batteries on low load over longer period of time to render the possibility of checking each battery cell).	PM	Emergency UPS	EM RESPONSE - Emergency power	SBS E1
	4	Alarm initiation from the F&G system shall be fully operational within 3 s after initiation.	Check that alarm initiation from the F&G system is fully operational within 3 s after initiation. Optionally, this test may be part of planned maintenance.	PM	F&G logic	DETECT - F&G logic	SBS D3
	5	A UHF radio and paging system shall be operational according to design specifications. The UHF system coverage shall allow error free communication across the entire installation. On-board UHF repeater system shall have capability to reach shuttle tanker when offloading.	Corrective and preventive maintenance activities - Reference measurements Function test through daily use	PM	UHF radio and paging system	EM RESPONSE - Emergency communication	SBS E2
	6	Hand-held UHF radios shall be available and operational according to design specifications to allow for effective communications between the control room(s) and the emergency response teams.	Corrective and preventive maintenance activities	PM	UHF radio and paging system	EM RESPONSE - Emergency communication	SBS E2

		7, 13	The PABX telephone system shall be available to enable platform personnel to contact the control room in emergency situations. PABX/Telephone System shall allow for communication with other installations, helicopters, vessels and shore.	Corrective and preventive maintenance activities Inspection and function test Check that the telephones are equipped with signs showing the emergency numbers.	PM	PABX telephone system	EM RESPONSE - Emergency communication	SBS E2
		8, 13	Crane personnel shall be able to communicate with the control room, ships and deck operators. Maritime VHF, UHF radio, PA loudspeaker and telephone shall be installed in crane cabins and work according to design requirements. Maritime VHF (including crane cabin) shall allow for communication with other installations, helicopters, vessels and shore.	Function test Corrective and preventive maintenance activities	PM	Crane communication	EM RESPONSE - Emergency communication	SBS E2
		9	Internal emergency communications systems shall remain powered after loss of main power generation and have dedicated UPS battery power suitable for 6 hours operation (based on 25% transmit, 75% standby) on event of loss of emergency power.	Ref. point 3	PM	Emergency UPS	EM RESPONSE - Emergency power	SBS E1
		10	A main telecommunication system (2 fiber links and a radio link) for transmission of voice and data to onshore operational centre or other platforms, including back- up routing, shall be operational at all times.	Corrective and preventive maintenance activities for radio links	PM	Emergency radio links	EM RESPONSE - Emergency communication	SBS E2
		11	Switched satellite services (Iridium or Inmarsat) shall be operational at all times as a backup system to the permanent main communication link in an emergency situation.	Corrective and preventive maintenance activities - Function test	PM	Emergency satellite	EM RESPONSE - Emergency communication	SBS E2

		12, 13	General radio systems, including Mandatory radio (GMDSS) shall provide marine and aeronautical communication for distress situations to allow for coordination of rescue, recovery and emergency assistance. Maritime VHF / Aeronautical VHF radio shall allow for communication with other installations, helicopters, vessels and shore.	Corrective and preventive maintenance activities - Function test Check that the use of GMDSS equipment is part of the exercise plan Check that relevant training for Maritime VHF is performed	PM	GMDSS	EM RESPONSE - Emergency communication	SBS E2
		14	Lifeboat VHF radio - On GMDSS (Global Maritime Distress Safety System) channel the lifeboat radios shall be proven to be operable and capable of two way communication. Batteries shall be within their expiry date.	Lifeboat VHF function test	PM	Lifeboat	EM RESPONSE - Lifeboats & Rafts w/escape chutes	SBS E5
		15	Platform equipment for external emergency communication shall remain powered after loss of main power generation and be powered from dedicated battery supplies and/or powered from platform UPS power system. Battery supply / UPS duration shall be 6 hours of operation on event of loss of emergency power.	Ref. point 3	PM	Emergency UPS	EM RESPONSE - Emergency power	SBS E1
PS	Function	PS No.	Functionality	Related Assurance Activities	Work Scope	Equipment group	Risk-reducing function group (technical only)	Role

PS12a Escape & Evacuation	<p>The purpose of the escape routes is to ensure that personnel may leave areas in case of a hazardous incident by at least one safe route and to enable personnel to reach the designated Mustering Area from any position on the installation they are likely to occupy.</p> <p>The purpose of the evacuation system is to ensure means of safe abandonment of the installation for the maximum personnel on board (POB), following a hazardous incident and a decision to abandon the installation.</p>	1	Escape route markings - The yellow coating for the escape routes on solid deck shall be in a satisfactory condition.	6-monthly inspection Verification of correct markings	PM	Escape routes & tunnel	EM RESPONSE - Evacuation	SBS E4
		2	The parallel yellow lines for the escape routes on deck grating shall be in a satisfactory condition	6-monthly inspection Verification of correct markings	PM	Escape routes & tunnel	EM RESPONSE - Evacuation	SBS E4
		3	Escape route condition - The escape routes shall not be blocked or in any other way altered such that the ability to function as escape route is impaired.	Included in check list for HSE Safety rounds	Operational	-	-	-
		4	Signage, arrows and directional lighting giving the preferred direction of escape shall be available and in satisfactory condition, both indoors and outdoors.	Included in check list for HSE Safety rounds	Operational	-	-	-
		5	Emergency preparedness station bills located around the platform (s) shall be in a satisfactory condition and updated, and they shall not be obstructed or covered.	Included in check list for HSE Safety rounds	Operational	-	-	-
		6	Doors in escape routes - The condition of all doors in doorways on the escape routes shall be such that they: •are capable of being easily opened from either side by one person, •are self-closing.	Inspection and maintenance activities HSE Safety rounds	Inspection	Fire doors/self-closing doors	MITIGATE - Passive fire protection	SBS M2

		7	Door seals - The seals on all external doors in the safe area shall be in such a condition that they are capable of maintaining control of leakage.	Inspection and maintenance activities	Inspection	Fire doors/self-closing doors	MITIGATE - Passive fire protection	SBS M2
		8	Escape tunnel - All external doors, dampers and permanent penetrations in the escape tunnel shall have their gas and smoke tight property intact.	Inspection and maintenance activities	PM	Escape routes & tunnel	EM RESPONSE - Evacuation	SBS E4
		9	Life rafts shall be in good condition, sealed and within certification and next inspection date.	Life raft maintenance activities. Inspection of life raft recertification date and sealing condition. Inspection of life raft containers and suspension system.	PM	Life rafts	EM RESPONSE - Lifeboats & Rafts w/escape chutes	SBS E5
		10	Escape chutes and containers shall be in good condition and within certification and next inspection date. The door to the container shall be easy to open.	Escape chute maintenance and inspection activities. Inspection of escape chute recertification date*.	PM	Escape chutes	EM RESPONSE - Lifeboats & Rafts w/escape chutes	SBS E5
		11	Launching and recovery appliances for life saving equipment (lifeboats and life rafts) shall be in accordance with NMD Regulation 853/2007 and NORSOK R-002. This check point covers the lifting arrangement from the hook downwards to the lifesaving equipment	Inspection and maintenance activities. Recertification of specific components (steel wires, chains, shackles, etc.)	PM	Launching and recovery appliances for life boats and life rafts	EM RESPONSE - Lifeboats & Rafts w/escape chutes	SBS E5
		12	Survival suits and life jackets shall be in good condition with no visible damage. Where equipment is in sealed packaging it shall be intact and within certification date.	Inspection of condition and expiry date of survival suits and life jackets, and replacement if necessary.	PM	Emergency escape equipment	EM RESPONSE - Evacuation	SBS E4

		13	Evacuation time - POB shall be able to evacuate the installation within the time requirement stated in the Emergency Preparedness Analysis (EPA).	<p>Mustering and evacuation drills.</p> <p>Check data sent to RNNP (Risikonivå i norsk petroleumsvirksomhet) to verify evacuation time</p> <p>Covered by HSE procedure</p>	Operational	-	-	-
		14	<p>The escape chute launch mechanism shall be function tested periodically to ensure that the escape chute will release in an emergency situation.</p> <p>Failure definition: Escape Chute launch mechanism does not work</p> <p>Failure frequency target: max 1%</p>	Escape chute launch mechanism test.	PM	Escape chutes	EM RESPONSE - Lifeboats & Rafts w/escape chutes	SBS E5
PS	Function	PS No.	Functionality	Related Assurance Activities	Work Scope	Equipment group	Risk-reducing function group (technical only)	Role
PS12b Lifeboats	The purpose of the lifeboat evacuation system is to ensure means of safe abandonment of the installation for the maximum personnel on board (POB), following a hazardous incident and a decision to abandon the installation	1	Lifeboat condition - There shall be no visible damage or deterioration to the lifeboat's hull or hatch seals that could compromise the lifeboat's ability to be considered seaworthy.	Lifeboat inspection and maintenance	PM	Lifeboat	EM RESPONSE - Lifeboats & Rafts w/escape chutes	SBS E5
		2	The life boat davits shall be free from signs of significant degradation, damage or deformation which could compromise their ability to provide structural support.	Inspection (corrosion, cracks, surface protection)	PM	Launching and recovery appliances for life boats & life rafts	EM RESPONSE - Lifeboats & Rafts w/escape chutes	SBS E5
		3	<p>Lifeboat clutch, steering and internal lighting shall be proven to be operational.</p> <p>Include launching arrangement - which it is not possible to stop the test underway - pull & go.</p>	Lifeboat inspection and maintenance (performed every 5 years)	PM	Lifeboat	EM RESPONSE - Lifeboats & Rafts w/escape chutes	SBS E5

		4	Lifeboat fuel tank shall be full ensuring 12 hours running and air bottles shall be charged at least 90% of full charge and be within certification date.	Lifeboat inspection and maintenance	PM	Lifeboat	EM RESPONSE - Lifeboats & Rafts w/escape chutes	SBS E5
		5	Lifeboat contents, including emergency provisions and survival equipment, shall be in accordance with the Inventory and shall all be within their 'use by' dates.	Lifeboat inspection and maintenance	PM	Lifeboat	EM RESPONSE - Lifeboats & Rafts w/escape chutes	SBS E5
		6	Emergency Radio Beacons – EPIRBs (Emergency Position-Indicating Radio Beacons) or SART (Search and Rescue Transponder) located in the lifeboat shall be fully operable, be free from damage and shall be powered by batteries within their expiry date.	EBIRP and SART inspection and maintenance	PM	Lifeboat	EM RESPONSE - Lifeboats & Rafts w/escape chutes	SBS E5
		7	Load testing of free-fall lifeboats – In accordance with SOLAS requirements the lifeboat on-load release gear, including free-fall lifeboat release systems, shall be operationally tested under a load of 1.1 times the total mass of the boat when loaded with its full complement of persons and equipment whenever the release gear is overhauled. Such over-hauling and test shall be carried out at least once every five years.	Carry out the applicable tests required by SOLAS	PM	Launching and recovery appliances for life boats & life rafts	EM RESPONSE - Lifeboats & Rafts w/escape chutes	SBS E5
		8	Deluge – Lifeboats shall have sufficient deluge coverage. On simulation of a wet deluge test there shall be adequate coverage of the lifeboat, with no blocked nozzles.	Lifeboat inspection and maintenance records Deluge test	PM	Lifeboat	EM RESPONSE - Lifeboats & Rafts w/escape chutes	SBS E5

		9	The lifeboat engine start system shall be tested to ensure that the lifeboat engine will start in an emergency situation. Failure definition: Lifeboat Engine does not start Failure frequency target: max 1%	Function test of the lifeboat engine start system.	PM	Lifeboat	EM RESPONSE - Lifeboats & Rafts w/escape chutes	SBS E5
		10	The lifeboat release mechanism shall be function tested to ensure that the lifeboat will release in an emergency situation. Failure definition: Lifeboat release mechanism does not work Failure frequency target: max 1%	Function test of lifeboat release mechanism.	PM	Launching and recovery appliances for life boats & life rafts	EM RESPONSE - Lifeboats & Rafts w/escape chutes	SBS E5
PS	Function	PS No.	Functionality	Related Assurance Activities	Work Scope	Equipment group	Risk-reducing function group (technical only)	Role
PS13 Blowdown	To vent, flare or blowdown plant, removing hydrocarbon inventory, discharging to atmosphere in a safe manner, consistent with the flare system	1	Manual operated isolation/block - valves in blowdown lines/ purge lines shall be secured in open position.	Check that the LO/LC register has been updated following procedure	Operational	LO/LC valve register control	-	-
		2	Blowdown time and end pressure shall be specified for each individual blowdown segment because required times/pressures vary. Pressure in blowdown segments must be monitored using control system trend functions in order to record depressurization profiles during operational shutdowns and during testing.	Blowdown times/pressures obtained from testing to be verified and checked towards specified time/pressure. Compensate by calculation if necessary. Flare knock out pressure from test report to be checked in order to verify the integrity of the flare tip. The Function shall be carried out by operation.	PM	Flare, valves	CONTROL - blowdown	SBS C5

		3	High liquid level in Knockout Drum shall initiate production shutdown activated by two transmitters linked to the PSD and ESD respectively. This is ensured by the calibration of the knockout drum level measurement to the required level of accuracy The Flare KO Drum shall be provided with the following alarms: - Low temperature - High/low liquid level Level alarms/trips shall be proven to be operable and alarm in the CCR	Check that the requirements in the SRS for the level and pressure transmitters is fulfilled PMRs Level Transmitter Pressure transmitter Calibration and Function Test	PM	Flare, instrumentation	CONTROL - blowdown	SBS C5
		4	Heat tracing in the Knockout Drums of level and pressure transmitters, if required, shall be provided and functional	Check that maintenance routines and function testing of heat tracing are carried out	PM	Flare, heat tracing	CONTROL - blowdown	SBS C5
		5	Response times for relief system shall ensure that overpressure in the flare system is avoided. The quick open valve in flare line shall open within specified time.	Check that maintenance and test routines (ref. ESD test) are carried out	PM	Flare, valves	CONTROL - blowdown	SBS C5
		6	Continuous purge flow rates for the flare system shall be monitored and an alarm to be activated if flow rate becomes too low.	Check that maintenance routines and function testing of purge line instrumentation is carried out	PM	Flare, instrumentation	CONTROL - blowdown	SBS C5
		7	Flare tip to be kept in operable condition	Check that visual inspection has been carried out	PM	Flare, tip	CONTROL - blowdown	SBS C5
PS	Function	PS No.	Functionality	Related Assurance Activities	Work Scope	Equipment group	Risk-reducing function group (technical only)	Role

PS14 Process Safety	The goal is to detect an unsafe process condition, stop the flow of hydrocarbon, shutdown process and utility equipment and overpressure within pipework, vessels and tanks before operating conditions exceed their design limit to prevent the failure of piping or equipment leading to release of hydrocarbon or toxic fluid leaks.	1	Manual valves in the flow path between pressure source and relief device and flare/vent system shall be secured in locked/interlocked open	Check that LO/LC register for LO/LC valves has been updated following procedure	Operational	LO/LC valve register control	-	-
		2	PSD and IOPPS valves shall be available at all times The closing time shall be sufficiently quick to ensure that the primary safety barrier has fulfilled its task without any activation of the secondary barrier The closing time should be less than 2 sec/inch if not otherwise specified PSD and HIPPS valves shall have defined criteria for leakage rates based on safety criticality	Check of ABB/Kongsberg reports extracted from event log for stroke times	PM	PSD (incl HIPPS & IOPPS) system (sensors, logic, final element - valves)	CONTROL - process safety	SBS C1
		3	All PSVs shall be tested and replaced at a frequency, taking account of degradation which could compromise their ability to provide the defined protection on demand All PSVs shall be routinely calibrated.	Valid calibration certificate and test log	PM	PSV	CONTROL - process safety	SBS C1
		4	FSVs (check valves) shall be in a condition that ensures that they perform their intended function and provide required protection	Check test records for check valves including acceptance criteria	PM	FSV	CONTROL - process safety	SBS C1
		5	The minimum opening time for the IOPPS valves, as determined by simulation, shall be as follows: •Flowline and Riser EV valves – 60 sec •Topside choke valve – 120 seconds •Diverter valves – 60 seconds	Function test	PM	PSD (incl HIPPS & IOPPS) system (sensors, logic, final element - valves)	CONTROL - process safety	SBS C1

		6	All trips shall be working at pre-defined levels to ensure the integrity of the Protective Systems	All trips set according to CPSR/Workmate and ABB/Kongsberg	PM	PSD (incl HIPPS & IOPPS) system (sensors, logic, final element - valves)	CONTROL - process safety	SBS C1
		7	PSD system shall be continuously available in CCR and the system shall raise alarms in CCR for operators awareness or actions <ul style="list-style-type: none"> •Alarm when valve and equipment are not activated on demand •PSD system status and defects/failures alarm •Sensor status i.e. value and condition •Length of time for inhibit and override activation 	Check PSD logs (deviation alarms)	PM	PSD (incl HIPPS & IOPPS) system (sensors, logic, final element - valves)	CONTROL - process safety	SBS C1
		8	The maximum response time for the pressure transmitter, contact relays, and proximity switches from when a dangerous process state is detected until the initiator is activated, shall be 100 ms	Function test (Response time, test records) Maintenance records in WorkMate (routine scheduled maintenance (suppliers job)	PM	PSD (incl HIPPS & IOPPS) system (sensors, logic, final element - valves)	CONTROL - process safety	SBS C1
PS	Function	PS No.	Functionality	Related Assurance Activities	Work Scope	Equipment group	Risk-reducing function group (technical only)	Role
PS15 Loss of Containment	The goal is to provide and maintain a safe containment of hydrocarbons during normal operation and a range of abnormal operating conditions within the design envelope.	1	The technical integrity of all topside piping (including pipe support, flanges/mechanical connections and vessel trims) shall prevent leakages.	Check that Inspection requirements, inspections have been fulfilled Relevant PM in separate excel sheet	Inspection	HC piping	PREVENT - Containment, piping and static process equipment	SCS P4
		2	Vessels/Heat Exchangers/Tanks technical integrity shall ensure that leakages do not occur (including vessel supports, saddles, flanges/mechanical connections and internals)	Check that Inspection requirements, inspections have been fulfilled Inspection and maintenance programs (internal and external conditions: - Coating - Insulation - corrosion management programs (incl. Chemical	Inspection	Coating and insulation	PREVENT - Containment, piping and static process equipment	SCS P4

				corrosion control)				
		3	The technical integrity of valves and other mechanical equipment shall ensure that leaks do not occur and that the equipment withstand vibrations	Check if vibration inspection has been completed as planned (check action log)	PM	Valves and other mechanical equipment	PREVENT - Containment, piping and static process equipment	SCS P4
		4	Primary integrity of the hull hydrocarbon containment equipment and systems (main Deck, cargo systems and connections) shall be maintained	Inspection and maintenance routines	PM	Integrity of the hull hydrocarbon containment equipment and systems	PREVENT - Containment, piping and static process equipment	SCS P4
		5	The integrity of the Cargo system's pumps, valves, piping, hydraulic power and vents/flare shall ensure that leakages do not occur.	Inspection and maintenance routines.	PM	The integrity of the Cargo system'	PREVENT - Containment, piping and static process equipment	SCS P4
PS	Function	PS No.	Functionality	Related Assurance Activities	Work Scope	Equipment group	Risk-reducing function group (technical only)	Role
PS16 Collision Prevention	To prevent collision between the installation and other vessels that are: - approaching, - passing, - drifting,	1	Lights - The 15 nautical mile primary lights and the 10 nautical mile secondary lights shall be functional and illuminate on demand	Maintenance routines and visual functional test (testing activation)	PM	Navigational lights	PREVENT - Collision	SCS P6
		2	Lights - All Navigation Aids shall be synchronized and simultaneously emit the Morse letter 'U' (installation specific) with a cycle period of 15 seconds.	Maintenance routines and visual functional test	PM	Navigational lights	PREVENT - Collision	SCS P6
		3	Fog Horns - The 2 nautical mile Omni-directional main foghorns	Fog detection and manual activation functional test	PM	Fog horns	PREVENT - Collision	SCS P6

			shall be functional on demand					
		4	Fog Horns - All fog horns shall be synchronized and simultaneously emit the Morse letter 'U' (installation specific) with a cycle period of 30 seconds.	Functional test (to confirm the Morse letter and the cycle period)	PM	Fog horns	PREVENT - Collision	SCS P6
		5	Radar - Radar shall continuously be able to display an area around the installation sufficient for an operator to detect approaching vessels at a distance of minimum 25 nautical miles	Functional test of the detection range. Maintenance routines for radar and AIS T(SKA)013 PM-011245	PM	Radar	PREVENT - Collision	SCS P6
		6	Radar – The main responsibility for monitoring the ship traffic is the Traffic Control Centre. In case of signal line breakdown to the Control Centre, the unit shall be self-contained to survey the nearby ship traffic. And as a back-up, use of standby vessel.	Function test of local equipment	PM	Radar	PREVENT - Collision	SCS P6
		7	Common Alarm - Navigational aids provide a common alarm to the CCR or manned areas, activated from the Nav-aids control panel which will indicate system failure or failure of any lantern or fog horn.	Functional test by simulating failures Maintenance routines	PM	Nav Aid Control panel	PREVENT - Collision	SCS P6
PS	Function	PS No.	Functionality	Related Assurance Activities	Work Scope	Equipment group	Risk-reducing function group (technical only)	Role
PS17 Wells	To provide effective containment of hydrocarbon gas and fluids within the wellbore, annuli and wellhead.	1	Production Tubing and Casing is required to contain their hydrocarbon inventory within the normal operating envelope and reasonably foreseeable conditions.	Continuous Pressure monitoring and alarms Opportunistic tubing caliper	Operational	-	-	-

		2	Xmas tree, DHSV and Wellhead shall contain hydrocarbon inventory within the normal operating envelope and reasonably foreseeable conditions. Wellheads, trees and DHSV shall meet a maximum internal leak criterion of 400CC /min for fluid, 15scf /min for gas. No external leakage is accepted	PM: in flow test of X-mas tree, DHSV PM: bleed of ports of Wellhead PM: Pressure test of xmas tree, dhsv, wellhead	PM	X-mas valves	CONTROL - well isolation	SBS C3
		3	The wellhead system wall thickness shall be maintained above the minimum allowable level as specified in the relevant design codes.	PM: visual inspection	PM	X-mas valves	CONTROL - well isolation	SBS C3
PS	Function	PS No.	Functionality	Related Assurance Activities	Work Scope	Equipment group	Risk-reducing function group (technical only)	Role
PS18 Rescue and Safety Equipment	The goal of the Rescue & Safety Equipment is to support search, rescue and recovery activities for persons who may have to be rescued from the sea for any reason, and to provide personnel with a comprehensive set of rescue equipment available for the use following a major accident hazard.	1	The MOB boat system(s) including the lifting frame installed on the installation shall be operational and in good condition. The MOB boat shall be ready for launch and recovery, and it shall be possible to launch a MOB by two independent means of lifting (e.g. deck cranes and davit) (Two MOB boat systems on the vessel)	MOB boat maintenance, inspection and function test. MOB boat exercises. Inspection of the MOB boat lifting frame Assurance of cranes covered in PS 24	PM	MOB boat and its lifting appliances	EM RESPONSE - Rescue	SBS E3
		2	Man overboard recovery time - The time from man overboard alarm is sounded to a person is recovered from the sea shall be within limits specified in EPA	MOB exercises. Availability of MOB boat(s) to be assured by assurance activities in F1	Operational	-	-	-

		3	MOB boat crew gear - The watertight cabinet for storage of MOB boat crew gear shall contain the required minimum equipment*. The equipment shall be functional and in good condition.	Inspection of contents and condition of equipment Function test of applicable equipment (e.g. VHF radio, torches)	PM	MOB boat and its lifting appliances	EM RESPONSE - Rescue	SBS E3
		4	Personnel basket (FROG) shall be in good condition. The basket shall float.	Inspection and function test of basket	PM	FROG	EM RESPONSE - Rescue	SBS E3
		5	Safety showers and eye baths showers and eyebaths installed on the installation shall functioning and in good condition. Potable water quality shall be used.	Inspection and function test of safety showers and eyebaths.	PM	Safety showers / Eye baths	EM RESPONSE - Rescue	SBS E3
		6	Safety station cabinets installed on the installation shall contain the required equipment and the equipment shall be in good condition.	Inspection and function test of safety station cabinet contents.	PM	Safety station cabinets	EM RESPONSE - Rescue	SBS E3
		7	Extended first aid kits provided around the installation shall contain all the equipment on the content list.	Replacement after use Inspect and resupply extended first aid kit	PM	First Aid Kits	EM RESPONSE - Rescue	SBS E3
		8	Smoke hoods and breathing masks shall be provided; one per bed in LQ in addition to where they are required by the safety evaluation. Smoke hoods and breathing masks shall be in good condition and within next certification date.	Inspection to ensure equipment is provided where required and within next certification date. Inspection of equipment condition	PM	Smoke hoods / Breathing masks	EM RESPONSE - Rescue	SBS E3
		9	The firemen's equipment sets shall contain the required equipment, and the equipment shall be in good condition. Firemen's breathing apparatus shall be within certification date. Air bottles shall be of composite type.	Inspection and function test.	PM	Fireman equipment	MITIGATE - Manual firefighting	SBS M8

		10	The compressor air quality shall be maintained within acceptable levels in accordance with NS-EN 12021:1998* - Carbon Dioxide (CO ₂): <500 ppm Carbon Monoxide (CO): <15 ppm Water Content: <50 mg/m ³ @ 200 bar <35 mg/m ³ @ 300 bar Oil (tasteless & odorless) < 0.3 mg/m ³	Inspection and function test of the equipment for refilling breathing apparatus.	PM	Fireman equipment	MITIGATE - Manual firefighting	SBS M8
PS	Function	PS No.	Functionality	Related Assurance Activities	Work Scope	Equipment group	Risk-reducing function group (technical only)	Role
PS24 Lifting Equipment	To, by lifting, moving and lowering, safely transfer loads on to, and around the installation, and safely transfer personnel off the installation (in special emergency circumstances)	F1	The technical integrity of all lifting equipment (cranes, lifting appliances and lifting accessories) shall be in a condition in line with performance requirements defined in the performance standard	Search for KAO with RC (start with restricted conformance) based on crane specific TAG/maintenance performance: - 1 monthly PMR (by operator) - 3 monthly PMR (by 2nd party) - 6 monthly PMR (by 2nd party) - 12 monthly PMR (incl. Verification of 3rd party) - 24 monthly PMR (incl. Verification of 3rd party) - 48 monthly PMR (incl. Verification of 3rd party)	PM	Lifting equipment	PREVENT - Lifting equipment	SCS P7
		F2	Incidents and accidents in crane operations shall be investigated for identification of improvements to crane operations	Check that all MIOs and HIPOs registered in TRACTION have been investigated and that all major findings with recommended corrective actions have been implemented and verified accordingly	Operational	-	-	-
		F5	Specific high criticality operations in lifting operations in the drilling area is defined and subjected to specific procedural handling	Check that lifting appliance operators are in compliance with requirements in addition may need a check drilling contractors own competence database)	Operational	-	-	-

		F6	Specific high criticality (red SIKAP) crane operations (such as lifting through hatchways, transfer between two lifting appliances, personnel lifting, MOB lifting) is defined and subjected to specific procedural handling	Check that lifting appliance operators are in compliance with requirements in addition may need a check sub-contractors own competence database, if relevant)	Operational	-	-	-
		7	Lifting zones shall be defined, available for the crane operator and adhered to.	Check that an updated lift map, clearly identifying the lifting zones, is available in the crane cabin.	Operational	-	-	-
		8	If lifting restrictions is applied on the installation, they shall be known and adhered to.	Check that the lifting restriction map is updated and available in the crane cabin. Check that pre-use check for lifting operations includes visible inspection for possible dropped objects including accumulation of ice during cold seasons.	Operational	-	-	-
		9	Crane operation above areas with restrictions on crane operation (e.g. above hydrocarbon equipment, high voltage equipment) shall be subjected to risk evaluation and be performed according to procedures. , and be subject to revision if consequence is regarded as unacceptable	Check that risk assessments has been performed and documented previous to any lifting operations in restricted areas (such as lifting above pressurized or high voltage equipment)	Operational	-	-	-
PS	Function	PS No.	Functionality	Related Assurance Activities	Work Scope	Equipment group	Risk-reducing function group (technical only)	Role
PS 30 Green Sea Barriers	To resist and remove energy from the overtopping by water in severe wave conditions such that structures, safety critical equipment and piping and personnel on the hull deck are shielded, and to protect the escape tunnel from	1	The Green Sea Panels shall retain their structural integrity under the hydrostatic pressures for the 100-year wave event based on maximum freeboard exceedance identified by model test.	General Visual Inspection (deformation, cracks, corrosion) BPSK-14006-K-0001 Close Visual Inspection of Green Sea Panels including bolts and supports (every 4 th year)	Inspection	Structural	MITIGATION - impact protection	SBS M1

	wave run-up along the ship side.	2	The Wave Deflectors shall lead the wave run-up away from the ship side and avoid damaging the escape tunnel and main process deck.	General Visual Inspection (deformation, cracks, corrosion, 45 degree) BPSK-14006-K-0001 General Visual inspection of Escape Tunnel Wave Deflectors – Annual inspection before winter	Inspection	Structural	MITIGATION - impact protection	SBS M1
		3	Where green sea impacts on structures, personnel or safety critical equipment are predicted, barriers designed to attenuate the green sea loadings shall be provided.	Experience log, damage reports, Updated risk analysis	Operational	-	-	-
PS	Function	PS No.	Functionality	Related Assurance Activities	Work Scope	Equipment group	Risk-reducing function group (technical only)	Role
PS 31 Bilge and Ballast System	To maintain stability, structural- and watertight integrity of the FPSO hull.	1a	The ballast system shall provide the means of transferring water in and out of the hull and between ballast tanks to maintain acceptable strength and stability performance.	Ballast systems operated daily : Weekly function test on all ballast valves	PM	Ballast valves	PREVENT - Bilge & Ballast	SCS P8
		1b	The ballast system shall provide the means of transferring water in and out of the hull and between ballast tanks to maintain acceptable strength and stability performance.	(Functional test of all ballast systems under Class – Every five years	Inspection	Ballast tanks	PREVENT - Bilge & Ballast	SCS P8
		2	The ballast system shall remain operational at reduced capability (one pump), powered from the emergency switchboard in the event of loss of main power generation. The local emergency hydraulic hand pumps for operation of the ship side valves (including the two forward, two aft seawater sea chests and aft bilge overboard valve) shall be tested every 3 months	Function Test (HPU) The ballast system shall be tested on emergency power annually	PM	Ballast HPU & pumps	MITIGATE - Emergency ballast	SBS M10

		3	Ballast tanks shall have the facility for their atmosphere to be monitored for the presence of hydrocarbon gas.	Function Test (gas alarm system calibration and PMR)	PM	Tank gas monitoring	PREVENT - Bilge & Ballast	SCS P8
		4	The ballast pumps shall provide the pressure needed to transfer ballast water within the ballast system.	Not formalized at the moment, talk to operators (equipment in daily use)	PM	Ballast pumps	PREVENT - Bilge & Ballast	SCS P8
		5	The hydraulic power units shall provide the power needed to operate one of the four ballast pumps in emergency mode	Inspection/Maintenance	PM	Ballast HPU	MITIGATE - Emergency ballast	SBS M10
		6	The Ballast piping shall ensure that ballast water is contained within the ballast system when ballast water is transferred in accordance with acceptance criteria.	Inspection (GRE) (leakage, decay, corrosion/erosion, wall thickness, flanges) NDT on steel piping and Cu Ni piping	Inspection	Ballast piping	PREVENT - Bilge & Ballast	SCS P8
		7	The ballast valves shall provide the means of controlling ballast water transfer between watertight compartments in the ballast water system (open/close). All ballast valves shall be capable of being remotely and manually operated.	Maintenance/Function Test (confirm "fail to safe", confirm both remote and manual operation, confirm position indicator)	PM	Ballast valves	PREVENT - Bilge & Ballast	SCS P8
		8	The ballast ring cross-over valves shall provide separation between port and starboard sides	Function test as part of general function test	PM	Ballast valves	PREVENT - Bilge & Ballast	SCS P8
		9	Ship-side valves shall provide a watertight isolation at all hull penetrations.	Function Test/ Maintenance (confirm functionality of the valves, leakage rate, confirm both remote and manual operation of the valves)	PM	Ballast valves	PREVENT - Bilge & Ballast	SCS P8
		10	Air vents fitted to ballast tanks shall provide unobstructed air flow and be provided with (fire screens) immersion closure devices to prevent down-flooding if submerged.	Visual inspection (Marine team) and function test (DNV annual check)	PM	Tank air vents	PREVENT - Bilge & Ballast	SCS P8

		11	Remote level gauging shall be provided for all cargo tanks, ballast (including peak) tanks, slop tanks, fuel storage tanks, distilled and domestic fresh water tanks.	Function Test - Annual calibration / verification of tank level monitoring, low level, high level and independent overfill (high-high) alarms - temperature monitoring (cargo and slop tanks) - confirm trim and list correction (sounding tables implemented in the Kongsberg system to Napa)	PM	Tank level instrumentation	PREVENT - Bilge & Ballast	SCS P8
		12	Remote control of all valves necessary for the safe and efficient operation of the cargo and ballast system during loading, discharge, tank washing and cleaning operations shall be provided through the CCR, and valve position indication shall be provided.	Check for trends through record of defects (KAO)	Operational	-	-	-
		13	All loading conditions shall have sufficient intact stability, maintain sufficient buoyancy and stability following collision damage or flooding, and comply with the limits for longitudinal strength. Manual operation and control shall be initiated immediately upon reduced or loss of functionality from any of the related systems (ballast, loading computer, tank level gauging).	Operational Procedure/Inspection - confirm that everything is being handled correctly by the loading computer (Napa) - confirm that the loading computer operator is aware of all the requirements to be - confirm permanent changes have been identified and implemented) (operation document for weight control procedure)	Operational	-	-	-

		14	The loading computer shall provide real-time information in the CCR on hull bending momentum; shear force, hydrostatics and stability status, based on input from the tank gauging system, draught sensors and strain gauges.	<ul style="list-style-type: none"> - Review Function Test (annually by DNV) - Check that operating procedure is in place and up to date - review of the loading computer certificate) (annual) - comparison with test conditions, comparison output with actual loading condition (manual readings) - confirm alarm for each implemented limit (draught, stability, longitudinal strength), - comparison of trim and list on loading computer and inclinometer - confirm permanent weight changes are reflected in the loading computer (annual) - confirm check towards all relevant requirements for intact and damage stability and strength - calibration of input data from sensors <p><i>No PM for loading computer found in Workmate</i></p>	PM	Loading computer	PREVENT - Bilge & Ballast	SCS P8
		15	All volumes contributing to the buoyancy of the FPSO shall at any time be protected by watertight and weather tight boundaries to prevent water ingress.	Inspection (DNV survey) (watertight and weather tight integrity survey (bulkheads, closing appliances) (load line survey))	Inspection	Bullheads, closing appliances	PREVENT - Bilge & Ballast	SCS P8
		16	The bilge system shall provide a means of removing water from normally dry compartments.	Function Test of pumps (PMR) (The main forward and aft bilge pumps (56-PA-501A/B and 56-PA-530A/B) and remote operated bilge valves shall be function tested every two months.)	PM	Bilge pumps	PREVENT - Bilge & Ballast	SCS P8

		17	Bilge level monitoring shall provide information to the CCR on flooding in dry compartments and provide high level alarms.	Instrument Test (PMR) (All bilge level alarms located in machinery areas, i.e. critical alarms in the event of flooding of the machinery areas, shall be function tested every two months. All other bilge alarms to be function tested at least annually.)	PM	Bilge level instrumentation	PREVENT - Bilge & Ballast	SCS P8
		18	The ballast control system emergency shutdown loop (logic and final element) shall have a minimum Safety Integrity Level (SIL) rating of SIL 1 and a Probability of Failure on Demand of 0.06 in accordance with the LOPA findings. This equates to approximately 1 (one) failure in every 20 (twenty) tests.	Review of failure rate. Loop testing. The emergency shutdown and restart of the ballast control system shall be tested annually	PM	Ballast ESD logic and valves	MITIGATE - Emergency ballast	SBS M10
PS	Function	PS No.	Functionality	Related Assurance Activities	Work Scope	Equipment group	Risk-reducing function group (technical only)	Role
PS 32 Station keeping	To maintain the installation on station within specified excursion limits. Further to: - Reduce the environmental loads on the hull to maintain structural integrity - Prevent the design capacity of the mooring system from being exceeded - To maintain the risers, dynamic umbilical's and flow lines within their operating envelopes	1	All structures and components of the mooring system shall be free from signs of significant degradation, damage or deformation which could compromise their ability to meet the design intent.	Inspection to be conducted according to DNV class within a 5 year period : General visual, Close visual, chain diameter measurements (cathode protection of mooring critical structures and components Corrosion allowances and/or protection of the mooring components which are not covered by the catholic protection system, such as mooring chain, fittings and mooring wire rope)	Inspection	Mooring system structures	PREVENT - Station keeping	SCS P9
		2	The turret mooring components shall ensure that the maximum excursion of the FPSO is limited to 100m	Continuous monitoring of excursions, excursion limits implemented, check for incidents	Operational	-	-	-

		3	Turret bearing shall allow the FPSO to rotate around the turret while transferring loads into the hull structure	Visual inspection of bearing assemblies Greasing of bearings	PM	Turret bearing	PREVENT - Station keeping	SCS P9
		4	The mooring lines at the turret base are to be monitored to ensure the integrity is being maintained.	Continuous monitoring, check for incidents Temporary solutions with transponders/general visual inspection Ref SKA-BP-O-MB-0056 – Station keeping Operating Instruction Function is continuous monitored by Anchor Leg Load Monitoring System (ALLMS) installed for detection of mooring line failure.	Operational	-	-	-
		5	The anchors shall keep the mooring lines fastened to the seabed.	Inspection of all lines within a 5 year period Reference: DNV exchange system	PM	Mooring lines	PREVENT - Station keeping	SCS P9
		6	The chain stoppers shall keep the anchor chain secured to the FPSO	Visual Inspection within a 5 year period (corrosion, deformation, cracks) Reference: DNV exchange system	PM	Anchor chain stopper	PREVENT - Station keeping	SCS P9
		7	The FPSO position shall be monitored by a DGPS based system which generates real-time data.	Continuous monitoring, check for incidents Yearly control	Operational	-	-	-
		8	Gyro compasses shall give accurate input to the Heading Control	Annual calibration of the Gyro compasses	PM	Gyro system	PREVENT - Station keeping	SCS P9
		9	The angle of each mooring line shall be monitored on an intermittent basis by the Anchor Leg Load Monitoring System (ALLMS) and the line tension shall be calculated.	Function test/Inspection (calibration, tension alarms, ALLMS alarms shall be investigated through visual and/or physical inspection of the mooring line/chain connector to confirm failure of a mooring line before remedial action is taken)	PM	ALLMS	PREVENT - Station keeping	SCS P9

		10	The thrusters, K-Pos, C-Joy & K-Thrust systems shall be able to maintain the	Condition based maintenance of thrusters (PMR numbers) Annual Performance Trial of Heading Control, Thrusters	PM	Thrusters	PREVENT - Station keeping	SCS P9
		11	The Power Supply to the AHC systems shall be given priority over other equipment and systems in the FPSO	Verified by trip	PM	PMS	PREVENT - Station keeping	SCS P9
		12	The prime mover for the Essential Generator shall be capable of being stopped automatically in the event of gas detection in ventilation air inlet, over speeding and loss of lubricating oil pressure.	Function Test of Diesel Engines (PMR) Test of gas detectors, oil mist and flame	PM	Diesel engines	PREVENT - Station keeping	SCS P9
		13	As a minimum the thrusters and the associated systems required for successful operation (e.g. hydraulic power, electrical power and switchboard, PMS, etc.), shall be available at all times and for 20 minutes after initiation of the Abandon Platform Shutdown level (APS) to enable personnel to safely evacuate the FPSO if necessary.	Function test, Annual ESD test		Essential Diesel Generator	EM RESPONSE - Emergency power	SBS E1
PS	Function	PS No.	Functionality	Related Assurance Activities	Work Scope	Equipment group	Risk-reducing function group (technical only)	Role
PS33 Dynamic Risers	To safely provide hydrocarbon containment and conveyance of the hydrocarbon inventory within a secure pressure envelope from the seabed to the FPSO turret connection.	1	All risers and associated subsea equipment are required to contain their hydrocarbon inventories within their design envelope The loss of buoyancy elements shall not affect the integrity of the riser configuration The subsea camera system used for visual inspection of the bend stiffeners shall be maintained in an operable conditions to enable its use when necessary, e.g. after bad	Inspection of the entire riser length from topside to riser base GVI report: - ROV full length fly-over (GVI) - GVI inspection of the buoyancy elements - GVI by means of camera based system of bend stiffeners including bend stiffener connector. - GVI of interface connection topside.	Inspection	Dynamic risers	PREVENT - Dynamic Risers	SCS P10

			weather.					
		2	FPSO position data and excursion data shall be recorded and used as an input to continual riser integrity management (fatigue etc.)	Verification of job performed by subcontractor (yearly report MCS Kenny) related to: 1.Excursion data. 2.Evaluation of significance of possible excursions outside original design	Operational	-	-	-
		3	Potential exceedance of design characteristics shall be identified through continuous and periodic monitoring. Pulsation causing critical resonance in pipework causing excessive vibration shall be identified through continuous monitoring, especially during ramp-up phase. The compounds that migrate from the bore to the annulus shall be safely vented away to prevent the outer protective sheath from bursting	Vent Gas Monitoring Annulus vacuum test compared to vacuum test carried out immediately after riser installation	PM	VGM	PREVENT - Dynamic Risers	SCS P10
		4	The degradation of the flexible pipe's internal pressure sheath shall be within predefined level	Polymer coupon sampling and analysis (4 yrs. after commissioning)	PM	Polymer coupon	PREVENT - Dynamic Risers	SCS P10
		5	Pipelines and risers shall be available at all times unless out of service and isolated in accordance with documented procedures	Revision of number of pipes and risers available, and assurance that any defects are managed appropriately through review of the quarterly integrity report and the annual assessment report	Operational	-	-	-

		6	The Vent Gas Monitoring (VGM) System for each riser shall be available and operational whenever the riser is pressurized and contains HC to ensure that potential blockages and breaches of the inner or outer sheath are rapidly identified	Verification of offshore procedures and planned maintenance system are followed and minimized downtime of the VGM	PM	VGM	PREVENT - Dynamic Risers	SCS P10
PS 34 Subsea Dropped Object Protection	To withstand mechanical damage to hydrocarbon containing subsea systems caused by dropped objects or other activity to prevent a loss of integrity.	1	Protection structure shall be free from significant damage and degradation in order to protect the subsea facilities	Inspection in accordance with: Overall Subsea IMS	Inspection	Structural	MITIGATION - impact protection	SBS M1
		2	The Idun flowline Direct Electrical Heating (DEH) system shall include an overcurrent monitoring and shutdown system to identify damage to the cable insulation (this include from dropped object/trawl impact) which could lead to loss of flowline integrity due to arcing between DEH cable and flowline.	Function Test, Inspection (monitoring system, shutdown system)	PM	DEH monitoring	PREVENT - Subsea containment	SCS P5
		3	There shall be no fishing activities around the subsea facilities	Assessment of fishing activity data provided from the government	Operational	-	-	-
		4	The inherent dropped objects/ overtrawlability resistance of pipelines and flowlines shall be maintained	Inspection in accordance with the Pipeline Integrity Management System	Inspection	Pipelines	PREVENT - Subsea containment	SCS P5
		5	Managing dropped objects from BP activities shall be undertaken by applying Skarv Subsea Simultaneous Operation Document	Simultaneous Risk Assessments BP Reps on subsea vessels and drilling rigs Function is out of maintenance scope	Operational	-	-	-
		6	The SSIV shall be able to close on demand	Annual test of SSIV to demonstrate closure (assure no crushing or leaks due to dropped objects) Inspections in accordance with Infield Flowlines and static umbilical	PM	SSIV valves	CONTROL - emergency shutdown	SBS C4

		8	The protection requirements included within this Performance Standard need to survive the impact energies specified in the functional requirements. No other survivability requirements are identified.	Assessment of any incidents Function is out of maintenance scope	Operational	-	-	-
PS	Function	PS No.	Functionality	Related Assurance Activities	Work Scope	Equipment group	Risk-reducing function group (technical only)	Role
PS 35 Subsea Loss of Containment	To minimize the risk of loss of containment from the subsea equipment from recognized integrity threats such as corrosion, erosion, pipeline stress and fatigue design, third party to maintain this integrity from installation) to end of field life	1	Integrity management (IM) strategy The integrity of the pipeline, including risers and associated subsea equipment shall be managed in accordance with the overall Integrity Management Strategies (IMS)	IM strategy SKA-JP-M-RB-0003 Inspection and monitoring - Internal inspection (e.g. ILI – metal loss) - External inspection (e.g. GVI, CVI, GI, CP monitoring) - Environmental data (e.g. met ocean data) - Monitoring of process parameters (e.g. chemical composition in the process fluid, pressure, vibration and temperature at inlet and outlet of the pipelines, dew point for gas lines) - Corrosion and erosion monitoring (coupons, probes)	Inspection	Integrity of the subsea hydrocarbon containment equipment and systems	PREVENT - Subsea containment	SCS P5
		2	Update of IM strategy - The IM strategies are live documents and shall be subject to regular review and update so that any non-compliances and anomalies existing at that time are fully accounted for in the strategies.	Remedial actions and relevant document updates etc. are managed in accordance with the MoC and Integrity Management System	Operational	-	-	-
PS	Function	PS No.	Functionality	Related Assurance Activities	Work Scope	Equipment group	Risk-reducing function group (technical only)	Role
PS 36 Offloading Operations	The goal is to ensure an effective and safe offloading operation with means of offloading equipment and communication and	1	Failure of the telemetry communication link shall result in shut down of the loading pumps (OSD) as per ESD Cause & Effect charts.	Function test (logic) on each operation according to requirements Check list in SKA-BP-O-KA-0085 App.E	Operational	-	-	-

monitoring systems.	2	Communications shall be established between the Shuttle tanker and the FPSO when the tanker enters the 10 nautical mile limit	Function test VHF communication 2h before 10 nm (Documented in Shuttle tanker Deck log) Yearly radio inspection by certifying body (FPSO by Telenor)	Operational	-	-	-
	3	The Shuttle Tanker shall initiate a 'Permit To Load', as a part of the FPSO Green line required to start offloading operations.	Check if the Shuttle Tanker initiates a "permit to load" Part of loading procedure	Operational	-	-	-
	4	Failure of positioning equipment (PRS, positioning reference system) at the Shuttle Tanker or FPSO shall be communicated to both vessels.	Verify through approach and start-up of system SKA-BP- Part of loading procedure	Operational	-	-	-
	5	The Shuttle Tanker Positioning System shall be powered by a separate and continuously charged UPS battery	Inspection (continuously charged and regularly load test of battery bank) (part of the shuttle tanker system and DP II class)	PM	Offloading UPS	PREVENT - Offloading operations	SCS P11
	6	The availability for the OSD system shall be confirmed prior to start transfer of hydrocarbons as part of the green line process.	Function test (confirmation of availability) Checklist Marine Manual SKA-BP-O-KA-0086 Part of loading procedure	Operational	-	-	-
	7	Shutdown sequence and valve closing time shall be according to DNV-OS-E201. (Valve closing times shall not exceed 20 seconds)	Function test (closing shutdown sequence and closing time)	PM	Offloading shutdown valve	PREVENT - Offloading operations	SCS P11
	8	A minimum of three independent position reference systems shall be available for the FPSO positioning system prior to commencing offloading operation	Check independence and availability of position reference systems	Operational	-	-	-

		9	The offloading system, including hoses, shall withstand defined loads and provide controlled separation if design loads are exceeded.	Leak test of hose, hose coupler and hose string Visual inspection of hawser assembly and offloading hose Inspection/maintenance of: 1.mooring system incl. hawser/chain/winch 2.Pressure test of offloading hose	PM	Offloading hose, hose coupler, hawser and hose string	PREVENT - Offloading operations	SCS P11
		10	Bolted flanged joints, swivel joints, instrumentation/small bore tubing and all hydrocarbon pipework, valves and orifice plates shall be free from degradation, damage or deformation.	Inspection program (static mechanical) Bolted joints: records of bolt torques or loads	PM	Offloading - static mechanical	PREVENT - Offloading operations	SCS P11
		11	The reliability of the Shuttle Tanker & FPSO Telemetry systems shall be achieved by the use of duplicated fail-safe telemetry systems operating in parallel and duplicated UHF radio transceivers with automatic changeover.	Inspection of fail-safe telemetry system and automatic changeover for UHF radio transceivers Part of loading procedure	PM	Offloading - telemetry	PREVENT - Offloading operations	SCS P11

Acronym

Definition

AFA	Authorization for Alteration (BP internal name for modification projects)
AFFF	Aqueous Film Forming Foams
AFP	Automatic Fire Protection
AHC	Active Heave Compensation
AIS	Automatic Identification System
AIT	Auto-Ignition Temperature
ALLMS	Anchor Leg Load Monitoring System
APS	Abandon Platform Shutdown

Acronym	Definition
ATEX	ATmosphere EXplosibles (French: Explosive Atmospheres)
BPN	BP Norway
CCR	Cargo Control Room
CPSR	Control Protection Safety Register
CVI	Close Visual Inspection
DEH	Direct Electrical Heating
DGPS	Differential Global Positioning System
DHSV	Down-hole Safety Valve
DIFFS	Deck-Integrated Fire Fighting System
DNV	Det Norske Veritas
DOP	Delayed Operation (Failure mode codes, ISO14224)
EBIRP	Electronic Position Indicating Radio Beacons
EPA	Emergency Preparedness Analysis
ERO	Erratic Output (Failure mode codes, ISO14224)
ESD	Emergency Shutdown
EUPS	Emergency Uninterruptable Power Supply
FPSO	Floating Production Storage offloading vessel
FROG	Offshore Personnel Transfer Device (FROG is typical model name)
FSV	Flow Safety Valve
FTC	Failure to close on demand (Failure mode codes, ISO14224)
FTF	Failure to function on demand (Failure mode codes, ISO14224)
FTO	Failure to open on demand (Failure mode codes, ISO14224)
FTS	Failure to start on demand (Failure mode codes, ISO14224)
GMDSS	Global Maritime Distress and Safety System
GPA	General Public Alarm
GRE	Glass Reinforced Epoxy

Acronym	Definition
GVI	General Visual Inspection
HIPPS	High-Integrity Pressure Protection System
HMI	Human-Machine Interface
HPU	Hydraulic Power Unit
HSE	Health, Safety, Environment
HVAC	Heating, Ventilation, and Air Conditioning
ICS	Integrated Control System
IMS	Integrity Management Strategy
INL	Internal Leakage (Failure mode codes, ISO14224)
IOPPS	Inlet Overpressure Protection System
ISC	Instrumented Safety Control
LCP	Leakage in closed position (Failure mode codes, ISO14224)
LOO	Low Output (Failure mode codes, ISO14224)
LOPA	Layers of Protection Analysis
MAC	Manual Alarm Call
MCP	Manual Call Point
MOB	Man Overboard Boat
MOC	Management of Change
NDT	Non-Destructive Testing
NMD	Norwegian Maritime Directorate
NOO	No output (Failure mode codes, ISO14224)
OSD	Offloading Shutdown
PABX	Private Automated Branch Exchange (telephone system)
PAGA	Public Address & General Alarm System
PFP	Passive Fire Protection
PLC	Programmable Logic Controller

Acronym	Definition
PLU	Plugged (Failure mode codes, ISO14224)
PMR	Preventive Maintenance Routine
PMS	Power Management System
POB	Personnel Onboard
PRS	Positioning Reference System
PSA	Petroleum Safety Authority
PSD	Process Shutdown
PSV	Pressure Safety Valve
PTIL	Petroleumstilsynet (Petroleum Safety Authority)
RNNP	Risikonivå i norsk petroleumsvirksomhet (The trends in risk level in the petroleum activity)
ROV	Remotely Operated Underwater Vehicle
SART	Search and Rescue Transponder
SBS	Safety Barrier System
SCE	Safety Critical Element
SCS	Safety Critical System
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SOLAS	Safety of Life at Sea (Organization)
SRS	Safety Requirement Specification
SSIV	Subsea Safety Isolation Valve
UHF	Ultra High Frequency (radio)
UPS	Uninterruptible Power Supply
VGM	Vent Gas Monitoring
VHF	Very High Frequency (radio)

Appendix B. The main table of the results

Due to the limited time and manpower, only SBE has been analyzed further, however, the same approach may be adapted for SCE as well. The technical barrier functions and equipment groups which represent technical barriers have been defined in the 1 and 2 steps of case study. This part connects these technical barriers with relevant data required for effective and efficient maintenance management and PM program creation; see the third part of the thesis “Maintenance of risk reducing measures”.

GL 070 (2004), former OLF – 070, is an adaptation of the IEC 61508 / 61511 standards for the NCS which contains the SIS-scope functionalities and predefined minimal SIL for them. If functionality falls under GL-070 then related equipment is subject to full function (proof) testing and relevant data from corresponding SRS should be used.

ISO14224 annex F “Classification and definition of safety-critical failures” contains some typical dangerous failures for some common safety systems/components. However, it must be noted that just a part of required functionalities are covered by the mentioned standard (“not defined” where it doesn’t, see table 4). It is believed that PS functionalities could be used to expand the standardized functionalities, but this is not in the scope of this study.

Finally, the list of standardized PM routines is established. This would help to optimize the maintenance activities as the same PM routine for equipment can be used without referring to its safety function, i.e. same type level transmitter will have the same standardized PM routine. But if the level transmitter is a part of SIS, then it is subjected to proof testing and corresponding test routine will be attached to it.

Technical barriers			PS		Proof testing	Functional testing (partial)			Periodic maintenance
Role	Risk-reducing function group	Equipment group	PS	PS No.	SIL min req. (GL-070)	Equipment class ISO14224	Failure definitions ISO14224	Applicable failure modes ISO14224	Generic periodic maintenance activities
SBS C1	CONTROL - process safety	PSD (incl HIPPS & IOPPS) system - initiator	PS14	2, 5, 6, 7, 8	SIL1-3, SRS scope	Input devices	Function Sensor does not give signal or gives erroneous signal (exceeding predefined acceptance limits).	NOO, ERO	Instrumentation, Transmitter, Pressure Instrumentation, Transmitter, Level Instrumentation, Transmitter, Temperature

Role	Risk-reducing function group	Equipment group	PS	PS No.	SIL min req. (GL-070)	Equipment class ISO14224	Failure definitions ISO14224	Applicable failure modes ISO14224	Generic periodic maintenance activities
SBS C1	CONTROL - process safety	PSD system - logic	PS14	2, 5, 6, 7, 8	SIL1-3, SRS scope	Control units	Not defined	Not defined	Instrumentation, Controller, Standard industrial PLC Instrumentation, Controller, Programmable safety system Instrumentation, Controller, Hardwired safety system
SBS C1	CONTROL - process safety	PSD system - final element	PS14	2, 5, 6, 7, 8	SIL1-3, SRS scope	Valves	Function Valve fails to close upon signal or within a specified time.	FTC, DOP, LCP, INL	Mechanical, Valve, PSD incl. actuator Valve, Solenoid/pilot
SBS C1	CONTROL - process safety	PSV	PS14	3	N/A	Valves	Function Valve fails to open at the lesser than 120 % of set pressure or at 5 MPa above set pressure.	FTO	Mechanical, Valve, Pressure relief
SBS C1	CONTROL - process safety	FSV	PS14	4	N/A	Valves	Not defined	Not defined	Mechanical, Valve, Flow restriction
SBS C2	CONTROL - ignition source disconnection	Ignition source disconnection system	PS6	5	SIL2, SRS scope	Not defined	Not defined	Not defined	Electrical, Circuit Breaker
SBS C3	CONTROL - well isolation	X-mas valves	PS17	2, 3	SIL3, SRS scope	Xmas tree	Function Valve fails to close upon signal or within a specified time limit.	FTC, DOP	Mechanical, Valve, X-mas tree
							Leakage Internal leakage higher than specified value at first test.	LCP, INL	
SBS C3	CONTROL - well isolation	DHSV	-	-	SIL3, SRS scope	Well completion equipment	Function Valve fails to close upon signal or within a specified time limit.	FTC, DOP	Mechanical, Valve, DHSV
							Internal leakage higher than specified value.	INL, LCP	

Role	Risk-reducing function group	Equipment group	PS	PS No.	SIL min req. (GL-070)	Equipment class ISO14224	Failure definitions ISO14224	Applicable failure modes ISO14224	Generic periodic maintenance activities
SBS C4	CONTROL - emergency shutdown	ESD - input	PS 4	10	SIL2, SRS scope	Input devices	Function The ESD logic does not receive a signal from the push button when activated.	NOO, LOO, FTF	Instrumentation, Pushbutton, ESD
SBS C4	CONTROL - emergency shutdown	ESD logic	PS 4	6, 9	SIL2, SRS scope	Control units	Not defined	Not defined	Instrumentation, Controller, Standard industrial PLC Instrumentation, Controller, Programmable safety system Instrumentation, Controller, Hardwired safety system
SBS C4	CONTROL - emergency shutdown	ESD Riser valves	PS 4	1, 2, 3	SIL2, SRS scope	Valves	Function Valve fails to close upon signal or within a specified time limit.	FTC, DOP	Mechanical, Valve, Riser ESD Mechanical, Valve, Solenoid/pilot
							Leakage Internal leakage higher than specified value.	INL, LCP	
SBS C4	CONTROL - emergency shutdown	SSIV valves	PS 4 PS 34	1, 2, 3 6	SIL3, SRS scope	Subsea isolation equipment	Not defined	Not defined	Mechanical, Valve, Subsea Isolation Mechanical, Valve, Solenoid/pilot
SBS C4	CONTROL - emergency shutdown	ESD topside valves	PS 4	3, 4, 5, 8	SIL2, SRS scope	Valves	Function Valve fails to close upon signal or within a specified time limit.	FTC, DOP	Mechanical, Valve, Topside ESD incl. actuator Mechanical, Valve, Solenoid/pilot
							Leakage Internal leakage higher than specified value.	LCP, INL	
SBS C5	CONTROL - blowdown	Blowdown, valves	PS13	2, 5	SIL2, SRS scope	Valves	Valve Valve fails to open upon signal or within specified time limit.	FTO, DOP	Mechanical, Valve, Blowdown incl. actuator Mechanical, Valve, Solenoid/pilot

Role	Risk-reducing function group	Equipment group	PS	PS No.	SIL min req. (GL-070)	Equipment class ISO14224	Failure definitions ISO14224	Applicable failure modes ISO14224	Generic periodic maintenance activities
SBS C5	CONTROL - blowdown	Blowdown, instrumentation	PS13	3, 6	SIL2, SRS scope	Input devices	Function Sensor does not give signal or gives erroneous signal (exceeding predefined acceptance limits).	NOO, ERO	Instrumentation, Transmitter, Pressure Instrumentation, Transmitter, Level Instrumentation, Transmitter, Temperature
SBS C5	CONTROL - blowdown	Blowdown, heat tracing	PS13	4	N/A	Heaters and boilers	Not defined	Not defined	Electrical, Heat Tracing
SBS C5	CONTROL - blowdown	Flare, tip	PS13	7	N/A	Not defined	Not defined	Not defined	Mechanical, Flare tip
SBS D1	DETECT - gas detection	Gas detectors	PS3a	1, 2, 3, 7	SIL2, SRS scope	Fire and gas detectors	Detector (catalytic, optical point, H2S and H2) Fire and gas logic does not receive signal equivalent to upper alarm limit when testing with prescribed test gas.	NOO, LOO	Instrumentation, Detector, Gas catalytic Instrumentation, Detector, Gas point Instrumentation, Detector, H2S/H2
						Fire and gas detectors	Detector (optical line) Fire and gas logic does not receive signal equivalent to upper alarm limit when testing with prescribed test filter.	NOO, LOO	Instrumentation, Detector, Gas line
						Fire and gas detectors	Detector (acoustic) Fire and gas logic does not receive signal when tested.	NOO, LOO	Instrumentation, Detector, Gas acoustic

Role	Risk-reducing function group	Equipment group	PS	PS No.	SIL min req. (GL-070)	Equipment class ISO14224	Failure definitions ISO14224	Applicable failure modes ISO14224	Generic periodic maintenance activities
SBS D2	DETECT - fire detection	Fire detectors	PS3a	1, 2, 3	SIL2, SRS scope	Fire and gas detectors	Detector Fire and gas logic does not receive signal from detector, when detector is tested.	NOO, LOO, FTF	Instrumentation, Detector, Smoke conv. Instrumentation, Detector, Heat conv. Instrumentation, Detector, Flame conv.
SBS D3	DETECT - F&G logic	F&G logic	PS3a PS3b PS11	4 4 4	SIL2, SRS scope	Control units	Not defined	Not defined	Instrumentation, Controller, Standard industrial PLC Instrumentation, Controller, Programmable safety system Instrumentation, Controller, Hardwired safety system
SBS D4	DETECT - Manual Call Points	Manual Call Points / Alarm	PS3a PS3b	5 5,8	SIL2, SRS scope	Input devices	Manual call point Fire and gas logic does not receive a signal from the pushbutton when activated.	NOO, LOO, FTF	Instrumentation, Pushbutton, Alarm
SBS E1	EM RESPONSE - Emergency power	Emergency generator	PS10	1, 4, 5, 13	IEC61508/11 is applicable	Electric Generator	Function Emergency generator fails to start or gives wrong voltage upon start.	FTS, LOO	Electrical, Electrical Generator
SBS E1	EM RESPONSE - Emergency power	Emergency switchboards	PS10	2	N/A	Switchgears/switchboards and distribution boards	Not defined	Not defined	Electrical, Electrical Boards
SBS E1	EM RESPONSE - Emergency power	Emergency UPS	PS10 PS11	7,11, 12, 14, 15 3, 9, 15	IEC61508/11 is applicable	Uninterruptible power supply	Function Battery capacity too low.	FOV	Electrical, Uninterruptible power
SBS E1	EM RESPONSE - Emergency power	Emergency lighting	PS10	8, 9, 10	N/A	Not defined	Not defined	Not defined	Electrical, Lightening fixtures

Role	Risk-reducing function group	Equipment group	PS	PS No.	SIL min req. (GL-070)	Equipment class ISO14224	Failure definitions ISO14224	Applicable failure modes ISO14224	Generic periodic maintenance activities
SBS E1	EM RESPONSE - Emergency power	Essential Diesel Generator	PS 32	13	IEC61508/11 is applicable	Electric Generator	Function Emergency generator fails to start or gives wrong voltage upon start.	FTS, LOO	Electrical, Electrical Generator
SBS E2	EM RESPONSE - Emergency communication	PA system	PS11	1, 2	N/A	Not defined	Not defined	Not defined	Telecom, PA
SBS E2	EM RESPONSE - Emergency communication	UHF radio and paging system	PS11	5, 6	N/A	Not defined	Not defined	Not defined	Telecom, UHF
SBS E2	EM RESPONSE - Emergency communication	PABX telephone system	PS11	7, 13	N/A	Not defined	Not defined	Not defined	Telecom, PABX
SBS E2	EM RESPONSE - Emergency communication	Crane communication	PS11	8, 13	N/A	Not defined	Not defined	Not defined	Telecom, Crane
SBS E2	EM RESPONSE - Emergency communication	Emergency radio links	PS11	10	N/A	Not defined	Not defined	Not defined	Telecom, Radio links
SBS E2	EM RESPONSE - Emergency communication	Emergency satellite	PS11	11	N/A	Not defined	Not defined	Not defined	Telecom, satellite
SBS E2	EM RESPONSE - Emergency communication	GMDSS	PS11	12, 13	N/A	Not defined	Not defined	Not defined	Telecom, GMDSS
SBS E3	EM RESPONSE - Rescue	MOB boat and its lifting appliances	PS18	1, 3	N/A	Evacuation equipment	Not defined	Not defined	Mechanical, Rescue, MOB
SBS E3	EM RESPONSE - Rescue	FROG	PS18	4	N/A	Evacuation equipment	Not defined	Not defined	Inspection, Rescue, FROG
SBS E3	EM RESPONSE - Rescue	Safety showers / Eye baths	PS18	5	N/A	Evacuation equipment	Not defined	Not defined	Mechanical, Rescue, Safety showers/eye baths

Role	Risk-reducing function group	Equipment group	PS	PS No.	SIL min req. (GL-070)	Equipment class ISO14224	Failure definitions ISO14224	Applicable failure modes ISO14224	Generic periodic maintenance activities
SBS E3	EM RESPONSE - Rescue	Safety station cabinets	PS18	6	N/A	Evacuation equipment	Not defined	Not defined	Inspection, Rescue, Safety station cabinets
SBS E3	EM RESPONSE - Rescue	First Aid Kits	PS18	7	N/A	Evacuation equipment	Not defined	Not defined	Inspection, Rescue, First Aid
SBS E3	EM RESPONSE - Rescue	Smoke hoods / Breathing masks	PS18	8	N/A	Evacuation equipment	Not defined	Not defined	Inspection, Rescue, Smoke eq.
SBS E4	EM RESPONSE - Evacuation	Escape routes & tunnel	PS12a	1,2, 8	N/A	Evacuation equipment	Not defined	Not defined	Inspection, Rescue, Escape route
SBS E4	EM RESPONSE - Evacuation	Lifejackets & Survival suits	PS12a	12	N/A	Evacuation equipment	Not defined	Not defined	Inspection, Rescue, Lifejackets / Survival suits
SBS E5	EM RESPONSE - Lifeboats & Rafts w/escape chutes	Lifeboat	PS12b PS11	1, 3, 4, 5, 6, 8, 9 14	N/A	Evacuation equipment	Not defined	Not defined	Mechanical, Rescue, Lifeboat
SBS E5	EM RESPONSE - Lifeboats & Rafts w/escape chutes	Life rafts	PS12a	9	N/A	Evacuation equipment	Not defined	Not defined	Mechanical, Rescue, Life raft
SBS E5	EM RESPONSE - Lifeboats & Rafts w/escape chutes	Escape chutes	PS12a	10, 14	N/A	Evacuation equipment	Not defined	Not defined	Mechanical, Rescue, Escape chutes
SBS E5	EM RESPONSE - Lifeboats & Rafts w/escape chutes	Launching and recovery appliances for life boats	PS12a PS12b	11 2, 7, 10	N/A	Winches	Not defined	Not defined	Mechanical, Rescue, Lifeboat launching
SBS M1	MITIGATE - Impact protection	Structural - green sea	PS 30	1, 2	N/A	Not defined	Not defined	Not defined	Inspection, Structural, Green sea

Role	Risk-reducing function group	Equipment group	PS	PS No.	SIL min req. (GL-070)	Equipment class ISO14224	Failure definitions ISO14224	Applicable failure modes ISO14224	Generic periodic maintenance activities
SBS M1	MITIGATE - Impact protection	Structural - subsea protection	PS 34	1	N/A	Not defined	Not defined	Not defined	Inspection, Structural, Subsea protection
SBS M10	MITIGATE - CO2/Inergen system	CO2/Inergen	PS8	27, 28, 31	SRS scope	Valves	Function Release valve fails to open upon test.	FTO	Mechanical, Valve, Inergen incl. act. & sol.
					N/A	Inert-gas equipment	Not defined	Not defined	Mechanical, Inert-gas eq.
SBS M11	MITIGATE - Water mist system	Water mist system	PS8	29, 31	SRS scope	Valves	Function Release valve fails to open upon test.	FTO	Mechanical, Valve, Water mist incl. act. & sol.
SBS M12	MITIGATE - Open drain	Open drain boxes, drip trays	PS7	1, 2, 3	N/A	Not defined	Not defined	Not defined	Inspection, Open drain
SBS M12	MITIGATE - Open drain	Open drain liquid seals	PS7	4	N/A	Not defined	Not defined	Not defined	Inspection, Open drain
SBS M12	MITIGATE - Open drain	Open drain piping	PS7	5, 6	N/A	Piping	Not defined	Not defined	Inspection, Open drain
SBS M12	MITIGATE - Open drain	Open drain level instruments	PS7	7	N/A	Input devices	Not defined	Not defined	Instrumentation, Transmitter, Pressure Instrumentation, Transmitter, Level Instrumentation, Transmitter, Temperature
SBS M12	MITIGATE - Open drain	Open drain nitrogen	PS7	8	N/A	Inert-gas equipment	Not defined	Not defined	Mechanical, Inert-gas eq.
SBS M12	MITIGATE - Open drain	Heaters, drain system	PS7	10	N/A	Heaters and boilers	Not defined	Not defined	Electrical, Heaters
SBS M2	MITIGATE - Passive fire protection	Structural: fire walls, blast panels	PS1 PS9	1, 2, 3, 4	N/A	Not defined	Not defined	Not defined	Inspection, Structural, Fire/Blast walls
SBS M2	MITIGATE - Passive fire protection	Fire dampers	PS6	6, 8, 9, 12	IEC61508/11 is applicable	Not defined	Function Damper fails to close upon signal.	-	Mechanical, HVAC, Fire Dampers
SBS M2	MITIGATE - Passive fire protection	PFP insulation	PS9	1, 6, 7	N/A	Not defined	Not defined	Not defined	Inspection, PFP
SBS M2	MITIGATE - Passive fire protection	Fire doors/self-closing doors	PS9 12a	5, 8, 6, 7	N/A	Not defined	Not defined	Not defined	Mechanical, Fire doors

Role	Risk-reducing function group	Equipment group	PS	PS No.	SIL min req (GL-070)	Equipment class ISO14224	Failure definitions ISO14224	Applicable failure modes ISO14224	Generic periodic maintenance activities
SBS M3	MITIGATE - FW supply	FW piping	PS8	2	N/A	Piping	Not defined	Not defined	Inspection, Piping, FW
SBS M3	MITIGATE - FW supply	FW strainers, screens	PS8	3	N/A	Piping	Not defined	Not defined	Inspection, Strainers, FW
SBS M3	MITIGATE - FW supply	FW chlorination	PS8	4	N/A	Not defined	Not defined	Not defined	Mechanical, Chlorination FW
SBS M3	MITIGATE - FW supply	FW heaters and heat tracing	PS8	5, 14	N/A	Heaters and boilers	Not defined	Not defined	Electrical, Heaters & Heater tracing
SBS M3	MITIGATE - FW supply	FW supply valves	PS8	6	N/A	Valves	Not defined	Not defined	Mechanical, Valve, FW
SBS M4	MITIGATE - FW pumps	Fire pumps	PS8	1, 8-12, 31	SIL2, SRS scope	Pumps	Function Fire pump fails to start upon signal.	FTS	Mechanical, Pump, FW Mechanical, Motor diesel Electric, Motor electrical
							Capacity Fire pump delivers less than 90 % of design capacity.	LOO	
SBS M5	MITIGATE - Deluge	Deluge	PS7 PS8	9 1, 13, 15, 31	SIL2, SRS scope	Valves	Deluge valve Deluge valve fails to open when tested.	FTO, DOP	Mechanical, Valve, Deluge incl. act. & sol.
						Nozzles	Nozzle More than 3 % of the nozzles are plugged/ choked. Failures are reported per skid/loop.	PLU	
SBS M6	MITIGATE - FW input	FW instrumentation	PS8	7, 20	N/A	Input devices	Function Sensor does not give signal or gives erroneous signal (exceeding predefined acceptance limits).	NOO, ERO	Instrumentation, Transmitter, Pressure Instrumentation, Transmitter, Level Instrumentation, Transmitter, Temperature

Role	Risk-reducing function group	Equipment group	PS	PS No.	SIL min req (GL-070)	Equipment class ISO14224	Failure definitions ISO14224	Applicable failure modes ISO14224	Generic periodic maintenance activities
SBS M6	MITIGATE - FW input	FW manual release	PS8	30	N/A	Input devices	Function The F&G logic does not receive a signal from the push button when activated.	NOO, LOO, FTF	Instrumentation, Pushbutton, F&G
SBS M7	MITIGATE - AFFF	AFFF	PS8	16-19, 31	N/A	Not defined	Function Water/foam does not reach fire area upon test.	-	Mechanical, Firefighting, AFFF
SBS M8	MITIGATE - Manual firefighting	FW hydrants	PS8	21--1	N/A	Fire-fighting equipment	Not defined	Not defined	Mechanical, Firefighting, Hydrants
SBS M8	MITIGATE - Manual firefighting	FW hoses	PS8	21--2, 25	N/A	Fire-fighting equipment	Not defined	Not defined	Mechanical, Firefighting, Hoses
SBS M8	MITIGATE - Manual firefighting	FW monitors	PS8	21--3, 24	N/A	Fire-fighting equipment	Not defined	Not defined	Mechanical, Firefighting, Monitors
SBS M8	MITIGATE - Manual firefighting	FW portable extinguishers	PS8	22, 26	N/A	Fire-fighting equipment	Not defined	Not defined	Mechanical, Firefighting, Extinguishers
SBS M8	MITIGATE - Manual firefighting	Fireman equipment	PS18	9, 10	N/A	Fire-fighting equipment	Not defined	Not defined	Mechanical, Firefighting, Fireman eq.
SBS M9	MITIGATE - Helideck firefighting	DIFFS	PS8	23,24,25, 26	N/A	Not defined	Not defined	Not defined	Mechanical, Firefighting, DIFFS
SBS M13	MITIGATE - Emergency ballast	Ballast critical valves	PS 31	18	SIL1-2, SRS scope	Valves	Function Valve fails to operate on signal.	FTO, FTC, DOP	Mechanical, Valves, Ballast critical
SBS M13	MITIGATE - Emergency ballast	Ballast pumps	PS 31	2, 5	SIL1-2, SRS scope	Pumps	Function Pump fails to start/stop on signal.	FTS	Mechanical, Pump, Ballast Mechanical, Pump, Ballast manual
SBS M13						Pumps (manual)	Not defined	Not defined	
SBS M13	MITIGATE - Emergency ballast	Ballast HPU	PS 31	2, 5	N/A	Hydraulic power units	Not defined	Not defined	Mechanical, HPU, Ballast

Role	Risk-reducing function group	Equipment group	PS	PS No.	SIL min req (GL-070)	Equipment class ISO14224	Failure definitions ISO14224	Applicable failure modes ISO14224	Generic periodic maintenance activities
SBS M13	MITIGATE - Emergency ballast	Ballast ESD logic	PS 31	18	SIL1-2, SRS scope	Control units	Not defined	Not defined	Instrumentation, Controller, Standard industrial PLC Instrumentation, Controller, Programmable safety system Instrumentation, Controller, Hardwired safety system

Appendix C. The pilot list of standardized PM routines

An example list of standardized PM routines is shown below. This would help to optimize the maintenance activities as the same PM routine for equipment can be used without referring to its safety function, i.e. same type level transmitter will have the same standardized PM routine. But if the level transmitter is a part of SIS, then it is subjected to proof testing and corresponding proof test routine will be attached to it.

Generic periodic maintenance activities
Electrical, Circuit Breaker
Electrical, Electrical Boards
Electrical, Electrical Generator
Electrical, Heat Tracing
Electrical, Heaters
Electrical, Lightening fixtures
Electrical, Uninterruptible power
Inspection, Open drain
Inspection, PFP
Inspection, Piping, FW
Inspection, Strainers, FW
Inspection, Structural, Fire/Blast walls
Inspection, Structural, Green sea
Inspection, Structural, Subsea protection
Instrumentation, Controller, Hardwired safety system
Instrumentation, Controller, Programmable safety system
Instrumentation, Controller, Standard industrial PLC
Instrumentation, Detector, Flame conv.
Instrumentation, Detector, Gas acoustic
Instrumentation, Detector, Gas catalytic
Instrumentation, Detector, Gas line
Instrumentation, Detector, Gas point
Instrumentation, Detector, H2S/H2
Instrumentation, Detector, Heat conv.
Instrumentation, Detector, Smoke conv.
Instrumentation, Pushbutton, Alarm
Instrumentation, Pushbutton, ESD
Instrumentation, Pushbutton, F&G
Instrumentation, Transmitter, Level
Instrumentation, Transmitter, Pressure
Instrumentation, Transmitter, Temperature
Mechanical, Chlorination FW
Mechanical, Fire doors
Mechanical, Firefighting, AFFF
Mechanical, Firefighting, DIFFS
Mechanical, Firefighting, Extinguishers
Mechanical, Firefighting, Fireman eq.
Mechanical, Firefighting, Hoses
Mechanical, Firefighting, Hydrants
Mechanical, Firefighting, Monitors

Mechanical, Flare Tip
Mechanical, HPU, Ballast
Mechanical, HVAC, Fire Dampers
Mechanical, Inert-gas eq.
Mechanical, Motor, Diesel
Mechanical, Pump, Ballast
Mechanical, Pump, Ballast manual
Mechanical, Pump, FW
Mechanical, Rescue, Escape chutes
Mechanical, Rescue, Escape route
Mechanical, Rescue, First Aid
Mechanical, Rescue, FROG
Mechanical, Rescue, Lifeboat
Mechanical, Rescue, Lifeboat launching
Mechanical, Rescue, Lifejackets / Survival suits
Mechanical, Rescue, Life raft
Mechanical, Rescue, MOB
Mechanical, Rescue, Safety showers/eye baths
Mechanical, Rescue, Safety station cabinets
Mechanical, Rescue, Smoke eq.
Mechanical, Valve, Blow down incl. actuator
Mechanical, Valve, Deluge incl. act. & sol.
Mechanical, Valve, DHSV
Mechanical, Valve, Flow restriction
Mechanical, Valve, FW
Mechanical, Valve, Inergen incl. act. & sol.
Mechanical, Valve, Pressure relief
Mechanical, Valve, PSD incl. actuator
Mechanical, Valve, Riser ESD
Mechanical, Valve, Solenoid/pilot
Mechanical, Valve, Subsea Isolation
Mechanical, Valve, Topside ESD incl. actuator
Mechanical, Valve, Water mist incl. act. & sol.
Mechanical, Valve, X-mas tree
Mechanical, Valves, Ballast critical
Telecom, Crane
Telecom, GMDSS
Telecom, PA
Telecom, PABX
Telecom, Radio links
Telecom, Satellite
Telecom, UHF

Appendix D. Brief presentation of Master thesis “Control of Safety Barriers through Maintenance System”



Control of safety barriers through maintenance system

Brief presentation of Master thesis

ALEKSANDRAS ŠEVČIK

Abstract

Main objectives of the thesis

- (1) to create a new framework for safety barrier concept based on the process model of an accident and discuss risk-reducing measures following ISO 17776 and national regulations such as the Management Regulations from the PSA and
- (2) the incorporation of risk-reducing elements into the maintenance system to assure that maintenance routines cover their functional requirements

Structure of thesis

3 parts:

1 - RISK REDUCING MEASURES – “what is a barrier”

2 - MAINTENANCE OF RISK REDUCING MEASURES – “how to maintain a barrier”

3 – Case study – Skarv FPSO

1 - RISK REDUCING MEASURES – “what is a barrier” - summary

- Wide topic, no standardized definitions
- Must be researched because no standard on safety barrier exist, i.e. different parties have different understanding about barrier. Systematic risk exists due to potential failure of risk communication between involved parties.
- A new framework have been proposed in the thesis based on ISO17776 and PSA Regulations.
- Two conference papers have been written in addition to present this topic : Risk Analysis 2014 in WIT, London, 04-06 Jun , ESREL*, Wroclaw, 02-06 Sept.
- *The annual European Safety and Reliability Conference ESREL stems from a European initiative merging several national Conferences into a major yearly conference under the auspices of the European Safety and Reliability Association (ESRA).

1 - RISK REDUCING MEASURES – “what is a barrier” - objectives

50% of the problems in the world result from people using the same words with different meanings. The other 50% come from people using different words with the same meaning (Kaplan, 1997)

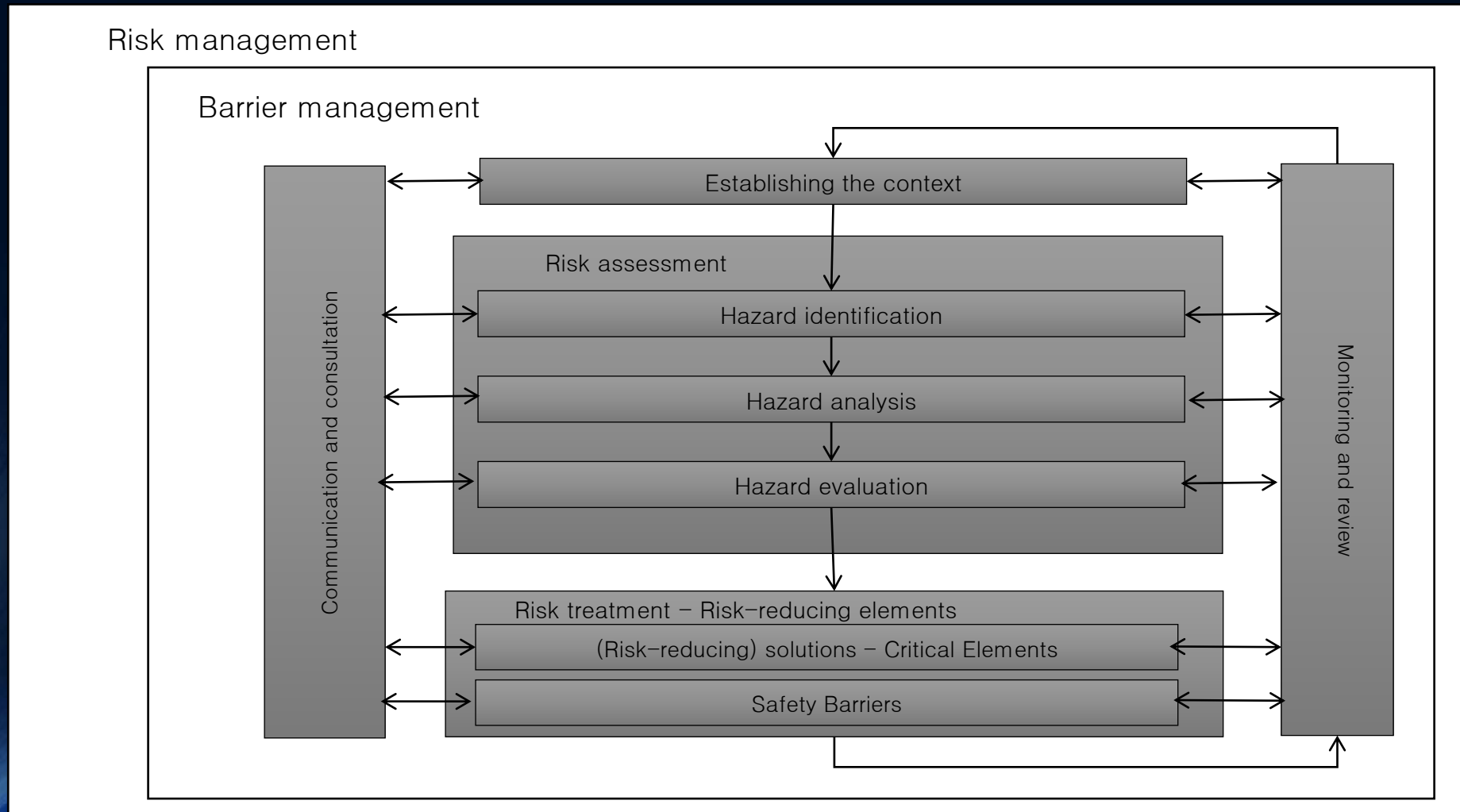
The main objective of this part is:

- (1) to discuss the concept of safety barrier and
- (2) to discuss the framework of work process from risk analysis to the maintenance of safety barriers

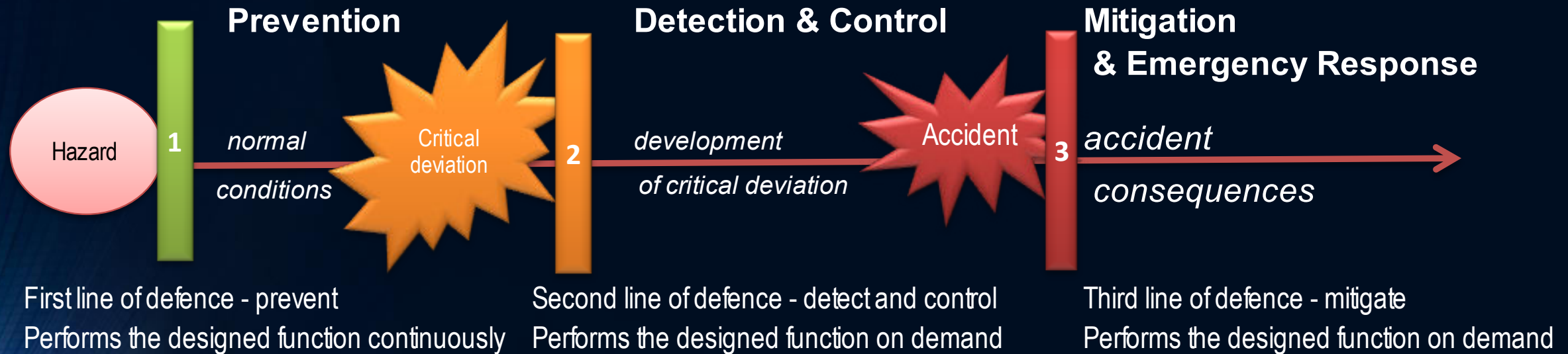
1 - RISK REDUCING MEASURES – “what is a barrier” – PSA Norway Regulations

- In reducing risk [...] 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.
- **The solutions and barriers** that have the greatest risk-reducing effect shall be chosen [...]

1 - RISK REDUCING MEASURES – “what is a barrier” – process (adapted from ISO31000)



1 - RISK REDUCING MEASURES – “what is a barrier” - linear accident model



1 - RISK REDUCING MEASURES – “what is a barrier” - proposed definitions

To prevent means

to reduce the likelihood that critical deviation occurs,

where critical deviation is seen as an initiating event of an unwanted chain of events (hazardous event)

To (detect&) control means

to reduce the likelihood that critical deviation will develop into a major accident once it occurs,

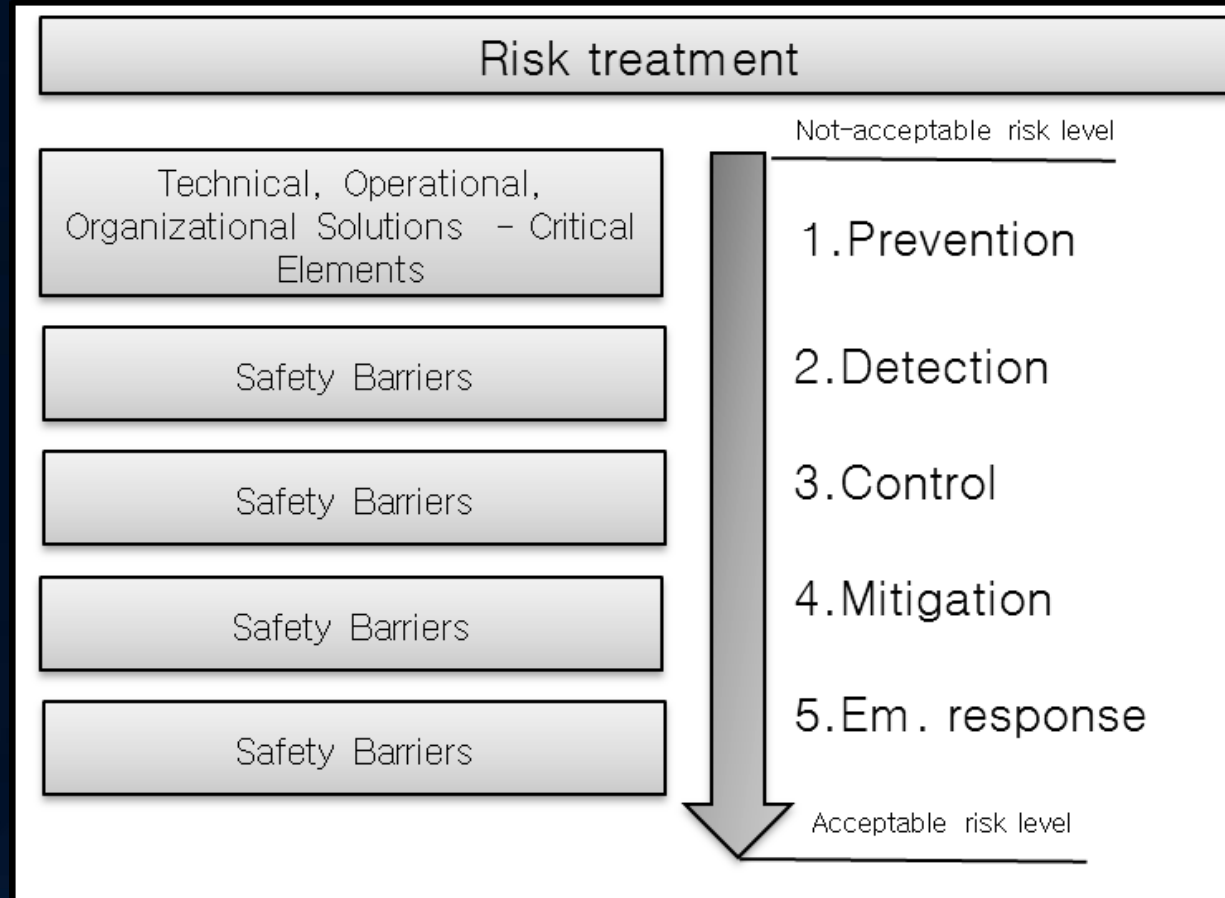
i.e. to stop the unwanted chain of events when critical deviation occurs

To mitigate (&emergency response) means

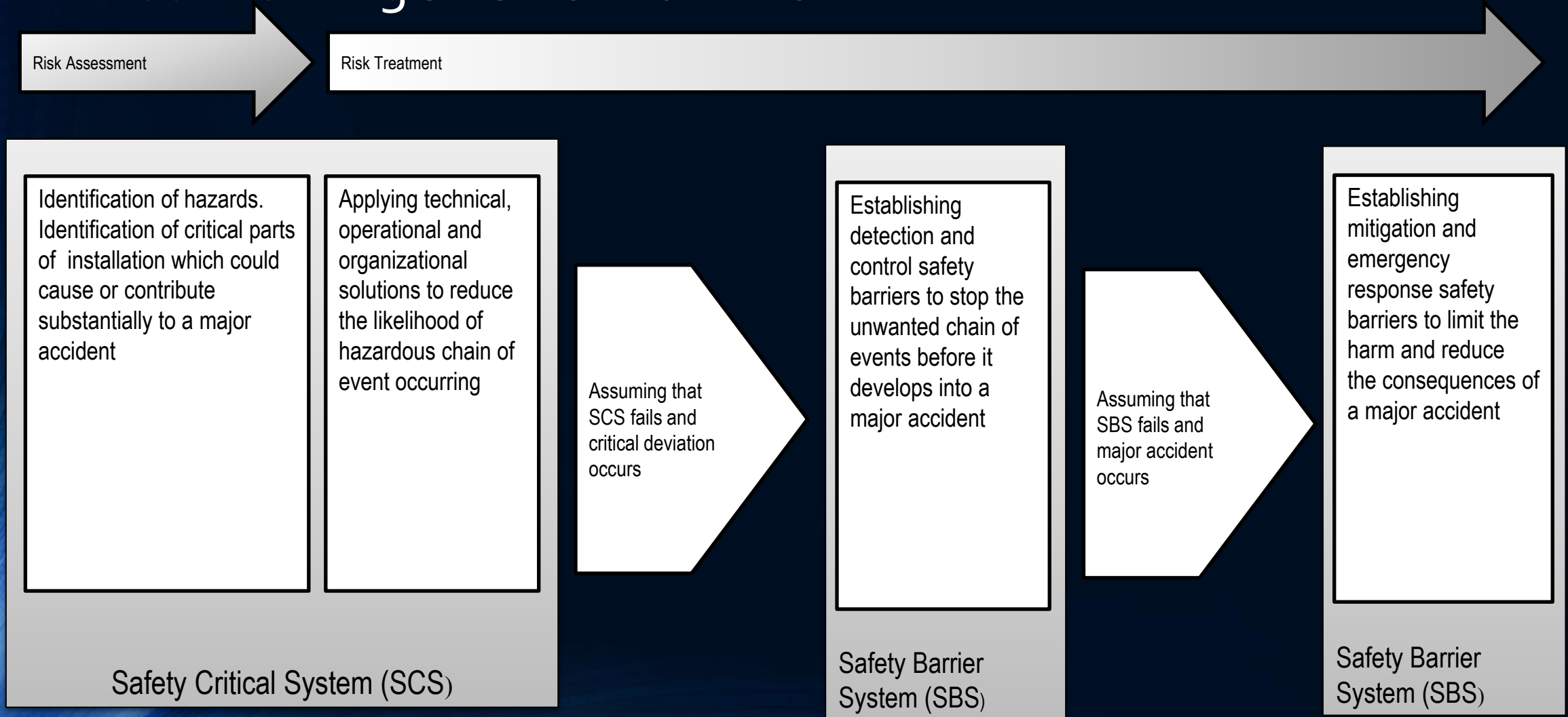
to reduce the consequences of a major accident once it occurs

i.e. to stop the unwanted chain of events when major accident occurs

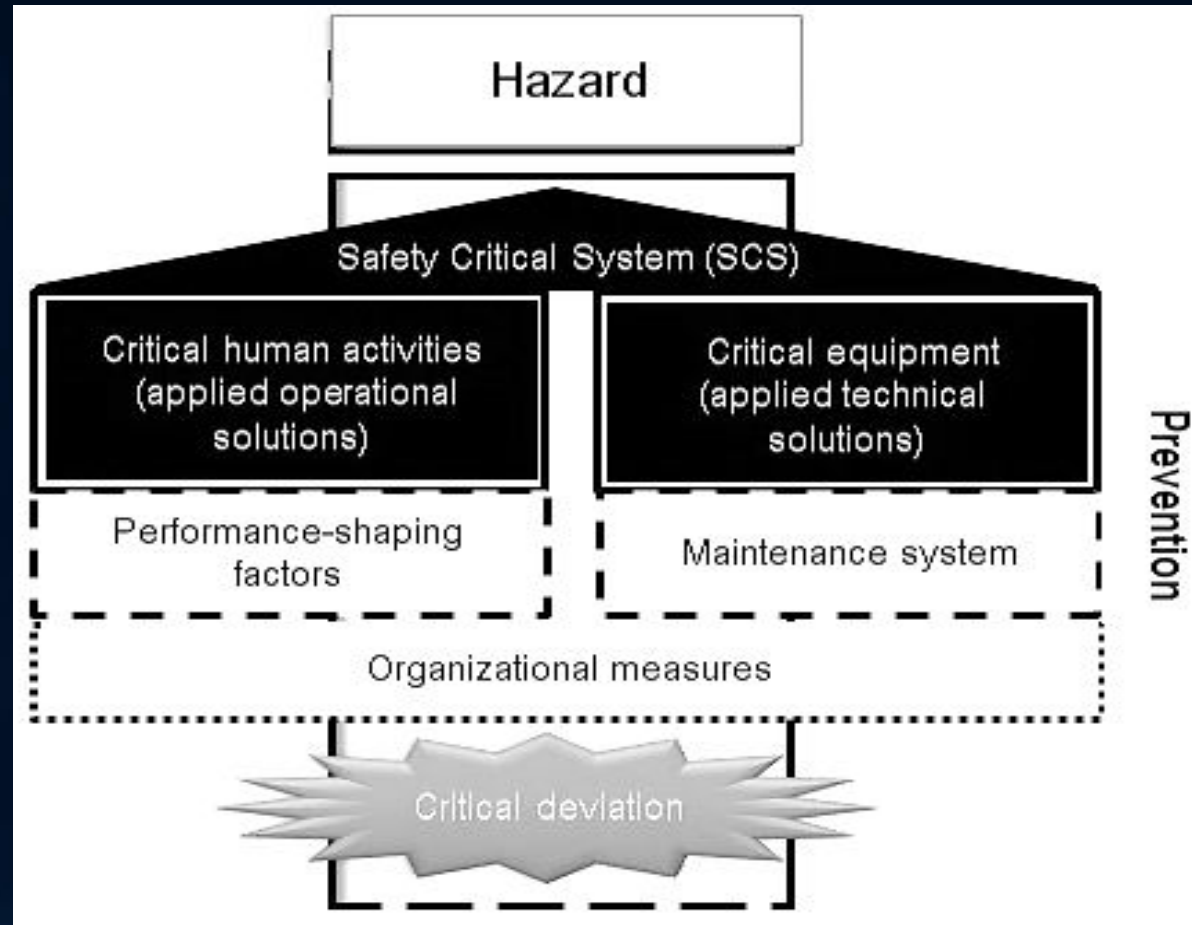
1 - RISK REDUCING MEASURES – “what is a barrier” - risk treatment (adapted from ISO17776)



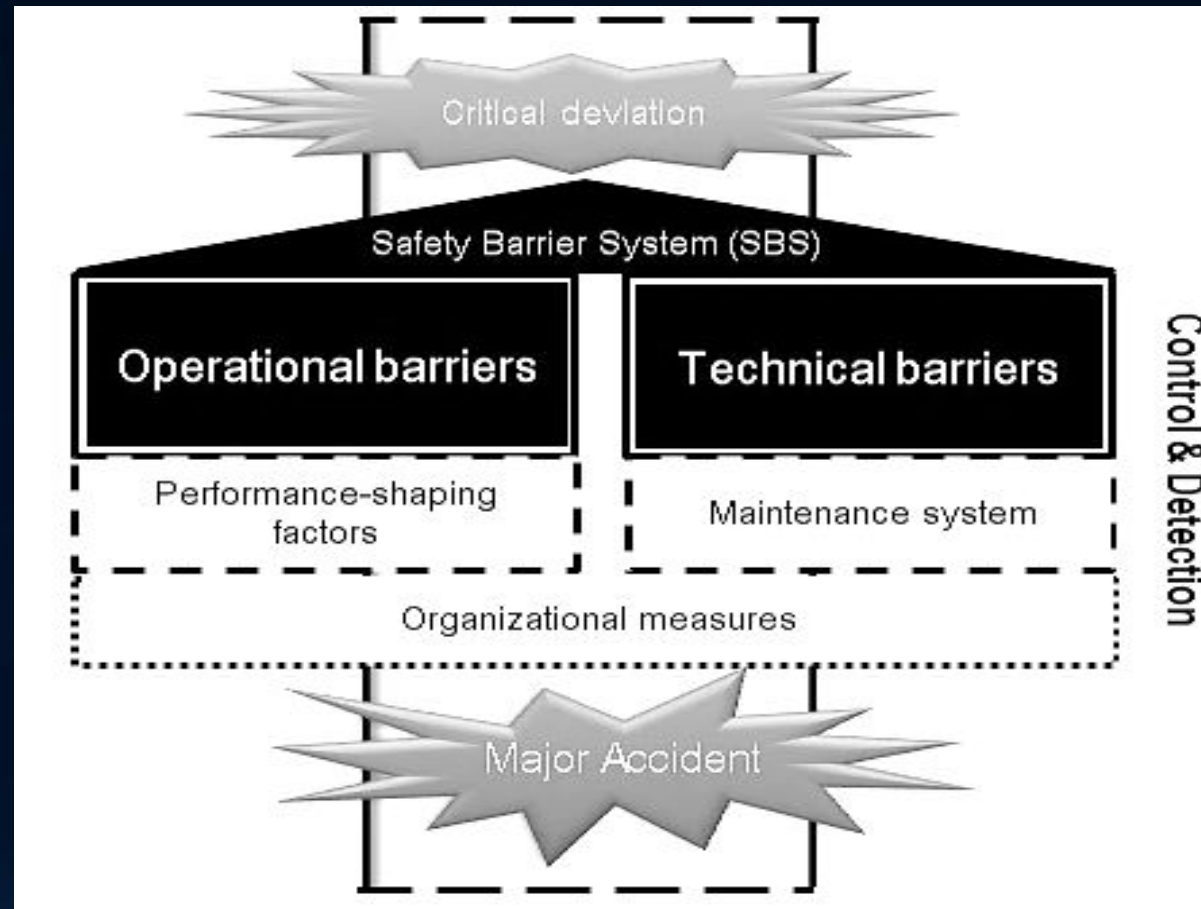
1 - RISK REDUCING MEASURES – “what is a barrier” - generic workflow



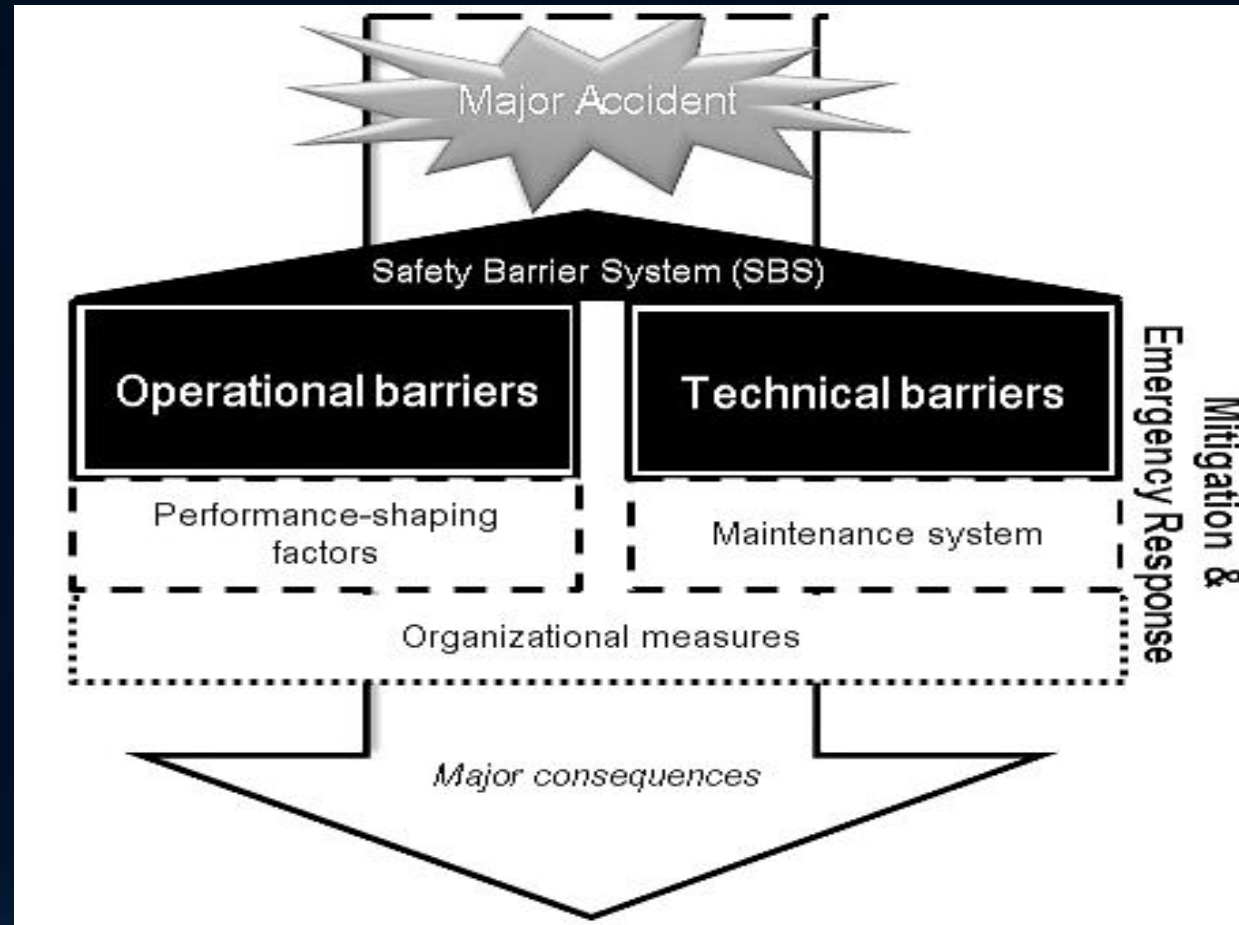
Safety Critical System – for prevention



Safety Barrier System – for detect & control



Safety Barrier System – for mitigation & emergency response



Comparison – technical elements

- Technical critical element - process equipment and related auxiliary equipment that is subjected to a specific hazard scenario. The failure of such equipment may result in critical deviation (initiating event). Example: hydrocarbon pipeline.
- Technical barrier element - a physical element that is established to perform safety functions related to stopping the unwanted chain of events when it has been started. Example: emergency shutdown valve.

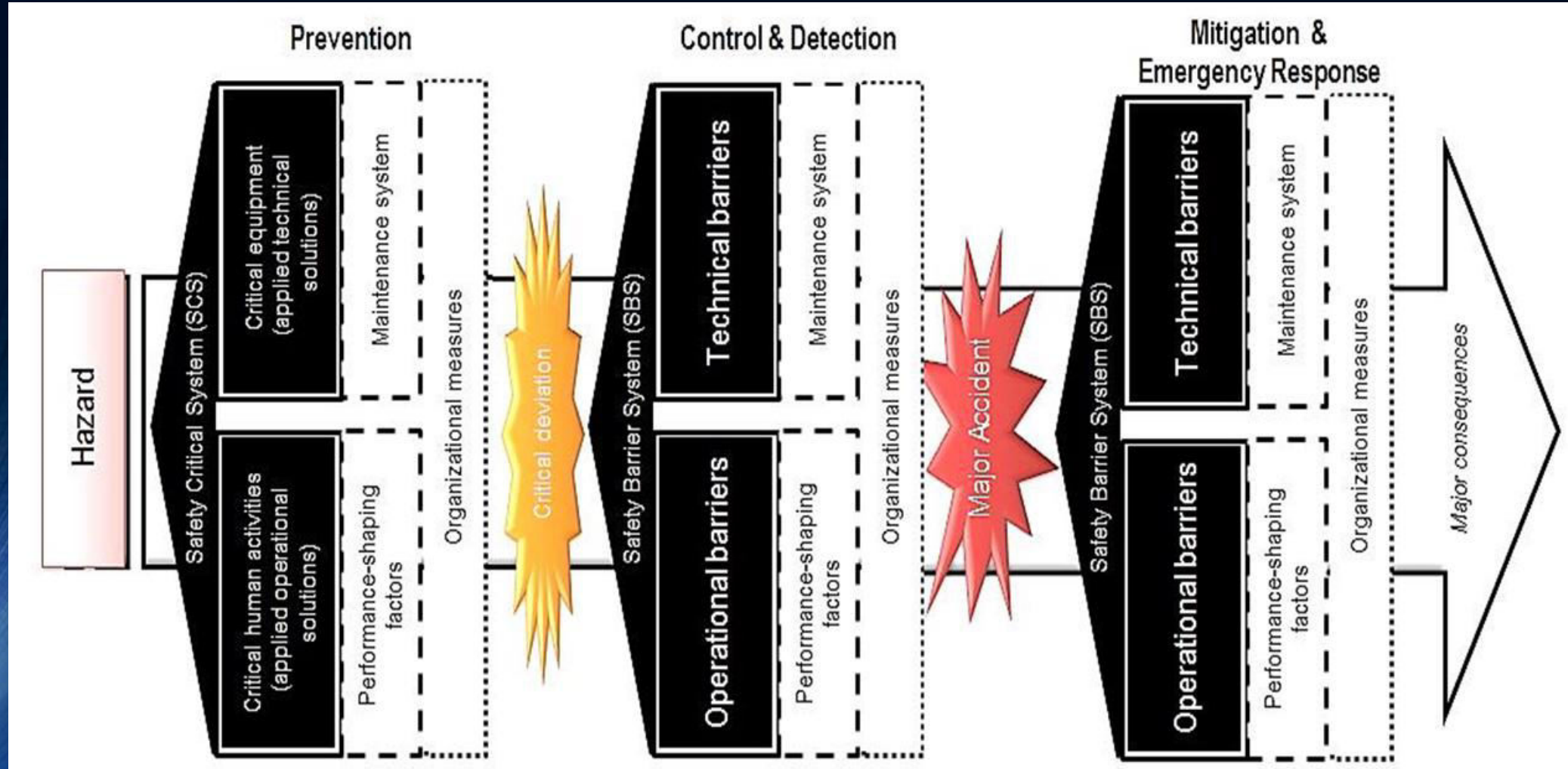
Comparison –operational elements

- Operational critical element - operational process activities performed by the operator. The failure of such activities may result in critical deviation (initiating event). Example: process control activities.
- Operational barrier element - specific actions that shall be carried out in the case of critical deviation to stop the development of an unwanted chain of events. Example: a manual activation of an evacuation alarm

1 - RISK REDUCING MEASURES – “what is a barrier” - SCS and SBS comparison

Safety Critical System (SCS)	Safety Barrier System (SBS)
Technical, operational and org. solutions applied to process, utilities, structural, etc. elements to reduce risk within them	Independent system designed only for risk-reducing functions
Reduces the likelihood of critical conditions occurring	Reduces the likelihood of critical conditions developing and limits the harm
Requirement to perform – constant (normal conditions)	Requirement to perform – on demand (abnormal conditions)
Cannot be removed without affecting process	Can be removed without affecting process

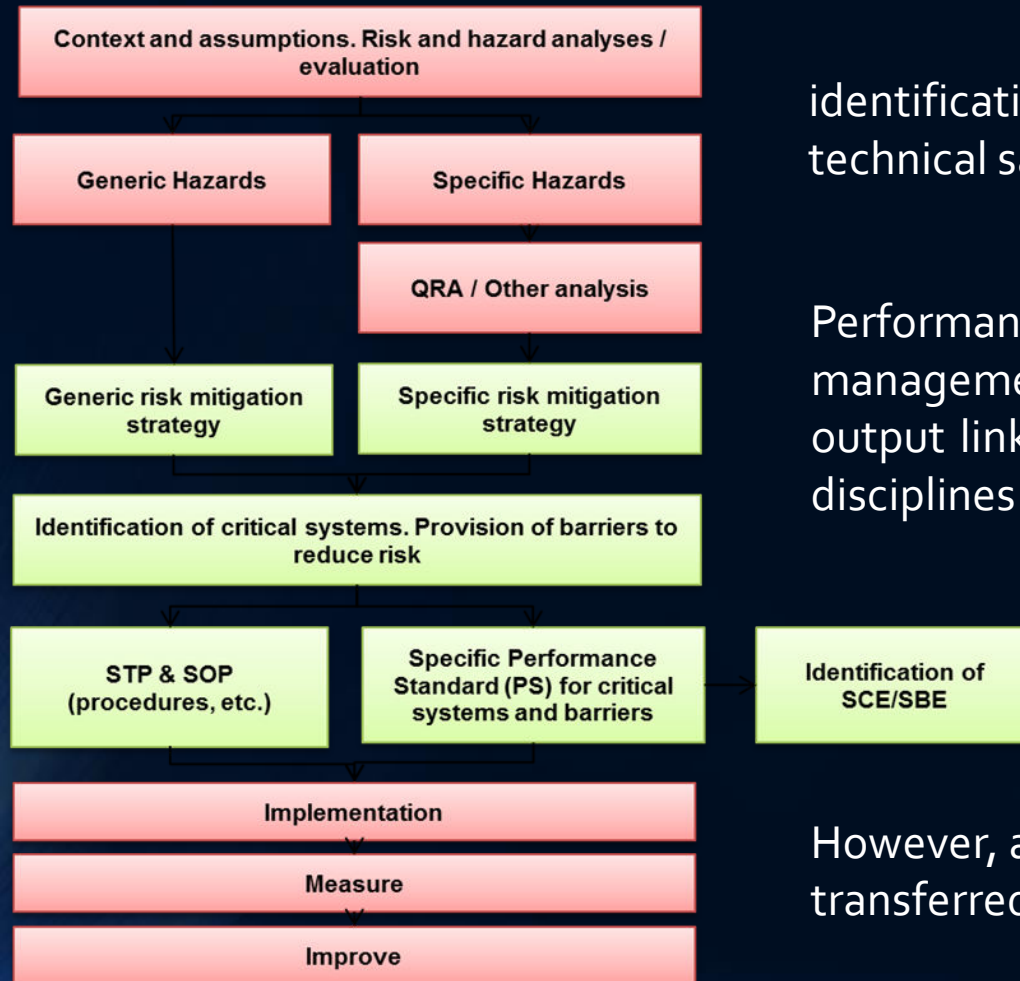
1 - RISK REDUCING MEASURES – “what is a barrier” – summary



2 - MAINTENANCE OF RISK REDUCING MEASURES – “how to maintain a barrier”

- The discussion is linked to the maintenance management for safety barriers
- Focus on actual problems in the current industry

PRACTICAL MAINTENANCE PROCESS FOR RISK REDUCING MEASURES

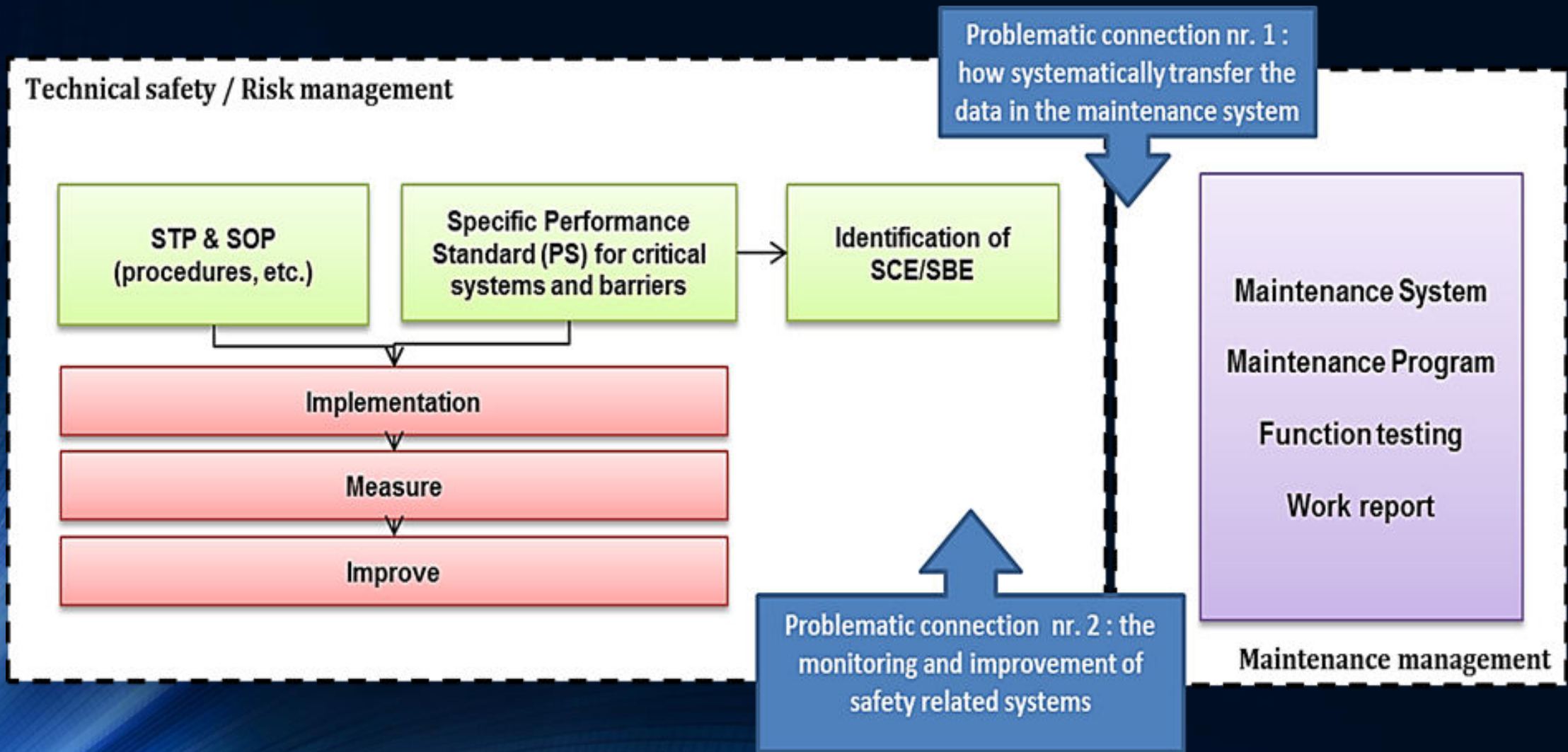


identification of systems and functions – is covered by technical safety / risk management disciplines

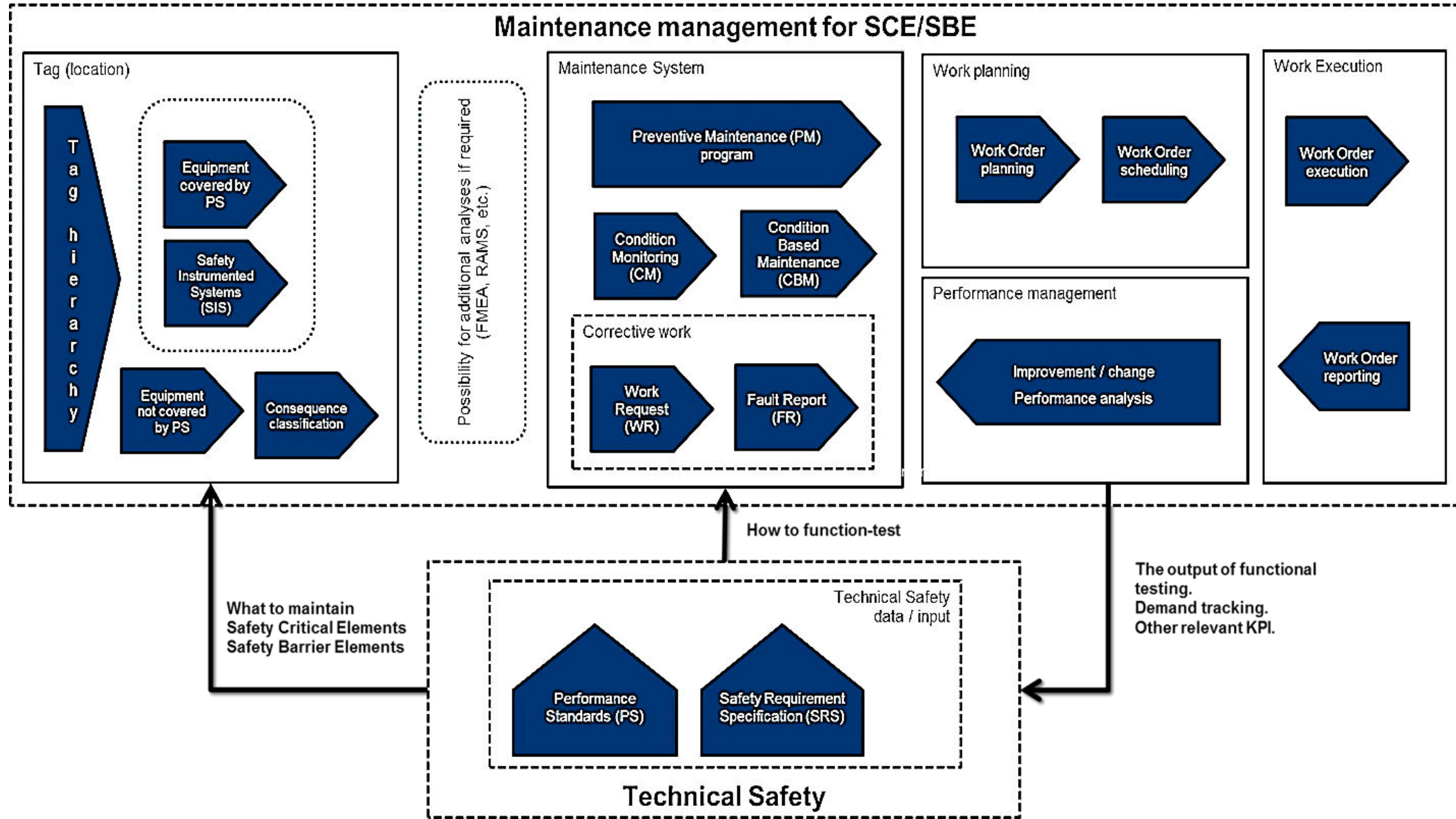
Performance Standards (PS) are derived from the risk management processes and may be seen as a final document – output link – produces by technical safety / risk management disciplines

However, an issue here is how this information shall be transferred to the operational / maintenance activities.

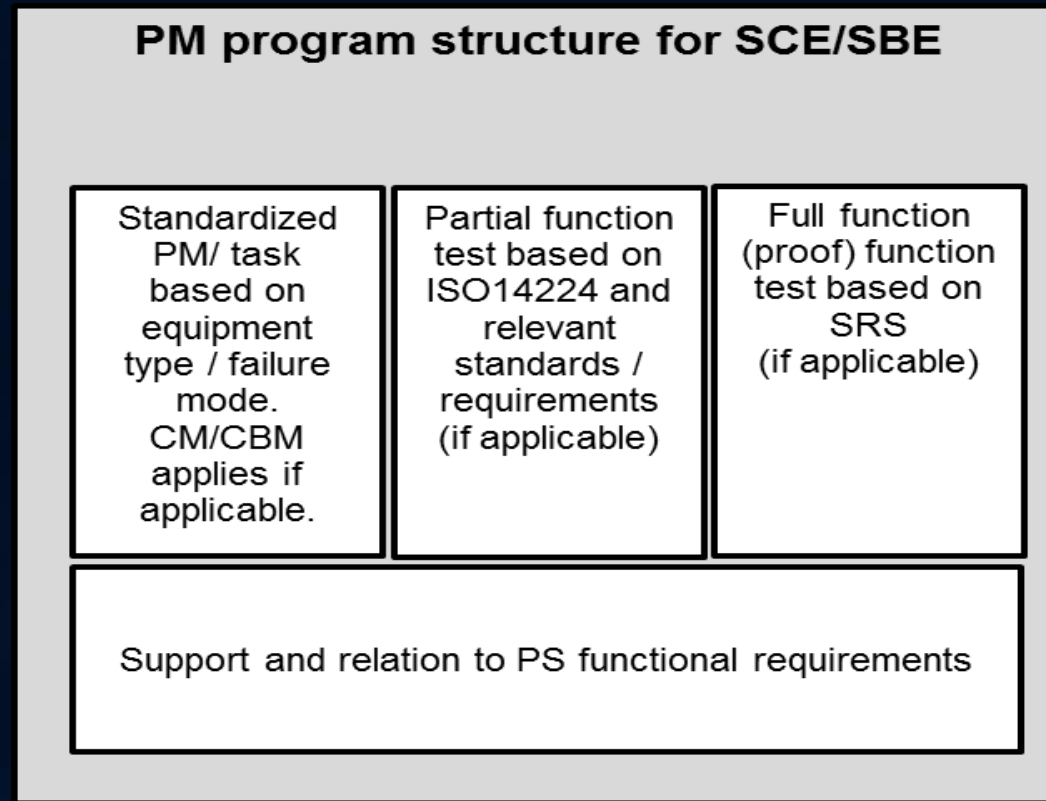
CHALLENGES IN THE LINKS BETWEEN TECHNICAL SAFETY AND MAINTENANCE



DISCUSSION FOR SOLUTIONS

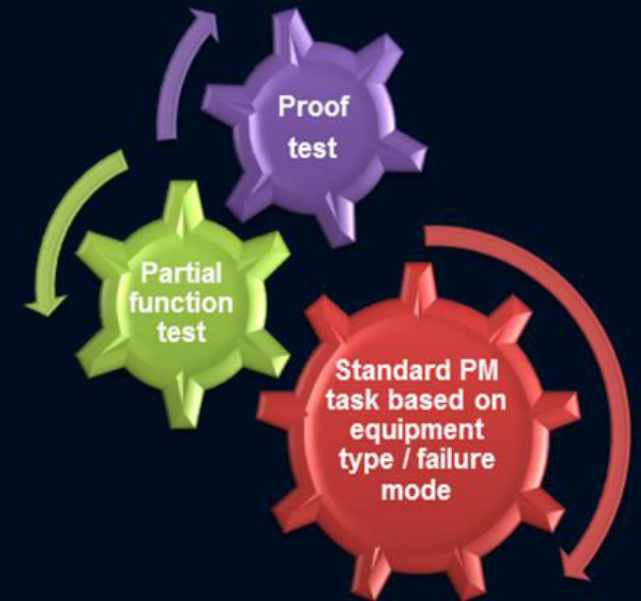


PM program structure for SCE/SBE



- Summarizing with the example of valve:

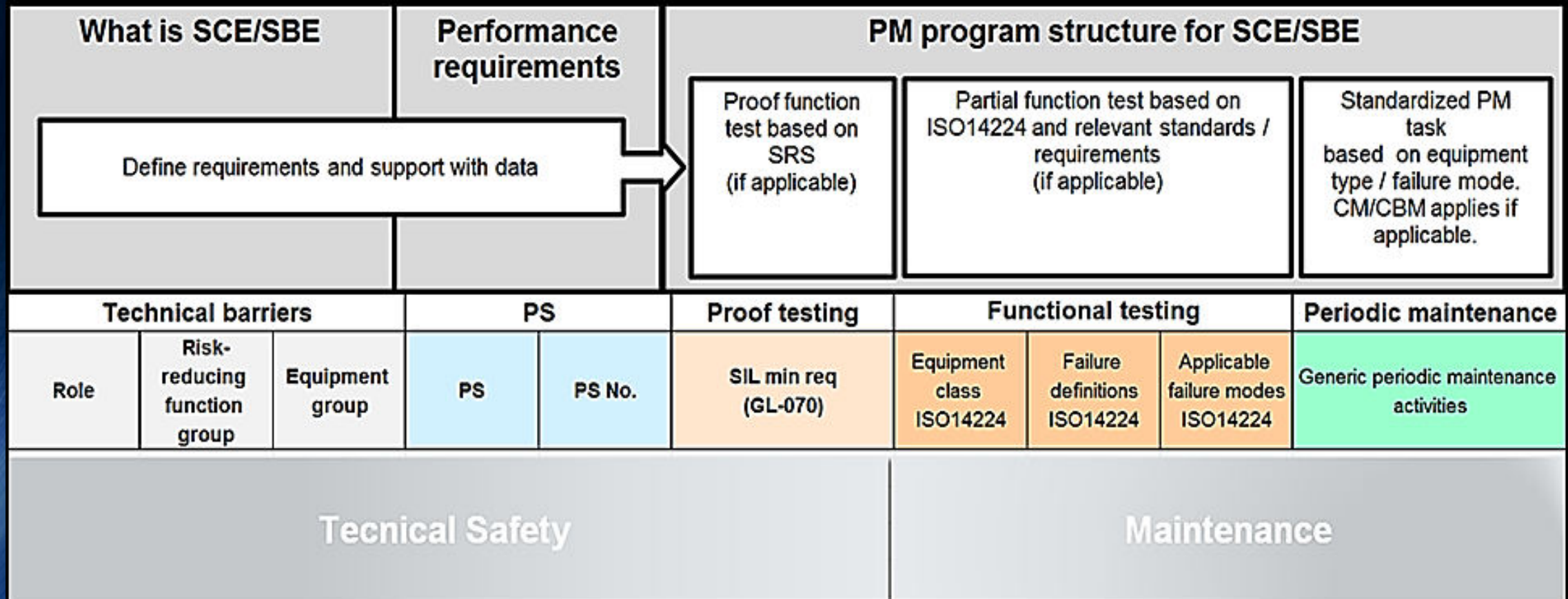
- - Generic PM task for valve. The equipment type (construction) is important here, for example, ball valve or butterfly valve may have different PM tasks due to different construction of the valve itself.
- - Partial function test for valve, i.e. valve testing. It can be based on ISO14224 (2006) or other relevant ISO/NORSOK standards, dependent on the functionality of the equipment. Valve can be tested for closing/opening on the signal, closing/opening time, or leakage rate.
- - Full function (proof) test is usually applicable for the whole Safety Instrumented Function (SIF) with SIL requirements. Generally it has a specific order, can have various methods (like partial stroke testing, etc.), defined intervals that should be re-updated time to time based on the actual demand rate of the function in the facility, etc. So if the valve is a part of any SIF, it is subjected to full function testing as well.
- It must be noted that standard PM task embraces inspection and CM / CBM scope as well, if applicable (for example, piping, rotating machinery, etc.) in this context.



Case study

- The major objective of this case study is to group and connect the safety functions to particular equipment through the established functionalities of relevant PS.
- The final result should present the particular equipment group, its connection to relevant safety function as well as corresponding functionalities of relevant PS and the incorporation of ISO:14224 (2006) that would enable further connections with relevant maintenance data.
- Additionally the list of generic maintenance routines required for SBE may be created that would facilitate to optimize the maintenance system by having standardized routines for the same type of equipment. The summary result should be able to ensure to create a required PM program in the structured and consistent way among the maintenance engineers .

Case study - summary



Thesis summary (1)

- Re-defined concept of a safety barrier and provided new definitions to improve the risk communication between involved parties. Closely based on the interpretation of PSA Regulations and common standards.
- The new framework for the safety barrier concept based on the accident modelling and recognized industry standards have been introduced and thoroughly described. A conceptual structure of safety critical and safety barrier systems consisting of technical and operational elements has been developed and presented in the thesis as practically applicable.

Thesis summary (2)

- Identified connection problems between technical safety and maintenance engineering; no systemized process to ensure forward ad back data flow.
- Possible solution proposed for forward link *technical safety-to-maintenance*.
- The new practical model of maintenance program for SCE/SBE was proposed with the high focus on standardization of activities to facilitate the optimization of maintenance system.

Further discussions

- The need to identify not only SCE/SBE, but SCS/SBS as well.
- The *maintenance-to-technical safety* connection should be established to allow continuous check and improvement of the critical elements/barriers performance.
- It is essential to understand that continuous process should be created rather the one-time workshops. Further studies are required to facilitate a synergy of separate work processes that would ensure adequate maintenance and follow-up of risk-reducing measures during their lifecycle.