University of Stavanger

Faculty of Science and Technology

MASTER'S THESIS

Study program/Specialization: Offshore Technology Risk Management	Spring semester, 2016 Open / ~~Restricted access~~
Writer: Valentina De Santis	………………………………………… (Writer's signature)
Faculty supervisor: Andreas Falck, University of Stavanger External supervisor(s): Anne Marie Wahlstrøm, DNV GL	
Thesis title: Method for assessing how deterioration of the safety system affect risk	
Credits (ECTS): 30	
Key words: Barrier Management, Barrier Performance, Risk analysis, Indicators, Risk level, Gas Detection System, Unmanned Platform.	Pages: 95 + enclosure: …0……… Stavanger, ……………….. Date year

ABSTRACT

In the Oil & Gas industry the fundamental element to control major accident hazard is the establishment of an efficient barrier management system. On the NCS the PSA has renewed the strong focus on the barrier and barrier management.

According to the PSA (Petroleum Safety Authority, 2015a) , the industry has to reinforce the link between the risk assessment and the barrier management and special interest should be given on the degradation of the barrier and the system and methodology used to measure it.

The barrier management in operation should be strongly and uniquely linked to the performance requirement, defined in the design phase. As explained in Falck, Flage, and Aven (2015) several methods may be used to identify the performance deviation from the design and operational basis. However, the main challenge is to find models able to reflect the effect of such deviations.

In this thesis work, a new methodology to measure the effect of deterioration of the barrier on risk is proposed. The methodology has been developed for the gas detection system of offshore installations, however it is believed that the methodology could be easily adapted to different barrier system.

The key aspect of the method is the identification of specific indicators; such indicators shall be easily updated by the operators using field data and connected to failure mechanisms of the barrier.

The combination of all indicators is used to build a total score of the barrier that is believed to measure the deviation from the barrier performance requirements; each indicator is combined considering their criticality with respect to the barrier function.

Finally, a relationship between the degradation of the barrier and the risk level is proposed.

The methodology is applied to a case study: an unmanned platform in North Sea.

TABLE OF CONTENTS

LIST OF TABLE

LIST OF FIGURE

LIST OF ACRONYMS

ALARP:	As Low As Reasonable Practicable
BAT:	Best Available Technology
CLU:	Control Logic Unit
DFU(s):	Defined hazard and accident conditions
ERO:	ERratic Output
ESD:	Emergency Shut Down
FAR:	Fatal Accident Rate
FMECA:	Failure Mode, Effect and Criticality Analysis
FTF:	Fail To Function on demand
FW:	FireWater
HAZID:	Hazard Identification Analysis
HIO:	High Output
HIU:	High Output, unknown reading
HRA:	Human Reliability Analysis
HSE:	Health Safety and Environment
ISC:	Ignition Source Control
LFL:	Lower Flammability Limit
LOO:	Low Output
LOU:	Low Output, Unknown reading
MAH:	Major Accident Hazard
m.s.l.:	mean sea level
NCS:	Norwegian Continental Shelf
NOO:	No Output
OTH:	Other
OTS:	Operational Safety Condition
PFD:	Probability of Failure on Demand

PFEER: Prevention of Fire and Explosion, and Emergency Response

PLL: Potential Loss of Life

PPE: Personal Protective Equipment

PSA: Petroleum Safety Authority

PSD: Process Shut Down

QRA: Quantitative risk analysis

RCM: Reliability Centred Maintenance

RNNP: Risk level in the Norwegian petroleum activity (Risikonivå i norsk petroleumsvirksomhet)

SAS: Safety and Automation System

SCE: Safety Critical Element

SER: Minor in-service problems

SHH: Spurious high level alarm signal

SLL: Spurious low level alarm signal

SPO: Spurious operation

SRA: Society of Risk Analysis

TTS: Technical Safety Condition;

TIMP: Technical Integrity Management Project

UNK: Unknown

VLO: Very Low Output

WSE: Written Scheme Examination

ACKNOWLEDGEMENTS

With this thesis work I conclude my studies at University of Stavanger in Offshore Technology.

I would like to thank my supervisors Andreas Falck, from University of Stavanger, and Anne Marie Wahlstrøm, from DNV-GL, for their great guidance during the writing of the thesis.

I would like to thank my colleagues and friends for the days spent together studying and psychologically supporting each other.

Finally, I thank my partner in life, Roberto, who has always believed and supported me in each step of our life together and, in particular, during this Master program.

Valentina De Santis

June, 2016

CHAPTER 1

1 INTRODUCTION

1.1 BACKGROUND

The Oil & Gas industry involves a significant amount of potential hazards. Each of them shall be identified, evaluated, controlled and monitored and risk management has such scope.

Each hazard and risk presents its characteristics, therefore the way to treat and control them is different. It is important to distinguish between two typologies of risk:

- Occupational risk is related to all the personnel injuries, its proper definition is given in the British Standards (2008, p. 826) OHSAS 18001:2007: *"occupational health and safety (OH&S) conditions and factors that affect, or could affect, the health and safety of employees or other workers (including temporary workers and contractor personnel), visitors, or any other person in the workplace (British Standards, 2008, p. 3)"*
- Major accident risk is defined as *"an accident where at least three to five people may be exposed*; " and "*a major accident is an accident caused by failure of one or more of the system's built-in safety and emergency preparedness barriers.(Petroleum Safety Authority, 2015b, p. 8)"*

The occupational risk is something that has a higher frequency of occurrence compared to the major accident risk and its consequences is mostly related to the personal injuries or limited number of fatalities (1 to 2). Such risk is mostly controlled, for example, by the use of the PPE (Personal Protective Equipment), and use of procedure that has the aim to modify and control the human behaviour.

A major accident risk is characterized, considering a probability consequences approach, by low probability of occurrence and high consequences. For example, a leak higher then 0,1 kg/s (precursor event) in the process area of an offshore installation does not occur very often, but the consequences of an undetected leak of this level can produce high consequences (major accident, such as: explosion, fire, high numbers of deaths) (Vinnem, 2014b). Thus, finding a strategy to mitigate the risk of major accidents is of main importance.

In the oil and gas industry one of the strategies identified against major accident is the use of safety barriers. The PSA has defined the safety barrier as: *"Technical, operational and organisational elements which are intended individually or collectively to reduce possibility for a specific error/hazard or accident to occur, or which limit its harm/disadvantages"(Petroleum Safety Authority, 2013, p. 3)*

Major accidents are related to release of unwanted energy to be released. In Figure 1-1 the eight basic forms of energy that can be released during operation is identified (DNV GL, 2014).

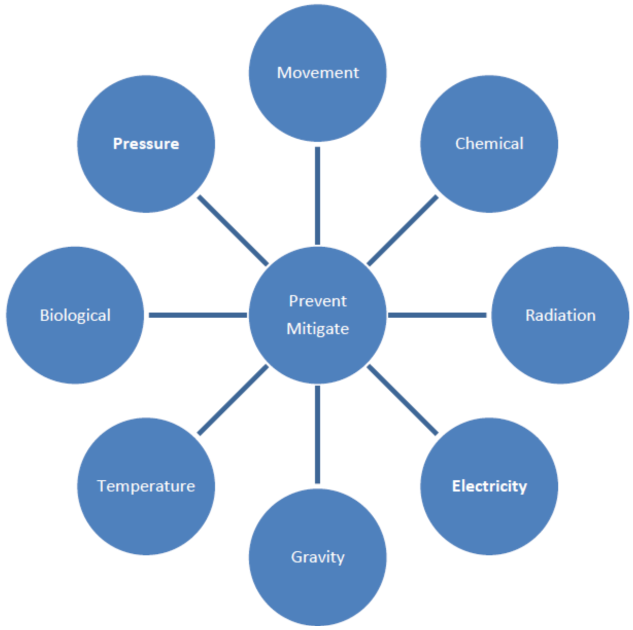


Figure 1-1 Energy released (DNV GL, 2014, p. 9)

The design and the status of the barriers are important to avoid that such energy will be released and major accident occur. The design and the status of the safety barriers are controlled by implementation of a barrier management system. The system has the aim to find solution which are able to help the reduction of the risk picture identified in the QRA analysis to an acceptable level (Petroleum Safety Authority, 2013).

Safety barriers are subject to performance requirements, defined as part of the design phase of a facility. In the operational phase the barriers must be monitored and controlled with respect to fulfilment of these requirements. Safety barrier degrades with time and use and such degradation may influence the performance of the barrier. Such deterioration is influenced by different factors, due to technical element degradation (e.g. normal deterioration of the material, failures) and due to human intervention (e.g. maintenance activities). The control of the barrier status is secured through the assurance (e.g. maintenance and testing) and monitoring of performance or degradation of the barrier element.

A deeper understanding of the status of the barrier(s) and their effect on the risk picture is of crucial importance in order to comprehend if and how the deterioration of one or more safety critical component influences the identified risk level.

In this thesis work a dynamic model, based on the identification of indicators able to identify the drift mechanism that brings barrier to fail, is proposed. The model is based on the analysis of the failure mechanism of the gas detection system on an offshore installation as case study.

1.2 SCOPE AND CHALLENGES OF THE THESIS

In order to define the model able to identify the drift mechanisms that bring the barrier to fail, some challenges have been identified.

As explained in Falck et al. (2015) in the industry several methods are available to identify the deviation from the design and operational basis; however the relationship between deviation from performance and degradation is not always well described by those methods.

The proposed model has the aim to well develop the effect of deviation from the performance requirements due to the deterioration of the barrier identifying specific indicators.

Several different methods are available of reporting the status of the barrier, meaning that if in an area two different barrier systems are tested, for example gas detection system and ESD valve, the correspondent reports could be different with misalignment in the level of details.

Another challenge is related to the used indicators; it is somewhat difficult to ensure that indicators are "monitoring" the performance or the deterioration of the system. For example based on the RNNP, typical indicators for the barrier status are related to the periodic testing (Skogdalen, Utne, & Vinnem, 2010). Such indicators are able only to report if a test has been performed but they do not give any information about the deterioration of the barrier.

For example, in the case of the gas detection system the periodic test failure indicator reports only that the detector has failed or not but not the cause that has carried the detector to fail. The same arguing may be done for the ESD valve testing of the closing time, the indicator reflects only the increasing of the closing time not the reason behind this failure.

Another issue may be related to the indicator characteristics; they can be expression of the percentage of the preventive maintenance or binary (e.g. barrier works or not) but the barrier deterioration usually shows different behaviour. For example, the gas detection system may be considered a binary system being a "working/not working" system while the ESD valve has failure mechanisms that are time dependent (e.g. increasing closing time). Therefore, the definition of indicators that are able to reflect the different failure mechanisms of the considered barrier is important.

Finally, it is important to understand how critical is the deterioration and the failure of the barrier related to the risk level.

Based on such challenges, the scope of this thesis is to answer the following question:

1. Why safety critical components (barrier elements) are important? (Chapter 2-3)
2. How is it possible to measure the degradation of a component of the barrier system? (Chapter 4)
3. What is the effect of deterioration of a component on the functionality of the entire barrier system? (Chapter 4)
4. What is the effect of deterioration of function on total risk level? (Chapter 4)
5. How the method can be applied to a real case? (Chapter 5)

This thesis work has the aim to answer to all these questions by the proposal of a methodology, using a hierarchy, linking indicators to failure mechanisms of the safety critical component, performance of the barrier system and impact on the risk level.

The methodology has been applied to the gas detection system correlating the failure of single element of the barrier to the overall deterioration of the barrier. A methodology to measure the deterioration of the barrier is also proposed.

1.3 THESIS STRUCTURE

The master thesis is structured in six different chapters. In Chapter 1 the scope of the thesis and the main challenges are described. Chapter 2 includes a theoretical background overview in which the risk, barrier, barrier management and indicator concepts are introduced. Chapter 3 describes the gas detection system and its functional requirement, Chapter 4 presents a proposal for the development of the dynamic modelling of the safety barrier status and the risk assessment. The case study is presented in chapter 5 and finally, in chapter 6 discussion and conclusions are reported.

CHAPTER 2

2 THEORETHICAL BACKGROUND

In this section an overview of the theoretical background relevant for the thesis is presented.

First of all, the risk concept is introduced. The risk concept and its understanding is important to manage, avoid and minimize the risk exposure.

According to the "Good Practice" by DNV GL (2014) it is possible to divide risk picture in two levels, basic risk level and variable risk level, as represented in Figure 2-1.

Figure 2-1 Interpretation of the risk picture (DNV GL, 2014, p. 11)

The basic risk level represents intrinsic risks that are managed during the design phases of the project and it is related to the nature of the business (production of hydrocarbons, offshore environment, etc..), while the latter represents risks related to the technical operational and organizational condition that influence risk picture continuously (DNV GL, 2014). The QRA evaluate both kind of levels; documenting basic risk level and establishing assumptions and limitations for the variable level. The variable risk changes according to the activities, the technical conditions, operational conditions; therefore, such changes need to be understood in order to define if activities are still performed with an acceptable risk level.

The need for understanding how the variable risk fluctuate with degraded barriers, in particular understand how the deterioration of the technical, operational and organizational factors of the detection system, influence the total risk picture is the scope of the proposed method.

A description of different risk concepts used in the industry is given in the Para 2.1. In this paragraph the risk concept is analysed and related to the scope of the thesis. Major accident risk is further described in Para 2.2.

Definition and description of the barrier in risk context is given in Para 2.3 with a focus on the barrier management. Barriers are used to avoid major accident risk; therefore, their management is of main importance to achieve this goal. Critical part of the barrier management is to define the status of the barrier to in order to ensure a system that is able to react in case of incident; an overview of the approach used on the Norwegian continental shelf and on the UK continental shelf is presented. A chapter describing indicators is given in Para 2.4.

2.1 RISK PERSPECTIVE

Different risk concept definitions have been developed in the different geographical sectors.

The risk concept, as defined in SRA (Society of Risk Analysis) (2015), is the representation of the consequences of an activity with respect to something that has human value. The consequences may be represented by a negative outcome like in the HSE sector (e.g. incidents, environmental damages), or by positive outcome as on the business sector (e.g. reward, bonuses).

Risk perspective has been considered for long time as: "*an objective characteristic or property of the activity being analysed, expressed by probabilities and statistically expected values of random variables such as the number of fatalities"(Aven, 2012, p. 13)*

This concept can be found in:

- Lowrance (1976), risk is defined as *"a measure of the probability and the measure of adverse effects"*,
- Ale (2002), risk is considered as the combination of probability and the extent of consequences
- Kaplan and Garrick (1981), define risk as the triplet (s_i; p_i; c_i) where:
    - s_i is the ith scenario
    - p_i is the ith probability;
    - c_i is the ith consequences

The risk perspective can be provided above can be summarized in the following way: R=(P,C). where P represents the probability and C the consequences (Aven, 2014).

In the last years, a new perspective in the risk concept has been developed. Such perspective represents a deviation from the probability-based risk concept, and it is used as basis from the PSA (Petroleum safety Authority), the ISO (International Standard Organization) and the SRA (Society of Risk Analysis).

Such risk perspective is called the bi-dimensional where *"risk is considered to be the two-dimensional combination of the consequences of an activity, C, and associated uncertainty, U."(Aven, 2014, p. 33)*.

Same definition of risk is given by the ISO 31000:2009*"risk is effect of uncertainties and objectives"(International Organization for Standardization, 2009, p. 2)*, reflects the bi-dimension risk perspective.

The above risk definition may be applied to a situation related to the scope of this master thesis. For example, given the event of an undetected leak in the process area; the risk related to failure of the detection system is a function of the potential consequences of the event (such as failure in the activation of the ESD, no alarm is given to the personnel, creation of an explosive atmosphere) and the uncertainties related to whether these consequences will happen or not. The consequences are then a function of different mechanisms such as whether it will ignite, and explode and if so with which overpressure? Will the structure be able to withstand to the explosion and so on? In the analysis of the consequences of an event it is needed to understand both the uncertainties and background knowledge related to the assumptions, input data and used methodology. Uncertainties and knowledge concepts are presented in Para 2.1.1 and in Para 2.1.2.

2.1.1 UNCERTAINTIES

In the International Organization for Standardization (2009, p. 2) uncertainties are defined as *"the state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequence, or likelihood"*. The uncertainty concept is linked to the knowledge of the consequences of an event.

In Aven (2014) three different categories of uncertainties can be defined:

1. Uncertainty about a quantity;
2. Uncertainty about the future;
3. Uncertainty about phenomena.

The first type is related to assign a quantitative value to the probability that an event *A* may occur (Aven, 2014). The uncertainty about the future are related to the consequences *C* of the event *A* (Aven, 2014). The last category represents the uncertainty about the cause-effect relationship between the event A and the related consequences C (Aven, 2014).

In the risk analysis context, the uncertainty can be divided into:

- Aleatory uncertainty: *"variability in populations and represents randomness in samples"(Aven, 2012, p. 17)*;
- Epistemic uncertainty: *"lack of basic knowledge about fundamental phenomena"(Aven, 2012, p. 17).*

The first uncertainties are described by the frequentist probability defined as the *"probability of expressing the fraction of times the event A occurs when considering an infinite population of similar situation or scenario to the one analysed"(Aven, 2013, p. 143)*, while the epistemic uncertainties are described by the subjective probability. The subjective probability is defined as the probability of *"expressing the assessor's uncertainty (degree of belief) of the occurrence of event A"(Aven, 2013, p. 143).*

A possible cause of uncertainties can be identified into the variability, that is a property of nature (Hafver et al., 2015). In Hafver et al. (2015) there is a distinction between variability and uncertainty, the first is *"real differences/changes in space and/or time, or between members of a population (Hafver et al., 2015, p. 826)"*, while uncertainty is *"imperfect or incomplete information/knowledge about hypothesis, a quantity, or the occurrence of an event (Hafver et al., 2015, p. 826)"*. Thus, the uncertainties are related to the strength of knowledge of the assessors, while the variability is a property of the nature (Hafver et al., 2015). When a risk assessment is performed the risk analyst uses models for the prediction of the future consequences. Models are interpretation of the reality and have their foundation on observable quantities, such quantities can be random or fixed quantities. The random quantity may be subjected to variability while the fixed quantity, subjected to uncertainty, may be observable and not observable (Hafver et al., 2015). Variability then may be modelled by the frequentist probability, while the uncertainty related to the fixed quantity are knowledge based probability.

For example, given gas leak scenario in the process area where the consequences of the event may be identified in the failure of the shutdown procedure it is possible to recognize:

- Fixed quantities: identified into the process area size;
- Random quantities, like the gas leak size, the number of persons present into the area and wind conditions (Weibull distributed).

The observable fixed quantity is related the size of the process area, while the non-observable fixed quantities are related to the probability of having person in the area during the leak, the parameter of the Weibull distribution for the wind variable and the volume of gas. Therefore, the risk analyst has to do assumptions to develop the risk assessment. Assumptions rely on the strength of knowledge of the analyst.

2.1.2 KNOWLEDGE

The evaluation of the strength of knowledge is a key aspect in the bi-dimensional risk definition. From the background knowledge that the risk analyst has depends the quality of the risk description (Flage & Aven, 2009).

Commonly knowledge is consider as a tool to "justify true belief" (Aven, 2014). But since in the risk and scientific context is difficult to express what precisely means the term "true" the knowledge is defined as: "justify belief" (Aven, 2014).

The strength of knowledge, based on Flage and Aven (2009), can be classified as strong or weak/moderate. The way to evaluate the strength of knowledge of the analyst consists in a scoring system based on four condition, if one or more of these conditions are true the knowledge is judged to be weak (Aven, 2013). The conditions are:

a) *"The assumption made represent strong simplifications;*
b) *Data are not available, or are unreliable;*
c) *There is a lack of agreement/consensus among expert;*
d) *The phenomena involved are not well understood; model are non-existent or known/believed to give poor prediction"(Aven, 2013, p. 138)*

On the other side, if it is true the opposite of all the above conditions then knowledge is considered strong (Aven, 2013).

Background knowledge for the undetected leak scenario may be related to the wind velocity and directions, or related to the amount of personnel in the area or to the volume of the gas cloud and gas composition. So that for each of them the risk analyst has to evaluate the strength of his background knowledge.

2.2 MAJOR ACCIDENT RISK

A major accident is defined by PSA as *"an accident where at least three to five people may be exposed*; " and "*a major accident is an accident caused by failure of one or more of the system's built-in safety and emergency preparedness barriers.(Petroleum Safety Authority, 2015b, p. 8)"*

Different definitions have been made by different organisations, however those differentiate mainly in consequence part (number of fatality, damage to asset or environment), all organisations define a major accident as an event of not acceptable consequences.

Such accidents are rare event, but when they occur their consequences may have large impacts with a great potential of escalation. The reason why they occur so rarely relies in the number of all the safety measures present in the installations. The seldom occurrence of such events does not mean that they do not need attention by the companies or during the risk assessment, on the contrary the nature of the major accident is complicated and hard to predict (DNV GL, 2014). As a matter of fact, they are characterised by a complex risk picture with different chain of events, different failures in the safety measures and the potential of escalation (DNV GL, 2014).

The risk related to such major events, in the new risk perspective introduced in the above paragraphs, can be identified as a black swan. A black swan can be considered as *"a surprising extreme event relative to the present knowledge/belief"(Aven, 2014, p. 116).* According to Aven (2014), the major accident risks are events that are on the list of known events but are judged to have low probability of occurrence.

The event of the gas leak, considered in this thesis work, it is defined by Petroleum Safety Authority (2015b) in the DFU(s) (defined hazard and accident conditions) as a major accident risk. The major accident risk has to be controlled and monitored in a systematic way in order to comprehend its complexity and to reduce its uncertainties. Such activities are the main scope of the barrier management introduced in the next paragraphs

2.3 BARRIER MANAGEMENT

In the Oil & Gas industry different major accident occurred in the past, one of the most important, that has represented the milestone for a better risk philosophy, is the Piper Alpha incident happened in 1988. The most recent major accident risk is represented by the Deepwater Horizon incident happened in 2010. Both incident, as highlighted by Vinnem (2014a), lead to a disaster that could be avoided if all the barrier were available, reliable, functioning, intact and robust. Therefore, a barrier management system during the operation with the aim to define and ensure that performances of the barriers are fulfilled is the right tool to control such risks.

In the next paragraphs the definition of barrier is given for understating the barrier concept, and then a brief description of the barrier management is also provided. Finally, an overview of the methodology used on the Norwegian and on the UK continental shelf for assessing the status of the barrier is given.

2.3.1 BARRIER CONCEPT

In order to avoid the occurrence of a major accident different types of barriers have to be designed and implemented on the installations. Barriers may be organizational, technical and human barrier. In case of an accident if all of them fail there is the high probability to have a disaster. In 1997 Reason proposes the "Swiss Cheese Model" (Reason, 1997) as an interpretation of the barrier failure. In Figure 2-2 a general representation of the model is presented and it is possible to notice that an accident (losses) occurs if in case of a hazard all the barrier present in the system fail.

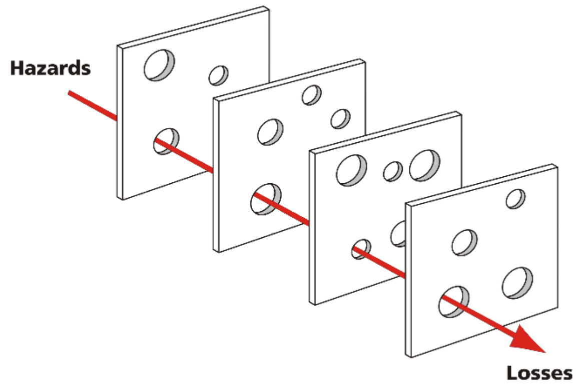


Figure 2-2 Swiss Cheese Model by Reason (1997); ("Swiss Cheese Model [image]," 2016)

In the oil and gas industry in the Norwegian continental shelf, PSA (Petroleum Safety Authority) in 2013 has given a definition of barrier:

“Technical, operational and organisational elements which are intended individually or collectively to reduce possibility for a specific error/hazard or accident to occur, or which limit its harm/disadvantages”(Petroleum Safety Authority, 2013, p. 3)

Technical barrier may be identified in equipment such as the gas detectors, blowdown, push buttons; operational barrier may be identified into the manual activities carried out (such as maintenance activities). Organizational barrier may be identified into the personnel with specific competences (Petroleum Safety Authority (Management Regulation), 2015). As defined above the PSA states that all three elements have to be in place to realize the barrier function.

It is possible to define also:

- Barrier function: it represents the role/scope of the barrier (Petroleum Safety Authority, 2013; Sklet, 2006);
- Barrier element: it represents the technical, operational or organisational measure or solutions that realize the barrier functions. (Petroleum Safety Authority, 2013)

In the case of a leak a barrier function can be identified as the “detection of the leak”. The functionality is realized by the technical barrier elements as the fire and gas detectors, the operational barriers is the operator who starts the push button while the organizational barriers is the operator with knowledge about the emergency procedures and when and how to push the call button.

Organizational elements are not considered in this thesis work. The analysis of such factors needs a study of all the connection (explicit and implicit) that influences both the performance and the risk level. The study of the connections is related to the decision making process and the management actions that are able to influence all the system. Such study could represent an updated of this thesis work.

The aim of the barrier management system is to coordinate activities in order to define the barriers to be taken in place and then the activities to maintain them in order to keep their function throughout the lifetime of the installation (Petroleum Safety Authority, 2013). The barrier management process is composed by different steps, as described in Petroleum Safety Authority (2013). In Figure 2-3 the process for the barrier management during design phases is represented.

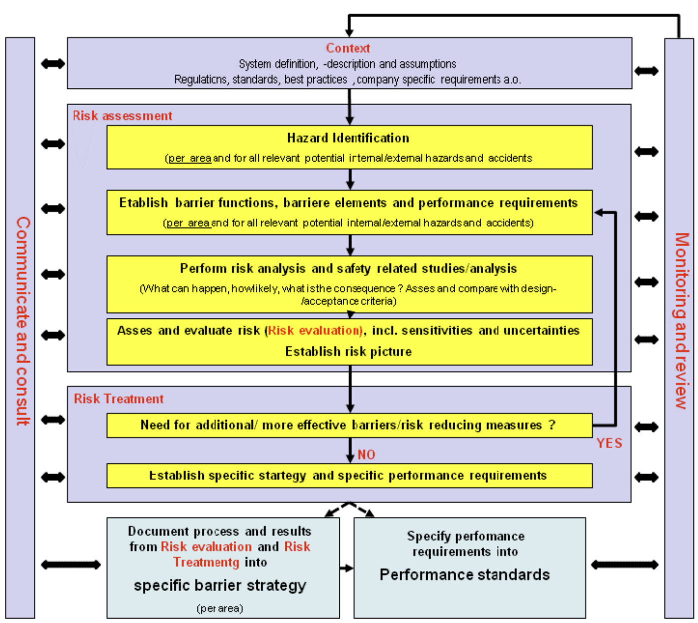


Figure 2-3 Barrier management framework (Petroleum Safety Authority, 2013, p. 9)

The steps represented in Figure 2-3 are summarized as follow based on the Petroleum Safety Authority (2013):

- Establishing the context: at this stage all the parameters are defined for the execution of the other steps. Thus at this stage it is possible to find the description of the system and of the assumption used in the next steps; the requirements. The applicable standards (internal and external) and the limit boundary for the scope;
- Risk assessment: at this level of the barrier management, different activities have to be performed in order to evaluate the risks connected to the specific installation/activity. This process has many similarities with QRA process and they are sometimes performed together.
    - HAZID (Hazard Identification Analysis). In this step all the potential hazards for a specific area of the considered installation are analysed.
    - Establishment of the barrier functions and elements based on the outcomes of the HAZID. In this step the process for the identification of the barrier performance requirements starts.
    - Perform risk analysis and safety studies. These are performed in order to establish the requirement for the barrier function and element. Based on the results of the risk analysis comparison between them and the acceptance criteria defined in advance have to be done and evaluation of the uncertainties and sensitivity analysis must be part of this stage. This will also give acceptance criteria for performance requirements for barrier functions and elements.
    - Establish a risk picture. The risk picture has to be established, refined and evaluated in the way that it will be used to establish the barrier strategy and to ensure that the barrier shall have the right requirements.
- Risk Treatment: at this stage the additional or more effective barriers have to be analysed according the principle that risk has to be always reduced as much as reasonable possible (ALARP principle).

- Define a barrier strategy: it has to be done area by area of the installation analysed and it has the aim to give an understanding of the requirements for each barrier functions and elements identified.
- Define performance requirement and standards: they are the properties that a barrier must have in order to develop its function successfully. They have to be established for the technical, organizational and operational barrier and be monitored and controlled during the operation in order to maintain the function of the barrier during the time.

Each of the above steps shall be communicated to the different stakeholders; they shall be consulted during the process as well. Finally, it is expected that each step is monitored and reviewed in order to ensure that the right quality is reached in the process and the lesson learned from the process are transferred and implemented.

On the Norwegian continental Shelf the performance requirements are defined by the NORSOK S-001 (Standards Norway, 2008) and be identified for each safety system as:

- Availability;
- Functionality;
- Reliability;
- Robustness;
- Integrity.

On the UK continental Shelf the performance requirements are defined by the PFEER regulation (Prevention of fire and explosion, and emergency response on offshore installation) (Health and Safety Commission, 1997) and are grouped by the acronym: FARSI. Where:

- F stands for functionality
- A stands for availability
- R stands for reliability
- S stands for survivability

- I stands for interaction with other safety critical element

In the following paragraphs activities intended to monitor and verify the performance requirements, developed in the two continental shelves, are briefly explained.

2.3.2 ASSESS STATUS OF THE BARRIER

Barriers are designed, implemented and maintained to fulfil relevant performance requirements. If barriers are degraded they cannot fulfil their role and hereby it represents an increased risk related to major accidents. Therefore, it is important to have a process in place to identify any deterioration of barrier performance. This can be done by monitoring different parameters/indicators and by verifying the performance of the specific barriers. Based on this an assessment of the barrier status can be done and the relevant risk should be evaluated. Different methods and processes maybe be applied to assess status of barriers. Status can be aggregated automatic based on predefined criteria or it can be assessed manually by experts (DNV GL, 2014). Different counters have different requirements towards the process of assessing/verifying status of barriers.

This paragraphs are considered the actual methodologies used on the Norwegian Continental Shelf and on the UK Continental Shelf. In Chapter 4 a new methodology for assessing the status of gas detection system is suggested.

2.3.2.1 NORWEGIAN CONTINENTAL SHELF

On the Norwegian continental shelf, the assessment of barrier status is contained in the barrier management framework. In the framework given in Petroleum Safety Authority (2013) (see Figure 2-3), once defined the performance requirements for the barrier it is necessary to monitor the performance to ensure that the acceptable requirements level is achieved and then to implement improvements to ensure that the established performance requirements are met. The monitoring and review activities are carried out during the operation (Petroleum Safety Authority, 2013).

The barrier management framework is based on the framework given in NORSOK Z-0013 related to the quantitative risk analysis (Standards Norway, 2010).

During the design phase a list of assumptions and prerequisites have usually been defined for safety technical systems and for operational activities, therefore performance requirements, list of assumption and prerequisites need to be monitored to avoid failure or an increased risk picture beyond acceptable level (Petroleum Safety Authority, 2013).

Therefore, the overview of operational activities is the first part of the monitoring phases. Then to ensure that the barrier system will work in accordance with the established performance requirements it is necessary to develop maintenance plan, tests plan, inspection plan and ensure that incidents have been recorded and thoroughly investigated (Petroleum Safety Authority, 2013). In this phase it is necessary to monitor the risk influences factors such as changes, deviation in the management/procedures and competence of the resource (Petroleum Safety Authority, 2013).

The monitor and review phase, therefore, can be understood as a barrier management during operation. The way the barriers are operated during their lifecycle, their degradation and their maintenance is part of this phase and they influence the final risk picture.

From the maintenance and tests activities a set of data related to the barrier performance are available, and acceptance criteria are established thus the status of the barrier can be outlined from this point (DNV GL, 2014). There are many different ways to define the barrier status, but the most common consists in the introduction of a rating system based on tolerance criteria, the rating is performed using a colour system (e.g.: red the system is not functioning; yellow: the system is degraded; green: the system is functioning) and guidelines can be used to interpreter the meaning of the rating (DNV GL, 2014). The available data will create a long list of information from different sources, therefore the need of a grouping and aggregation as explained in DNV GL (2014) is present.

Companies working on the NCS have developed methodology to fulfil the requirements stated by the PSA. In particular Statoil has developed a methodology called TIMP (Technical Integrity Management Project) that has the aim to monitor the performance requirements. In the methodology, data are analysed and collected by a group of expert that has the aim to evaluate the status of the equipment, the system and barriers (SINTEF, 2015). The results are presented in a bow-tie diagram (see Figure 2-4) and updated on a monthly or bimonthly basis.

Figure 2-4 TIMP bow-tie representation (SINTEF, 2015, p. 34)

In addition to monitor activities some companies have implemented verification activities, such as TTS (Technical Safety Condition) and OTS (Operational Safety Condition); the TTS, executed every 5th year, has the scope to verify that sufficient performances requirements are established and that the acceptance criteria to performance still is valid according to the risk picture; the OTS verify the operational performance standard (SINTEF, 2015). To develop/implement such verification scheme, checklists are developed and used to assess the performance of the barrier function, barrier elements, technical assessment and to have a trend for the barrier condition. Results are summarized in the red, yellow and green condition to identify the status of the system.

The reason why the identification of the barrier status is so important is the control of the major accident risk but is also to provide information for the decision making during the operations. For example, the status of the detection system in a particular area is important in order to plan and organize the work permits to perform hot work in that area.

2.3.2.2 UK CONTINENTAL SHELF

In the UK continental shelf, the assessment of the barrier status is done building a management system that has the aim to control and reduce the major accident hazard.

The major accident hazard can be reduced considering a management process divided into two moments: the first is the installation safety case and the second is the written scheme examination (WSE) (Step change in safety, 2012a). The two moments are connected one each other, as a matter of fact the installation safety case represents the basis for the written scheme of examination. In Figure 2-5 a summary of all the steps are reported.

Figure 2-5 Major accident hazard management process according UKCS (Step change in safety, 2012b)

In the first phase, the installation safety case, all the hazards are identified and assessed, a risk management is defined and the basis of safety is documented and demonstrated. All these activities are done in three steps as described in Step change in safety (2012a). The first step is the identification of the major accident hazards (MAH), the second one consists in the safety assessments and the last step is the development of the safety case document. In the first step all the hazards related to death or personal injuries caused by fire and explosion or release of dangerous substances are identified; hazards related to serious damage to structure, blowout, loss of containment, ship collision and any event that can cause more than five deaths are considered (Step change in safety, 2012a). All these activities are developed in the HAZID (hazard identification analysis) activity. In the safety assessment all the analysis necessary to understand what can go wrong during the operations and the activities to mitigate the effect of MAH are presented (Step change in safety, 2012a). Therefore, analysis such as detailed risk assessment, fire and gas explosion risk analysis, dropped object analysis, ship collision and evacuation escape and rescue analysis are prepared.

Finally, the safety case is developed. This document has the aim to prove that all the formal assessment have been done and that the company's management system is consistent with the safety requirements in the operation phase; and that the duty holder has the ability and means to control a major accident (Step change in safety, 2012a). In the safety case a description of all the installation and of all the arrangements available to protect personnel from hazardous event is given (Step change in safety, 2012a). In particular, the regulations related to prevention of fire and explosion, and emergency response (PFEER) (Health and Safety Commission, 1997) has the aim to require the Duty Holder to protect personnel from major hazard related to fire or explosion and the need to escape and rescue to avoid or minimise the consequences of the major accident.

The result of the analysis related to this regulation is a list of performance that the plant and the equipment need to meet, therefore the performance defined in the PFEER are also safety critical elements and they are part of the same Assurance and Verification activities (Step change in safety, 2012a).

In the WSE all the requirements for the plant and performance for the equipment are set, activities related to the assurance and the verification related to performance and requirements are established. This actions, as described in Step change in safety (2012a), are divided into: identification of the Safety Critical Elements (SCEs), definition of performance standards (PS), assurance scheme and finally verification scheme and independent competent person. The identification of the SCEs is the key factor for the success of the risk management, it consists on those elements which failure give substantial contribute to a major accident. Since in the MAH they have been already established during the HAZID activity, the SCEs are identified considering those hazards and set up the means to manage the associated risk (Step change in safety, 2012a). For example, in case of major hazard as fire and explosion the safety critical element are identified as process containment, ignition control, safeguarding systems, fire protection. For each SCE there are sub-element like fire and gas alarm, water firefighting, ESD (emergency shutdown) that represents the relative associated equipment. The performance standards, defined as the acronym as FARSI (see Para 2.3.2) are established for each of the SCEs. Therefore, the performance reliability of the SCEs in relation with their PS will minimise the consequences of a MAH (Step change in safety, 2012a). The performance standards need to be reviewed periodically under the concept of continuous improvement.

The assurance and verification activity are all those activities that has the aim to ensure and to confirm that the performance standard are met and performed. The assurance activities are related to the procurement constructions phase, but also activity related to the operation phases such as preventive and corrective maintenance, inspection and tests activities. Verification activities are all those activities carried out by a third party, also known as ICP (Independent Competent Person) defined by the duty holder to confirm that *"SCEs will be, are, and remain suitable, or adequately specified and constructed, and are being maintained in adequate condition to meet the requirements of the Performance Standards"* (*Step change in safety, 2012a, p. 6).*

As a conclusion the WSE represents the system to assess the status of the barrier, which is the most effective mean to prevent MAHs.

2.4 INDICATORS

Indicators can be used to monitor performance and activities on the installation.

It is often recognised in the accident reports that warnings are detected prior the accident occurrence and if such early warnings where managed in advance the accident should be avoided. This is true for example for the Deepwater horizon accident, for the BP Texas City Refinery (Skogdalen et al., 2010).

Based on the identified early warnings, or precursor events, it is possible to define indicators that provide information regarding the probability of major accident.

Indicators have been identified as the strategy to follow and to control continuously the major accident risk. They can be described as: *"a measurable/operational variable that can be used to describe the condition of a broader phenomenon or aspect of reality (K. Øien, Utne, & Herrera, 2011, p. 149)".* They are usually identified considering assumption on their effect on safety or through correlation (K. Øien et al., 2011).

On the NCS in 1999, the PSA has developed, together with a team work, the RNNP project with the aim to define the indicators in the oil and gas industry. The aim of this project is to measure the impact of the safety-related work, to help in the identification of critical area for safety considering also the major accident risk and to improve the understanding of the causes of the incident and unplanned situations with respect to risk in order to create a more reliable decision-making stage. For the major accident risk two indicators has been identified:

indicators on occurrence of incident and indicators related to performance of barrier (Vinnem, 2010).

Indicators have been considered in this thesis work as a way to dynamic monitoring the deterioration of the barrier system.

CHAPTER 3

3 THE DETECTION SYSTEM

The methodology suggested in this thesis work is tested on a case study on the barrier function "to detect gas". Therefore, a description of the detection system will be given in this chapter.

The detection system has an important role in any oil and gas facility, that is: detect leakages (such as hydrocarbon leak, toxic gases leak) as soon as possible to avoid or control the creation of an explosive and/or flammable atmosphere (Standards Norway, 2008). Leakage events are categorized as major accident hazard (Petroleum Safety Authority (Management Regulation), 2015); therefore, detection system together with containment system can be considered the most important barrier system to control such hazard and its good functioning and the respect of the barrier function performance requirement is of main importance.

Given the importance of the barrier system, it is important to understand the different components of the system and how they work together to realise the barrier function and how they are modelled in the QRA.

This chapter has the aim to provide such information. Thus, in para 3.1 the description of how the component of the system work, in para 3.2 it is possible to find a description of the maintenance activity of the system and in para 3.3 the description of how it is modelled in the QRA is given.

3.1 FUNCTIONAL DESCRIPTION OF DETECTION SYSTEM

As defined in Sklet (2006), *"The barrier functionality/effectiveness is the ability to perform a specified function under given technical, environmental, and operational conditions. (Sklet, 2006, p. 10)"*.

The main function of the detection system is to detect gas leak and fires. The fire and gas detection system is integrated with some other safety system such as:

- ESD system (Emergency shutdown system);
- Blowdown system.

In Figure 3-1 a description of how the different system are connected is represented, following the Standards Norway (2001).

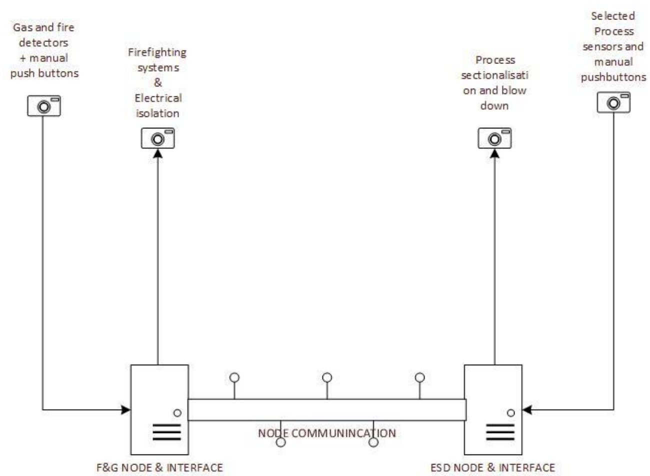


Figure 3-1 Link between detection system and other system – Simplified SAS topology

The fire and gas system is the first barrier involved in the detection of a leak and its good functioning is of main importance, it has the aim to detect the leakages and the fire as soon as possible to avoid or reduce the risk of creating an explosion or flammable atmosphere.

It is composed by: gas detectors, fire detectors and manual push bottom. The gas and fire detectors are active barriers that have to function on demand, that means that they are supposed to work when required. While, the manual push buttons are manually activated by the operators in case of need. The importance of such barrier relies in the fact that it starts other component of the safety system, this is why in this paragraphs are described the gas detection system and the other component of the safety system. The description of the connection of the different components is important to understand the importance of the gas detection system in the success of all the system and to understand that the failure or a wrong functionality of such system may be the starting point of a major accident.

There are two kinds of gas detectors: point and line detectors. Both of them has the aim to detect leakages higher than 0,1 kg/s, in particular in the NORSOK S-001 it is stated that *"The gas detection function shall provide reliable and fast detection of flammable and toxic leaks before a gas cloud reaches a concentration and size which could cause risk to personnel and installation (Standards Norway, 2008, p. 27)"*. The main differences can be found in the amount of gas to detect, the reaction time and area covered. Point detector has the aim to evaluate the percentage of the lower flammability limit (e.g. %LFL) of the target gas in a point of the area where it is localized. The line detector evaluates the amount of the target gas along the beam path between the two components (e.g. LFLm). The line detectors use infrared technology and they are composed by a transmitter and a receiver. The coverage capability is small for the point detectors while is quite high for the line detector, as a matter of fact the line detector can cover different length of path length, from 5 meter to 40 meter (defined as short range) to 120meter to 200 meter (defined as long range) (Honeywell Analytics, 2015).

To guarantee in an area a good gas detector system a mix of the two technology is required (Standards Norway, 2008). Their location is based on the hazardous area definition, they need to be allocated in correspondence of natural flow "corridors"(walkways along flow 2 direction), ventilation outlet from hazardous area, enclosed area and air inlets (Standards Norway, 2008). In case of an HC leak the confirmation of alarm is given considering a k-out-of-n reliability approach, usually it is 2ooN where N≥3 (Standards Norway, 2008). The confirmation of the alarm is given based on the amount of gas detected; thus the system confirms the alarm when one detector advises low alarm and the other one gives a high alarm. The low and high alarm, defined by the standards as performance requirements, are the following: low alarm for point detector is 10% LFL and the high alarm is 30% LFL; while for the line detector the low alarm is 1 LFLm and the high is 2 LFLm (Standards Norway, 2008). Therefore, the confirmation is given, for example, when one point detector reaches the 10%LFL and one line detector reaches the 2LFLm out of N.

When the alarm is confirmed all the other components react immediately. The Emergency shutdown (ESD) is automatically activated by the gas detectors, the ignition source control (ISC), Blowdown and firewater can be activated both by the ESD or by the F&G system, in case of fire the firewater (FW) pump is activated, the ventilation system is blocked and public alarms start to advise personnel (Standards Norway, 2008).

The fire detectors have to detect a fire as soon as possible, their coverage is based on the assessment of fire scenario, where within all the area are considered potential fire sources, characteristics consequences and environmental conditions (Standards Norway, 2008). Therefore, for a fire in a hazardous area a fire detector must detect a flame size of 0,5m in diameter and 1m length, while two detectors must detect a flame size of 1m diameter and 3m length. Moreover, fire detectors must be present all over the installation based on the fire and safety system. In the fire detector systems manual call point, flame detectors, smoke detectors and fire detectors are included. The manual call point is located in strategic area easy to reach in case of necessity. As for the gas detectors, the confirmation of a fire is given considering a k-out-of-n strategy. The confirmation of smoke follows a 2ooN with N≥3; confirmation of flame follow, according to the area where they are located, 1ooN with N≥2 and 2ooN with N≥3 (Standards Norway, 2008).

When the confirmation of a fire is given the emergency shutdown valve for hazardous area, the blowdown system, the ventilation, fire dumper are automatically activated and the firewater and the alarm system to personnel start.

The F&G system has continuous feedback in the control room to monitor both the alarm and the good functioning of the system.

The emergency shutdown (ESD) has the scope to prevent escalation in case of a major hazard. It is the last barrier that has the scope to isolate the installation or part of it. It is possible to identify three different shutdown system in offshore installation; they are ESD0/APS, ESD1 and ESD2 (Standards Norway, 2008).

The ESD0/APS is activated manually only and has the aim to totally isolate the installation. The ESD1 is located typically in non-hazardous area, such as living quarter and utility areas. It can be activated manually by the use of pushbuttons, activated by the ESD0/APS or by the confirmation from the gas detector. The ESD2 is located in hazardous area such, such as drilling and process area. It can be activated using a pushbutton, by the ESD1 and by the gas detection system (Standards Norway, 2008).

The system is composed by valves that have the aim to create isolatable section in the installation as fast as possible to reduce the amount of hydrocarbons in case of a gas leak event. The valves are defined as shutdown valve in case their failure creates consequences that exceed the dimensioning accidental load.

The main requirement for such valve is close the hydrocarbon supply as soon as possible, so that the closing time should not exceed 2 sec/inch (Standards Norway, 2008). In order to control the status of the position, the valves shall be equipped with both remote and local position indicators. Its location shall be independent from local instrument room.

Alarm has to be started as soon as possible, in particular: the general alarm is initiated upon ESD1 and ESD2, muster must be initiated manually.

The status of the ESD system, like for the F&G system status, is continuously available in the control room and in case of alarm the operator will take decision according to the alarm received.

The F&G system and the firefighting system are connected into an interface node that is connected via cable to the ESD node interface

All such activities are controlled using a control logic unit. Its role is to translate the input from the F&G system to the other component of the safety system and give feedback in the control room. It is mainly composed by hardware and software component, such as CPUs, Input and Output cards, application software. The software should be in accordance to the IEC 61508 and be certified by an independent body (Standards Norway, 2008).

Moreover, the logic unit has the role to permit the diagnostic of the safety system by testing of the functions within specified limitation regarding degradation of safety and impact on the production regularity including the trip signal between the SAS units (Safety and Automation System) (Standards Norway, 2008).

The location of the control logic, given its importance, shall be far from hazardous area and from external interference; therefore, it is located near the control room and/or living quarter.

3.2 ASSESSMENT OF BARRIER STATUS

All technical systems are subjected to maintenance activities, defined into maintenance management system. Maintenance activities are carried out in order to retain and/or restore an item into a state in which it can perform the required function (Standards Norway, 2011).

Two type of maintenance activities are basically carried out: preventive and corrective maintenance. The preventive maintenance is defined as: *"maintenance carried out at predetermined intervals or according to prescribed criteria and intended to reduce the probability of failure or the degradation of the function of an item (Standards Norway, 2011, p. 10)"* . The corrective maintenance is defined as *"maintenance carried out after fault recognition and intended to put an item into a state in which it can perform a required function (Standards Norway, 2011, p. 8)"*.

Therefore, based on the definition of preventive maintenance it can be stated that it is the main activity to assess the status of the technical system.

To assess that the detection system is able to perform its function different maintenance activities are present in the maintenance program such as:

- Inspection of explosion protection for detectors in classified area;
- Cleaning of lenses from salt or other impurities;
- Checks of detector alignment for line detectors;

- For particular kind of detectors calibration activity is required;
- Functional testing

The functional tests are developed based on a maintenance plan, usually bi-weekly tests are performed on the installations, and the confirmation of functional testing is given in the control room through the Operator interface.

In case of failure of the gas detector after the preventive maintenance activity, corrective maintenance is required.

3.3 QRA MODELLING DESCRIPTION OF DETECTION SYSTEM

On the NCS the QRA methodology is defined in the NORSOK Z-013 (Standards Norway, 2010). The standard, based on the ISO 31000 and ISO 17776 (International Organization for Standardization, 2002, 2009), defines the steps to take in order to develop and implement the risk analysis.

The QRA procedure is summarized in see Figure 3-2.

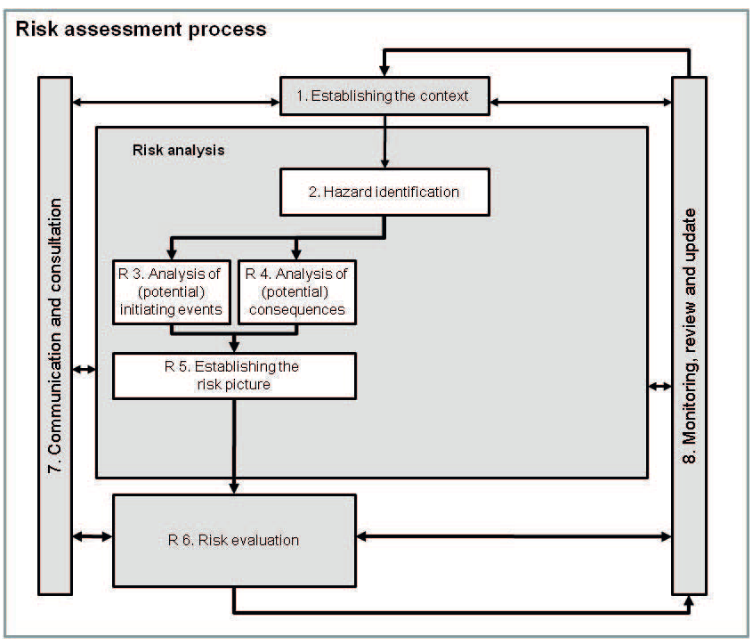


Figure 3-2 Risk assessment process (Standards Norway, 2010, p. 19)

The process in Figure 3-2 can be applied to all the hazards that are typically included into the risk analysis. Risk assessment process includes separate steps related to the identification of the potential hazards. A list of the steps is provided:

- Establishing the context;
- Hazard identification divided into: Analysis of the (potential) initiating and consequences event;
- Establishing of the risk picture;
- Risk evaluation.

In the NORSOK Z-013 the typical hazards that are necessary to be included into the QRA, are listed, some of the hazards are: blowout, process leaks, leakages of toxic or suffocating, transportation accidents, collisions (Standards Norway, 2010).

During the establishment of the context, following the Standards Norway (2010), are defined:

- Objectives;
- Scope;
- Responsibilities;
- Methods;
- Models;
- Tools;
- System boundaries;
- Risk acceptance criteria;
- Deliveries and the execution plan

The establishment of the context give the necessary input to the calculation step. Each company developed their own calculation methodology; however, the methodology described later on in this paragraph is the one provided by DNV-GL called SAFETI OFFSHORE (DNV GL, 2016).

Considering a leak scenario in the process area (i.e. hazardous area), it is necessary as first step to develop a definition of the main areas. This procedure consists in different steps that allow the analyst to move from the drawings (e.g. plot plans, PFDs and P&IDs) to different scenarios to analyse. Therefore, in the process area the procedure consists in:

1. identify isolable sections based on the P&IDs;
2. divide the installation into areas;
3. identify subsections from the isolable section;
4. divide the sub-section based on the fluid present;
5. relate the components of the isolatable section to each area;
6. assess the leak frequencies of each component;
7. define the leak frequency of each sub-sections.

Thus, on an offshore installation the main areas are typically divided into:

- Process area(s);
- Drilling and well area;
- Utility area;
- Living quarter.

The process area is composed by different modules in which different machinery and equipment are present. Each of them is connected via piping, so it is necessary to identify the isolable section. The isolable sections are identified by the emergency shutdown valves (ESDV) which have the role to isolate the section (i.e. stopping the amount of fluid in the piping and the equipment in case of leakage). For each section a leak frequency is evaluated considering different leak sources, such as valves, flanges and instruments. The leak frequency obtained, as the sum of all the leak frequency of all the leak source, is then divided into different leak sizes typical small, medium and large leak.

At this point a repartition of the process area with related leak frequency for each isolatable section is given and the last step is to define a case with related failures cases.

The failure cases analysis starts considering an isolatable section in the process area and a leak location, then the size of leakage (small, medium and large) is defined and for each of them and cases related to the safety system functioning are developed.

The analysis of the consequences has to take into account a considerable number of variables, such as: the geometry of the installation and in particular of the isolatable section, weather conditions, ventilation, wind directions and the interaction between the safety systems (e.g. F&G system, ESD, manual push button).

In order to have a good understanding of the complex phenomena of the leak event, many tools can help in the analysis of the consequences. Such tools are CFD models (Computational Fluid Dynamics) (e.g. FLACS by GexCon) or simpler text book models and integral model (e.g. PHAST by DNV GL). In the NORSOK Z-013 (Standards Norway, 2010) it is suggested to use CFD models for the probability explosion modelling.

In the industry, nowadays, different risk models are available that reflect the status of the safety system at different degree of detail, the approach introduced in this work, i.e. SAFETI OFFSHORE by DNV GL (2016) is depended on a QRA tool that is able to reflect the interaction of the different safety barrier in slightly detailed manner.

In order to model the detection system in the QRA the possible combination related to the following parameters are combined into a dynamic event tree, from which the results necessary for the calculation of the risk acceptance criteria related to potential loss of life, and availability of main safety functions (e.g. PLL and FAR) in the QRA is provided:

- Leak size;
- Safety system cases that represents the combination of the safety system necessary to be reflected in the modelling (e.g. F&G system, Blowdown, Ignition control, isolation);
- Wind speed and direction;
- Type of ignition;
- Time of ignition;
- Overpressure;
- Fire water;
- Early failure

The safety system cases are set to develop the behaviour of the barrier present into the isolatable section and to better understand the consequences that can arise from the leakage scenarios given the combination of different safety system. The considered safety systems are: emergency shutdown, gas detection system, fire detection system, blowdown system and ignition source control.

Some assumptions may typically be defined in order to model the system behaviour, such as:

- The failure is related to the system as a whole event though in the reality, for example, one\two or three gas detectors are not functioning;
- The leak point is defined using representative leak locations;
- The probability for having an undetected fire is regarded as negligible;
- Gas detectors are considered to be uniformly distributed within the area;
- Even if there are both point and line gas detectors, within the area necessary to guarantee the detection of the gas cloud, all detectors are modelled as point detectors.
- Detection time may be divided into intervals such as 10s, 120 s and 280 s.
- The behaviour of the personnel is modelled considering escape plan;
- Manual detector of the gas cloud may be included in the model;
- Human reliability assessment may be included;
- Difference in risk exposure between leaks from different areas and isolatable section is modelled.

For the safety system an event tree is built where the probability of failure is considered as starting point and question related to the behaviour the system is formulated in order to analyse the consequences of the scenario considered.

The result of the analysis provides the probability of failure on demand (typical value for the PFD for a gas detection system is $1*10^{-3}$) of the system related to the scenario analysed and such value then is used to evaluate the FAR.

CHAPTER 4

4 METHODOLOGY FOR ADDRESSING RISK RELATED TO DETERIORATION OF PERFORMANCE

Five questions have been presented at Para 1.2 and the first four are:

1. Why safety critical components (barrier elements) are important?
2. How is it possible to measure the degradation of a component of the barrier system?
3. What is the effect of deterioration of a component on the functionality of the entire barrier system?
4. What is the effect of deterioration of function on total risk level?
5. How the method can be applied to a real case?

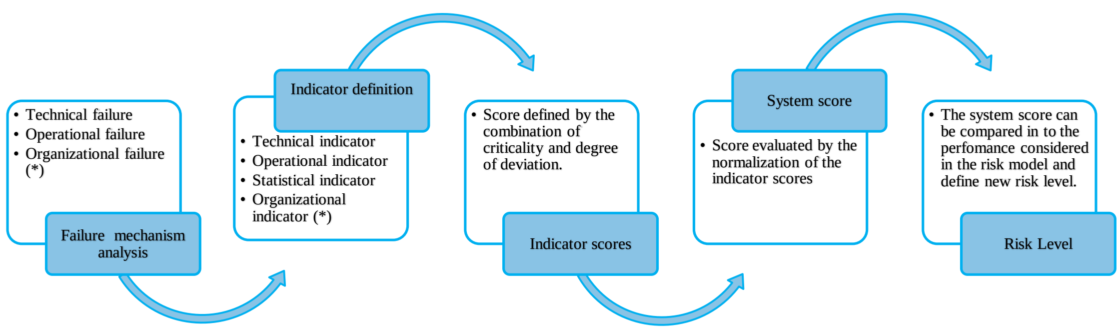
The proposed methodology applied to the detection system (introduced in Chapter 3) has the aim to find the link between the above given questions in a systematic way.

Deterioration of the system, in the method proposed, can be identified by the analysis of the failure mechanisms of the safety system. Based on such analysis it is possible to define indicators able to monitor/control these failures and define a score of the performance deviation of the system from the initial condition. The obtained performance of the safety system shall be then compared to the performance requirement for the system and evaluate the effect of the variation, if there is, of the risk level.

The method is composed considering the following elements:

- Failure mechanism of the safety critical component;
- Indicators defined based on the failure mechanisms;
- Indicator score level;
- System score that represents the performance deviation;
- Risk level.

All the elements are connected in a hierarchical chain, represented in Figure 4-1



*Not analysed

Figure 4-1 Method hierarchy representation

The first level is the identification of the failures mechanisms by for example the analysis of the maintenance activities reports of each component of the considered technical system. Other source of information can be also considered, like the OREDA book (Sintef & Oreda, 2009) or data from other installations. The identified failure mechanisms are divided into technical, operational and organizational failure. In this thesis work only the technical and operational aspect are considered while the organizational aspects are not. The reasons behind such choice are further discussed in Para 2.3.1.

The definition of the indicators is a process based on the failure mechanisms related to the component of the technical system. The aim of the indicator is to monitor directly the performance of the considered barrier system.

The third level is represented by the definition of scores for each identified indicator. The definition of the scores has been made considering the combination of the criticality and degree of deviation of the barrier system, with respect to the barrier function.

The fourth level represents the performance deviation score of all the system. The performance deviation is the result of the normalization of the combination of indicator scores from the previous level.

The last level is evaluating the effect on the risk level by use of two available methods: the relative risk approach and the QRA sensitivity approach. The relative risk approach is based on an idealized risk level that goes from 0 to 100, where 0 (system score is 0) represents that all barriers are in perfect state while and 100 (system score is 100) represents that all the barrier are critical (SINTEF, 2015). The QRA sensitivity approach uses the QRA in a more formal manner and the risk is evaluated in absolute value, e.g. FAR, PLL (SINTEF, 2015). In this thesis work the QRA sensitivity approach is considered to evaluate the effect on the risk level, identifying as referred absolute value the PFD.

The proposed method is a further development of the "Handbook for monitoring of barrier status and associated risk in the operational phase" by SINTEF (2015) applied to gas detectors system.

4.1 FAILURE IDENTIFICATION

Failure is defined as *"the termination of the capability of an item or a system to perform the required function (Standards Norway, 2011, p. 8)"*.

In this thesis the deterioration of the system has been identified as the deviation from the performance requirement of the safety system, therefore a certain level of deterioration indicates a certain percentage of deviation that the system is not performing as intended.

"Failure mechanisms are physical, chemical or other processes which lead or have led to failure"(Standards Norway, 2011, p. 8); while *"failure mode is an effect by which a failure is observed on failed item"(Standards Norway, 2011, p. 8).*

Failure mode and failure mechanism are, in this thesis, identified using the OREDA book 2009 (Sintef & Oreda, 2009), however it is suggested to integrate them with the use of real data (such as accident reports, test reports, audits etc) from the specific field(s) if available and considered reliable.

Based on the analysis of the failure mechanisms of the safety critical component it is possible to define the drift mechanisms that bring the component to fail and herby not able to fulfil its role required as barrier function and therefore significant indicators to be monitored.

For each safety critical component, the failure mechanisms are different, as a matter of fact gas detector system failures mechanisms are different compared with failure mechanisms of an ESD valves, for example. The gas detection system, being an electronic equipment, has a behaviour called like "working"/ "not working"; while the ESD valve, being a mechanic equipment, has different failure mechanism (for example internal leaks, increasing closing time) that can be the identified like a symptom of deviation from the performance of the system. Therefore, the analysis of the failure mechanisms shall be performed for all the safety system of an installation.

It is defined three different failures: technical failure, operational failure and organizational failure. Technical failures are related to the failure of the engineered system that has to perform the barrier function. Operational failures are related to the errors related to the operation to carryout in order to ensure the barrier functionality. Organizational failures are related to the failure of the managerial aspects that may influence all the system. In this thesis work organizational aspects are not considered.

In the Table 4-1 Failure mechanisms versus failure mode of the fire and gas detection system are reported and for each combination the percentage failure over the total failure rate is reported.

Table 4-1 Failure mechanisms vs Failure mode for gas detector system (Sintef & Oreda, 2009, pp. 432-433)

	ERO	FTF	HIO	HIU	LOO	LOU	NOO	OTH	SER	SHH	SLL	SPO	UNK	VLO	SUM
Clearance/Alignment Failure	0.32	-	-	-	-	-	-	-	1.3	-	-	-	-	-	1.62
Common mode failure	-	-	-	-	-	-	-	-	3.57	-	-	-	-	-	3.57
Contamination	1.62	0.65	0.32	-	0.32	-	0.32	-	0.32	0.32	0.32	0.97	-	-	5.19
Corrosion	-	-	-	-	-	-	-	-	-	-	0.32	-	-	-	0.32
External influence - General	-	1.95	-	-	-	-	-	5.84	-	-	-	0.97	-	-	8.77
Faulty signal/Indication/Alarm	5.19	-	-	-	-	-	-	-	-	-	-	-	-	-	5.19
Instrument failure - General	-	1.3	-	0.32	0.32	0.32	-	-	0.65	1.3	0.65	0.32	0.32	-	5.52
Leakage	-	-	-	-	-	-	-	-	0.32	-	-	-	-	-	0.32
Looseness	-	-	-	-	-	-	-	-	-	-	-	0.32	-	-	0.32
Material Failure - General	0.32	-	-	-	-	-	-	-	-	-	-	-	-	-	0.32
Misc. External Influences	-	-	-	-	-	-	-	-	-	-	-	0.32	-	-	0.32
Miscellaneous - General	-	-	-	-	-	-	-	-	-	-	-	0.32	-	-	0.32
Out of adjustment	7.14	0.97	1.62	6.82	0.32	0.32	0.32	1.62	2.6	1.3	0.65	0.97	0.97	38.31	63.96
Short Circuiting	-	0.32	-	-	-	-	-	-	-	-	-	-	-	-	0.32
Unknown	-	-	-	-	-	-	-	-	-	-	-	-	0.65	-	0.65
Vibration	1.95	0.65	-	-	-	-	-	-	-	-	-	0.65	-	-	3.25
Total	16.56	5.84	1.95	7.14	0.97	0.65	0.65	7.47	8.77	2.92	1.95	4.87	1.95	38.31	100

As it is possible to see from the Table 4-1 some of the combination failure mode vs mechanism has a very low probability of occurrence; therefore, it has been decided to focus the attention on the combinations with higher probability. This is believed to be a reasonable assumption in order to simplify the method without significantly affecting the outcome. However, when maintenance reports, accident reports and/or audits reports are available the list of the failure mechanisms may be modified according to the particular installation and in particular of the area analysed.

The selected combinations, to be used as basis for the definition of the indicators, are described in Para 4.1.1 and Para 4.1.2.

4.1.1 TECHNICAL FAILURES

Technical failures represent the degradation of the technical element. Thus, for each technical element present in the area of the installation analysed the technical failure shall be identified. In this thesis work they have been identified considering the combination failure mechanism vs failure mode in Table 4-1 related to the functional deterioration of a gas detection system in the OREDA book (Sintef & Oreda, 2009); and the results are listed in Table 4-2.

Table 4-2 Technical failures for gas detectors

Technical failures for gas detectors	
Failure mechanisms	***Failure mode***
Clearance/alignment	Minor in-service problems
Contamination	Erratic output
External influence - general	Other
Faulty signal/indication/alarm	Erratic Output
Instrument failure – general	Fail to function on demand

For each of the failure mechanisms it is possible to define then a failure mode, moreover for each of them it is possible to identify one or more indicator.

4.1.2 OPERATIONAL FAILURES

For operational failure it is intended failures connected to the operational aspects of the barrier system such as lack of maintenance, non-conformities, quality deviations etc…

Maintenance activities have an important role in the performance of the system. The role consists in all the activities that have the aim to preserve part of the system and the system itself from degradation. However, maintenance activities if not performed and/or if not correctly performed as defined in the maintenance procedure can increase the performance degradation.

Moreover, maintenance activities are borderline activity between the operational and organizational failures. As example, it has been stated by the Norsk Olje og Gass (2015) that the 58% of HC-leaks of the 77 recorded on the NCS between the 2008 and 2014 were caused by human intervention on the technical system (see Figure 4-2). For human intervention is considered maintenance activity on valves, seals etc. not performed as defined in the procedures.

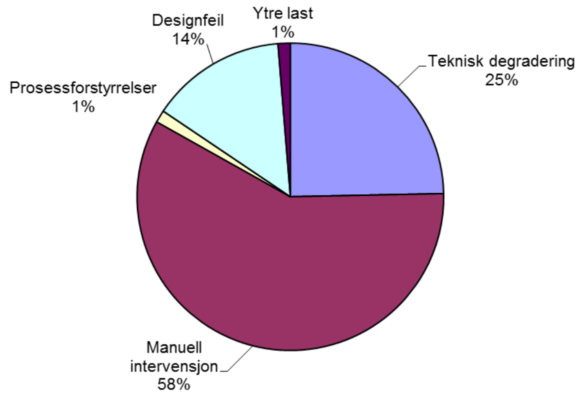


Figure 4-2 HC-leak cause (Norsk Olje og Gass, 2015)

Human interference are an important aspects of the phenomena of the degradation of technical safety system.The analysis of the human interference can be a future development of the proposed method. A structured approach to identify the human performance is the HRA (Human Reliability Analysis). This analysis has been largely utilised in the nuclear plant, but recent studies demonstrate that such analysis can be part of the QRA in the Oil and Gas industry (e.g. PetroHRA) (Koen van de, Sondre, Sandra, & Andreas, 2015). However, different challenges arised during the integration of the HRA in the QRA. One of the main challenges is related to the alignment of the HRA objectives and scope according the defintion of the context of the QRA. A guidance to integrate the HRA in the QRA is provided in Koen van de et al. (2015).

In the case of gas detectors, automatic system, the operational failures can be mostly identified in the maintenance (corrective and preventive maintenance) activities, in the quality of the maintenance procedures and documents updates.

The way the failure is identified is the same used for the technical failure identification.

Table 4-3 Operational failures for gas detectors

Operational failures for Gas detectors	
Failure mechanism	***Failure mode – operational failure***
Out of adjustment (calibration)	Very low output
Maintenance documentation	Non-Conformities
Update documents	Overdue in the updating
Near miss report	Failure not reported

4.2 IDENTIFICATION OF THE INDICATORS

Based on the definition of indicators given in Para 2.4 and the barrier given in Para 2.3.1, in this chapter the operational and technical indicator for the safety critical component are suggested/identified. As clarified earlier no organizational indicators have been considered.

The identification of the indicator is carried out with the aim to monitor the performance of the safety system based on the failure mechanisms identified in the previous chapter.

Four main concepts are used to identify the most suitable indicators for each safety system of the area subject of the analysis:

- Understand how the system degraded or fail;
- Understand how the system work;
- Understand how the system interact with the other component of the safety system;
- Understand how it is used in reality.

The activities defined in the barrier management system can give a clear understanding of how the system can degrade as all the activities to establish and maintain barriers are identified and implemented. Such activities have the aim to preserve barrier function during the lifetime of the installation (Petroleum Safety Authority, 2013) (see Chapter 2.3).

The interaction between different safety system is reflected in the QRA, where all the interactions between the detection system and the other safety system are modelled (see Para 3.3). It is, therefore, reasonable to analyse each safety system present in the installation one by one and identify the specific set of indicators. It is then obvious that some indicators may be the same, i.e. have the same impact on the performance of the barrier function, for different safety system on the installation.

The second concept represents the link between the QRA and the barrier management. Several methods have been developed in the industry with the aim to find such link of reflecting the barrier status defined in the barrier management (traffic jam identification of the barrier status, see for example (DNV GL, 2014)) in the QRA, but such link is weak as highlighted by Falck et al. (2015)

The weak link can be reinforced by the identification of specific indicators defined for each area of the installation and related to each system in order to monitor the drift mechanism that bring the barrier to not work as intended.

In the definition of the indicator it has been considered all the condition which influence the function of the barrier system. Therefore, the identification of the indicator shall be done from safety system to safety system because of the different failure mechanisms.

The main function of a gas detector system is to detect the leak when needed. Therefore, in the definition of the indicators for the single gas detector all the conditions able to inhibit the capability to detect the leak shall be considered.

As for the failure mechanisms identification, two different kind of indicators are identified for the considered safety system: technical and operational indicators.

Technical indicators are related to technical performance requirements that a barrier has to maintain in order to perform its function. In Para 4.2.1 the technical failure related to the gas detector system are identified.

Operational indicators are related to activities that have the aim to ensure the integrity of the barrier, such as maintenance activity, procedures, human activities that can influence the performance function of the barrier element. In Para 4.2.2 the operational failures related to the gas detector system are identified.

A particular operational indicator is considered in this thesis work. This is connected to the statistical indicator and is related to the probability of failure on demand of the considered safety system. The aim of such indicator is to have a continuous feedback on the maintenance activity of each barrier element. In Para 4.2.3 the statistical indicator is described and defined.

Indicators have different importance in the control of the performance of the barrier function, therefore a ranking of the criticality of each indicator using a numerical scale is suggested in order to differentiate from indicator to indicator.

Indicators, in this thesis work, are identified analysing common failure mechanism and maintenance report of gas detectors. During this process different challenges can arise: one can be the choice of the right indicator for the particular failure mechanism and thus find strong correlation between them; another can be represented by poor quality of the maintenance report upon which the failures are reported or by poor quality of the maintenance procedure. For example, a maintenance report can report: during the test, one gas detector fail. This maintenance report has poor quality in the identification of the cause of the failure (why the detector has failed) and on the identification of the detector tested. Another issue may be related to the systematic wrong performance of the available procedure by the operator; the errors rely on the wrong performed maintenance and mistakes by the operator.

4.2.1 TECHNICAL INDICATORS

Technical indicators are related to the technical issues that are able to influence the functional deterioration of the detection system (Knut Øien, 2001).

Such indicators have the aim to reflect the current status of the barrier and be able to define if the barrier is capable to perform its function (e.g. detect the leak). As mentioned in the introduction of this master thesis, often the indicators are binary while the technical failure mechanisms have different characteristics, for example the gas detectors system that has a “working/not working” behaviour and the ESD valve (ESDV) that has different failure mechanisms that gradually bring the system to fail. Thus, the indicators have to be able to reflect the differences between the failure mechanisms.

The identification of such indicators is based on failure mechanism of technical elements and they can be identified in:

- Deviation from performance requirement during operation that are not corrected when the operation is over;
- Obstruct of the barrier;
- Failures detected through self-diagnostics/loop monitoring
- Temporary exemptions

Based on this general list (part of the list is taken by DNV GL (2014)) of indicators they can be translated to the considered detection system. In Table 4-4 the connection between the list above and the considered barrier element is reported.

Table 4-4 Technical indicators for gas detectors

Technical Indicators for Gas Detectors	
Deviation from performance requirement during operation that are not corrected when the operation is over.	Gas detector is not available after tests activity, maintenance activity.
Obstruct of the barrier	Coverage of the barrier due to salt and/or mechanical coverage.
Failures detected through self-diagnostics/loop monitoring	Gas detector fails at the loop test.
Temporary exemptions	This can be related to the presence of work permit in the considered area.

4.2.2 OPERATIONAL INDICATORS

Operational indicators are related to different activities and processes with the scope to ensure that barriers are able to work as intended. As described in Para 4.1.2 operational failures are different from safety system to safety system. Thus, such indicators shall be defined for all the safety system according to their specifics characteristics. The example given above is still valid, the operational indicator for a blowdown should consider the fact that they are manually activated (human interference, that are not considered in this thesis work), while in the case of gas detectors, automatic system, the operational indicators can be mostly identified in the maintenance (corrective and preventive maintenance) activities developed.

As stated in the NORSOK Z-008 the preventive and corrective maintenance has to be organised by a maintenance plan. The maintenance plan has the aim to define the timing of the activity to be carried out on defined element of a system. the choice is made considering an FMECA or a RCM (Standards Norway, 2011). In case of gas detectors, the timing of inspection is defined on bi-weekly basis.

A list of general indicator, considering only the operational factors and not the human interference, can be identified:

- Maintenance and testing;
- Documentation update;
- Compliance to the procedure;
- Backlog on audit verification;
- Near miss report in case of barrier failure.

The list is a suggestion and can be further integrated.

In Table 4-5 a suggested list of the operational indicators for gas detectors based on the general listed above is suggested.

Table 4-5 Operational Indicators for gas detectors

Operational indicators for Gas Detectors	
Functional test	Gas detector not calibrated
Documentation update	Gas detector documents to be updated
Compliance to the procedure	Gas detectors tests done according to the procedure
Backlog and outstanding maintenance	Outstanding corrective maintenance activities, Backlog of preventive maintenance activities
Near miss report in case of barrier failure	Gas detector failure not recorded

4.2.3 STATISTICAL INDICATOR

A stated in Para 4.2 a particular operational indicator is included. The statistical indicator, in the described method, is represented by the PFD of the single barrier element. The aim of such indicator is to measure the deterioration of the single indicators by the increased probability of failure of the sensor with the time.

To include in such indicator, the maintenance activities performed on the sensor, the PFD of the sensor is set to 0 after the maintenance is performed. This is a simplification as the maintenance activity may not restore the sensor to its original status however in such way the indicator is able to monitor the maintenance/tests activities of all the barrier elements present in the considered area of the installation.

The indicator is evaluated considering the cumulative distribution function of the exponential distribution representative of the probability of failure on demand, expressed by the following expression:

$$PFD_{CDF} = 1 - e^{-\lambda t} \qquad (1)$$

Where:

- λ is the total failure rate of the considered safety system. In this thesis work this is taken from the OREDA book (Sintef & Oreda, 2009) however, if available, more reliable data should be used;
- t is the time, expressed in millions of hours, when the probability of failure on demand is evaluated.

Such indicator shall be updated on daily basis. Deviation of this indicator is defined considering two threshold levels of PFD. The first threshold is related to the planned maintenance schedule (e.g. 340h for a gas detection system) and the second one is related to the double of the maintenance program timing (e.g. 680h for a gas detection system). Thus, it is possible to have a feedback of the status of the barrier element with respect of the maintenance/tests activity, e.g. if barrier element is not tested or not maintained as stated in the procedure the single sensor PFD will increase above to the first threshold level and eventually above the second one.

The selection of the threshold levels should be based on the planned maintenance activity and a proper assessment.

The evaluation of the PFD shall be done for all elements of the safety system present in the analysed area on the installation.

4.3 DEFINITION OF INDICATORS' SCORE

For each barrier system indicator, it is necessary to define a scoring system in order to measure the impact of the indicator on the performance of the barrier system.

The scoring of each indicator is based upon considering the combination of the criticality and the degree of deviation of the indicator with respect of the barrier function. For example, considering an ESD valve it is reasonable to consider the internal leak be a critical indicator of the barrier status and a maximum criticality score may be assigned to this, but small deviation in the indicator are not so critical. Thus using the combination criticality and degree of deviation is possible to reflect the gradually development of the failure mechanisms with respect to time.

The list of the identified indicators in the previous section is the reported in Table 4-6.

Table 4-6 Indicators list

INDICATORS	
Technical indicators	
Indicator No	**Indicator description**
1	Deviation from performance requirement during operation that are not corrected when the operation is over.
2	Obstruct of the barrier
3	Failures detected through self-diagnostics/loop monitoring
4	Temporary exemptions
Operational indicator	
Indicator No	**Indicator description**
5	Functional tests
6	Documentation update
7	Compliance to the procedure
8	Backlog and outstanding maintenance
9	Near miss report in case of barrier failure
10	Statistical indicator

The criticality scale shall be defined considering the deviation of the indicator related to barrier function. In the method proposed the criticality of the indicator has been identified considering a scale from 1 to 5 for each indicator.

In the definition of the criticality the following question should be answered: "at what degree the deviation from the initial status is important for the barrier function?". An example of the indicator criticality scale is given in the Table 4-7, it has to be noted that the provided list is general and has to be defined separately for each barrier present on the installation. The definition of the criticality of the indicator is a fundamental step of the proposed method and it involves a deep understanding of the functionality of the barrier function and of the connection between the different barrier element. A risk based approach should be used to perform such activity with involvement of personnel with extensive experience both from operation and design. Moreover, it should also be revisited at regular interval or when significant modification to the barrier function or to the installation is introduced. The assignment of the criticality scores has to be done considering the criticality of one indicator with respect to others in relation with the barrier function. For example, technical indicators may have higher criticality score than some of the operational indicators because the functionality of the system is guaranteed by a "good" condition of the technical elements; while the operational indicators may only indicate that the management of the barrier shall be improved.

Table 4-7 Indicators criticality scoring

Indicators criticality scoring	
1	Deviation of the indicator does not lead to a significant jeopardize of the barrier function
2	High deviation of the indicator has small effect on barrier function
3	Deviation of the indicator will have effect on barrier function
4	Small deviation of the indicator has effect on barrier function
5	Deviation of the indicator has significant effect on barrier function

In order to measure the degree of deviation of each indicator a scale shall be defined for each indicator. A scale from 0 to 5 is suggested where 0 represents the perfect condition of the barrier system while value 5 represent the corrupt condition of the barrier system.

For each indicator the scale shall be defined separately for each defined indicator and taking into consideration the degradation mechanism intended to be monitored. It is important as well to ensure that the deviation can be simply measured on field using available data.

The deviation scale for each indicator presented in Table 4-6 is reported below. For the technical indicators and the operational indicator number 5 the deviation scale is generally presented in Table 4-9.

Table 4-8 General scoring for the indicator 1 to 5

Degree of deviation scoring for indicator 1 to 5	
0	All barrier elements are functioning
1	Minimal acceptable number of barrier element that are not functioning
2	Number of barrier element that are not functioning
3	Number of barrier element that are not functioning
4	Minimal unacceptable number of barrier element that are not functioning
5	Unacceptable number of barrier element that are not functioning

A score 0 is assigned when all the barrier element (gas detectors in our case study) are functioning and 5 it is related to the system that is not working (i.e. a specific number of barrier element are not able to perform the barrier function). In Table 4-9 the degree of deviation for the gas detection system is presented. Important step of the definition of the scale for the deviation is to identify the condition for which the barrier system is considered not acceptable. As suggested for the definition of the criticality also this step may be based on a risk assessment involving different disciplines.

Table 4-9 Degree of deviation scoring for indicator 1 to 5

Degree of deviation scoring for indicator 1 to 5	
0	all detectors functioning
1	1 detector not functioning
2	2 detectors not functioning
3	3 detectors not functioning
4	4 detectors not functioning
5	more than 4 detectors not functioning

For the operational indicators related to the maintenance activities different degree of deviation score shall be identified according the analysed indicator. For example, the indicator "compliance with procedures", that means that the operations are carried out according the established procedure, is different to the indicator "documentation update", that means that the documentation related to the barrier element is updated. Based on this difference it is suggested to analyse the identified indicator in order to group them according the activity they are monitoring. The score to assign shall be 0 when no deviations are registered and 5 when the number of deviation is no more acceptable according the applicable requirements.

The suggested scale for the different operational indicators from 6 to 9 are reported in the Table 4-10 and Table 4-11.

Table 4-10 Degree of deviation scoring for operation indicator (indicator 6)

Degree of deviation for indicator 6	
0	No overdue document
1	1 document overdue
3	more than 1 less 5 documents overdue (could be on documentation percentage)
5	more than 5 documents overdue (could be on documentation percentage)

Table 4-11 Degree of deviation for operational indicator (indicator 7 to 8)

Degree of deviation Indicator 7-8-9	
0	0 NC/OA/NM
1	No major NC/OA/NM, max 3 minor NC/OA/NM
2	No major NC/OA/NM, max 5 minor NC/OA/NM
3	No major NC/OA/NM, more than 5 minor NC/OA/NM
4	1 major NC/OA/NM
5	more than 1 major NC/OA/NM
NC = Non-Conformities *OA = Open Action* *NM = Near Miss*	

It may be noted for the indicator 6 it has been chosen to do not use all the scale from 0 to 5. It is believed that minor added value is introduced if all scale is used.

The impact of a documentation overdue on the barrier function is considered limited however a large number of overdue documents may indicate a lack of "continuous improvement approach" in the organisation.

For the indicators 7, 8 and 9 it has been chosen to consider as 5 the presence of more than one major Non-Conformities/Open Action/Near Miss. However, this upper bound should be based on the management system of the installation and on the definition of the "major" category. As example in several cases only one major Non-Conformities can be considered not acceptable.

The deviation scale for the statistical indicator is suggested in Table 4-12. In Para 4.2.3 the threshold levels of the statistical indicator were defined. The score is then defined accordingly. Again the upper bound level shall be defined in accordance to the management system and a proper risk assessment. For example, the upper bound is related to the maintenance schedule (e.g. 340h for a gas detection system) and the second one is related to the double of the maintenance schedule (e.g. 680h for a gas detection system).

Table 4-12 Degree of deviation for statistical indicator (indicator 10)

Degree of deviation Indicator 10	
0	All detectors have PFD below threshold
1	At least 1 detector above low threshold
2	More than 1 detector above low threshold, none above high threshold
3	At least 1 detector above high threshold
4	1-5 detectors above high threshold
5	More than 5 detectors above high threshold

The degree of deviation score shall be regularly updated based upon on frequency of the tests, as a maintenance activity, quality reports preparation, work permit approval etc…. An example of the frequency of the updates of the degree of deviation score is provided in Table 4-13. It has to be noted that the frequency of the updates is dependent on the type of the barrier (gas detection system, ESD valve, Blowdown) and should be based on the barrier management system of the specific installation.

Table 4-13 Degree of deviation timing update

Update frequency for the degree of deviation scores		
Technical indicator		
Indicator No	Indicator description	Update frequency
1	Deviation from performance requirement during operation that are not corrected when the operation is over.	After test activity
2	Obstruct of the barrier	Daily
3	Failures detected through self-diagnostics/loop monitoring	Daily
4	Temporary exemptions	Shift based
Operational indicator		
5	Functional test	After any calibration activity
6	Documentation update	Monthly based
7	Compliance to the procedure	Monthly based
8	Backlog and outstanding maintenance	Weekly/monthly based
9	Near miss report in case of barrier failure	Monthly based
10	Statistical indicator	Daily (PFD of the i-sensor back to 0 when i-sensor is maintained)

Finally, the value of the indicator is given multiplying the criticality and the degree of deviation.

$$Indicator\ value_i = Criticality_i * Degree\ of\ deviation_i \qquad (2)$$

Where:

- $Criticality_i$ is the criticality of the indicator i
- $Degree\ of\ deviation_i$ is the degree of deviation of the indicator i.

It has to be noted that all this analysis shall be done per area of the installation and per considered safety system.

Summarising, in order to well define the scale (both criticality and degree of deviation), it shall be necessary to apply expert judgements from operational personnel and define procedures to do it in a systematic way (e.g. questionnaires, interviews in the workshops etc.). Moreover, further analysis for the definition of the link between criticality and degree of deviation of the indicators shall be considered in order to better tailor the scoring system. In this thesis work the definition of the indicator scoring is developed in a qualitative way. However, the definition of a systematic procedure to define more precisely the score of each indicator may be a future development of the proposed method.

4.4 SYSTEM TOTAL SCORE

Assuming that the identified indicators and the assigned scoring system well represents the potential failures of the barrier it is possible to correlate the total score to the performance of the barrier.

In Figure 4-3 the graphic representation of the safety score is reported.

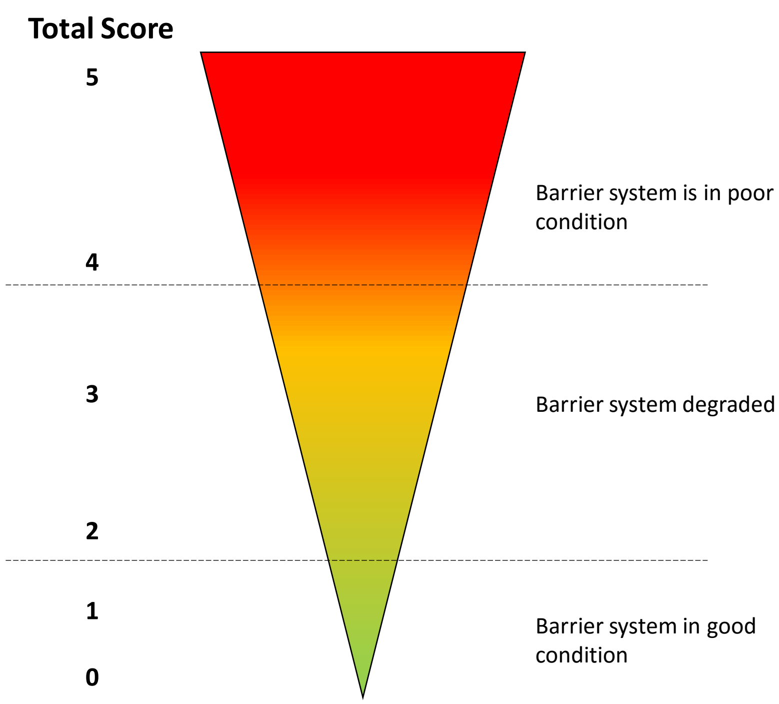


Figure 4-3 Performance deviation representation

The total score level may indicate when the performance of the system relies in the red area that the system considered is in poor conditions. At same time when the performance of the system relies in the orange area the system is able to perform its functions but activities may be performed in order to bring the system in more acceptable conditions; attention must be given in this area because represents the more uncertain area of the performance condition of the system. Finally, when the performance of the system relies in the green area the system is supposed to be in good conditions.

The measure of performance of the safety system in the considered area is given by:

$$Total\ Score = \sum_{i=1}^{n} Indicator\ value_i \Big/ \sum_{i=1}^{n} Criticality_i \qquad (3)$$

Where:

- $\sum_{i=1}^{n} Indicator\ value_i$ is the sum of all the indicator values from 1 to n;
- $\sum_{i=1}^{n} Criticality_i$ is the sum of all the criticality score of the n indicators.

The above formula gives the safety system score in a scale from 0 to 5 regardless of the number of the indicators and of the criticality score.

Some considerations have to be done with respect to equation 3. If from one hand it gives a total score independent from the number of the indicator on the other hand may occur that if the number of the indicators increase the effect of one indicator on the total score is diluted. However, the same situation may rise without the normalized scale, i.e. considering only the $\sum_{i=1}^{n} Indicator\ value_i$. For example, considering the following situation: one technical indicator with assigned criticality to 5 and degree of deviation assigned to 5, the total score will be equal to 0,73, while if the total score is given considering only the sum of the indicator $value_i$ the total score will be equal to 25. The two values have the same likelihood to happen if the number of indicators are increased, the “25” will appear more often and could be interpreted as less critical situation, as the correspondent value of 25 will be lower than 0.73 and could be interpreted as less critical situation. This effect is partially solved introducing the special consideration below.

A special consideration shall be applied in the case in which the technical indicators and operational indicator n.5 (indicators n. 1-5 in Table 4-6) have the combination criticality equal to 5 and degree of deviation equal to 5; in this case the system is supposed to not be able to perform the functionality as intended therefore the total score will be directly considered as 5. Such consideration will guarantee that critical indicator(s) will have the right influence on total score avoiding the diluting effect of increased numbers of indicators. The choice of the indicator where this special consideration apply shall be carefully performed to avoid unnecessary over conservatism in the method or to exclude indicators that have critical effect on the performance.

The performance of the barrier system may be assumed to have a normal distribution with an average value in the limit of green area of Figure 4-3 and a standard deviation that may be dependent on the quality of the barrier management system (for example, high standard deviation may represent a management system with high potential of improvement). If the construction of the total score well represents the performance of the barrier, such score should show the same behaviour with the time with average 2 and similar standard deviation.

Therefore, statistical analysis of the evolution of the total score of the barrier in specific field may be used to tailor the method to better represents the performance of the barrier.

A correlation between the total score and risk level is suggested at Para 4.5.

4.5 RISK LEVEL

The last step in the method proposed by the hierarchical structure in Figure 4-1 is the definition of the link between the barrier management activities and the risk level.

This can be done considering the sensitivity approach in the QRA analysis, proposed in the SINTEF (2015), using the obtained performance deviation to evaluate new PFD on demand of the barrier in order to assess if the risk level it is still acceptable.

The performance deviation, evaluated for all the safety system available in the considered area of the specific installation, should be used in the QRA to evaluate the correspondent change in the risk level.

The approach consists in different steps to follow:

1. Definition of the QRA parameter to consider: in this thesis work the parameter considered is the PFD of the barrier system e.g the gas detection system.
2. Identification of value of the identified parameter used in the QRA: in this thesis work it is assumed $PFD_{QRA} = 1*10^{-3}$
3. Identification of the maximum technical value of the identified parameter when the barrier is not able to perform its function: in this thesis work the maximum PFD is assumed to be $PFD_{max} = 1$.
4. Definition of the total score representing the nominal value of the parameter used in the QRA: in this thesis work the total score that is assumed to represent the $PFD_{QRA} = 1*10^{-3}$, is the one given when all indicators degree of deviation equal to 2.
5. Definition of the total score representing the worst condition of the parameter: the worst condition PFD value (e.g. 1), called PFD_{max}, is assumed when Total score is 5.
6. The correlation between the PFD and the total score is assumed to be linear with the logarithm of the PFD. This may be assumed taking into account that if the Total score go from 2 to 5 (2.5 times the original value) the PFD change from 10^{-3} to 1 (1000 times the original value). Small change of the Total score would have large change in PFD if a simple linear correlation would be used.

   Then the correlation between the total score and the PFD is given by the following formula (see. Equation 4). The correlation is reported in Figure 4-4.

$$PFD_{new}(t) = 10^{\left(log_{10} PFD_{max} + \frac{\left(log_{10} PFD_{max} - log_{10} PFD_{QRA}\right)}{(max_S - mid_S)} * (S_t - max_s)\right)} \quad (4)$$

Where:

- $PFD_{new}(t)$ is the probability of failure on demand at time (t) of the barrier system;
- max_s is the max value of the system total score (e.g. 5);
- mid_s is the mean value of the system total score (e.g. 2 see Para 4.4);
- PFD_{max} is the PFD value considered being the worst condition of the safety system (e.g.1);

- PFD_{QRA} is the PFD value considered as base case in the QRA (e.g. 10^{-3});
- s_t is the value of the total score at time t.

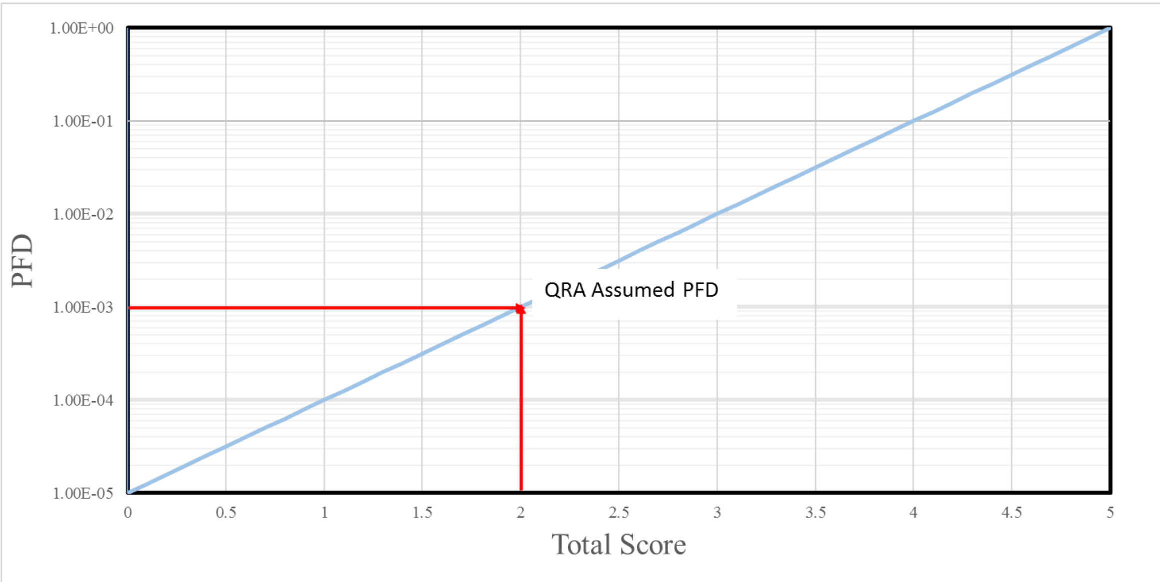


Figure 4-4 Correlation representation

The value of PFD_{new}, then, may be inserted in the event tree model of the risk analysis to evaluate a new risk picture. Such results can be useful to analyse how the risk picture is evolving during the life of the system and give the necessary information to the decision makers.

Some considerations have to be done when it comes to the definition of the value of PFD_{max} and mid_s value.

The mid_s value should be identified considering the PFD value used in the QRA. In this thesis work it is assumed that the value of total score 0 represents the system in perfect condition and 2 represents the system with small deviation in the performance.

The identification of the value should be done analysing at what condition the system is performing its function. For example if the working condition of the analysed system recognises that the system has worked with small deviation in the performance compared to the requirements and the QRA condition are still reflecting this ($PFD_{QRA} = 1 * 10^{-3}$) then the value should be fixed at 2; on the other hand, if the working condition of the analysed system recognises that the system has worked in accordance with the performance requirements ($PFD_{QRA} = 1 * 10^{-3}$) without any deviation in the performance then the value should be fixed at 0.

This kind of analysis should be done in accordance to the condition of the considered installation. It is reasonable to think that new installations could have the mid_sfixed at 0, but for elder installation the analyst should argue which value of the mid_sfits the real working conditions of the installation that still satisfies the value of $PFD_{QRA} = 1 * 10^{-3}$. In this thesis the mid_shas been considered equal to 2.

The identification of the PFD_{max}value shall be done analysing the condition in which the system is considered to not be able to perform the function according to the identified indicators. The identification of the value should be done considering a semi-quantitative analysis of the data available, for example it is reasonable to think that if in an area 5 gas detectors out of 10 are not working the system is not able to perform the function as intended (i.e. technical indicator criticality 5 and degree of deviation 5) but this does not mean that all the system has failed; therefore, an analysis of the correspondent PFD_{max} should be done considering the drift mechanisms (technical and operational) that bring the barrier to deviate from the performance requirement and the value should be define accordingly. In this thesis work the value of PFD_{max} has been set at 1 when the total score is equal to 5, the choice relied on the fact that the total score 5 can be the result of the combination of technical and operational conditions that bring the system to not perform as intended.

It has to be noted that all the evaluation shall be done with involvement with an expert team in order to well define the scale range and then to define the PFD value to refer to. The accuracy of this method is dependent on the quality of such process.

It has to be noted that the definition of the indicators for each barrier system (together with the criticality and degree of deviations) shall be regularly revisited in order to make the needed improvements to represents the performance of the barrier at required level of quality.

CHAPTER 5

5 CASE STUDY

In this chapter the method proposed is applied to a case study.

The case study consists in the application of the proposed method to an unmanned installation in the North Sea. The main characteristics of the platform are reported in Para 5.1.

The use of the method to the case study is reported in Para 5.2, then discussion on the results is reported in Para 5.3.

5.1 DESCRIPTION OF THE INSTALLATION

The case study is about an unmanned well head platform in the North Sea.

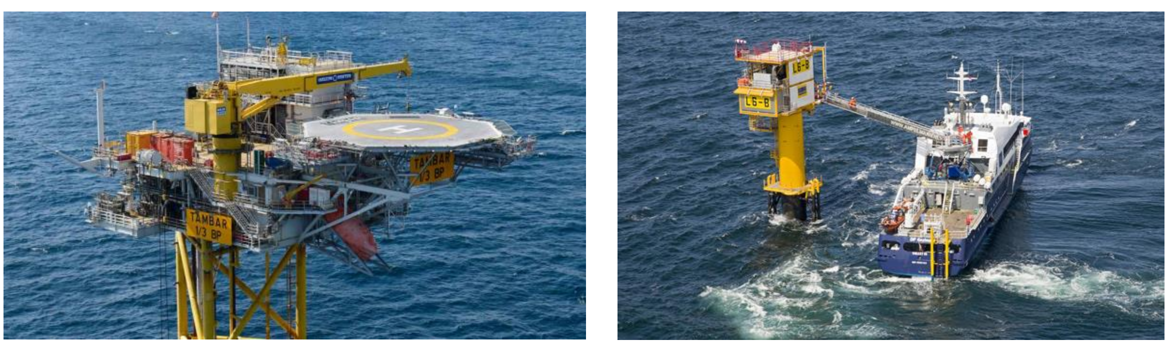


Figure 5-1 Unmanned platforms examples ("Unmanned well head platform Tambar in the North Sea. [image]," 2015; "Wintershall's Unmanned North Sea Platform Produces First Gas [image]," 2015)

This type of installation is considered to be a valid alternative to the subsea installation for shallow water condition (Oljedirektoratet Norway, 2016). There are different design options available in the industry, such as simple well head (e.g. type 4 in Figure 5-2) to more complex installation with helideck, crane and process equipment (e.g. type 0 in Figure 5-2).

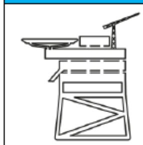
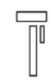
Type 0	Type 1	Type 2	Type 3	Type 4
				
Complex platform with helideck and fire water system and various process equipment. Crane. Automated to allow remote operation for typically 1-5 weeks.	Simple platform with helideck. Typically, 2-12 wells. Crane. No fire water. Test separator or multiphase metering. Designed to operate unmanned for periods of 2 – 3 weeks at a time.	Simple platform without helideck. Typically, 2-10 wells, however, up to 30 wells have been seen. Crane. No fire water. No process facilities. Designed to operate unmanned for periods of 3 – 5 weeks.	Minimalistic platform. Typically, 2-12 wells. No crane, no fire water, no process facilities. Designed to operate unmanned for periods of 6 months to 2 years.	Super minimalistic platform. Typically, only one well (max. two) on one small deck. Well connected directly to pipeline. Lift gas may be included.

Figure 5-2 Designs available for Unmanned wellhead platform (Oljedirektoratet Norway, 2016, p. 6)

The main characteristics of an unmanned platform are:

- No personnel are normally present on the installation;
- Limited maintenance activities;
- Remotely controlled;
- Used as satellite development of existing field.

This makes an installation simpler than the manned platform, in terms of placed equipment. Due to longer period between planned maintenance the selection of technology to use must follow the BAT principle (Best Available Technology) (Oljedirektoratet Norway, 2016). The limited (or none) presence of personnel on the installation may be seen as a positive aspect because it may reduce the exposure risk to personnel. However, safety condition related to HSE must be guaranteed.

On the Norwegian continental shelf this kind of technology is considered new and as announced by Statoil the first unmanned platform will be developed in the NCS in the next future (Statoil ASA, 2015, 2016).

The selected unmanned platform has the following characteristics:

- Remotely controlled by a manned platform through a subsea umbilical
- Main systems are: wellhead and xmas tree, production manifold, gas injection manifold, crane, risers and fire and gas system
- Planned maintenance twice per year using a service vessel
- No helideck
- No temporary living quarter

5.2 APPLICATION OF THE METHOD TO THE CASE STUDY

The method is applied to the gas detection system of an unmanned installation in the North Sea. The number of gas detectors, divided between the different platform decks, is reported in Table 5-1:

Table 5-1 Installation gas detectors locations and amount

Installation gas detectors locations and amount		
Deck name	Height [m.s.l.]	n. of detectors
Top Deck	35.80	0
Xmas tree Deck	30.80	9
Cellar Deck	25.80	5
ESDV Platform	22.80	3
Spider Deck	18.00	
		Tot = 17

It has to be noted that the gas detectors are located at different height, so, for example, the detectors located in the Xmas tree deck are distributed at different height between 30.80 and 35.80 in order to guarantee a good coverage in case of leak.

5.2.1 MAIN ASSUMPTIONS

The following assumptions have been used in the application of the method.

1. Due to the limited amount of data collected from the field it is assumed that total score of the barrier will be updated on monthly basis.
2. The first two years of operation are simulated in the case study. It has to be noted that the events reported in Para 5.2.4.1 does not come from field data but assumed for the purpose of showing the method.
3. Due to the limited dimension of the platform, the method is applied to the entire installation, without differentiate between the different area.
4. The degree of deviation updating frequency is defined by the maintenance plan and it is, then, different by the one given in Para 4.3 in Table 4-13. The updated frequency is given in Table 5-4.
5. The Statistical indicator has an important role in the monitoring of the maintenance activity, so attention may be given to the identification of the threshold levels. In this case the value of 0.1 has been assumed. The used failure rate is the upper value of failure rate given by the OREDA book 2009 (Sintef & Oreda, 2009) in order to have more conservative results.

5.2.2 INDICATORS' IDENTIFICATION

The identification of the indicators is performed according the procedure explained in Para 4.2 together with the assumption discussed in Para 5.2.1.

Not all the indicators identified in Para 4.2 are applicable to the case study, therefore some of them have been excluded from this example.

In Table 5-2 the indicators are listed, the one in grey are the indicators not considered applicable to the case study.

Table 5-2 List of indicators - highlighted not considered

Indicator No	Indicator description
1	Deviation from performance requirement during operation that are not corrected when the operation is over.
2	Obstruct of the barrier
3	Failures detected through self-diagnostics/loop monitoring
4	Temporary exemptions
5	Functional testing
6	Documentation update
7	Compliance to the procedure
8	Backlog on audit verification
9	Near miss report in case of barrier failure
10	Statistical indicator

Due to the unmanned condition it is assumed that the temporary exemptions, calibration tests (functional testing) and the obstruction of the barrier is not relevant to the evaluation of the total score for this case and therefore their criticality will be set to 0 for all the length of the monitoring activity, i.e. two years.

It has to be noted that all the data used are not related to real data but are data assumed in order to be able to show the potentiality of the method.

5.2.3 INDICATORS' CRITICALITY

When the criticality of the indicators is established the specific characteristics of the platform shall be considered.

Indicators 1 and 3 are assumed to be more critical because no deviation from performance had to be pendent after the operation because the maintenance are rare. The loop monitoring (indicator 3) represents the main feedback on the status of the gas detection system so its result is more critical than the others. In the same way the indicators 7 and 8 are considered at fairly high criticality because high quality maintenance activity is deemed a critical factor due to limited access possibility on the platform.

The proposed criticality for the gas detection system indicators is reported in Table 5-3.

Table 5-3 Criticality score for the gas detection system

Criticality score for gas detection system		
Indicator No	Indicator description	Criticality
1	Deviation from performance requirement during operation that are not corrected when the operation is over.	5
2	Obstruct of the barrier	0
3	Failures detected through self-diagnostics/loop monitoring	5
4	Temporary exemptions	0
5	Functional test	0
6	Documentation update	1
7	Compliance to the procedure	3
8	Backlog and outstanding maintenance	4
9	Near miss report in case of barrier failure	2
10	Statistical indicator	4

5.2.4 INDICATORS' DEGREE OF DEVIATION

The degree of deviation has to be updated according frequency of the tests or as soon as a maintenance report are filled out etc. an example of the updating timing it is reported in Table 5-4.

Table 5-4 Degree of deviation update schedule

Update frequency for the degree of deviation scores		
Indicator No	Indicator description	Update frequency
1	Deviation from performance requirement during operation that are not corrected when the operation is over.	After test activity
2	Obstruct of the barrier	
3	Failures detected through self-diagnostics/loop monitoring	After test activity
4	Temporary exemptions	
5	Functional test	
6	Documentation update	Monthly based
7	Compliance to the procedure	Monthly based
8	Backlog and outstanding maintenance	Bi-monthly based
9	Near miss report in case of barrier failure	Monthly based
10	Statistical indicator	Monthly (PFD of the i-sensor back to 0 when i-sensor is maintained)

5.2.4.1 TIMELINE

The method is applied considering a timeline of two years.

Some considerations have to be done:

1. In the timeline different events are considered that may arise during the operation of the installation;
2. At month 0 the installation is considered to be new
3. The events are assumption made to explain the use of the method

In Table 5-5 the considered timeline is reported. It has to be noted that in the table are reported only the months with identified event.

Table 5-5 Event Timeline

TIMELINE			
Month	Event ID	Event description	Remark
0	A	Gas Detection system commissioned and ready for operation. No open punch item.	It is assumed all deviation is 0
3	B	Loop test - 1 sensor fail	Such sensor is excluded from the statistical indicator.
4	C	Statistical indicator: lower threshold level met	
6	D	Planned Maintenance - All gas detectors are checked and maintained - 3 minor non conformity are identified from the maintenance report	
8	E	Loop test - 4 sensor fails	Such sensors are excluded from the statistical indicator.
9	F	Unplanned Maintenance on the 4 sensors - 3 open action from the maintenance activity: 1 major and 2 minor Documentation update overdue - One document overdue	
10	G	Documentation update overdue - One document overdue – Statistical indicator at Lower threshold	
11	H	Documentation update overdue - Action closed	

TIMELINE			
12	I	Planned Maintenance: All gas detectors are checked and maintained	
13	J	Gas Detection system assumed to have the same condition as at month 0.	It is assumed all deviation is 0
15	K	Loop test: 5 sensor fail	Such sensor is excluded from the statistical indicator. The system is considered to be no more able to perform its function
16	L	Unplanned Maintenance on the 5 sensors	
17		Statistical indicator: lower threshold level met	
18	M	- Planned Maintenance: All gas detectors are checked and maintained except for the 5 detectors maintained two months earlier - One minor Non conformity on the compliance to procedure	It is assumed statistical indicator is 0 due to maintenance except of the 5 detectors already maintained
19	N	- Documentation update overdue (more then 5) - 5 minor non conformity - Statistical indicator at the upper threshold level	
20	O	- Documentation update overdue - Non conformity Action closed	
23	P	Loop test fail on 3 detectors	
24	Q	Planned Maintenance: All gas detectors are checked and maintained, 3 minor non conformity are identified from the maintenance report	

The timeline reported in Table 5-5 corresponds to a values of the indicators reported in Table 5-6.

Table 5-6 Development of degree of deviation of the Indicators

	INDICATORS						
Month	**1**	**3**	**6**	**7**	**8**	**9**	**10**
0	0	0	0	0	0	0	0
3	0	1	0	0	0	0	0
4	0	0	0	0	0	0	2
6	0	0	0	1	0	0	0
8	0	4	0	1	0	0	0
9	0	0	1	1	4	0	0
10	0	0	1	1	4	0	2
11	0	0	0	0	0	0	2
12	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0
15	0	5	0	0	0	0	0
16	0	0	0	0	0	0	0
17	0	0	0	0	0	0	2
18	0	0	0	1	0	0	4
19	2	0	3	2	2	2	4
20	0	0	3	2	2	2	4
23	0	3	3	2	2	2	4
24	0	0	1	0	0	0	0

5.3 DISCUSSION OF THE RESULTS

Based in the timeline in Table 5-5 it is possible to evaluate the Indicator value (see Equation 2), the Total Score of the system (see Equation 3) and finally the new value of PFD (see Equation 4) to insert in the dynamic event tree to define the risk level.

An example of the intermediate steps is reported is reported in Table 5-7

Table 5-7 Intermediate steps

INTERMEDIATE STEP EXAMPLE							
Month	Event ID	Indicators n.	Criticality	Degree of deviation	Indicator Value	Total score	PFDnew
19	O	1	5	2	10	2.208	1.616E-03
		3	5	0	0		
		6	1	3	3		
		7	3	2	6		
		8	4	2	8		
		9	2	2	4		
		10	4	4	16		

Based on the timeline in Table 5-8 the obtained results of total score and PFD_{new} are reported.

Table 5-8 Results

RESULTS			
Month	Event ID	Total Score	PFDnew
0	A	0.000	1.000E-05
3	B	0.208	1.616E-05
4	C	0.333	2.154E-05
6	D	0.125	1.334E-05
8	E	0.958	9.085E-05
9	F	0.833	6.813E-05
10	G	1.167	1.468E-04
11	H	0.333	2.154E-05
12	I	0.000	1.000E-05
13	J	0.000	1.000E-05
15	K	5.000	1.000E+00
16	L	0.000	1.000E-05
17	M	0.333	2.154E-05
18	N	0.792	6.190E-05
19	O	2.208	1.616E-03
20	P	1.542	3.481E-04
23	Q	1.542	3.481E-04
24	R	2.167	1.468E-03

In Figure 5-3 the trend of the PFD_{new} and of the total failure rate is reported.

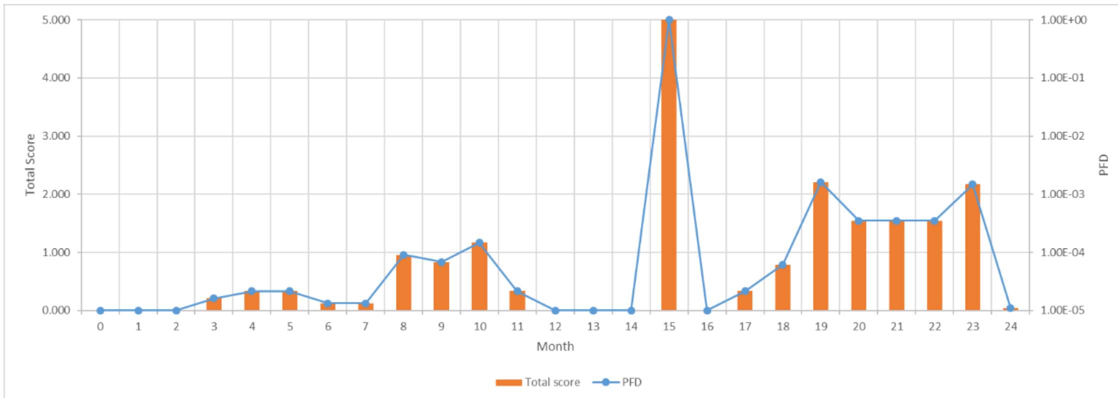


Figure 5-3 Results trend

Based on the events defined in the timeline, the system has mostly worked in the green area (defined in Para 4.4). Attention need to be paid at months 15, 19 and 23. The first represents the special condition (technical indicator with criticality 5 and degree of deviation 5) and the other two months are correspondent to the orange zone.

Some consideration has to be done regarding month 15. The gas detection system is considered to be no more able to perform its function. The value of PFDnew is equal to 1, in this condition the operations on the installation may be stopped. Such value of PFD represents the degraded system and has to be inserted in the dynamic event tree to analyse the interaction with the other safety system on the installation.

In Figure 5-4 the representation of the most significate results of the total score is reported.

Assuming that the performance of the barrier system has a normal distribution the mean value of the total score is equal to 0.783 meaning that the system has mostly worked in safe condition, however the standard deviation value is 1.104. Such high value for the standard deviation may indicate that quality of the barrier management system shall be improved, however the limited amount of considered data is probably insufficient to derive any final conclusion.

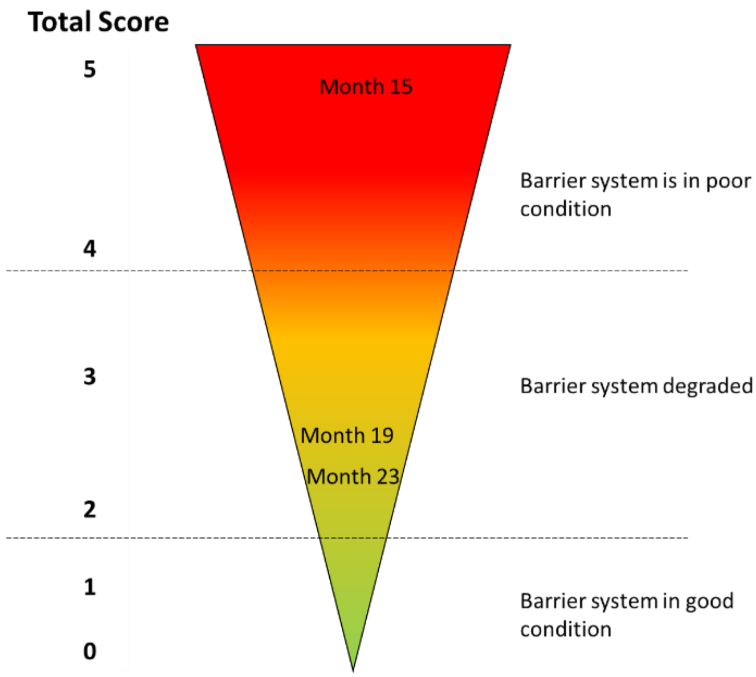


Figure 5-4 Total score

In the use of the proposed method some strength points have raised:

- Possibility to modify the method according the specific needs of the analysed installation. In this case study, for example, the update of the data has been modified from the suggested daily to monthly update due to the peculiarity of the installation;
- The list of the indicators has been modified according the characteristic of the installation as explained in Para 5.2.1;
- Different threshold levels, compared to the one identified in Para 4.2.3, have been considered for the statistical indicator.
- The application of such method to an unmanned installation suggests that the method may be applied to different system as subsea safety systems.

In the use of the method some limitations have raised:

- The limited amount of data used can't give an extensive feedback on the quality of the barrier management system, as highlighted above;

- The method need to be applied together with a team of expert in order to made the right choices related to the definition of the indicator criticality and degree of deviation;
- The definition of the PFDmax shall be done considering the characteristic of the gas detection system to be consistent with the QRA.
- The data used are assumed.

CHAPTER 6

6 DISCUSSION AND CONCLUSION

The scope of this thesis work was the establishment of a methodology able to define at what degree the deterioration of the safety system influences the risk level. The deterioration of the barrier system has been identified in the analysis of the failure mechanisms of the safety system. From this basic assumption the method has been established following different steps, as reported in Figure 6-1.

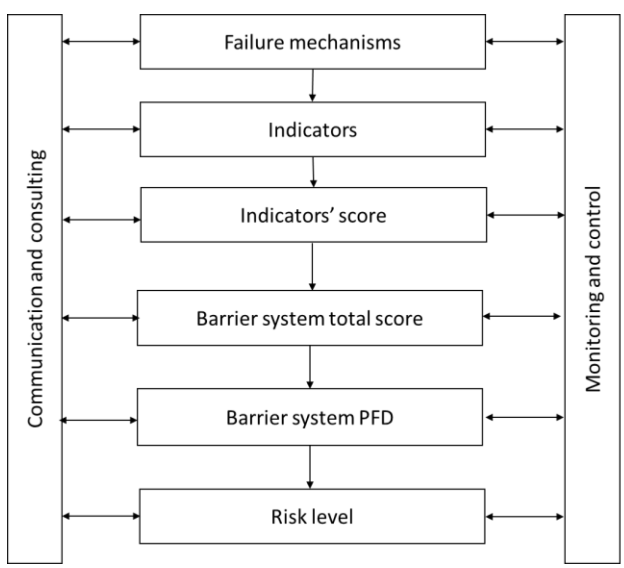


Figure 6-1 Method steps summary

The analysis of the failure mechanisms can bring the analyst to the identification of the of the drift mechanisms that bring the component to fail and hereby not able to fulfil its role required as barrier function. Based on the failure mechanisms analysis, indicators can be identified to monitor such failures. For all the steps the communication and consulting with expert and the continuous monitoring and control are important for the success of the method and for establishing a management process around performance of barriers.

As said at the beginning of Chapter 4 the methodology proposed is a further development of the *"Handbook for monitoring of barrier status and associated risk in the operational phase"* (SINTEF, 2015). The main differences rely in the aim to monitor the deterioration of the barrier system and by it evaluate if the system is still able to perform as required. Another difference is the definition of the indicators based on failure mechanisms and their weights is defined considering the combination of criticality and the degree of deviation of the barrier from the performance requirements.

Several strength points may be identified for the proposed method. The first strength point is that the proposed method uses as base case the gas detection system but it is believed that can be easily applied to all the other safety system following the steps summarised in Figure 6-1. This represents a strength point because it is possible to monitor the deterioration of all safety systems present on an installation and connect them directly to the risk level of the installation.

The identification of indicators shall be based on the analysis of the failure mechanisms of the barrier element able to reflect the deterioration of the barrier system. One important element is that the identification of the indicators must reflect the nature of the different barrier systems present on the installation, for example the behaviour of a gas detection system is different compared to the ESD system. Based on the methodology proposed the number of the indicators is not fixed and the list of indicators can be easily modified.

The indicators are characterised by the combination of the criticality and the degree of deviation of the barrier system with respect of the barrier functionality. The criticality value indicates how dependant is the barrier function from the specific indicator, while the degree of deviation has the aim to reflect the real condition of the barrier system of the installation. This is described in detail in Para 4.3.

The introduction of the statistical indicator may be seen as good tool to have a real time measure of the maintenance activity quality as explained in Para 4.2.3.

The method has the aim to monitor and to assess the effect of the deviation of the barrier performance of the barrier system on daily basis in order to have a real time update of the risk level. This is possible by updating the degree of deviation value. The frequency of update of the degree of deviation depends on the specific indicator; for example, the degree of deviation score for the "statistical indicator" may be updated on daily basis while the "document updated" may be updated on monthly/bi-monthly basis.

If the method proposed will be used on different installations, it can be used to monitor the different risk level and compare them in order to benchmark and share knowledge between installations.

The proposed method may be used as decision tool to set better mitigation actions and maintenance activities. The use, indeed, in the long run of such method and its continuous monitoring of the barrier performance can be used by the management to optimise maintenance plan that may fit better the needs of the specific field and lifetime of the asset.

It is probably compatible with the actual barrier management activities available in the industry and, perhaps, easy to be implemented by operators.

If widely adopted by the industry the method may be used to better analyse the interaction of the incident with a technical root cause and the barrier performance by the analysis of the indicators and total scores.

The application of the method on a specific barrier system of a specific installation extensively depends on expert judgement and the success of the method relies on the right choices made. The use of the expert judgement shall be done wisely and the experts' knowledge must be evaluated. Different studies have been development on the use of the expert judgement in the engineering studies and challenges are related to the uncertainties related to the assessment of the knowledge, traceability and consistency of the assessment developed by the experts.

The organizational aspects are not considered in the method proposed; this choice may be considered as a weak point of the method, but at the same time it may represents a starting point for a future development of the method itself.

In the development of the method a high number of uncertainties may arise and has to be evaluated and assessed. Uncertainties are related to the development of the method such as the definition of the scoring system for the indicators and the identification of the indicators itself. There are uncertainties related to the use of historical data, the quality of the maintenance plan and report able to reflect the real behaviour of the system. Finally, there may be uncertainties related on how personnel is going to use and implement the proposed method.

The main uncertainties are related to the use of maintenance report as basis for the identification of the failure mechanisms, this is true if the quality of the maintenance procedure and reports are high. However, quality indicators are introduced in order to partially mitigate this issue.

In the development of the method different potential development points have been identified.

The use of the Bayesian Network to analyse the interactions between all the technical, operational and organizational aspect, of the barrier system may be another tool to describe the correlation between such aspect. However different challenges may arise in the use of such tool, as pointed out in Nyheim et al. (2010). The main one is probably the high number of the conditional probability tables to set in advance and the correspondent difficulties to build a practical system to be used by operators on daily basis (e.g. operators).

Another developing aspect may be identifying a ranking procedure of the barrier element. The raking methodology may start from the basic assumption that each component of the barrier system influences the total performance of the system and a way to analyse the relative importance of each component among other may be considered. The ranking of the barrier element may be easily implemented for barrier element of the system such as ESD valve, while it is difficult to implement for system with high redundancy such as the gas detector system considered in this thesis.

Some challenges have raised in the establishment of the equation for the evaluation of the Total Score (Equation 3). The strength of such equation is that it gives a total score value independent from the number of the indicator but on the other hand may occur that if the number of the indicators increase the effect of one indicator on the total score is diluted. To mitigate such effect, the method includes the possibility to apply a special consideration to indicators that are considered critical for the performance of the barrier. The complete discussion is given in Para 4.4.

Another important aspect of the method relies in the definition of the PFDmax value. A complete analysis of the system should be done in order to define the most suitable value of PFDmax that well represent the condition in which the system is not able to perform as intended. Refer to Para 4.5 for further details.

Another important assumption made for the development of the method and the definition of the indicator score is the independence of the indicator. In fact, indicators are considered independent one each other and the definition of their criticality is independent as well. However, it can happen that second order effect are present between indicators; this aspect is not considered in the proposed method but can be part of its future development.

Finally, the definition of the criticality and degree of deviation scale may be done in a more systematic way, considering particular probability distribution and more detailed procedure to be followed.

As conclusion of this thesis work, the method proposed may represent a starting point in the identification of the deterioration of the barrier element that can influence the risk level. The scope of the thesis, find a stronger link between the QRA and the barrier management activities has been identified by the definition of specific indicators for each barrier. Furthermore, some developments have been identified as well.

REFERENCES

Ale, B. J. M. (2002). Risk assessment practices in The Netherlands. *Safety Science, 40*(1), 105-126. doi:10.1016/S0925-7535(01)00044-3

Aven, T. (2012). *Foundations of Risk Analysis* (2nd ed. ed.). Hoboken: Wiley.

Aven, T. (2013). Practical implications of the new risk perspectives. *Reliability Engineering and System Safety, 115*, 136-145. doi:10.1016/j.ress.2013.02.020

Aven, T. (2014). *Risk, Surprises and Black Swans : Fundamental Ideas and Concepts in Risk Assessment and Risk Management*. Florence: Taylor and Francis.

British Standards, I. (2008). *Occupational health and safety management systems : guidelines for the implementation of OHSAS 18001:2007* (2nd ed. ed. Vol. OHSAS 18002:2008). London: OHSAS Project Group.

DNV GL. (2014). *Good Practices - Barrier Management in operation for Rig Industry* D. GL (Ed.) *Reliab. Eng. Syst. Saf.* Retrieved from https://www.rederi.no/DownloadFile/?file=12349

DNV GL. (2016). The new standard for offshore QRA modelling - Safeti Offshore. Retrieved from https://www.dnvgl.com/services/the-new-standard-for-offshore-qra-modelling-safeti-offshore-1727

Falck, A., Flage, R., & Aven, T. (2015). Risk assessment of oil and gas facilities during operational phase. *Safety and Reliability of Complex Engineered Systems: ESREL 2015*, 373.

Flage, R., & Aven, T. (2009). Expressing and communicating uncertainty in relation to quantitative risk analysis (QRA). *Reliability & Risk Analysis: Theory & Application, 2 (2),* 9-18. Retrieved from http://www.researchgate.net/publication/228623141_Expressing_and_communicating_uncertainty_in_relation_to_quantitative_risk_analysis_(QRA)

Hafver, A., Lindberg, D. V., Jakopanec, I., Pedersen, F. B., Flage, R., & Aven, T. (2015). *Risk—from concept to decision making.* Paper presented at the Safety and Reliability of Complex Engineered Systems - Proceedings of the 25th European Safety and Reliability Conference, ESREL 2015.

Health and Safety Commission. (1997). *Prevention of fire and explosion, and emergency response on offshore installations - Offshore installation (Prevention of fire and explosion and emergency responce) Regulations 1995*. Suffolk (UK) HSE Book.

Honeywell Analytics. (2015). Searchline Excel. Retrieved from http://www.honeywellanalytics.com/~/media/honeywell-analytics/products/searchline-excel/documents/11256_searchline-excel-ir_ds0282_v8_0215_emea_lr.pdf?la=en

International Organization for Standardization. (2002). *Petroleums- og naturgassindustri - produksjonsinstallasjoner til havs retningslinjer for verktøy og metoder for fareidentifikasjon og risikovurdering NS-EN ISO 17776 = Petroleum and natural gas industries - offshore production installations guidelines on tools and techniques for hazard identification and risk assessment (ISO 17776:2000)* (Vol. 17776). Oslo: Pronorm Norges Standardiseringsforbund.

International Organization for Standardization. (2009). *Risk management : Principles and guidelines* (Vol. ISO 31000). Geneva: ISO.

Kaplan, S., & Garrick, B. J. (1981). On The Quantitative Definition of Risk. *Risk Analysis, 1*(1), 11-27. doi:10.1111/j.1539-6924.1981.tb01350.x

Koen van de, M., Sondre, i., Sandra, H., & Andreas, F. (2015). Guidance on integrating Human Reliability Assessment in Quantitative Risk Assessment *Safety and Reliability of Complex Engineered Systems* (pp. 3147-3155): CRC Press.

Lowrance, W. (1976). Of acceptable risk (Vol. 101, pp. 1434).

Norsk Olje og Gass. (2015). Hva er årsakene til HC-lekkasjer? . Retrieved from http://www.norskoljeoggass.no/no/Hydrokarbonlekkasjer/Hva-er-arsakene-til-HC-lekkasjer/

Nyheim, O. M., Gran, B. A., Pedersen, L. M., Seljelid, J., Vinnem, J. E., & Vatn, J. (2010). Use of bayesian network for modeling risk influencing factors. Boca Raton, Fla.: CRC Press, cop. 2010.

Øien, K. (2001). *Risk control of offshore installations : a framework for the establishment of risk indicators.* (2001:22), Department of Production and Quality, Norwegian University of Science and Technology, Trondheim.

Øien, K., Utne, I. B., & Herrera, I. A. (2011). Building Safety indicators: Part 1 – Theoretical foundation. *Safety Science, 49*(2), 148-161. doi:10.1016/j.ssci.2010.05.012

Oljedirektoratet Norway. (2016). *Unmanned Wellhead Platforms - UWHP* [s.n.] (Ed.) *Summary report* Retrieved from http://www.npd.no/Global/Norsk/3-Publikasjoner/Rapporter/Unmanned-wellhead-platforms/ROGC-Z-RA-000027-1-003.pdf

Petroleum Safety Authority. (2013). *Principles for barrier management in the petroleum industry* Retrieved from http://www.ptil.no/getfile.php/PDF/Barrierenotatet%202013%20engelsk%20april.pdf

Petroleum Safety Authority. (2015a). The goal of the main priority is that technical, operational and organisational barrier elements are maintained in an integrated and consistent manner in order to minimise risk. Retrieved from http://www.psa.no/barriers/category1215.html

Petroleum Safety Authority. (2015b). *Trends in risk level in the petroleum activity* Retrieved from http://www.psa.no/getfile.php/PDF/RNNP%202014/RNNP_2014_ENG.pdf

Petroleum Safety Authority (Management Regulation). (2015). *Guidelines regarding the management regulations*. Retrieved from http://www.psa.no/management/category401.html.

Reason, J. (1997). *Managing the risks of organizational accidents*. Aldershot: Ashgate.

SINTEF. (2015). *Handbook for monitoring of barrier status and associated risk in the operational phase. The risk barometer approach* (Vol. SINTEF F27045). Trondheim SINTEF, Technology and Society, Safety and Reliability.

Sintef, & Oreda. (2009). Control and safety equipment - Fire and gas Detectors. In [s.n.] (Ed.), *OREDA : offshore reliability data handbook : Vol. 1 : Topside equipment* (5th ed. ed., pp. 427-454). Trondheim: OREDA Participants.

Sklet, S. (2006). Safety barriers: Definition, classification, and performance. *Journal of Loss Prevention in the Process Industries*, *19*(5), 494-506. doi:10.1016/j.jlp.2005.12.004

Skogdalen, J. E., Utne, I. B., & Vinnem, J. E. (2010). Looking back and forward: could safety indicators have given early warnings about the deepwater horizon accident? *The macondo Blowout, 3rd progress report. Issued on December*, *5*.

SRA (Society of Risk Analysis). (2015). SRA glossary. Retrieved from http://www.sra.org/sites/default/files/pdf/SRA-glossary-approved22june2015-x.pdf

Standards Norway. (2001). NORSOK STANDARD I-002 Safety and autimation system (SAS) Rev. 2. Norway Oslo Standards Norway.

Standards Norway. (2008). NORSOK S-001 Technical safety, Edition 4. Norway: Standards Norway.

Standards Norway. (2010). NORSOK STANDARD Z-013 Risk and emergency preparedness. Norway: Standards Norway.

Standards Norway. (2011). NORSOK STANDARD Z-008 Risk based maintenance and consequence classification. Norway: Standard Norway

Statoil ASA. (2015). Unmanned wellhead platform chosen concept for Oseberg Future development Retrieved from http://www.statoil.com/en/NewsAndMedia/News/2015/Pages/09Feb_Oseberg_wellhead.aspx

Statoil ASA. (2016). Statoil awarding contracts for Oseberg Vestflanken 2, Johan Sverdrup and Gina Krog Retrieved from http://www.statoil.com/en/NewsAndMedia/News/2016/Pages/03feb-contracts.aspx

Step change in safety. (2012a). *Assurance & Verification summary guidance* Vol. 2. S. c. i. safety (Ed.) *Managing risks to prevent and minimise the impact of major accident* Retrieved from https://www.stepchangeinsafety.net/safety-resources/publications/assurance-and-verification-summary-guidance

Step change in safety. (2012b). Assurance and Verification Workforce Summary [image]. Retrieved from https://www.stepchangeinsafety.net/safety-resources/publications/assurance-and-verification-workforce-summary

Swiss Cheese Model [image]. (2016). Retrieved from https://en.wikipedia.org/wiki/Swiss_cheese_model

Unmanned well head platform Tambar in the North Sea. [image]. (2015). Retrieved from http://subseaworldnews.com/wp-content/uploads/2015/10/NPD-Studies-Unmanned-Wellhead-Platforms-as-Alternative-to-Subsea-Tie-Back.jpg

Vinnem, J. E. (2010). Risk indicators for major hazards on offshore installations. *Safety Science, 48*(6), 770-787. doi:10.1016/j.ssci.2010.02.015

Vinnem, J. E. (2014a). Offshore Risk Assessment : Principles, Modelling and Applications of QRA Studies : Vol 1Springer Series in Reliability Engineering (3rd ed. ed.).

Vinnem, J. E. (2014b). Offshore Risk Assessment : Principles, Modelling and Applications of QRA Studies : Vol 2Springer Series in Reliability Engineering (3rd ed. ed.). London: Springer.

Wintershall's Unmanned North Sea Platform Produces First Gas [image]. (2015). Retrieved from http://images.rigzone.com/images/home/article/hf_139146_article.jpg