



NTNU – Trondheim
Norwegian University of
Science and Technology

Classifying and Defining Operational and Organizational Aspects of Barriers for the Offshore Oil and Gas Industry

Arve Olaf Alvik Torgauten

Master of Science in Mechanical Engineering

Submission date: June 2013

Supervisor: Stein Haugen, IPK

Co-supervisor: Sondre Øie, Det Norske Veritas (DNV)

Norwegian University of Science and Technology

Department of Production and Quality Engineering

*Give me six hours to chop down a tree
and I will spend the first four sharpening the axe.*

Abraham Lincoln

MASTER THESIS
SPRING 2013
for
stud.techn. Arve Olaf Alvik Torgauten

**Operational and organizational barriers in the offshore industry
(Operasjonelle og organisatoriske barrierer i offshoreindustrien)**

The Petroleum Safety Authority in Norway has had an increasing focus on barriers and barrier management over the last few years and has placed this as one of their top five priorities for several years. Traditionally, barriers have mainly been associated with technical systems, but the use of the term has widened significantly and includes both operational and organizational aspects. However, this has also led to confusion. Partly, the definitions of terms that are available are not necessarily well suited for the purpose and partly the terms are not defined at all. A clarification of terms is therefore considered to be useful and necessary.

The master thesis will cover the following tasks (the tasks may be changed as the work progresses, in agreement with the supervisor):

1. Perform a comprehensive review of literature on the topic of barriers, and in particular human and organizational barriers. This should build on the review performed in the project thesis and summarize additional literature found during the search.
2. Discuss existing definitions of barrier, barrier functions, barrier elements and influencing factors with a view to determine their suitability in relation to operational and organizational barriers. Use examples and consider in particular if the definitions make it possible to distinguish between barrier elements and influencing factors.
3. Evaluate how operational and organizational barriers can be modeled in risk analysis.
4. Consider barrier classifications/categories proposed in the literature and see if they are suitable for classification of operational and organizational barriers. Propose a classification scheme that is helpful in relation to monitoring of operational and organizational barriers and also in relation to modeling.
5. Based on the review of how barriers can be modeled in risk analysis, evaluate the suitability of using SPAR-H as a method for modeling barriers in the oil and gas industry.

Within three weeks after the date of the task handout, a pre-study report shall be prepared. The report shall cover the following:

- An analysis of the work task's content with specific emphasis of the areas where new knowledge has to be gained.
- A description of the work packages that shall be performed. This description shall lead to a clear definition of the scope and extent of the total task to be performed.
- A time schedule for the project. The plan shall comprise a Gantt diagram with specification of the individual work packages, their scheduled start and end dates and a specification of project milestones.

The pre-study report is a part of the total task reporting. It shall be included in the final report. Progress reports made during the project period shall also be included in the final report.

The report should be edited as a research report with a summary, table of contents, conclusion, list of reference, list of literature etc. The text should be clear and concise, and include the necessary references to figures, tables, and diagrams. It is also important that exact references are given to any external source used in the text.

Equipment and software developed during the project is a part of the fulfilment of the task. Unless outside parties have exclusive property rights or the equipment is physically non-moveable, it should be handed in along with the final report. Suitable documentation for the correct use of such material is also required as part of the final report.

The candidate shall follow the work regulations at the company's plant. The candidate may not intervene in the production process in any way. All orders for specific intervention of this kind should be channelled through company's plant management.

The student must cover travel expenses, telecommunication, and copying unless otherwise agreed.

If the candidate encounters unforeseen difficulties in the work, and if these difficulties warrant a reformation of the task, these problems should immediately be addressed to the Department.

The assignment text shall be enclosed and be placed immediately after the title page.

Deadline: June 10th 2013.

Two bound copies of the final report and one electronic (pdf-format) version are required.

Responsible supervisor:

Stein Haugen
E-post: stein.haugen@ntnu.no
Telefon: 73590111 / 93483907

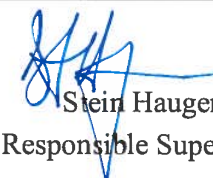
Company supervisor:

Sondre Øie, DNV
E-post: Sondre.oie@dnv.com
Telefon: 94861628

**DEPARTMENT OF PRODUCTION
AND QUALITY ENGINEERING**


Per Schjølberg

Associate Professor/Head of Department



Stein Haugen
Responsible Supervisor

Preface

This master thesis is written at the Norwegian University of Science and Technology, Faculty of Engineering Science and Technology, Department of Production and Quality Engineering, in collaboration with Det Norske Veritas. It is carried out during the spring semester of 2013. The thesis is within the field of risk management, with an emphasis on barrier management and analysis. It is a continuation of the work done in the project thesis on Risk Assessment, which also focused on barrier definitions.

The thesis is written for readers with an understanding of the basic methodologies and terms used in risk assessments and analysis, that either conduct studies within the field of safety and risk, or works with safety and risk.

Trondheim, 2013-06-10

A handwritten signature in black ink, reading "Arve Olaf Alvik Torgauten". The signature is written in a cursive style with a large, sweeping initial 'A'.

Arve Olaf Alvik Torgauten

Acknowledgment

I would like to thank my supervisors, Professor Stein Haugen at the department of Production and Quality Engineering (NTNU), and Sondre Øie, Risk Management & Human Factors Consultant at Det Norske Veritas, for their guidance and help with the thesis throughout the semester.

I also acknowledge the contributions of Det Norske Veritas, and their department of Risk Management, for their interest in my thesis topic. Especially I would like to thank Koen van de Merwe, and his help during the literature search.

A.O.A.T.

Summary

This master thesis is written on the topic of barrier management, and specifically the human and organizational aspects of this field. The main objective of the thesis is to clarify the use of terms related to human and organizational aspects of barrier management. The thesis is restricted to major accident risks in the offshore oil and gas industry.

There have in the later years been an increasing focus on the operational and organizational aspects of risk reduction. In addition to this focus, the Petroleum Safety Authority in Norway have stated that barriers are one of their most important areas of focus. There are however a large number of different definition sets and classification schemes for barriers and risk reducing measures, both within the oil and gas industry, and in other industries. These definitions and classifications integrate to a varying extent human and organizational aspects of the risk reducing measures. There are also difficulties incorporating the human and organizational contributions into accident scenario modeling, both because of the lack of data on these aspects and the lack of modeling methods that are adaptable for the oil and gas industry.

Some of the main differentiation between the definitions that are described in the thesis is the differentiation between what aspects that are a part of the barrier, and what aspects that influences the barrier. Here there are some definitions that operates with a wide scope of what constitutes a barrier, where human actions, rules, regulations, procedures and plans can be considered a part of the barrier, while other definitions strictly limits the scope of barriers to only include technical and physical elements. The barrier definitions are often broken down into sub-definitions. Some of the most common terms that are used are *barrier elements*, *barrier systems*, *barrier functions*, and of course *barrier*. Some definition sets also include *influencing factors*. Though correlations exists between the different barrier definitions, there are some significant differences, especially on the operational and organizational aspects.

Some modeling methods, that incorporates or focuses on human and organizational aspects are described and discussed in the thesis. The main focus is on Human Reliability Analysis methods. This is a set of methods that are mainly developed and used in the nuclear power

industry to model human actions. These models differentiate between human actions, performance shaping, or influencing, factors, and uses probabilities to model human error or failure. These modeling methods have not previously been used, to any great extent, in the oil and gas industry, because of the challenges of adapting the data and models to the operations performed on an oil rig, from the operations on nuclear power plants. The other modeling methods that have been described and discussed are the use of Bayesian Belief Networks, the Functional Resonance Modeling Method and the System-Theoretic Accident Model and Process methodology. These all have pros and cons regarding application for barrier modelling in the offshore oil and gas industry.

Some of the definitions that was found and discussed in the literature survey, are applied to different major accident related scenarios, in order to examine the differences between these closer, in case scenarios. The cases that are used, are in different stages of an accident scenario. The first case is an maintenance operation, where the different steps in the operation are described. The second case is in relation to a drilling operation. Here the different elements in well kick-detection are described. The last case is a hydro carbon leak scenario, where different safety measures and procedures are described. For these three cases, four different definitions or classifications of barriers are applied. The comparison shows that most of the differences between the definitions are related to operational and organizational aspects of the procedures and measures.

The findings in the thesis points towards that a focus on the function of the barriers is the best way of incorporating operational and organizational aspects of barrier management into modeling. This is opposed to a hardware focused barrier definition. A set of barrier definitions that is based on this function-oriented view is proposed. Also a framework to identify barriers, based on the new set of barrier definition is proposed. The proposed definition set is applied to the same cases as the definitions found in the literature survey. The barrier identification framework is exemplified through the application on a hydro carbon leak scenario. The findings and the proposed definition are discussed, and some areas that are in need of future work are proposed.

Samendrag

Denne masteroppgaven er skrevet om temaet barrierestyring, med fokus på de menneskelige og organisatoriske aspektene av barrierer. Hovedmålet med oppgaven er å avklare bruk av termer knyttet til menneskelige og organisatoriske aspekter av barrierestyring. Oppgaven er begrenset til storulykkesrisiko innen offshore olje-og gassindustri.

Det har i de senere år vært et økende fokus på operasjonelle og organisatoriske aspekter av risikoreduksjon. I tillegg til dette fokuset, har Petroleumstilsynet uttalt at barrierer er ett av deres viktigste satsningsområder. Det er imidlertid flere forskjellige definisjoner og klassifiseringer av barrierer og risikoreduksjons tiltak, både innen olje-og gassindustrien, og i andre næringer. Disse integrerer i varierende grad menneskelige og organisatoriske aspekter av risikoreduksjons tiltak. Det er også utfordringer, som omfatter de menneskelige og organisatoriske bidragene i ulike modelleringsmetoder, både på grunn av manglende data om disse aspektene og mangel på modelleringsmetoder som er tilpasset olje-og gassindustrien.

Noen av de viktigste forskjellene mellom de definisjonene, som er beskrevet i oppgaven, er differensiering mellom hvilke aspekter som er en del av barrieren, og hvilke aspekter som påvirker barrierer. Her er det noen definisjoner som opererer med et bredt scope i forhold til hva det er som utgjør en barriere. I disse er menneskelige handlinger, regler, forskrifter, prosedyrer og planer betraktet som en del av barrieren. Andre definisjoner begrenser scopet til definisjonene ved å bare inkludere tekniske og fysiske elementer som barrierer. Det er også forskjeller i måten barrieredefinisjonene er brutt ned i under-definisjoner. Noen av de vanligste elementene er; barriere elementer, barriere systemer, barriere funksjoner, og selvfølgelig barrierer. Noen definisjonssett inkluderer også påvirkende faktorer. Selv om det er korrelasjoner mellom de ulike barrieredefinisjonene, er det også noen vesentlige forskjeller, særlig i forhold til operasjonelle og organisatoriske aspekter.

Noen modelleringsmetoder, som inkorporerer eller fokuserer på menneskelige og organisatoriske aspekter er beskrevet og diskutert i oppgaven. Hovedfokuset er på metoder innen

Human Reliability Analysis. Dette er en samlebetegnelse på metoder, som har blitt utviklet og brukt i kjernekraftindustrien, for å modellere menneskelige handlinger. Disse modellene skiller mellom menneskelige handlinger, ytelses influerende/påvirkende faktorer. Metodene bruker feil-sannsynligheter for å modellere menneskelige feil og svikt. Modelleringsmetodene har til nå ikke vært så mye brukt i olje-og gass-industrien, på grunn av utfordringene med å tilpasse data og modeller fra operasjoner på atomkraftverk til operasjoner utført i olje og gass industrien. Andre modelleringmetoder, som er beskrevet og diskutert, er bruk av *Bayesian Belief Networks*, *Functional Resonance Modeling* metoden og *Sytem-Theoretical Accident Model and Process* metodikken. Det er fordeler og ulemper med alle disse modeleringsmetodene i forhold til barrieremodellering i olje- og gass-industrien.

For å undersøke forskjellene mellom barriere definisjoer, nærmer er noen av de definisjonene som ble funnet og diskutert i litteraturstudiet, anvendt på ulike storulykke relaterte scenarier. Casene som er brukt, er i fra ulike stadier i et mulig ulykkesscenario. Den første casen er baser på en vedlikeholdsoperasjon, hvor de forskjellige trinnene i operasjonen er beskrevet. Det andre tilfellet er i forbindelse med en boreoperasjon. Her er de forskjellige elementene i brønnsparke-deteksjon beskrevet. Den siste casen er et hydrokarbon lekkasje scenario, der ulike sikkerhetstiltak er beskrevet. For disse tre tilfellene var fire forskjellige definisjoner, eller klassifiseringer av barrierer anvendt. Sammenligningen viste at de fleste av forskjellene mellom disse definisjonene var knyttet til operasjonelle og organisatoriske aspekter av prosedyrer og tiltak.

Funn i besvarelsen viser at den beste måten innlemme operasjonelle og organisatoriske aspekter av barrierestyring i modellering kan være å fokusere på funksjonen barrierene utfører. Dette er i motsetning til et hardware fokusert barriereperspektiv. Det er foreslått et sett med barrieredefinisjoner, som er basert på et funksjons-orienterte barriereperspektivet. Det er også et rammeverk for å identifisere barrierer, basert på det nye settet med barrieredefinisjon er foreslått. De foreslåtte definisjonene er vurdert opp mot definisjonene som ble funnet i litteraturenstudiet. Barriere-identifikasjonsrammeverket er også eksemplifisert gjennom programmet på en hydrokarbon lekkasje scenario. Funnene og det foreslåtte definisjonssettet er diskutert, og det er foreslått områder, som bør belyses ytterligere.

Contents

Assignment	
Preface	i
Acknowledgment	ii
Summary	iii
Summary in Norwegian	v
1 Introduction	1
1.1 Background	1
1.2 Objectives	2
1.3 Limitations	3
1.4 Structure of the Report	3
2 Literature survey and review	5
2.1 Literature overview	5
2.2 Definitions and Classifications	7
2.3 Discussion	23
3 Modeling Methods	27
3.1 Human Reliability Analysis	27
3.2 Bayesian Networks	33
3.3 FRAM	36
3.4 System theoretical methods	37
3.5 Discussion	38

<i>CONTENTS</i>	0
4 Evaluation of Current Barrier Definitions and Classifications	43
4.1 Case Example - A	44
4.2 Case Example - B	53
4.3 Case Example - C	56
4.4 Discussion	59
5 Classification of Operational and Organizational Barriers	63
5.1 Basis of a New Barrier Classification and Definition	63
5.2 Proposed Barrier Definitions and Classification	66
5.3 Possible Framework for Barrier Identification	74
5.4 Discussion of the Proposed Definitions and Classification	78
6 Summary	83
6.1 Summary and Findings	83
6.2 Discussion	87
6.3 Further Work	88
A Acronyms	91
B Case Example A	93
C Comparison of Barrier Definitions	107
C.1 Case A	107
C.2 Case B	119
C.3 Case C	123
Bibliography	129
Curriculum Vitae	132

Chapter 1

Introduction

1.1 Background

The term barriers are used in many different contexts. Within the field of safety and risk management, the term is used to describe certain risk reducing measures. The focus of this thesis is barriers in the context of major accidents within the oil and gas industry. There are no well defined consensus on the use of the term '*major accident*'. There are several definitions in use, and most include severe damage to material assets, severe environmental damage and loss of human life. Some definitions also include financial losses, though that can be regarded as an implicit loss in most major accidents. Though it is not a critical part of this thesis, the following definition, used by the Norwegian Petroleum Safety Authority (PSA), of a major accidents is used for this thesis;

■ An acute event such as a major emission, fire or explosion, immediately or later causing several serious injuries and / or loss of life, serious environmental damage and / or loss of greater economic value.

(translated from Norwegian) PSA (2012a)

Within the field of risk management and safety engineering, there is a growing understanding that the increasing complexity of the technical and technological systems is a challenge that must be taken seriously. In the oil and gas industry it have also, through incidents and accidents, become clear that the consequences of failure of these systems can be catastrophic. These acci-

dents have severe consequences in terms of economical cost, environmental damage and loss of life. Neither of these consequences are accepted in today's society. An aspect of these challenges that have received increasing attention is the interaction between these new technologies, and the human operator and the surroundings of the operation. Though it seems to be clear that the operational and organizational aspects influence the risk, there are not any clear consensus on how these elements are to be modeled. Barrier is a widely used term for risk reducing measures. The term is defined differently in different industries and within specific industries, and ranges from quite narrow descriptions to an all-including expression, both including and excluding the socio-technical aspect of safety measures. Barrier management have been listed as one of the top priorities of the PSA, and have been a focus of the yearly evaluation of the risk level in the petroleum industry (PSA, 2012b) on the Norwegian continental shelf. There have been a discussion both in the academia and the industry on how to implement the operational and organizational factors influencing barrier integrity. This may partly be contributed to the lack of consistency within the definitions and standards used.

The main objective of the thesis is then a clarification of the terms used. This is done through describing, evaluating and discussing the use of operational and organizational aspects in barrier management, and proposing a barrier classification and a set of barrier definitions, where operational and organizational aspects of barrier management are taken into account.

1.2 Objectives

The following tasks are formulated in order to answer the main objective of the thesis:

1. Perform a comprehensive review of literature on the topic of barriers, and in particular human and organizational barriers. This should build on the review performed in the project thesis and summarize additional literature found during the search.
2. Discuss existing definitions of barrier, barrier functions, barrier elements and influencing factors with a view to determine their suitability in relation to operational and organizational barriers. Use examples and consider in particular if the definitions make it possible to distinguish between barrier elements and influencing factors.

3. Evaluate how operational and organizational barriers can be modeled in risk analysis.
4. Consider barrier classifications/categories proposed in the literature and see if they are suitable for classification of operational and organizational barriers. Propose a classification scheme that is helpful in relation to monitoring of operational and organizational barriers and also in relation to modeling.
5. Based on the review of how barriers can be modeled in risk analysis, evaluate the suitability of using SPAR-H as a method for modeling barriers in the oil and gas industry.

The last objective, evaluating suitability of the Human Reliability Analysis (HRA) method, Spar-H for modeling barriers in the oil and gas industry, is emphasized less than the other objectives in the thesis. The Spar-H method is reviewed, and the use of HRA methods in general is discussed. This change is done in agreement with the supervisor.

1.3 Limitations

There are several limitations to this thesis, the most profound being time. Time limits both the amount of research, and the amount of verification of the results the author is able to perform. Another limitation is the authors knowledge of practical utilization of barrier modeling. Though a theoretical understanding have been established through , practical challenges may unintentionally be overlooked. This is counteracted by the use of resources that has this knowledge, such as the supervisors, literature and example cases. The authors lack of practical experience in the application of the theoretical models are in general a limitation of the thesis.

1.4 Structure of the Report

This masters thesis is structured in two main parts. The first part is Chapters 2 and 3. Here a literature survey and theoretical background needed is summarized, and a list of the main literature that is found and used in the literature survey, are found. Chapter 2 is focused on barrier definitions, classification and use, with an emphasis on human and organizational elements. This Chapter is to a great extent a continuation of the authors project thesis. Chapter 3 focuses

on literature regarding modeling methods that are used to model human and organizational factors.

The second part of the thesis is focused on the evaluation and development of barrier definitions and barrier classifications. Chapter 4 consists of three case studies, where barrier definitions are compared using possible scenarios. Chapter 5 discusses the findings in Chapter 2 through 4, and proposes a possible solution of how human and organizational elements can be incorporated into barrier modeling through a set of barrier definitions. For each chapter the findings are discussed. Chapter 6 contains a summary, and conclusion, in addition to a final discussion and some suggestions for further work.

In agreement with the supervisor, the pre-study report and progress reports are not included in the thesis.

Chapter 2

Literature survey and review

2.1 Literature overview

This chapter is an overview of relevant literature on the topics of barrier classification, integration of operational and organizational elements in barrier analysis and use of barriers in the quantitative risk analysis. This is a continuation of the literature survey done in the project thesis (Torgauten, 2012), but with a stronger focus on the operational and organizational aspects of the classification schemes. The list below shows some of the key literature that is read, and used in this thesis. Other sources are also used. Although the literature focuses on different industries, the focus of the review is to describe and discuss the definitions and classifications, and if possible find applicable definitions and classifications for the offshore oil and gas industry.

- Safety barriers: Definitions, classification, and performance (Sklet, 2006)
- Principles of barrier management in the petroleum industry (translated from Norwegian, PSA (2012a))
- Risk Assessment | Theory, Methods, and Applications (Rausand, 2011)
- System Reliability Theory | Models, Statistical methods, and Applications (Rausand and Høyland, 2004)
- The Human Contribution: unsafe acts, accidents and heroic recoveries (Reason, 2008)

- Managing Risk of Organizational Accidents (Reason, 1997)
- Risk Level in the Petroleum Industry (PSA, 2012b)
- Barriers to prevent and limit acute releases to sea | Environmental barrier indicators (Hauge et al., 2012)
- Engineering a Safer World (Leveson, 2011)
- Human and organizational factors in the operational phase of safety instrumented systems: A new approach (Schönbeck et al., 2010)
- NEK IEC 61511, Functional safety | Safety instrumented systems for the process industry sector (Part 1 and Part 3) (NEK-IEC, 2003a) and (NEK-IEC, 2003b)
- NEK IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems | Part 1: General requirements (NEK-IEC, 2010)
- ARAMIS User Guide (Accidental Risk Assessment Methodology for Industries in the context of the SEVESO II directive) (H.Andersen et al., 2004)
- Guidelines for Safe and Reliable Instrumented Protective Systems (CCPS, 2010)
- Basic Safety Principles for Nuclear Power Plants (INSAG, 1999)
- Good Practices for Implementing Human Reliability Analysis | Final Report (U.S. NRC, 2005a)
- Evaluation of Human Reliability Analysis Methods Against Good Practices (U.S. NRC, 2006)
- ISO 31000 Risk management - Principles and guidelines (ISO, 2009)
- NS-EN ISO 17776:2000 Petroleum and Natural Gas Industries | Offshore production installations | Guidelines on tools and techniques for hazard identification (ISO, 2002)
- Risk Assessment (Torgauten, 2012)

Some of the literature have been used as support literature, and is not mentioned explicitly in the text, but read, to gain a better understanding of the challenges and solutions.

2.2 Definitions and Classifications

There have been made several significant contributions to classification and defining risk reducing measures. Several of the models and methodology is reviewed in Torgauten (2012). The review shows that there are a wide variety of terms describing these risk reducing measures, as well as different definitions of these terms. The inconsistency in use of terms are quite evident. This is quite possibly mainly caused by the differences in the industries that these definitions and models have been developed in. As stated by Torgauten (2012), a general definition, that can be used in all industries may be hard to achieve. There is however great benefits of getting input from different points of view, in order to get a holistic view of the matter in question. James Reason have in several books and papers worked with human and organizational elements in risk analysis. Some of the most important works are the 'Managing risk of organizational accidents' (Reason, 1997) and 'Human Error' (Reason, 1990). The Swiss Cheese model, also known as the Reason model, is often used as a basis for barrier understanding. The conceptual model is shown in Figure 2.1. In the model there are several layers of defenses, between the hazard or hazardous event and the asset that needs protection to prevent losses. The possibility of the defense failing is illustrated as a hole in the defense. These are directly influenced by unsafe acts and latent conditions, and indirectly influenced by workplace factors and organizational factors. The model is used in different industries with different understanding of what constitutes a defense. Examples of this are given in Torgauten (2012). Reason (1997) uses a wide definition, probably to provide possibilities of use in different industries.

As seen from Figure 2.1 there is a clear distinction between the defenses in place and the conditions that can lead to the failure of these defenses. Reason (1997) categorizes defenses based on the function they perform, as shown in the list below. In addition to the functional categorization, Reason (1997) proposes a differentiation between soft and hard defenses. '*Hard*' defenses are typically physical barriers, alarms, interlocks, keys, non-destructive testing and other technical or physical elements or functions. Legislation, training, oversight and front-line operators are considered '*soft*' defenses. The main concerns of risk reducing measures, and barriers are according to Reason (1997) considered to be as following:

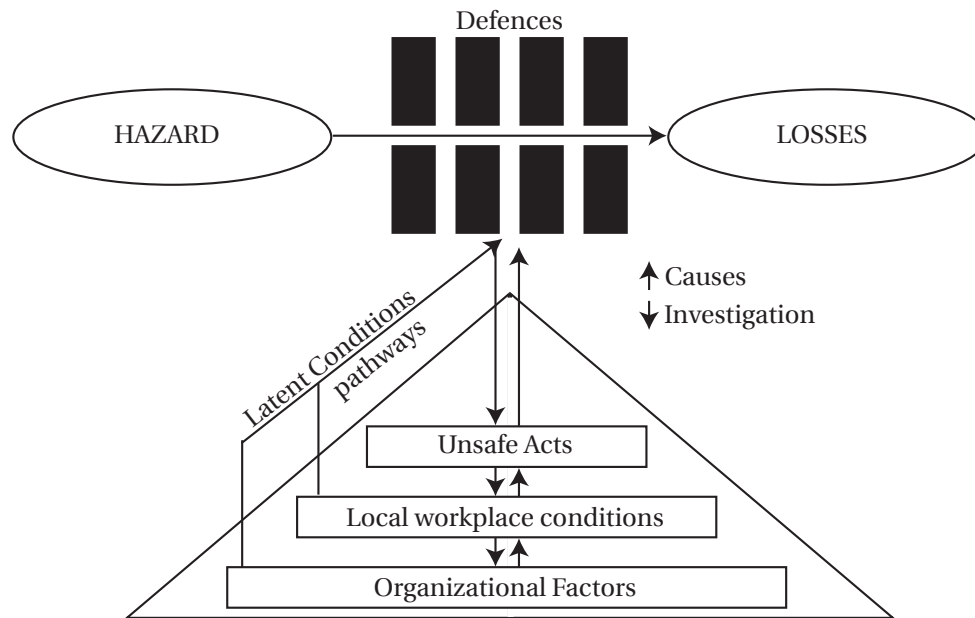


Figure 2.1: Conceptual barrier model presented by Reason (1997) (based on Figure 1.6 by Reason (1997))

- to create *understanding* and *awareness* of the local hazards
- to give clear *guidance* on how to operate safely
- to provide *alarms and warnings* when danger is imminent
- to *restore* the system to a safe state in an off-normal situation
- to impose *safety barriers* between the hazards and the potential losses
- to *contain* and eliminate the hazards should the escape this barrier
- to provide the means of *escape and rescue* should hazard containment fail

One of the more recent and most comprehensive reviews of barrier definitions and classifications is the doctoral work by Sklet (2005). As Sklet (2006), and also the review of barrier theory by Torgauten (2012) also shows, there are many different barrier classifications and definitions. Torgauten (2012) shows that within oil and gas, the most common term to use to describe risk reducing measures is the term barrier, while the nuclear industry uses '*layers of defense*', while the aviation industry uses '*defenses*'. Within the nuclear industry the term barrier is used in the context of physical barriers. It is also noteworthy that within the oil and gas industry is a degree of variation in the extent of the scope the term barrier, but the tendency is that the scope is

wide, and includes physical, technical, operational and organizational aspects. The definition recommended by Sklet (2006), given below, also reflects this. The definition recommended by Sklet (2006) is based on several other definitions.

☛ **Safety Barrier:** *Safety barriers are physical and/or non-physical means planned to prevent, control, or mitigate undesired events or accidents*

Sklet (2006)

☛ **Barrier Function:** *A function planned to prevent, control or mitigate undesired events or accidents*

Sklet (2006)

☛ **Barrier system:** *A system that has been designed and implemented to perform one or more barrier functions*

Sklet (2006)

Sklet (2006) also proposes a classification of barriers, as shown in Figure 2.2. This classification distinguishes between active and passive barriers, and then again between physical and operational/human passive barriers, and technical and operational/human active barriers.

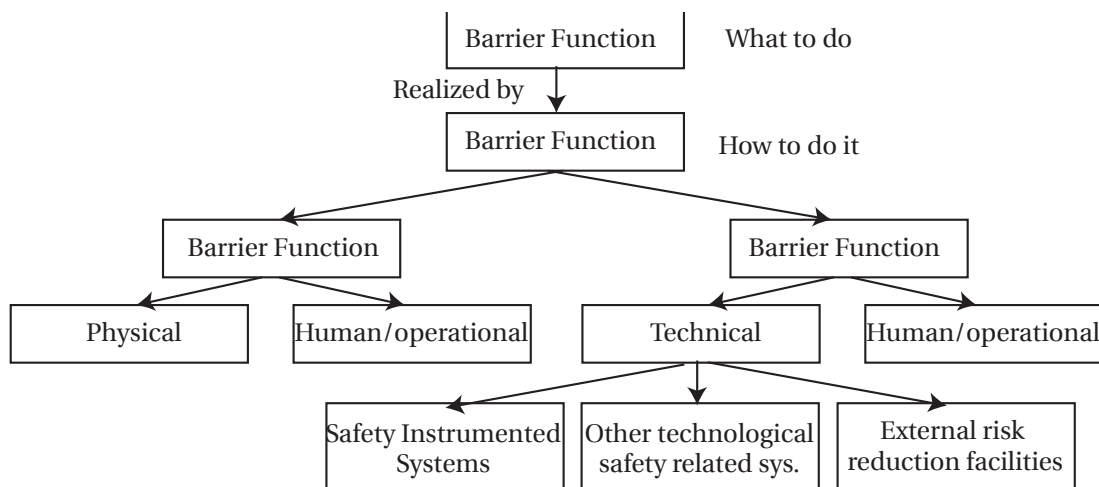


Figure 2.2: Classification of barriers based on Sklet (2006)

As seen in Figure 2.2 there are both active and passive human/operational barriers. Sklet (2006) notes that active human/operational barriers often are part of a work process, such as self-control of work or third party control of work, while passive operational/human barriers are for instance safety distance. Both of these can either be functioning continuously or on demand.

As mentioned, in the nuclear industry, and specifically the International Nuclear Safety Agency (INSAG, 1999) a more narrow definition of barriers is used. Here barriers are only physical elements, meaning walls and physical separation. Other risk reducing measures are defined as levels of defense. Different levels of defense model can as described by INSAG (1999) are based on the objective of the level; prevention (level 1), control (level 2, 3 and 4) and mitigation (level 5). The defense in depth principle, as it is named, is focused on the reducing the possibility of single human or equipment failures leading to harm to the public. The defense in depth principle does not focus specifically on humans as a safety function, but states that *'all safety activities, whether organizational, behavioral or equipment rested are subject to layers of overlapping provisions'* (INSAG, 1999).

The defense in depth principle in the nuclear power industry have strong resemblance to the layers of protection principle used in the process industry. This principle can best be described as shown in Figure 2.3. The layers of protection principle, as described by CCPS (2010), defines a protection layer as *'(a) physical entity supported by a management system, which is capable of preventing a hazardous event from propagating into undesired consequences'* CCPS (2010). The human and organizational elements are thus defined as supportive elements.

H.Andersen et al. (2004) gives through the ARAMIS (Accidental Risk Assessment Methodology for Industries in relation to the Seveso II directive) user guide, a framework to give a higher degree of consistency for risk-based decision making within the chemical process industry. The user guide gives among other steps information on identification of major accident hazards, identification of safety barriers and assessment of their performance, and evaluation of safety management efficiency to barrier reliability. H.Andersen et al. (2004) gives the following defini-

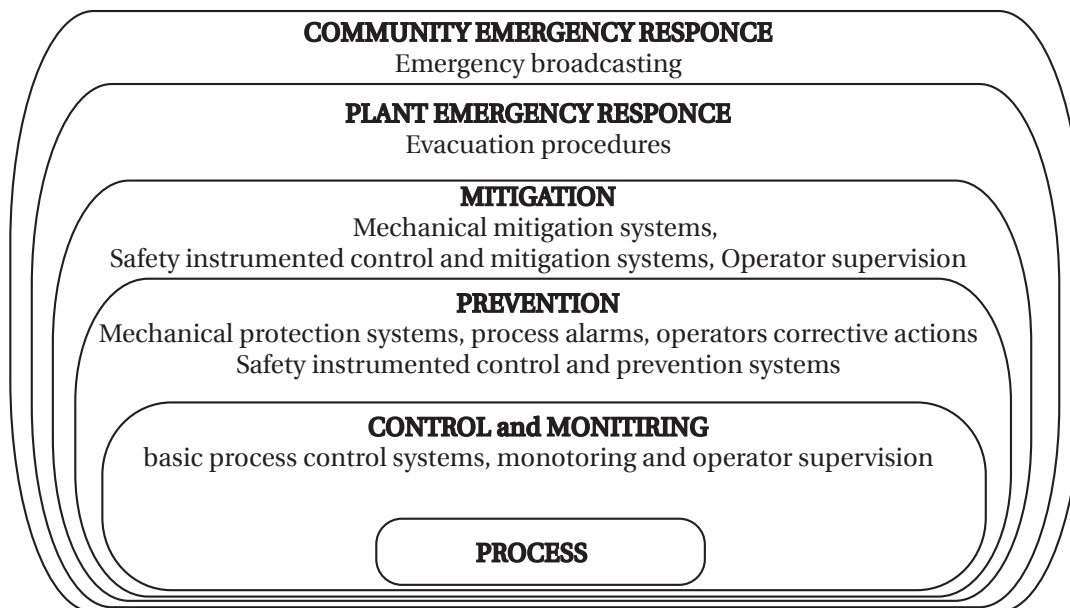


Figure 2.3: The layers of defense (based on NEK-IEC 61511 part 1, figure 9 (NEK-IEC, 2003a))

tion of a safety barrier:

☛ **Safety Barrier:** *The safety barrier can be physical and engineered systems or human actions based on specific procedures or administrative controls. The safety barrier directly serves the safety function. The safety barrier are "how" to implement safety functions.*

H.Andersen et al. (2004)

H.Andersen et al. (2004) also uses the term *safety function* to describe 'the "what" needed to assure, increase and/or promote safety'. A safety function is defined as 'a technical or procedural action, and not an object or a physical system'. The action is then carried out 'in order to avoid or prevent an event or to control or limit the occurrence of the event.'

The ARAMIS definitions are clearly based on the energy-barrier accident model, and utilizes the *Bow-Tie*-model to a great extent to visualize the accident development and the barriers. As shown in Figure 2.4, H.Andersen et al. (2004) defines the as a combination of fault trees leading in to the *critical event* and event tree to determine the different consequences.

H.Andersen et al. (2004) divides the different safety barriers into four groups based on the actions they realize; *to avoid, to prevent, to control or to limit* an event. The user guide also refers

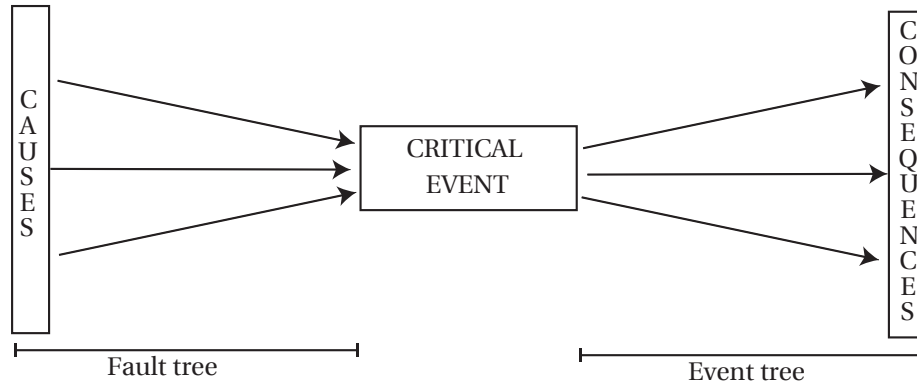


Figure 2.4: A simple representation of the Bow-Tie (based on Figure 3 by H.Andersen et al. (2004))

to three types of barriers; *active* or *passive* barriers, and *human action*.

The user guide presented by H.Andersen et al. (2004) are to a great extent focused on the standards related to Safety Instrumented Systems (SIS), mainly the standards IEC 61508 and IEC 61511 (NEK-IEC, 2010, 2003a,b). The requirements related to these standards are described in Section 2.2.3. When modeling safety barriers, H.Andersen et al. (2004) proposes a similar way of assessing the frequency of failure as the Safety Integrity Level (SIL) is for a SIS. This is called Level of Confidence and is denoted LC. The LC gives, as the SIL, a probability range of failure for the subsystems that the safety barrier consists of. Here human actions are seen as a subsystem of a safety barrier. As for a SIS, the requirement for LCs are divided into low demand and high demand or continuous demand safety barriers. In addition to LCs the safety barriers are also measured on efficiency and response time (RT).

H.Andersen et al. (2004) proposes a quite comprehensive classification scheme for safety barriers. There are eleven types of barriers, as shown in Table 2.1. The terminology that differentiates between control and barrier stems from the MORT (management oversight and risk tree) methodology (H.Andersen et al., 2004). An introduction of the MORT methodology is found in Rausand (2011).

Table 2.1: Types of barriers (simplified from Table 14 by H.Andersen et al. (2004))

Barrier type	Detect	Diagnose / activate	Act
Permanent - passive - control	-	-	Hardware
Permanent - passive - barrier	-	-	Hardware
Temporary - passive	-	- (human must put in place)	Hardware
Permanent - active	-	- (may need activation by operator)	Hardware
Activated - hardware on demand - barrier or control	Hardware	Hardware	Hardware
Activated - automated	Hardware	Software	Hardware
Activated - manual	Hardware	Human	Human/ remote control
Activated - warned	Hardware	Human	Human
Activated - assisted	Hardware	Software - human	Human/ remote control
Activated - procedural	Human	Human	Human/ remote control
Activated - emergency	Human	Human	Human/ remote control

There are a differentiation made between the detection, diagnose/activation and act, as the three basic functions of the barriers. A barrier can have one or more of these basic functions, and the functions can be realized by different types of hardware and software or by humans.

Another, and in some aspects fundamentally different view on barriers is present by Hollnagel (2004). The basic element of Hollnagels classification is also a barrier system. The view is based on normal operation, and not an accident sequence model, as most other barrier classifications and definitions are based on. The following four types of barrier systems are suggested by Hollnagel (2004):

- Physical or material barrier system
- Functional (active or dynamic) barrier system
- Symbolic barrier system

- Incorporeal barrier system

Especially the symbolic and incorporeal barrier systems are differentiated this barrier classification from the other classifications. The focus on understanding and knowledge as parts of a barrier system shows a high focus on human interaction and also on normal operation. These barrier systems are to a great extent focused on pre-event conditions, seen from a sequential accident model perspective. While other barrier classifications are industry specific, is this classification more a general classification, border-lining to a non-industrial perspective. Hollnagel (2004) also emphasizes this by stating that the term *barrier* usually is understood from context.

2.2.1 Regulations and Regulatory Requirements

An important aspect to include, when reviewing barrier definitions and risk reducing measures, is how the regulatory bodies use the terms, and also how they enforce the regulations and standards. In Norway, the Petroleum Safety Authority (PSA) is the most important regulatory body. The management regulations and the accompanying guidelines (PSA, 2010b,a), section five, is the basis for how barriers are to be managed, and gives guidelines for the basic requirements of barriers. The guideline to the management regulations section five states that '*(b)arriers (...), can consist of either physical or non-physical measures, or a combination*' (PSA, 2010a). There are no further clarification on what '*non-physical measures*' are, in these guidelines. However, in the document 'Principals for barrier management in the petroleum industry' (PSA, 2012a, 2013) it is given some explanations on what these measures consist of. As mentioned in the previous section, operational and organizational elements are incorporated into the PSA (2012a) definition.

☞ **Barrier:** *Technical, operational and organizational elements that individually or together shall reduce the possibility of a specific error, hazards and accidents occur, or that mitigates or prevents damage/nuisance.*

(translated from Norwegian) PSA (2012a)

PSA (2012a) goes further than Sklet (2006) to specifically include operational *and* organizational elements as a part of the definition of barriers. However in the second edition of this

document (PSA, 2013), the descriptions of what constitutes organizational and operational barrier elements are somewhat changed. An example of these changes are found in an example given on a barrier function '*depressurize leaking segment*', where PSA (2012a) describes an organizational barrier as following (translated from Norwegian);

'if a CCR operator have to initiate manual actions to realize the function 'depressurize leaking segment', the operator is a part of an organizational barrier element. Actions that is initiated would be an example of an operational barrier element.'

This is changed in the new version of the document (PSA, 2013), where the following used to describe the operational and organizational barrier elements (translated from Norwegian);

'Documentation of the depressurization system would be an organizational barrier element, while procedures, emergency preparedness plans and personnel that are to secure and initiating potential manual depressurization, would be examples of operational barrier elements'

This is a quite drastic change as to what constitutes operational and organizational barrier elements, but also clarifying, especially regarding organizational barrier elements. It is however still unclear from the new description whether it is the plans, procedures and personnel that are the operational barrier elements, or the actions an operator performs based on the procedures, that constitutes the barrier elements in question.

Another definition of barriers used by PSA in their report on the risk level in the petroleum industry (PSA, 2012b), is from the standard NS-EN ISO 17776:2000 for Petroleum and Natural Gas Industries | Offshore production installations | Guidelines on tools and techniques for hazard identification (ISO, 2002), given below.

☞ *Measures which reduce the probability of realizing a hazard's potential for harm and which reduces its consequences*

ISO (2002)

ISO 17776 also notes that '*(b)arriers may be physical (materials, protective devices, shields, segregation, etc.) or non-physical (procedures, inspections, training, drills etc.)*'. PSA (2012b)

notes that the term is used in a broad sense, and therefore includes procedures, inspections, training and drills within non-physical barriers.

PSA (2012b) states that barriers is one of areas of importance for the PSA, and this topic has a significant focus in this report. The following barriers are listed, that have been the focus of the information gathering:

- Fire detection
- Gas detection
- Shutdown (Riser-EDSV, Production tree, DHSV)
- Blowdown valves (BDV)
- Pressure safety valve (PSV)
- Active fire prevention (Deluge valve, start tests for pumps)
- Well integrity
- Main systems (Ballast systems valves, watertight doors, reference systems)
- Maintenance management
- Response times
- Blowout preventor (BOP)

These barriers, or barrier elements, are mainly technical systems, where the focus of data gathering is in the number of failures on test relative to the number of tests. It is also noteworthy that these elements are closely related to the NORSOK standard S-001 (NORSOK standards, 2008) that covers requirements to technical safety. For neither of these barriers, or barrier elements, the human or organizational influence are mentioned. There are however two elements that stands out, maintenance management and response time. Whether or not these elements should be defined as barrier elements can be discussed, when utilizing the definition presented by PSA (2012a).

PSA (2013, 2012a) also focuses on the requirement given in the management regulations (PSA, 2010b), where performance requirements must be set for barrier elements. Aspects that can influence safety, such as culture can therefore not be considered a barrier element (PSA,

2010b), nor can *monitoring and review*. Within the context of monitoring and review are elements of training and management. There are also made an important distinction between risk influencing factors and barrier elements.

2.2.2 Integration of Human and Organizational Barriers in the Literature

Several of the articles and research papers that are listed in the literature survey have made suggestions on how operational and organizational factors should be considered in relation to risk assessments.

Hauge et al. (2012) have, as a part of a joint-industry project called '*Development of barriers and indicators to prevent and limit pollutants to sea*', developed indicators for environmental barriers. As a part of the report, the differentiation between indicators influencing factors and barrier elements have been discussed. As shown in Figure 2.5, the basis for finding indicators on the barriers, are through influential factors, that then again are related to the barrier element.

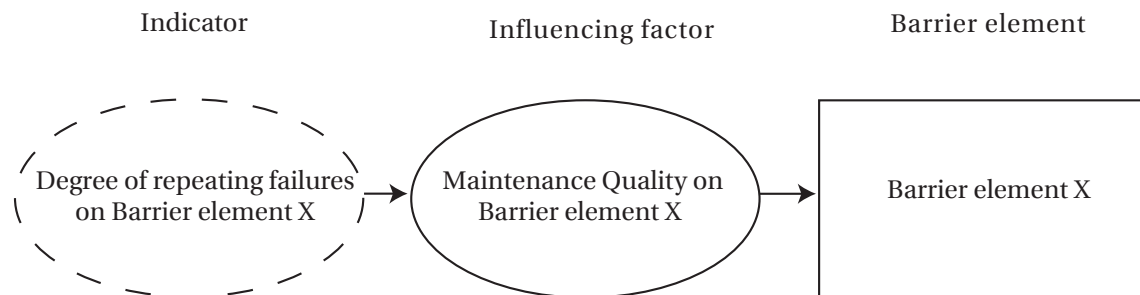


Figure 2.5: Relation between indicator, influencing factor and barrier element (Generalized from Figure 5-1 by Hauge et al. (2012))

The definitions that are used as a basis for the report by Hauge et al. (2012) are as following:

- ☛ **Barrier** - A barrier can be regarded as a function which prevents a specific sequence of events from taking place, or which directs the sequence of events in an intended direction to limit harm
- ☛ **Barrier function** - The assigned responsibility or action of the barrier, e.g. prevent leakage, limit amount of release or prevent ignition

☛ **Barrier element** - The personnel, equipment or systems that implement the barrier function

It is noteworthy to notice that the personnel that implements the barrier function is defined as a barrier element. When illustrating the barrier elements that have been used as examples for the development of indicators, Hauge et al. (2012) also includes a layer of organizational barrier elements, as shown in Figure 2.6, where the barrier elements for a blowout preventor (BOP) are shown. There is a distinct succession to the different barrier elements, where the organizational barrier elements influences the human barrier elements, which then again influences some of the technical barrier elements. There are also an arc indicating influence from the technical systems, or human-machine interface (HMI) to the human barrier element.

The OTS project (Sklet et al., 2010) proposes a way of monitoring the organizational and operational aspects of safety barriers. Here are operational safety barriers described as '*human and organizational factors*', and 7 operational safety barriers or performance standards as listed below are covered (Sklet et al., 2010):

1. Work practice
2. Competance
3. Procedures
4. Communication
5. Workload and physical working environment
6. Management
7. Management of Change

The OTS-method is described as a proactive independent and systematic assessment of the status of operational safety barriers. This differentiates it from other methods in being solely focused on the operational phase of the lifecycle. The goal is here to monitor the condition of the organizational and operational aspects of the barriers that are in place, in order to get a more holistic view of the risk-picture on an installation. The OTS project is an addition the TTS project that monitors the technical condition of the barriers. These are intended to be complement each other, and are both intended for larger oversight, and not for continuous monitoring.

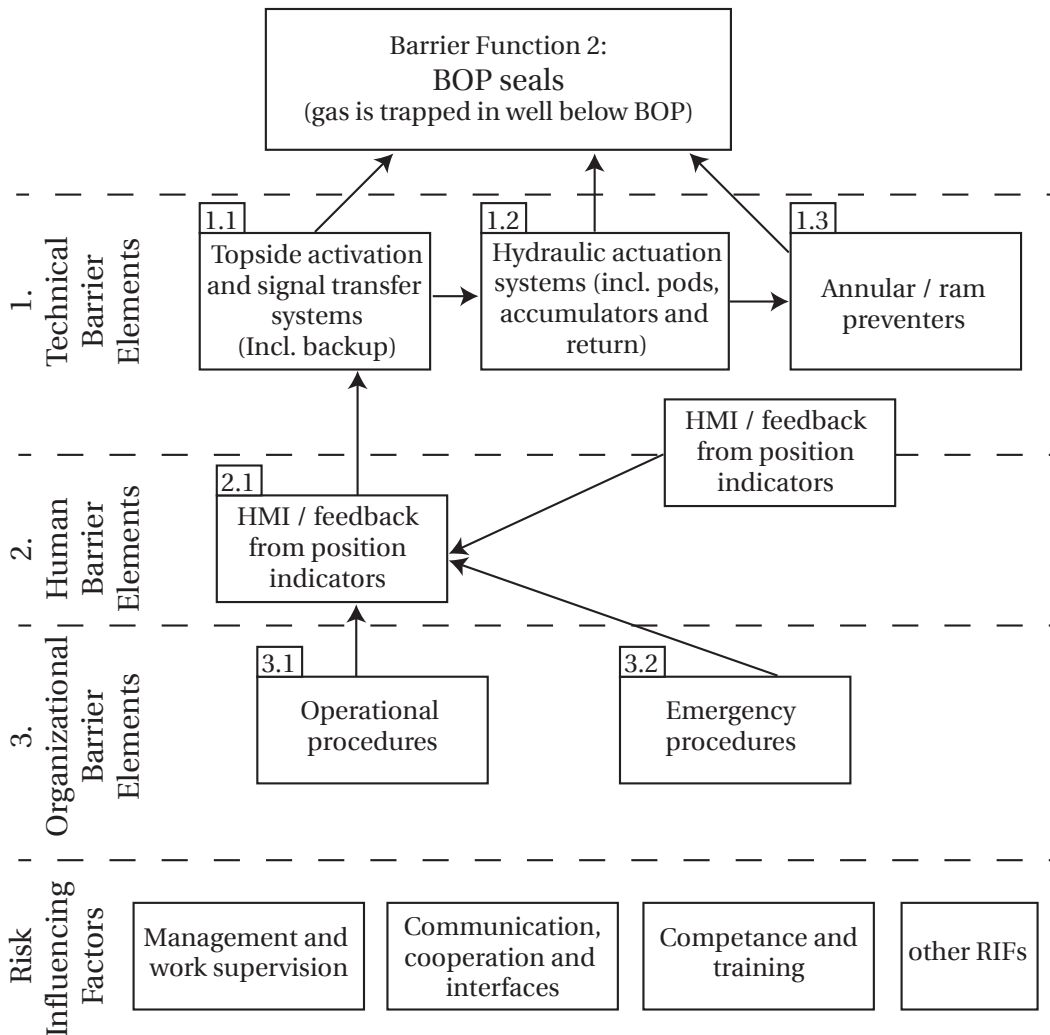


Figure 2.6: Example of barrier elements for a BOP seal function (Based on Figure C-3 by Hauge et al. (2012))

2.2.3 Safety Instrumented Systems

A large amount of safety systems in the offshore industry are a part of a safety instrumented systems, or SIS. A SIS consists of several technical elements and in some cases also human interaction. A typical SIS consists of a set of sensors or other input elements, a logic solver, and an actuating unit, for instance to give the system the ability to operate a valve, as shown in Figure 2.7.

The SIS shall fulfill one or several purposes, defined as safety instrumented functions (SIFs). The requirements as it is formulated in the standards IEC 61511 (2003a; 2003b) and IEC 61508

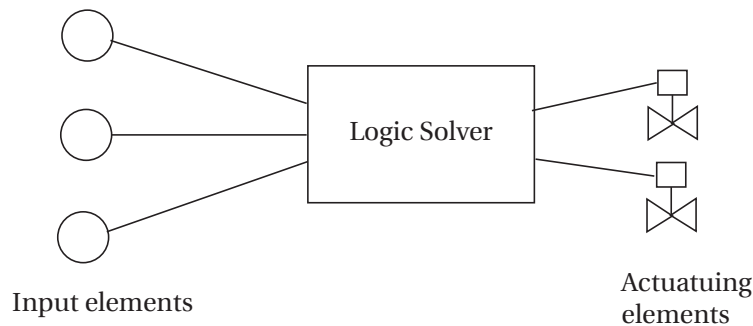


Figure 2.7: Typical elements in a safety instrumented system (based on Figure 12.4 Rausand (2011))

(2010), are given by the safety integrity level (SIL) requirements to the SIS. These can be established in different manners, but one of the common ways of establishing a SIL requirement is through a Layers of Protection Analysis (LOPA). LOPA has a set of specific requirements related to the selection of what layers of protection that can be considered in the analysis. The protective layers have to be considered independent of each other in order to be taken in to account in a LOPA. The criteria for independent protection layers (IPL) are given in NEK-IEC (2003b) 61511 part 3, and are as following:

- **Specificity:** An IPL is designed solely to prevent or to mitigate the consequences of one potentially hazardous event
- **Independence:** An IPL is independent of the other protection layers associated with the identified danger
- **Dependability:** It can be counted on to do what it was designed to do. Both random and systematic failures are addressed in the design
- **Auditability:** It is designed to facilitate regular validation of the protective functions. Proof testing and maintenance of the safety system is necessary.

With regards to types of failures, the PDS handbook (Hauge and Onshus, 2009), which describes a method of quantification for safety unavailability of a SIS, uses two main categories of failure; *Random hardware failure* and *Systematic failure*. For this thesis it is the systematic failures that are of interest. The types of systematic failure are shown in Table 2.2, as they are described by Hauge and Onshus (2009).

Table 2.2: Types of systematic failures (Hauge and Onshus, 2009)

Failure type	Example
<i>Software faults</i>	Programming errors, error during updating
<i>Installation failure</i>	Gas detector left on after commissioning, Valve installed in wrong direction
<i>Design related failure</i>	Inadequate or erroneous specifications, Inadequate or erroneous implementation
<i>Excessive stress</i>	Excessive vibrations, Too high temperature
<i>Operational failure</i>	Valve left wrong position, sensor calibration failure, detector override mode

The systematic failures for a SIS is often regarded as the most difficult to quantify, since the failures have a higher degree of dependence on influencing factors. Unlike the *random hardware failures*, which can be estimated with the help of accelerated testing and experience data.

Schönbeck et al. (2010) have developed a new approach to modeling human and organizational factors in the operational phase of safety instrumented systems. The approach introduces a way of including human and organizational factors in the operational SIL, by estimating the proportion of the design SIL that can be explained by human and organizational factors. These factors are then weighted and normalized, before the safety influencing factors are rated and used to calculate the operational SIL. This is proposed done thorough a BBN structure, where the different influencing factors are modeled, and the contribution on the SIL is can be calculated. The safety influencing factors that is mentioned us listed in Table 2.3

Table 2.3: Safety influencing factors (Table 2 in Schönbeck et al. (2010))

Safety influencing factor	Description
1. Maintenance Management	Management, rather than execution, of maintenance activities
2. Procedures	Quality, accuracy, relevance, availability and workability of operation and maintenance procedures
3. Error-enforcing conditions	Conditions that force people to operate in a manner not foreseen during system design
4. Housekeeping	Orderliness in the workplace
5. Goal comp ability	Compatibility of goals at and between individual, group and organizational level
6. Communication	Possible lack of communication due to system failures, message failures, and misinterpretation
7. Organisation	Possible deficiencies on organizational structure and responsibilities
8. Training	Spesific expertise relevant to the operators' jobs

2.3 Discussion

Based on the literature survey and review, it can be concluded that there are in many cases a lack of consensus on terms and definitions. The lack of fundamental definitions makes it harder to be precise when describing the different aspects of a risk assessment. One can not be certain that the same definition applies to a defense as it applies to a barrier. In some industries these are fundamentally different, while others treat them as equivalents. As shown in this chapter, and in Torgauten (2012) there are a diversity of definitions and terms when describing risk reducing measures. But there are also some agreement in some areas. Within the oil and gas industry there are a tendency to include most kinds of risk reducing measures in the definition of barriers, including operational and organizational barriers. There are however no specific definitions on what constitutes a operational, nor organizational barrier or barrier element. There are made attempts to differentiate between factors influencing the barrier and the elements that constitutes the barrier it self, for instance by Hauge et al. (2012). The distinction is not always well defined and the line is at best blurry. Hollnagel (2004) states that the term barrier is understood from the context. Though this may be true, the singular form of the word barrier leads to believe that it is a single element. Even though most of the definitions takes this into account by specifying that a barrier is for instance *one or more barrier elements*, a barrier in the context of oil and gas industry is rarely a single element, but rather a system of technical elements and actions. These actions can either be performed by technical systems, such as a SIS, or by a human. This is mainly a challenge when characterizing the hardware as the basic element. If one considers barriers as a set of hardware elements, the human contribution to barriers is basically influencing factors, or in some cases simple actions, such as *activate deluge system*, and so on. The human ability of reasoning will then be reduced to a procedural element where only what is written in the procedure is accounted for.

Another view that is presented, is the functional view of barriers. Both the definitions presented by ARAMIS (H.Andersen et al., 2004) and in the report by Hauge et al. (2012) are focused on barrier functions, rather than barrier systems. In both cases, the barrier elements or systems are secondary to the barrier function. In these definitions, human actions can be a part of, or

be a barrier, if the action realizes a barrier function, and is planned and assigned to do so. This does not differ greatly from the definitions presented by Sklet (2006), but in the classification of barriers presented by Sklet, the only actions that are mentioned is the procedural checking of actions, and not the actions them self.

Another distinction that can be made is whether the human/operational action is a part of the fulfillment of the barrier function, or if it is an interaction with the technical system, that then again realizes the barrier function. An obvious example is the maintenance of a barrier system. It is clear that the human interaction with the system, the maintenance action, influences the barrier systems ability to fulfill its function. But when modeling barriers, it can be argued that the maintenance of the barrier does not directly influence the realization of the barrier function, but rather affects its effectiveness, or the performance of the barrier element. For instance a poorly maintained valve, that closes slower then the technical specification should lead to believe, can still realize its intended function, but with a lower performance. This is a possible way of categorizing human actions in relation to barriers. On the other hand there, one can make the argument that an activation of a barrier would be within this category. For instance an activation of a SIS system, where the system is performing the actual risk reduction, for instance fire extinguishing, but the human activates the system, since the human detects and assesses the situation different from the SIS.

Another element in the human contribution is the term human error. There are several uses for this term, and not all are applicable in the case of barriers, even though they are related to barriers or barrier systems. When Hauge and Onshus (2009) describes types of systematic failures, these may all be seen as different types human error, except from the excessive stress failure type. These failure types are of course related to SIS failures, and not specifically related to barriers, though a SIS normally can be considered a barrier, or a part of a barrier. This shows that the term human error can be used in all stages of a elements lifecycle, and that a lot of failures can be contributed to the human element. Though for the sake of argument, it must be drawn a line were one considers the direct human influence to the safety as a separate contribution from the indirect contribution from design and manufacturing.

In the list of safety influencing factors, that Schönbeck et al. (2010) presents, most of the factors can be seen as organizational elements or factors. These are high level preconditions, that in relation to the barrier model presented by Reason (1997) are *local workplace conditions* and *organizational factors*, that can act as latent conditions on barriers or defenses.

The last distinction to be made is the difference between single-element and multi-element barriers. Those barriers that consist of a single element are in most cases physical structures. These are what Sklet (2006) refers to as passive, physical barrier elements. This is the term that there are the most consensus with regards to what can be called a barrier. There are non that disputes that physical walls can be barriers. It is the multi-element barriers that the discussion should focus on.

PSA have, as the '*Principles of Barrier Management*' (translated from Norwegian)(PSA, 2012a, 2013) documents reflects, made a increasing effort to include organizational and operational factors and elements into the requirements to barrier management for the oil and gas industry on the Norwegian continental shelf. The focus in barrier management, seems, to a great extent, to have been dictated by the NORSOK S-001 standard (NORSOK standards, 2008) of technical safety. The keywords of the NORSOK S-001 standard, and the barrier management guidelines correlates to a great extent. This may lead to believe that the operational elements of barriers are less important. It is therefore easy to assume that the safety performance standards that is proposed in the NORSOK S-001 standard are covering all aspects of the performance standards related to a specific barrier. The standard does, however, not take organizational or operational elements into account. There are therefore few standards that can be used as guidelines for how these influence the barrier integrity. Some mentions of human contributions are made in the NEK-IEC standard 61511 (NEK-IEC, 2003a), though not much emphasis is made on this subject. The shift in the explanation that PSA is giving, of what constitutes an operational and organizational barrier element in the 2012 and the 2013 version of the '*Principles for barrier management...*' PSA (2012a, 2013) also shows that there are discussions and further need of clarification.

The discussion shows that there are inconsistencies, and little consensus on how the operational

and organizational aspects of barriers should be treated. Some trends can be found, such as the focus on functions. Though there are quite large discrepancies between what is considered a barrier function, from high level descriptions that borderlines to be goals or objectives, and to low level, single function, descriptions, the functional view of barriers have some benefits since it describes the risk reducing act, rather than a hardware function. There are, however definitely room for improvement and clarification, on what constitutes a barrier function, barrier element or a barrier system.

Chapter 3

Modeling Methods for Operational and Organizational Factors and Elements

This chapter reviews and discusses different methodologies and methods that are proposed used for modeling operational and organizational aspects, mainly in relation to barriers, but also in general. The main focus is on quantitative models, but qualitative models are also reviewed. Four main methodologies are described; Human Reliability Analysis, Bayesian Belief Networks, Functional Resonance Analysis Method, and System-Theoretical Analysis and Process methodology.

3.1 Human Reliability Analysis

Human reliability analysis (HRA) is one of the methods of quantifying human behavior that have been used and tested in risk assessments in different industries. The method have mainly been developed and tested in the nuclear industry, since the 1980s. Here HRA is a part of the probabilistic risk assessment (PRA), also called probabilistic safety assessment. According to the Nuclear Energy Agency (NEA, 2004) the main objectives of HRA are:

1. To ensure that the key human interactions are systematically identified, analyzed and incorporated into the the safety analysis on a traceable manner
2. To quantify the probabilities of their success and failure
3. To provide insight that might improve human performance.

There are several methodologies related to HRA. Most of these are based on the use of human error probability (HEP) as the quantitative elements of the analysis. HEP data in most cases based on expert judgement and test scenarios (NEA, 2004). This means that there are uncertainty related to these values. In most cases HEP data is incorporated into event tree analysis, that aggregates the HEP values into failure probabilities. The main steps of HRA often consists of the following (Rausand, 2011):

1. Identify critical operations where human errors could lead to accidents and/or operational problems
2. Analyze the relevant tasks and break them down onto subtasks and task steps.
3. Identify potential human error modes and, if possible, error causes and performance-influencing factors.
4. Determine the HEPs for each error mode and for the complete task.

Reason (1990) describes four types of human error or unsafe acts that can lead to major accidents. These are *slips*, *lapses*, *mistakes* and *violations*. This division is often used as a basis in HRA models according to Rausand (2011). There are also some other methods of classification that in use. What constitutes human errors and human failures are therefore defined several different ways. Rausand (2011) lists, in addition to the classification given by Reason (1990), the following models of classification:

- Skill-, rule-, and knowledge-based behavior modes, proposed by Rasmussen (1983)
- Errors of omission and errors of commission, proposed by Guttmann and Swain (1983)

There are also some other models, that do not derive directly from the HRA methodologies, that uses HEP data as a source of information on human actions. Vinnem et al. (2012) reflects on the use of HEP data in the oil and gas industry. The argument is made that the amount of data available that are applicable for the oil and gas industry is too low. HEP data available from for instance the nuclear industry, is often not directly transferable to the oil and gas industry. The differences between the industries are quite significant on a large scale. Since Risk_OMT to a great extent only focuses on maintenance operations, and other technical elements that deviates in many aspects, there still might be other areas of operation where HRA data can be

transferable. For instance some operation-room tasks and procedures could be transferable between nuclear and oil and gas.

3.1.1 HRA methods

There are several HRA methodologies that are used to model human reliability. Some of the most used are THERP (*technique for human error rate prediction*) and HEART (*human error assessment and reduction technique*). In addition is SPAR-H (*standardized plant analysis risk-human reliability analysis*) a technique that is under research to be used in the oil and gas industry by DNV and Statoil (van de Merwe et al., 2012), and therefore also of interest.

Both THERP and HEART are methods developed to provide input to a QRA to integrate human action and human error into risk analysis (Rausand, 2011). It is not in the scope of this thesis to go in depth of these methods, but the mathematical basics of both these methods are quite similar. The difference is that THERP handles the error probabilities on a basic action level, while HEART uses HEPs on task level (Rausand, 2011). This means that THERP breaks the tasks further down than HEART does. Both of these methods have limitations, which are more thoroughly presented by Rausand (2011). Some main limitations of the HEART method is that it only assess single tasks, and does not have any task classification.

Two of the methods that can be used in order to identify, and analyze tasks and break them down into subtasks is functional analysis and task analysis. One of the methodologies is the *functional analysis system technique* (FAST). This form of analysis is called hierarchical task analysis. The analysis starts with a goal that shall be fulfilled. The goal is then broken down into system functions needed to fulfill the task, that again is broken down into functions. As for fault trees there are *AND* and *OR* gates that can be used to divide the different functions into sub functions or sub tasks. As seen in Figure 3.1, from the left to right one can follow the 'how' of fulfilling the intended function, and from the right to left one can find 'why' the different sub-tasks needs to be done. This method can be used for technical systems, and for human actions, or a combination of both.

Task analysis is structured around the sequence of tasks, rather than the function. So while the basic elements can be the same as in a functional analysis, the sequence will be different. An example of the use of a task analysis could be a set of tasks needed to realize a barrier function.

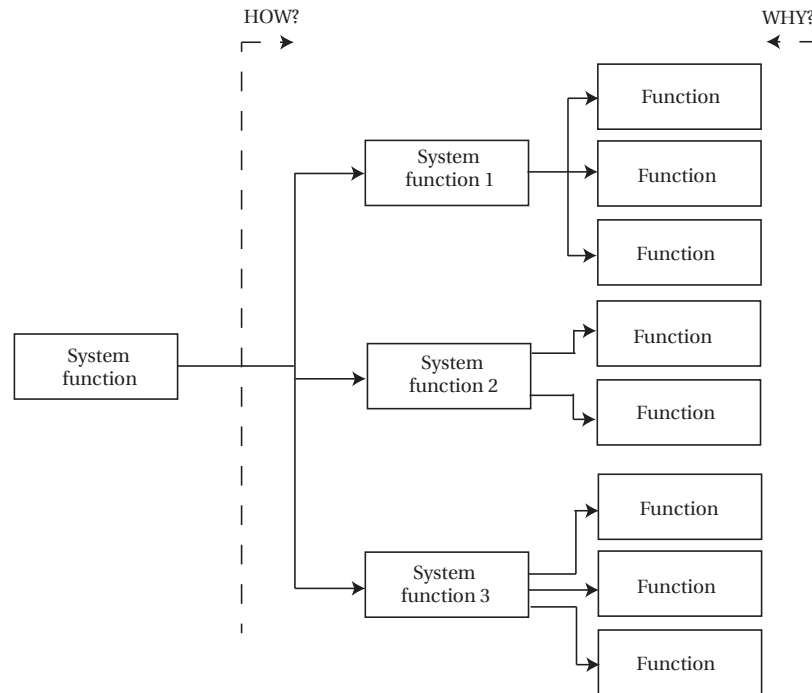


Figure 3.1: FAST diagram (based on Fig. 3.5 by Rausand and Høyland (2004))

Spar-H

Gould et al. (2012) are in the paper *'Human Reliability Analysis in Major Accident Risk Analysis in the Norwegian Petroleum Industry'* investigating the applicability of HRA to the oil and gas industry. Among the evaluated HRA methods, Spar-H (Standardized Plant Analysis-Human Reliability Analysis) was found to be the most applicable to the petroleum industry. Gould et al. (2012) notes that the method have mainly been applied to post-initiator tasks, since the amount of variables in pre-initiator tasks makes them more complex. In their discussion Gould et al. (2012) notes that some of the main difficulties with adapting HRA to the petroleum industry is that the nuclear power plants, the models are made for, have more standardized operator tasks and event trees, and that the number of possible accident scenarios are much higher in the offshore oil and gas industry then in the nuclear power industry.

The application of Spar-H in managed-pressure drilling operations have also later been explored by van de Merwe et al. (2012). Spar-H is *'a structured approach to identify and assessing the potential for human error in complex tasks'* (van de Merwe et al., 2012). The method have

been applied to drilling floor operations by van de Merwe et al. (2012). The main challenges mentioned for this application was the interpretation of results, the prioritization of recommendations and the applicability of the performance shaping factors (PSF). Spar-H uses eight PSFs to adjust the HEP data, and by that increase the resolution of the model. The PSFs used are (U.S. NRC, 2006);

- Available Time
- Stress/ Stressors
- Complexity
- Experience/ Training
- Procedures
- Ergonomics/ HMI
- Fitness for Duty
- Work Processes

The Spar-H method is according to U.S. NRC (2006) *'a simplified HRA method for estimating the HEPs associated with operator and crew actions and decisions at commercial U.S. power plants*. It is categorized as mainly a quantification tool and that it provides limited support for identification of human failure events and modeling of these in a probabilistic risk assessment (U.S. NRC, 2006).

U.S. NRC (2006) presents, in the report of *'Evaluation of HRA methods Against Good practices'*, some strengths and limitations of the SPAR-H method. These strengths and limitations are summarized in Table 3.1

3.1.2 Performance Influencing Factors

Performance influencing factors (PIF), also known as performance shaping factors (PSF) (Rausand, 2011), is an important part of most HRA analysis (U.S. NRC, 2005b). The HEP values are often a generic, meant to fit a wide range of circumstances related to a operation. PIFs are used to adjust the HEP according to the environment, and to better fit collected data and experience. A definition of a PIF can be found in Rausand (2011) where a PIF is defined as following:

Table 3.1: Summary of strengths and limitations of Spar-H, based on U.S. NRC (2006) Table 4.1.

Strengths	Limitation
<ul style="list-style-type: none"> - Simple underlying model makes Spar H easy to use - The eight PSFs included may cover many situations where more detailed analysis is not required. - Even though the effects of time on performance is treated similar to that in the THERP and ASEP TRCs, other potentially important PSFs are considered in conjunction with the time factor. - Provides a detailed discussion of potential interaction effects between PSFs (but see related limitation). - Acknowledges that the method may not be appropriate where more realistic, detailed analysis of diagnosis errors is needed. - THERP like dependence model can be used to address both subtask and event sequence dependence. 	<ul style="list-style-type: none"> - Resolution of PSFs may be inadequate for detailed analysis - Despite detailed discussion of potential interaction effects between PSFs, treats PSFs as independent. - No explicit guidance is provided for addressing a wider range of PSFs when needed, but does encourage analysts to use more recent context developing methods if more detail is needed for their application, particularly as related to diagnosis errors. - Although authors checked underlying data for consistency with other methods, basis for selection of final values was not always clear.

■ **PIF:** A factor that influences human performance and hand human error probabilities. Performance-influencing factors may be external to humans or may be part of their internal characteristics.

Rausand (2011)

Rausand (2011) specifies three types of PIFs; (1) *External*, (2) *Internal* and (3) *Stressors*. *External* are factors external to the operator such as human-machine interface (HMI), organizational factors and procedures. *Internal* are factors internal to the operator, such as training, motivation and experience, while *stressors* are factors producing mental and physical stress such as fatigue, speed and load.

3.2 Bayesian Networks

Bayesian networks, or bayesian belief networks (BBNs) are one of the methods used to model influence between different factors. It describes causal relationships between different factors, that results in one or more outcomes Rausand (2011). It can bare resemblance to fault tree analysis and event tree analysis, and these methods can, with minor difficulties, be modeled as a BBNs. A BBN can be both quantitative and qualitative, or a combination of these. The method is based on acyclic graphs, in combination with probability tables for quantitative analyses. The graph consists of nodes and directed arches. A simple BBN network is shown in Figure 3.2. Here node A is the *parent node* of node B and C, and node B and C are the *child nodes* of node A. The nodes B and C cain also be called the *decedents* of node A while node A is then the *ancestor* of node B and C.

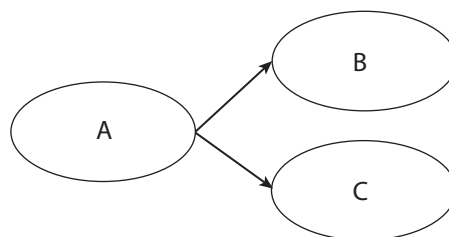


Figure 3.2: A simple BBN example with three nodes

That the graph is acyclic means that a node can not be dependent or influenced by it self, through other nodes. This means that if a node A have an arc to node B, and a node B have an arc to node C, neither node B nor C can have an arc to node A. When using BBNs for a quantitative analysis, the nodes can be discrete or continuous variables. Each node can then be given a set of states that the node can exist in. An example can be a machine that can either be working or not. This gives the node two states. Each state then is given a probability, either discrete or continuous.

3.2.1 Analysis Methods Utilizing BBN

There are a number of different analysis methods that have proposed the use of BBNs. The main use of BBN in these methods are to model human and organizational aspects of hazardous scenarios, but there have also been research on full BBN implementation. Most of these methods and analysis models have been developed during the last ten years, and have therefore not been extensively tested in the industry. Some of the methods are the Risk_OMT method (Vinnem et al., 2012), that is based on the BORA project, that to some degree have been utilized by the RNNP (PSA, 2012b). Risk_OMT is mainly a hybrid approach, where the BBNs are combined with event tree and fault tree analysis, in order to take organizational and operational factors in to account. These are denoted risk influencing factors (RIF) and is divided into organizational and operational layers, in the model. A conceptual model of the Risk_OMT hybrid modeling method is shown in Figure 3.3.

There have also been shown fully integrated BBN models, using the Risk_OMT method. Here both fault trees and event trees are converted to BBNs, in addition to the operational and organizational factors. As seen in Figure 3.3, the influencing factors are influencing an act, or activity performed by a human. The factors that are listed by Vinnem et al. (2012) are shown in Table 3.2. Most of these are related to what can be considered local workplace conditions and organizational factors in the model of defenses presented by Reason (1997).

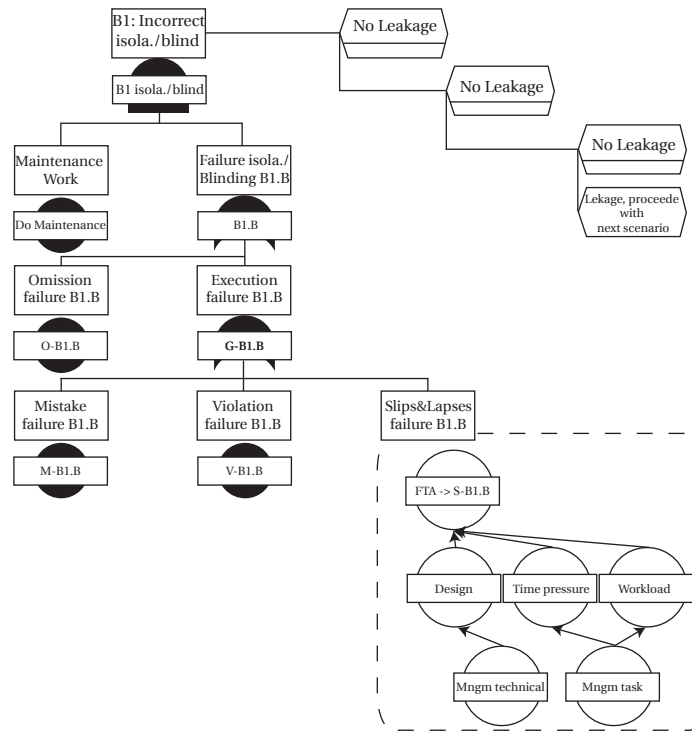


Figure 3.3: The hybrid approach presented in Vinnem et al. (2012)

Table 3.2: Risk influencing factors in the Risk_OMT model by Vinnem et al. (2012)

Level 1 RIF	Competance Disposable work descriptions Governing documents Technical documentation Design HMI Communication Supervision Time pressure Workload Work motivation
Level 2 RIF	Management Competance Management Information Management Technical Management General Management Task

3.3 FRAM

Functional resonance analysis method (FRAM) is an analysis method developed by Eirik Hollnagel. The method is strongly influenced by the principle of resilience engineering, and is therefore considered fundamentally different from the energy-barrier event based models, that most other methods are based on. Though Hollnagel (2012) argues that FRAM is not related to any specific accident model, both Hollnagel (2012) and Halseth (2012) shows that resilience engineering is an accident model that fits FRAM. A review of the modeling method is found in Torgauten (2012). FRAM is based on mapping the relations between different functions. Each function has six nodes, that represents the four restrictions that can influence the function, in addition to the input and output to and from the function. The four restrictions are *Time*, *Resources*, *Control* and *Preconditions*. The variability of the function will then change based on these restrictions, and the input to the function. The visual representation of the FRAM model is shown in Figure 3.4. The variability is considered a quality, rather than a quantity, of the function by Hollnagel (2012). This means that it is not a range uncertainty of a probability value, such as the variation is described in normal PRAs. The variability is instead expressed verbally. The variability of a technical function are normally lower then of a function based on human action.

It is also important to note that Hollnagel (2012) specifies that the term *failure* is not a part of the FRAM methodology and model. This constitutes a significant differentiation from the energy-barrier based accident models. The aim of the FRAM model is then to visualize the influence between functions, in order to better understand the system as a whole. This means that the model does not look at a specific accident scenario, but at normal operations, where a variation in a function can resonance through other functions, creating larger variations, that again can lead to an accident. Because of these fundamental differences from the energy-barrier related view, risk reducing measures and barriers are to greater extent related to decrease the variability of the functions, rather than imposing some measure between an energy source and an asset. This is also reflected by the barrier definitions presented by Hollnagel (2004). However, the modeling method is focused on functions, and there are therefore no differences in modeling human actions, technical action or combinations of these.

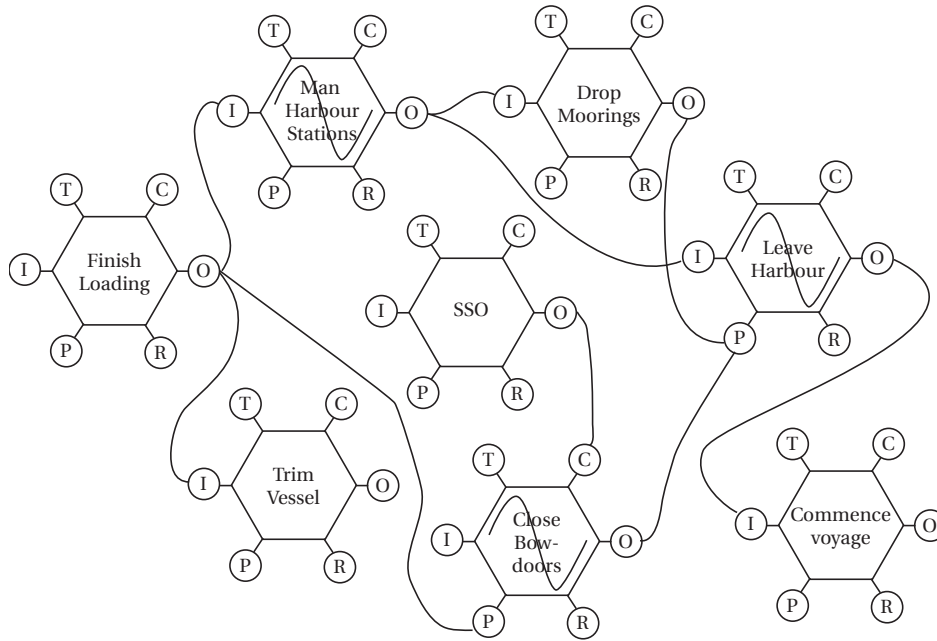


Figure 3.4: Simplified example of a FRAM network (based on Hollnagel (2012))

3.4 System theoretical methods

Leveson (2011) describes a fundamentally different approach to model systems from the event and sequence based models, in a system theoretical approach of modeling. The main difference from the traditional modeling methods is the fundamentally different accident model. The system theoretical accident model presented by Leveson (2004), called System-Theoretic Accident Model and Process methodology (STAMP), is based the notions of *constraints*, *process under control* and *control loops*. The accident model is based on enforcement of safety constraints. An unwanted event is then described as an unsuccessful enforcement of a safety constraint (Leveson, 2011). The modeling methods is based on a process under control. This process is then monitored by a sensor of some kind, that sends data on the state of the process to a controller. The controller can be either be human, a technical system, or a logic solver that evaluates the state of the process. If changes are needed, in order to keep the process under control, an actuator makes the control loop complete. The control loop is then an example of active control, and enforcement of safety constraints. A conceptual example of the modeling method is given in Figure 3.5. Passive control is for instance shields and barriers such as containment vessels.

These are not explicitly modeled when utilizing this method.

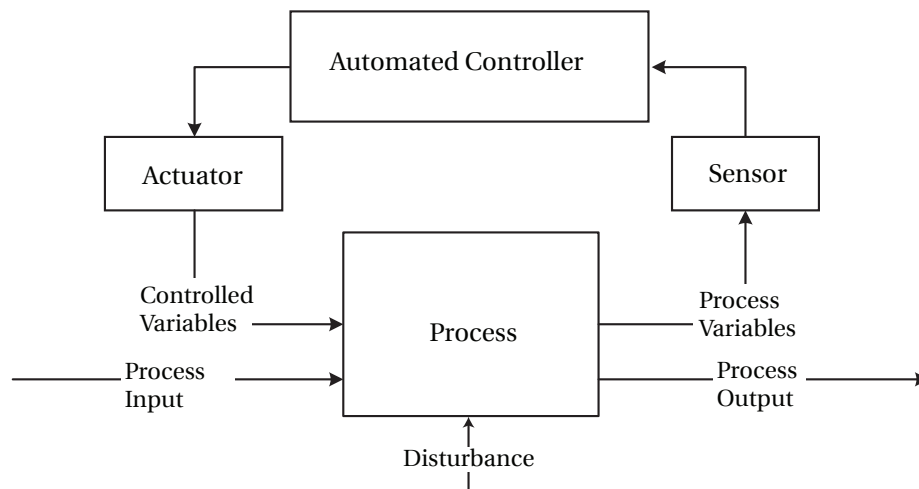


Figure 3.5: Conceptual example of a control loop as used in STAMP, with automated controller

3.5 Discussion

The models described in this chapter, are only covered in a theoretical manner. It is difficult to assume how differences in the results of applying these methods to cases could be, and the qualitative and quantitative differences in the results of a test of these models, other than the obvious theoretical differences. The scope of this thesis is therefore limited to the evaluation of how human and organizational elements are treated in the different methods, and not their impact on quantitative or qualitative risk assessments.

HRA methods are well known, and tested within nuclear industry. Unlike most methods, there are a set and tested framework for modeling, that takes both human action and underlying factors, through PIFs, into account. This seems to be the most thoroughly evaluated and tested methodology for assessment of human error probabilities, both qualitatively and quantitatively. The variety of methods and modeling tools makes the possibility of being able to adapt the methodology greater. One of the main challenge of adapting HRA methodology and HEP data, is that the existing data is developed for the nuclear energy industry. The data is often not

applicable to the oil and gas industry because of the differences in work conditions and the type of tasks that have been in focus of the nuclear industry. In the nuclear energy industry most human interaction is done through a control room. This differs widely from the conditions in the production areas of a offshore oil or gas installation where much of the human-machine interaction takes place in the oil and gas industry. Of course there are control room activities on a offshore installation as well, but the degree of standardization or similarities of both work procedures and work environment that can be achieved in the nuclear energy industry, is nearly impossible to recreate in the oil and gas industry. The collection of data, and the flexibility of the data, is therefore a main concern before it is possible to fully utilize HRA methodology in risk assessments for a offshore installation. There is the possibility of using expert judgement in addition to measured data, in order to create HEP data for offshore installations. This will possibly lessen the workload and costs of collecting data, but can also give a greater degree of uncertainty in the data.

Another concern about HRA is the linearity of the modeling methods that is used. Analysis methods, such as FAST and other task or function oriented analysis methods, describes a linear relation between tasks, such as task A follows task B and so on. In a complex work environment, and especially during unwanted or unexpected events, a set of tasks may be cyclic, repeated, or be carried out close to simultaneously. A modeling method is of course always only a theoretical representation of the real world scenario, and it is impossible to get an exact match between the model and the real world. The possibilities of improving the way these actions are modeled should nevertheless be explored.

Spar-H is found through collaborative research projects in the oil and gas industry to be a possible HRA model to use, in order to include human failure in post-initiator task analysis. This can be a first step to fully integrate HRA into both QRA and operational modeling. The model does however have many of the same challenges, with regard to data shortage and applicability, as mentioned in the general description of HRA. That the Spar-H method seems to be fairly simple, and less comprehensive compared to other methods, does not diminish it, rather the opposite. By introducing a less complex and user-friendly model the possibility of getting the model tested and implemented should increase. Though the model uses, what seems to be

quite generic PSFs, these probably needs to be adjusted in order to work in the oil and gas industry.

Critique of the way a HRA treats human actions, is also presented by supporters of both the system theoretical and the resilience based accident models, such as Leveson (2011) and Hollnagel (2004). The two accident models comes at the HRA methodology from two different angles. Leveson (2011) discusses the conflicts between reliability and safety. It is argued that increased reliability does not mean an increase in safety, and that in some cases the opposite is true; *'higher reliability leads to a less safe system'* (Leveson, 2011). This is exemplified by Leveson (2011) by a pressure vessel; A pressure vessel with an increase pressure to burst ratio will be more reliable, but if a rupture occur, the pressure will be higher, and therefore cause more damage and be less safe. This notion can also be translated to human reliability; decisions and actions can be reliable, but an accident can still occur if the information these are based on is incorrect. The information can be correct on a 'local' level, in which the decision and action is taken, but be incorrect on a system level in a larger socio-technical system that the local system is a part of. The fact that HRA does not address safety, but reliability of human actions, directs the critique of reliability focused models at HRA methods.

The control loop model presented by Leveson (2011) does however seem to be a very logical way of modeling repetitive elements, also for barrier systems. It also allows easy integration of human detection, actions and reasoning, as sensors, controllers and actuators. There does not seem to be any restrictions on what one can model using this method. Though this might not be the intended purpose of the modeling method, it is a possible area of interest to model some barrier functions as control loops, rather than linear sequences, where that is needed. Though the fundamentals of system theory and normal operation focus is not directly applicable to the energy-barrier principle, there seem to be room for both points of view within risk reduction methods. However it seems that the energy-barrier principle best represents the post-initiating event scenario.

The FRAM methodology presented by Hollnagel (2004, 2012) is based on the notion of variety in functions. The model addresses the question of treating human actions in the same way as technical systems. The notion that human action can be given a failure probability is not within the scope of the FRAM methodology (Hollnagel, 2012). The argument is that the variation of the performance of a human is an inherent quality of the "human condition". This can be seen as a critique of the assignment of reliability probabilities or error probabilities to humans.

It can however be debated whether or not the different points of view that these models that are described in this chapter, represent are mutually exclusive or complementary. In the opinion of the author, the models seem to supplement each other, rather than exclude each other. For instance are resilience thinking and the energy-barrier model, in the opinion of the author not mutually exclusive. There must be room for applying resilience thinking, as an addition to the energy-barrier principle. A more resilient organization and resilience engineering of systems does not exclude the need of barriers or risk reducing measures when an undesired event occurs. Though resilience might reduce the probability of such an event occurring, the probability can never be expected to reach zero.

Even though there are possibilities of further developing the alternative analysis methods that are in use are present, and new elements should be included, the energy barrier model is both an effective, straightforward, and comprehensible way of modeling an accident scenario, especially of post-initiating event scenarios. For this type of scenario, the simplicity of the traditional event tree and fault trees seems to be the easiest way of conveying the possible outcomes, also when including the human and organizational aspects of the event and barriers.

Chapter 4

Evaluation of Current Barrier Definitions and Classifications

This chapter will discuss the current barrier definitions and describe the differences between these definitions through example cases. The definitions that are examined are the definition and classification presented by Sklet (2006), the classification presented in the ARAMIS project by H.Andersen et al. (2004), the definitions presented by PSA (2013) and the classification presented by Hollnagel (2004). The three cases that are used are chosen based on where in the accident sequence the event takes place.

The first case, Case example A, is based on a maintenance procedure. This is clearly taking place before an hazardous event, and is a purely a preventive measure.

The second case, Case example B, is based on a drilling operation, specifically kick detection during the drilling operation. This is in a middle ground where the operation is not in the normal operation phase, and not after a hazardous event, but rather in the middle between these phases, where a failure almost instantly will cause a hazardous event.

The third case, Case example - C, is a post initiating event scenario, where a leak have occurred on an offshore installation.

4.1 Case Example - A

The example case A is a procedural description of tasks or steps in a maintenance operation on equipment that normally is containing hydrocarbons (HC) under pressure. The operation is divided into 78 steps, and was used in the BORA project. For the case in question, objective for the barriers, barrier systems or barrier elements is assumed to be *to prevent or avoid a HC leak during maintenance operation*. Four different definitions or classifications of barriers are applied to the procedure, to identify which elements in this kind of procedure can be categorized as barriers, barrier elements, or influencing factors within the different classification. Table C.1 shows the results of the categorization.

A complete description, of each of the steps in the operation, is found in Appendix B.

Table 4.1: Procedures related to maintenance operation, based on BORA.

	Work description	Sklet Classification	ARAMIS Classification	PSA Definitions	Hollnagel Definitions
Planning					
1	Receives Work Order (WO)			Performance Influencing Factor	
2	Draw up work description			Performance Influencing Factor	
3	Requisite resources, materials etc. after need			Performance Influencing Factor	
4	Draw up plan for shutdown/start-up			Performance Influencing Factor	
5	Draw up valves and blindings -package (V&B)			Performance Influencing Factor	

6	Split point marked in the P&ID			Performance Influencing Factor	
7	Draw up V&B list			Performance Influencing Factor	
8	Valve position marked in P&ID			Performance Influencing Factor	
9	Mark blindings on P&ID			Performance Influencing Factor	
10	Draw up AC-form			Performance Influencing Factor	
11	Identify and mark common barriers			Performance Influencing Factor	Symbolic barrier system ?
12	Control and sign V&B package	Active Human& Operational		Performance Influencing Factor	
13	Draw up Work Permit (WP), level 1			Performance Influencing Factor	
14	Pre-approval of WP	Active Human& Operational		Performance Influencing Factor	

15	Coordinating with (Central Control Room) CCR and other activities	Active Human& Operational		Performance Influencing Factor	
----	---	---------------------------	--	--------------------------------	--

Preparing equipment/system

16	Provide the necessary tools, etc.			Performance Influencing Factor	
17	Finds the correct seal				
18	Perform operation and maintenance preparation according to the WP			Barrier Element	
19	Process shut down	Active Human& Operational	Activated Procedural	Barrier Element	Functional barrier system
20	Isolate equipment using shutdown valves	Active Human& Operational	Activated Procedural	Barrier Element	Functional barrier system
21	Pressure release to flare or other system	Active Human& Operational	Activated Procedural/ Assisted	Barrier Element	Functional barrier system
22	Drain fluid to closed system (including all low points and instrumental pipes)	Active Human& Operational	Activated Procedural	Barrier Element	
23	Freeing gas	Active Human& Operational	Activated Procedural	Barrier Element	

24	Isolation with blindings	Active Human & Operational + Passive Physical	Temporary - Passive	Barrier Element	Physical barrier system
25	Lock/disconnect valves	Active Human & Operational + Passive Physical	Temporary - Passive	Barrier Element	Functional barrier system
26	Disconnect pumps, heat cables etc.	Active Human & Operational + Passive Physical	Temporary - Passive	Barrier Element	Functional barrier system
27	Label valves	Active Human & Operational	Activated Warned		Symbolic barrier system
28	Label blindings	Active Human & Operational	Activated Warned		Symbolic barrier system
29	Label flanges to be split	Active Human & Operational	Activated Warned		Symbolic barrier system
30	Sign WO form	Active Human & Operational			
31	Draw up SJA	Active Human & Operational		Barrier Element	Incorporeal barrier system
32	Perform operation and maintenance preparations according to the WP				Incorporeal barrier system
33	Work place control and sign WP	Active Human & Operational			
34	Approve work location and sign work permit	Active Human & Operational			

35	Authorize WP (activate in SAP)	Active Human& Operational			
36	Before work call/ review WP	Active Human& Operational			
37	Handover between shifts				
38	Disconnect safety system	Active Human& Operational	Temporary - Passive	Barrier Element	Functional barrier system
39	Sign splice log	Active Human& Operational		Barrier Element	Functional barrier system
40	Keep V&B-list in central space				
41	Control of spark and ignition sources	Active Human& Operational		Barrier Element	

Conduction of maintenance

42	Control that the flange is the one in question, and that the system is emptied of HC	Active Human& Operational		Performance Influencing Factor	Incorporeal barrier system
43	Disassembly of flanges				Incorporeal barrier system
44	Supervision of opening flanges	Active Human& Operational			
45	Sign AC-form				
46	Venting tank		Activated Prece- dural	Barrier Element	
47	Gas measurement			Barrier Element	

48	Control of flanges, seal surfaces and tracks.	Active Human& Operational		Barrier Element	Incorporeal barrier system
49	Work performed according to WO				
50	Sign form for “work performed”	Active Human& Operational			
51	Control seal, bolts and tracks	Active Human& Operational		Barrier Elements	
52	Assembly of flanges				
53	Label assembled flanges	Active Human& Operational	Activated Warned		Symbolic barrier system
54	Fill inn AC form				
55	AC-form saved for a week at minimum.	Active Human& Operational			
56	Clean work area				
57	Sign form “check out before returning equipment after completed work”	Active Human& Operational			
58	Perform final inspection, sign WP	Active Human& Operational			
59	Connect safety system	Active Human& Operational	Activated Procedural/ Activated Assisted		Functional barrier system
60	Sign splice log	Active Human& Operational			

Resetting system and production start up

61	Removes blindings	Active Human & Operational	Activated Procedural		
62	Resetting valves	Active Human & Operational	Activated Procedural		
63	Removes labelling on valves and blindings	Active Human & Operational			
64	O2-freeing				
65	Leak test performed				
66	Connect hoses	Active Human & Operational	Activated Procedural	Barrier Element	
67	Reset valves	Active Human & Operational	Activated Precedural	Barrier Element	
68	Disconnect hoses	Active Human & Operational	Activated Procedural		
69	Log possible leakages in relation to the leak test	Active Human & Operational			
70	Unlock border valves				
72	Connect pumps, heat exchangers etc.	Active Human & Operational + Active Technical			
73	Open border valves				
74	Remove labels on border valves				
75	Perform final control	Active Human & Operational			

76	Authorize work, sign WP, complete SAP				
77	Debriefing				
78	Start-up of normal production		Activated Procedural		

4.1.1 Comments on Results of Case Example - A

From Table C.1 there are some trends that are evident. The case listings shows that for the definitions and classification presented by Sklet (2006), a high number of both third-party and self-check of procedures and actions can be classified as an *'active; human & operational'* part of a barrier system. These are all within the preparation of equipment and the actual execution of the maintenance procedure.

Very few of the tasks in the planning process falls under Sklets definition of barrier system or safety barrier. There is room for discussion on this point, where it could be argued that the planning process in as a whole is a safety barrier. This interoperation is based on that there are rules, regulations and guidelines, both from authorities and often company specific, that specify that the planning procedures shall be executed. These planning procedures can then be interpreted as *'planned to prevent accidents'*, and thereby a safety barrier. The interpretation used in Table C.1 is somewhat more conservative, where the planning process is seen as the planning of means to prevent an accident.

The control of work done in the planning procedures are in this case considered a part of an active; human&operational part of a barrier system.

The classification and definitions presented by H.Andersen et al. (2004) has a higher focus on execution and actions. The *'activated - procedural'* and the *'temporary - passive'* barriers covers some of the same steps that the PSA (2013) and Sklet (2006) covers with respectively *barrier element* and *active; human&operational*, but is more specific on what the action is, and who or what it is that carries out the action to realize the barrier function in question. There are

also steps, such as *'start up of normal procedure'* that is in the ARAMIS classification considered a barrier, that the other classifications does not. In general the ARAMIS classification is more specific on the requirement to the function of the barrier. The barriers as defined by ARAMIS (H.Andersen et al., 2004) is the easiest to identify, as the description and the specificity of what constitutes a barrier is quite clear.

The barrier definitions presented by PSA (2013, 2012a) has introduced *'performance influencing factors'* in addition to the barrier, barrier element, and barrier function definitions. As Table C.1 shows, most of the planing procedures can be categorized as *performance influencing factors* within the scope PSA (2013) presents. The definitions for barrier and barrier elements are somewhat vague, or at least wide. The clarification that is given in PSA (2013) can be interpreted so that the entire procedure presented in Table C.1 is as a whole a performance influencing factor on for instance a containment barrier. On the other hand, since the definitions are as they are, it must be possible to relate it to the context of operations as well. This is the way it have been interpreted for this case. This interpretation leads to a conservative approach, where only elements that is possible to assign performance requirements to, in accordance to the statements by PSA (2013) are considered barrier elements.

The classification Hollnagel (2004) presents, is quite different from the other classifications used in this case study. The focus is more specifically on means to warn or prevent human interaction to cause unwanted incidents, especially through the *symbolic barriers* and the *Incorporeal barriers*. The *physical barrier* are also represented, while more interactive physical barriers, such as the locking of valves and disconnection of equipment is *functional barriers*, because of the need of interaction in order to function. It can definitely be argued that the focus of Hollnagel (2004) is on normal operation, and the barriers classification that is presented is therefore more focused on embedded procedures, not additional measures in extra ordinary circumstances, such as a accident sequence.

4.2 Case Example - B

This case is based on the case example used by Hauge et al. (2012) in the SINTEF report '*Barriers to prevent and limit acute releases to sea | Environmental barrier indicators*', and Chief Counsel's Report (Bartlit et al., 2011) on the Macondo accident.

The case is based on the drilling process, more specifically on kick detection and avoidance, where the main hardware is the blowout preventer (BOP) and mud control. The technical elements are in place to prevent releases to sea. There are also human machine interaction and interpretation, in addition to rules, regulations and procedures related to this operation. The operation itself can more accurately be described as a loop of operations where several of the elements are either a continuous operation or a task that can be performed several times within the time period, rather than a linear sequence where one thing leads to the next. There are however also more linear sequences, especially if a kick is detected. A list of procedures and other elements is found in Table C.2. These elements are then assessed against the four classifications and definitions.

For the case in question, objective for the barriers, barrier systems or barrier elements is assumed to be *to detect signs of kicks to prevent and minimize the effects of an escalation*.

Table 4.2: Description of kick detection operational elements

Element description	Sklet Classification	ARAMIS Classification	PSA Definitions	Hollnagel Definitions
Pit gain	Active Technical		Barrier Element	Incorporeal barrier system
Flow out measurement	Active Technical	Activated - warned	Barrier Element	Functional barrier system
Flow in measurement	Active Technical	Activated - warned	Barrier Element	Functional barrier system
Flow in/out comparison	Active Human & Operational	Activated - warned / assisted	Barrier Element	Incorporeal barrier system

Operator knowl- edge			Performance in- fluencing factor	Incorporeal barrier system
Visual inspection of flow line (video)	Active Human & Operational		Barrier Element	Incorporeal barrier system
Mudlogging	Active Technical		Barrier Element	Incorporeal barrier system
Drill pipe pressure measurement	Active Technical	Activated warned	Barrier Element	Incorporeal barrier system
Gas content mea- surement	Active Technical	Activated warned	Barrier Element	Incorporeal barrier system
Overboard valve	Active Technical	Activated Hardware on demand	Barrier Element	Functional barrier system
Drilling operation				
Drilling supervision	Active Human & Operational		Barrier Element	Incorporeal barrier system
Emergency re- sponse manual			Barrier Element	Incorporeal barrier system
Driller Training			Performance Influencing Factor	
Emergency discon- nect system (ESD)	Active Technical	Activated - manual / automated / emergency	Barrier element	Functional barrier system
BOP blind shear ram	Active Technical	Activated - manual / automated / emergency	Barrier Element / Barrier	Functional barrier system

4.2.1 Comments on Results of Case Example - B

In this case there are to a great extent consensus between the different definitions on what is considered a part of a barrier, barrier elements and/or barrier system. In the case of the definitions and classifications presented by Sklet (2006), most of the barriers can be classified as active technical parts of a barrier system, and with some Active Human & Operational elements of supervision. Most of the elements included in the case can be classified as parts of the barrier system, when using the Sklet (2006) classification. The elements that does not fall within this classification are related to the drilling process itself, and not specifically to kick detection.

The ARAMIS classification (H.Andersen et al., 2004) has least amount of elements that falls within any of the barrier categories. The classifications focus on execution is evident in this case. The measurement elements are here seen as part of the barriers, the detection, but the action and diagnose of the condition is done by an operator. Another possible interpretation here would be only activation of counteracting elements should be included as barriers or barrier elements. These differences from the other definitions is maybe the strongest evidence that the ARAMIS classification is made for process plants and not for drilling operations. There is absolutely room in the definition of barrier presented by H.Andersen et al. (2004) for classifying other elements in the case as barriers or parts of barriers.

When applying the PSA (2013) definition, most of the technical and operational elements can be considered as barrier elements. The exceptions are the training and knowledge elements that are considered performance influencing factors.

Most of the elements requiring some kind of human understanding and interpretation of the system is considered incorporeal barrier systems, when applying the classifications presented by Hollnagel (2004). The technical or mechanical elements are considered functional barrier systems or parts of functional barrier systems. It seems that Hollnagel (2004) definition and classification is quite applicable for this type of operation. The focus on human understanding of the system and the signs from the systems, seem to coincide with the barrier view of Hollnagel.

Not considered a barrier element is the drilling operation itself. Though some might consider all elements mentioned in Table C.2 as part of the drilling operation, the element is in this context considered the practical execution of tasks on the drilling deck. Since no detailed description of this operation is found, this is seen as a single element in this case. There might well be elements within such a operation that might fall within one or more of the definitions that is applied to the case study.

4.3 Case Example - C

The third case is constructed around a leak scenario, and is strongly influenced by the NORSOK standard S-001(NORSOK standards, 2008), and base on the leak scenario described the paper *'Risk assessment in the offshore industry'* by Brandsæter (2002). The leak scenario is described on a more general level in the event tree in Figure 4.1, and the elements is described in Table 4.3.

For the case in question, objective for the barriers, barrier systems or barrier elements is assumed to be *minimize repercussions and consequences of HC leak on offshore installation.*

TREE: HYDROCARBON LEAK

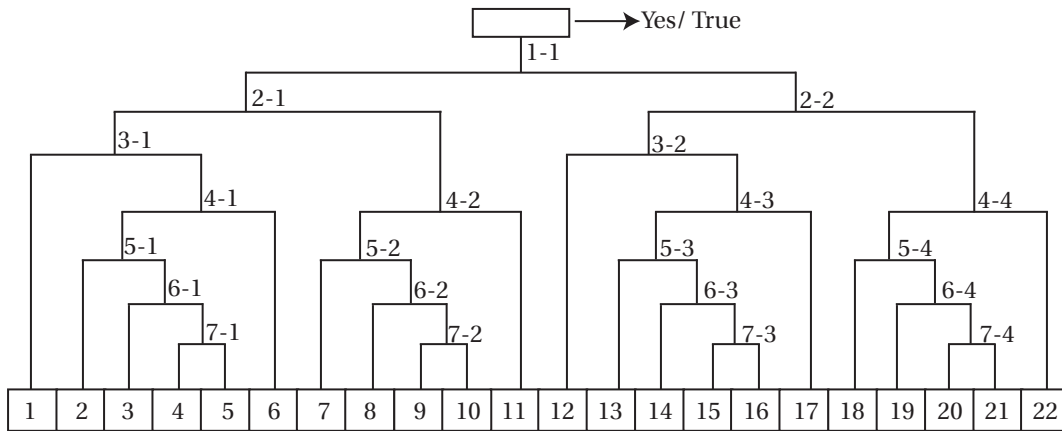


Figure 4.1: Event tree of leak scenario(Based on Fig.5 from Brandsæter (2002))

The leak event have seven stages or levels of escalation, as seen in the event tree; (1) *Isolation failure*, (2) *Ignition inside area*, (3) *Ignition outside area*, (4) *Strong explosion*, (5) *Fire water*, (6) *Spread to other equipment* and (7) *Spreads to other areas* (Brandsæter, 2002)

Table 4.3: Description of elements in the leak scenario

Element description	Sklet Classification	ARAMIS Classification	PSA Definitions	Hollnagel Definitions
Isolation of HC gas	Passive Physical	Permanent Passive	Barrier Element	Physical Barrier system
Detection of HC gas in leak area (Sensor)	Active - Technical	Activated - Automated	Barrier Element	(Functional Barrier System)
Detection of HC gas in leak area (Human)		Activated Procedural	Barrier Element	Incorporeal Barrier System
Detection of fire in leak area (Sensor)	Active - Technical	Activated - Automated	Barrier Element	(Functional Barrier System)
Detection of fire in leak area (Human)		Activated - Procedural	Barrier Element	Incorporeal Barrier System
Detection of fire in other area (Sensor)	Active - Technical	Activated - Automated	Barrier Element	(Functional Barrier System)
Detection of fire in other area (Human)		Activated - Procedural	Barrier Element	Incorporeal Barrier System
HC to flare/ vent	Active Technical	Activated - Automated	Barrier Element	(Functional Barrier System)
Ventilation of leak area (evacuate gas or seal off)	Passive Physical / Active Technical	Permanent Active	Barrier Element	(Functional Barrier System)
Separation of leak area (seal of area for humans)	Passive Physical / Active Technical / Passive Human	Activated Emer- gency	Barrier Element	Physical Barrier System

Alarm activated (Technical)	Active Technical	Activated - au- tomated	Barrier Element	Symbolic Bar- rier System
Alarm activated (Human)		Activated - manual	Barrier Element	Functional Bar- rier System
Alarm activated (CCR)		Activated - as- sisted	Barrier Element	Functional Bar- rier System
Activation of ESD (automatic)	Active Technical	Activated - au- tomated	Barrier Element	(Functional Barrier system)
Activation of ESD (manual)		Activated man- ual	Barrier Element	Functional Bar- rier System
Activation of ESD (CCR)	Active Technical	Activated as- sisted	Barrier Element	Functional Bar- rier System
Activation of Fire- water in leak area (Activator)	Active Technical	Activated auto- mated	Barrier Element	(Functional Barrier System)
Activation of Fire- water in leak area (Human)		Activated man- ual / emergency	Barrier Element	Functional Bar- rier System
Activation of water curtains	Active Technical	Activated - hardware on demand	Barrier element	Functional Bar- rier System
Firewalls	Passive Physical	Permanent Pas- sive barrier	Barrier Element	Physical Barrier System
Evacuation proce- dure	Active Human& Operational		Barrier Element	Incorporeal Barrier system
Evacuation	Passive Hu- man& Opera- tional	Activated emer- gency	Barrier Element	

4.3.1 Comments on Results of Case Example - C

As it is for the case B example, some of the operations and events are happening simultaneously or in a loop of interactions, but there is a somewhat more sequential progression of events. This is also the case where there are the most consensus on what is to be considered a barrier and not. Some differences are there, especially related to the human activation of different safety related systems. The description of human & operational elements by Sklet (2006) does not include activation of safety systems. A possible reason for this may be that this is assumed to be included in other safety systems, such as a SIS, where human activation is included in the reliability of the SIS, as shown in NEK-IEC standard 61508 (NEK-IEC, 2010). Since there are a high degree of technical elements present in this case there is also a high degree of consensus between the different barrier definitions. This shows quite clearly that it is the human and organizational contributions that is difficult to handle. As PSA (2013) notes, is it not what one calls the risk reducing measure that matters, but rather the differentiation between what is and what is not a barrier. All elements in this case, except the evacuation itself, can be classified as a barrier element within scope of the classification presented by PSA (2013), for this case.

4.4 Discussion

The three cases used represent different states of in the operation, and also different levels of human interaction. Case A is focused on operations carried out by humans. There are no automated elements, and depending on the view on barriers, either few or no technical barrier functions. Most of the human actions can be considered rule based and/ or knowledge based. Case B have a combination of both operational and technical elements, both separate and together. Here the operational elements are also skill based. The third case, Case C, has a predominance of technical elements, but also some operational element or human actions.

When comparing the results of the cases, there are some trends and characteristics of the different barrier definitions and classifications, that may not be so evident from a purely theoretical point of view. Minor differences in wording, can give quite significant differences in

practical application.

To sum up the main differences and characteristics of the different definitions and classifications with regards to operational and organizational elements can be listed as following:

- Sklet (2006) - Focus on control functions and checking procedures
- H.Andersen et al. (2004) - Focus on actions and specificity
- PSA (2012a, 2013) - does not (specifically) differentiate between different barrier elements, or barrier types. Only definition set that includes influencing factors.
- Hollnagel (2004) - Focus on normal operation, and thereby more focused on "embedded" barriers.

The distinguishing characteristic for the PSA (2013) classification is that it takes the performance influencing factors into account. On the other hand there is less room for differentiation in the PSA (2013) than in the other definitions and classifications. Even though PSA (2013) discusses organizational and operational barrier elements, in addition to technical barrier elements, it also makes the argument that what one calls the barrier element is not important, but rather which elements that are barrier elements and not. This is a sound and practical approach in general, but it also leaves much room for interpretation. This can be both positive and negative. Because of a large diversity of operations and safety procedures, a strict set of definitions of barrier types, may constrict what elements are put in place in order to reduce risk of major accidents. It may also lead to believe that elements vital to major accident avoidance are not. This can for instance be manifested through less focus on maintenance on important elements, because they do not get categorized as '*safety critical*', or human operations and actions is seen as less important since its not a part of a barrier or safety system. On the other hand a wide definition may give a unbalanced risk picture, where the weight can go either way, for instance that elements that reduces risk are not taken in to account, or that risk reducing ability is allocated to elements that in fact does not reduce risk in any significant way. When the definition is as wide as it is, the amount of elements that needs to be considered may also increase. This may lead to less attention on the elements that actually reduces risk in a significant way.

The ARAMIS definitions (H.Andersen et al., 2004) is, as opposed to the PSA (2013) definition, quite specific on what elements are considered barriers. The trisection of the different barriers

with *detect, diagnose/activate, and act* gives a quite diverse and complex breakdown of the different types of barriers, while still having a manageable subset of barriers. The term barrier is used by ARAMIS, much in the same way as *barrier system* is used by both Sklet (2006). This allows to break the barriers down into what could be considered barrier elements. The drawback of this is as mentioned above, there might be elements that are not taken into account, even if they have risk-reducing effects.

Sklet's proposed definition and classification (Sklet, 2006) has a stronger hardware perspective than both the PSA (2013) definition and the ARAMIS (H. Andersen et al., 2004) definition and classification. The basic levels of the barrier systems are here the hardware that carries out the function, that may be characterized as barrier elements. The classification then seems to be based on hardware characteristics, rather than functional characteristics. These are not mutually exclusive, shift the focus of analysis. The choice of not including human action as *human&operational* parts of the system is maybe a strict interpretation of the definitions that are presented by Sklet (2006), but based on the examples given in the paper this is a very plausible interpretation.

The Hollnagel (2004) definitions are somewhat different from the rest. The focus on *normal operation*, and to some degree *resilience*, is quite evident, both from the classifications themselves, and in the case studies. It is never the less an interesting comparison to make. The focus of this definition is clearly on the human part of the system, and especially on understanding and interpretation. This is something the other definitions and classifications do not cover to the same extent. The other side of this is that technical systems are not as well covered in this set of definitions. There can be made an argument for classifying technical systems as functional barrier systems, though this is not obvious. Automated technical systems, such as many types of SIS's are not in need of any human interaction in order to function as intended. Also purely mechanical systems, such as pressure release valves, that automatically opens at a certain pressure level will fall outside the scope of the *functional barrier system* definition. A single purpose technical element, such as the measurement of pressure have in case example B been classified as a functional barrier system. The reason for this is that this is seen as an element in a func-

tional barrier system. This interpretation may be somewhat ambiguous, but seems reasonable. All of these technical systems would also fall outside the scope of the *physical barrier system* definition, where the main concern is the passive protection elements. The lack of consistency and possibility of categorizing technical systems is the main drawback of the Hollnagel (2004) definitions and classification. For the cases used in this chapter, it may be argued that the *incorporeal barrier system* have been used at to many of the elements in the cases. However the argument used when applying the *incorporeal barrier system* is that these elements are based on thought processes and thereby knowledge, which is the basis for the incorporeal barrier system definition.

Chapter 5

Classification of Operational and Organizational Barriers

As shown in previous chapters, there are both a wide variety of types of human error and types of organizational factors that can be influential both in a QRA and in the operational phase. This chapter proposes a new way of classifying barriers. The treatment of operational and organizational elements is one of the main focus areas. The classification is also done with strong emphasis towards modeling and possible quantification of risk related to barrier failure. The proposed classification and definitions are strongly influenced by the definitions and classifications presented by Sklet (2006) and ARAMIS (H.Andersen et al., 2004), as well as the underlying goal of the barrier management document presented by PSA (2013) and the management regulations and guidelines presented by PSA (2010b,a).

5.1 Basis of a New Barrier Classification and Definition

As shown in the previous chapter there are several well thought out definitions and classifications of barriers. There have been several attempts to include human and organizational elements in different ways. It is an general consensus that the human and organizational elements in risk reduction are important, but many of the presented definitions have added them to already existing definitions and classifications, that have a bias towards the technical and physical barrier elements, and are made to fit these.

When classifying and defining barriers, there are several aspects that needs to be considered. It is important to recognize the limitations of the modeling methods available, and the ability of collecting reliable data. Even though the results of a risk assessment, or a QRA, must be seen as an estimate and the considerable uncertainty that is embedded in the models should be emphasized, there should also be an emphasis on restricting the types of elements that are modeled to those elements that are possible to quantify with a measurable degree of accuracy and verifiability. This should be reflected in the definition and classifications that are to be used.

5.1.1 Human Factors and Organizational Factors in Models and Definitions

There are, as shown in Chapter 3 several methodologies that have been developed to model the influence of human factors on technical systems, and the influence of human interaction on safety in general, both quantitative and qualitative. It is important to take these methods and models into account when proposing a new set of barrier definitions. Also in the classification scheme, it is important to bring in the practical application of the classification.

When comparing the different methodologies that are presented in Chapter 3, it is evident that there are some types of human factors that are the main focus areas. One of the most important is the human action. There are two main ways to address these; direct and indirect. HRA have mainly a direct approach, by addressing a set of tasks that can either be carried out correct, or incorrect. This is more or less consistent with the types of barriers that ARAMIS (H.Andersen et al., 2004) presents. Sklet (2006) presents a more indirect approach to this, by classifying self control and peer control of tasks as elements in a barrier system, but seemingly not the action it self. This limits the overuse of the barrier term is eliminated, since if actions are to be considered barriers, the possibility of adding too many and nearly all actions as barrier elements, even though the risk reducing abilities of these actions are negligible or non-existing.

The BBN (Bayesian Belief Network) methods can be adapted to many different barrier classifications and definitions, since the purpose of the modeling method is not risk-specific, but

has a rather general cause-and-effect focus. This coincides with most energy-barrier based accident models. The models main drawback is the amount of computing and values needed in order to present a complete model. On the other hand, the BBN approach can be combined with more traditional modeling methods, such as fault trees (FT) and event trees (ET). One of the main reasons for choosing BBN instead of FT and ET is the ability to weight the parent nodes impact on the child node. This seems to mostly be needed in relation to human and organizational elements, and the amount of computation can thereby be reduced. Also the possibility of using both quantitative, and semi-quantitative or qualitative measures gives the BBN approach an advantage. Whether or not these advantages outweigh the drawbacks of the method is not considered to be within the scope of this thesis.

The FRAM modeling method presented by Hollnagel (2012) is heavily focused on human actions, but also on the inability to calculate or quantify anything that predicts human actions. The fundamental view is that human performance is by definition variable. Though this may be true, it is also important to be reminded that risk assessments are not an exact science. All modeling is an approximation of the world or a system, with a varying degree of accuracy, in order to visualize important aspects. Quantifying the probability of failing a task, with a given uncertainty attached, is an approximation that makes it simpler to add these factors to the totality of the model of a socio-technical system. Despite the unwillingness to quantify human actions, the FRAM methodology and Hollnagel (2012) illuminates an interesting approach to modeling human action with a strong emphasis on the function of the action. This also coincides to some degree with the safety instrumented system approach, that also sets the function of the system as the most important element.

The only definition of barriers, of the four used for the case study, that uses the term organizational barrier elements is the definitions presented by PSA (2013). It may be argued that the classification presented by Hollnagel (2004) also includes organizational elements in the incorporeal barrier system definition, in the sense of rules and regulations being part of a barrier system. Though this is somewhat ambiguous since the definition also can be interpreted so that it is the knowledge that is needed in order to carry out tasks, and thereby the human element that is the actual barrier system.

The definitions that PSA (2013) presents seems to focus on the ability to adapt to any modeling method, in order to not constrain the user to much. Since PSA is a governmental regulatory body, this is a natural approach. Also, since the focus on human and organizational elements is relatively new, this approach might be a way of facilitating innovation in the industry, and then later find a '*best practice*', and adapt it into regulatory guidelines. This may be the reason that organizational elements are included by PSA (2013), in order to not constrict the users.

Since the models that include human factors seem to focus on the actions or tasks that are carried out, the barrier definitions should reflect that. Also based on the functions of defenses, described by Reason (1997), the focus of defenses is the action taken to avoid, control or mitigate an unwanted event.

When evaluating the different definitions, it is in many cases evident that the human factors and organizational factors is added on already existing definitions, and thereby only makes it more complex. Since the focus seems to have been on the hardware, in these definitions, adding a complex 'component' as a human or an organization, makes the definitions and classifications more complex as well. This is, in the opinion of the author, an unnecessary level of complexity. By switching to a more function oriented point of view, the complexity of the hardware become a secondary concern. This implies that the the ability of performing a function is the main aspect to be modeled and monitored, and by that specifying the conditions of the modeling and the monitoring.

5.2 Proposed Barrier Definitions and Classification

In the opinion of the author, the most important question to ask when establishing barriers is *why*. The need, and purpose of the barrier must be the fundamental element of barrier management. If the need and the purpose of establishing a barrier function is not possible to articulate, or describe, the need is probably not well established. As a consequence of a well defined need and purpose, it can be easier to communicate the importance and justification of the barrier, both to management and to operators, operating and maintaining the barriers. The objective of the barrier must therefore be one of the fundamental aspects of the barrier classification, and

must be based on a need found through hazard or risk identification. The objective of a barrier is realized by successfully performing the functions needed, when they are needed. The choice have therefore been made to classify barriers based on the need of functions, not hardware. The following set of definitions is therefore developed.

A barrier objective is defined as following:

☞ **Barrier Objective:** *The intended purpose of the barrier, in order to prevent, control or mitigate the risk of a specific undesired event, disclosed by hazard analysis.*

The barrier objective is found by asking *why* a barrier is needed, and is thereby answered by for instance; to minimize leak, to prevent ignition, to shield evacuation route from fire, to prevent escalation of fire, to prevent leak, or to contain HC gas. It is a higher level description of why a barrier is needed. This is found after assessing the potential hazards of the area in question. There might also be possibility of introducing a more specific objective, or requirement that the barrier functions need to fulfill. A barrier objective is realized by performing of one or more barrier functions. The barrier functions are then found by asking *how* the barrier objective can be met. These are specific function related to the realization of the barrier, not the function of the equipment used. For instance a pump in a firewater pump arrangement has the hardware function of pumping a given amount of water, but the barrier function that the firewater pump performs is to supply a given water to the sprinkler. The barrier function is the actual actions or task that needs to be carried out to prevent, control or mitigate a specific undecided event. A single or a set of barrier functions is "*the barrier*", since it is what is done in order to prevent, control or mitigate the event in question. A barrier function can then be defined as following:

☞ **Barrier Function:** *A function that is required in order to realize the barrier objective, and is performed by one (or more) barrier element(s).*

Barrier functions can be categorized by the use of six basic barrier functions; (1) *monitor*, (2) *detect*, (3) *decide*, (4) *activate*, (5) *confine*, and (6) *take action*.

1. *Monitor* - continues surveillance of input to discover trends and errors
2. *Detect* - the discovery of unwanted parameters or circumstances
3. *Decide* - the combining of available information, reaching a conclusion
4. *Activate* - the initiation of a technical system that takes action on or warns
5. *Confine* - the interposing between hazard and asset
6. *Take action* - an intervention that prevents, controls or mitigates a specific event

The basic functions are intended as a starting point, or *guidewords*, when describing the barrier function. The barrier functions can be realized by one or more barrier element, and a barrier element can partake in realizing one or more barrier functions. Barrier elements can be *technical system, a physical structure, and / or a human*. A barrier element is then defined as following:

☛ **Barrier Element:** *A physical structure, a technical system, or a human that is intended and implemented to perform one or more barrier functions, or a specific part of a barrier function.*

There are however several influential factors that can affect the ability of a barrier element to perform its intended function. These factors does not take part in realizing the function it self. These may either impede or facilitate the performance of the intended function. These are for instance environmental factors, the level of training of the operators, planning activities, the maintenance quality, stressors in the workplace (local workplace conditions (Reason, 1997)). Other factors can in a positive way influence the barrier elements ability to perform its function as it was intended. These factors can for instance be inspections, self-check procedures, and peer-check procedures, and organizational and external factors such as regulations, rules, and guidelines.

☛ **Influencing factors:** *Factors that influence to perform the intended function, when needed, either in a positive or a negative manner.*

Based on these definitions, a classification scheme have been developed. The classification is based on the basic functions mentioned in the definitions. The classification scheme is shown

in Figure 5.1, and a visual representation of the hierarchy of elements realizing a barrier objective is shown in Figure 5.2.

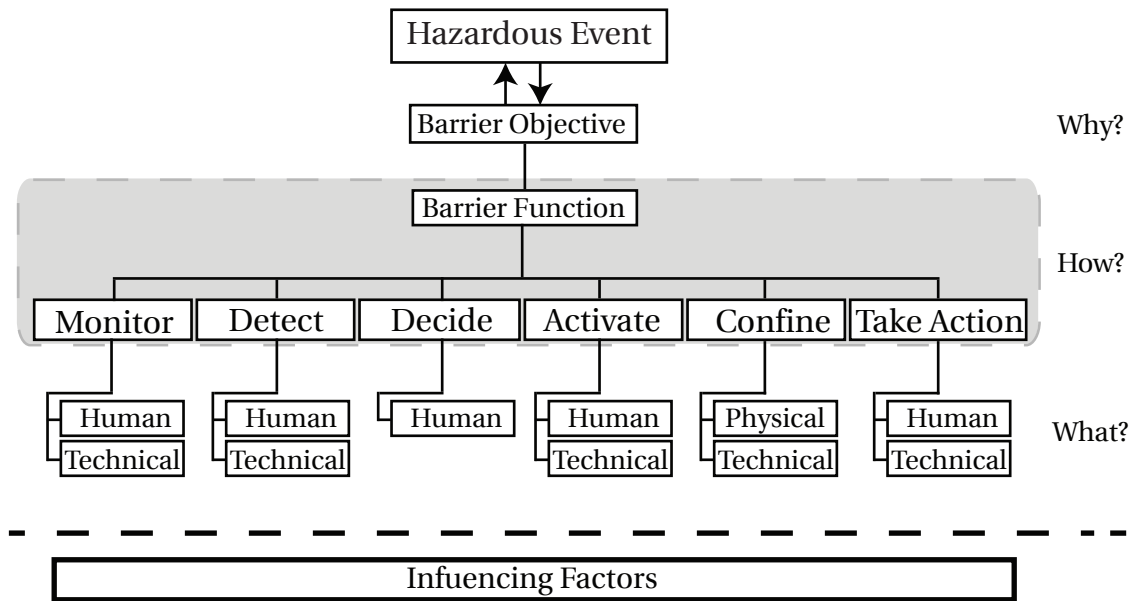


Figure 5.1: Classification for barriers

5.2.1 Impact on Operational and Organizational Factors

The proposed definition set is attempting to both reduce the gap, that is introduced between the human and the technical elements, while still drawing a clear line between what can be considered a barrier and what can not. A holistic approach to risk reducing measures must be based on the functions that needs to be performed in order to reduce risk, and allocate risk reduction to the elements that have the appropriate reliability and availability, to perform the required function. The organizational factors in this definition set and classification scheme are considered influencing factors, since they do not directly perform the actions that achieves the barrier function. An organization does not take action, even though the expression is used often. The people in the organization uses the rules and regulations that is developed and adopted by the organization.

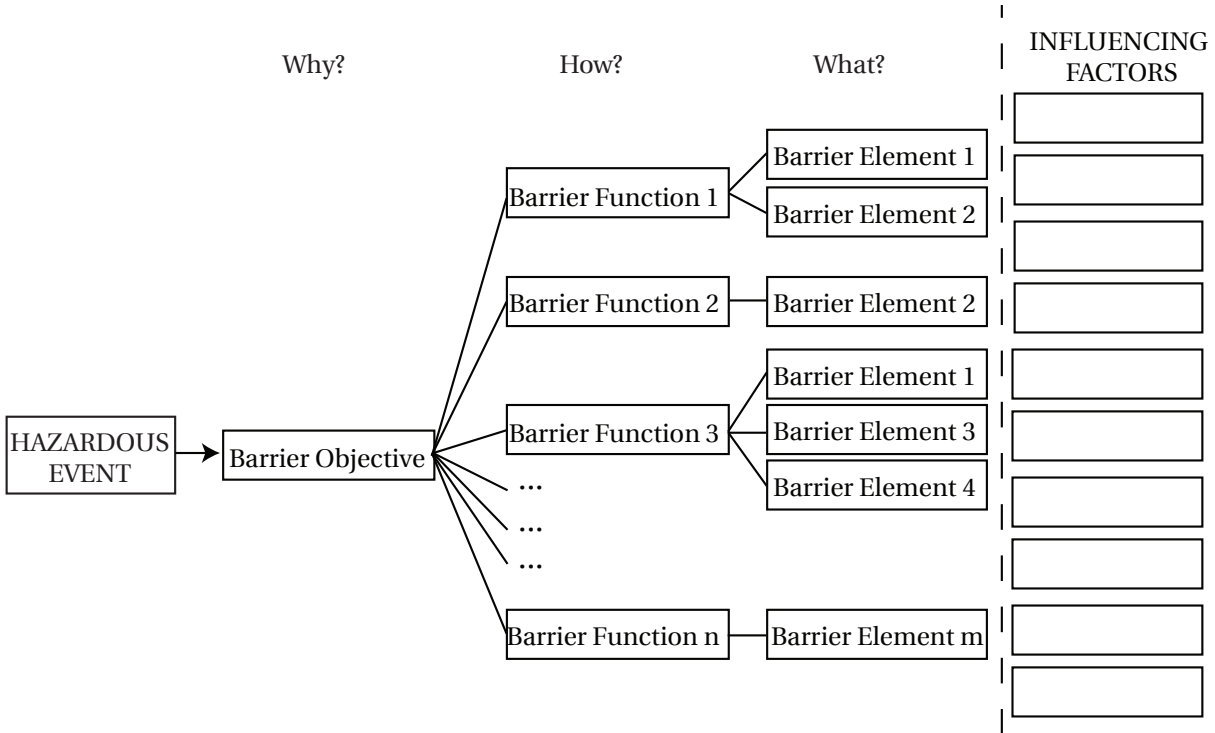


Figure 5.2: Example of hierarchy of elements realizing a barrier objective

Modeling Methods

The changes that are proposed does not impact the modeling methods that are used for QRA and similar analyzes in a significant way with regards to technical and physical elements and systems. It is however intended to give a gateway to include more operational elements and tasks into the analyzes. By creating awareness on what functions are needed to achieve a barrier objective, rather than focusing solely on the hardware functions, it will perhaps make it simpler to consider the functions humans can perform, and not overlook these during the design phases. Also by limiting the human contribution to functions, which is tangible and if not always directly measurable, then at least possible to estimate using expert judgement, the inclusion of human contributions becomes more manageable then, for instance the wider definitions used (i.e. PSA (2013) and Hollnagel (2004)). Also the fact that organizational elements are considered influential factors, makes the set of elements to include more manageable, even though the contribution of organizational factors might be an increase of data needed to be processed.

In a QRA or other similar quantitative analysis methods, it is the barrier function that should be modeled, as a risk reducing factor. Based on hardware reliability, human error probabilities and factors influencing both human and hardware, it should be possible to calculate the availability and reliability of the barrier functions, that then are incorporated into the QRA models.

It is however important to recognize the fact that when focusing on several barrier functions, that may or may not be performed by the same or a subset of the same barrier elements, one need to adjust the availability of the barrier elements based on what other barrier functions it is needed to perform.

Operational Monitoring of Barriers

The proposed changes in definitions and classification might have a bigger influence on operational monitoring of barriers than on the quantitative risk analysis made in the design phase. By focusing on the ability to realize the function and thereby achieve the objective, the totality of function that the barrier elements are to achieve must be in focus, rather than a single element. Both in terms of what to monitor, and methods to use, the definitions and classification provides a functional approach. The barrier can be monitored in several ways; use of functional tests on elements, use of indicators either on the elements, the functions, or the influencing factors, monitoring technical condition of elements, or a combination of these. The hierarchy presented in Figure 5.2 can also be a guideline of how the barrier objectives can be monitored in a near-continuous fashion, or within a given time interval. By including color coding of the different elements, functions and the objectives, a dashboard of failures or degradation of either can be shown. A failure of an objective would here be critical. Both the functions and elements can have redundancy, so even if one function or one barrier element fails, the barrier objective can still be met. Though the interconnections between the barrier elements must then be clear. This can be done by introducing *AND* and *OR* gates between the barrier functions and barrier elements, or by displaying the barrier elements in *serial* and *parallel* structures. With the functional view it may also be easier to consider alternative options for performing a function, if a system fails or an operator becomes unavailable, without getting caught up in the hardware, when using a functional approach rather than a hardware focused approach. It may also be

easier to incorporate and identify the impact of degradation of hardware on barrier functions in the modeling methods, since the focus always should be on the ability of the hardware to realize the barrier function, and not the hardware function. For instance a degraded firewater pump may still be able to perform its intended hardware function of pumping water, but may not be able to realize its barrier function of delivering a certain amount to the sprinklers at any give time. The functional view then forces the user to look at the whole systems ability to perform its intended function. It is also in relation to the barrier functions that performance standards should be made, if using the proposed barrier definition set.

Relation to HRA

There are some distinct similarities between the hierarchy of elements and functions presented in Figure 5.2, and the FAST method for HRA, briefly presented in Chapter 3. The same *why* and *how* questions are used in both. Though the definitions and the classifications are not made to fit a HRA methodology, the similarities could possibly make the transition easier to include human factors to a greater extent. Also the influencing factors described in the definitions and the PSFs used in HRA methodologies coincides. The organizational elements are in both cases seen as influences rather than elements. The use of HEP on human barrier elements, and PIFs on the organizational factors seems therefore to be a obvious possibility. Since HRA are based on the reliability of human performance, the functional approach seems to be a good fit, since the reliability of the barrier function is a key measure for design phase modeling methods, such as QRAs, where HRA methodologies are likely to be used.

Relation to Other Modeling Methods For Human and Organizational Factors

One of the methods that have been tested, to some degree, for modeling human and organizational factors in the oil and gas industry is bayesian belief networks (BBNs). The ability to have levels of influencing factors, and the ability to combine BBNs with fault trees and event trees. Here there are some concerns regarding the amount of data and calculations needed in order to get the resolution of the model at an acceptable level. The lack of data is a general concern with regards to human error or failure integration, but the exponential increase in amount of data in the data table.

The FRAM methodology presented by Hollnagel (2012) based on variation in functions and the relation between the different functions. The fundamental principle of the FRAM method is the variability of performance of these functions. Even though the FRAM method is based on functions, one can not assume that a functional approach to barrier definitions provides the possibility of modeling barriers as done in the FRAM method. It might be possible on a high level with the proposed barrier definitions. It may be a possibility of lower level (i.e. sub-system level) if one defines barrier element functions, in addition to the proposed definitions. This level is however intentionally left out of the proposed definition set, because of the level of detail needed to classify barrier element functions would be too comprehensive for modeling, at least with the information available for this thesis. The normal operation focus of the method does also set some restrictions on the use of FRAM in relation to energy barrier focus that is inherent in the barrier definition presented.

The system theoretical method presented by Leveson (2011) is also based on normal operation, and thereby have the same restrictions as the FRAM method. The modeling method itself is based on control loops, which have some properties that may be interesting for human and organizational factors. Some operations that are cyclic in nature, such as monitoring, control loops can give a more realistic representation of such a process.

5.2.2 Comparison to Definitions used in Cases A, B and C

The proposed definitions and classification is applied to the cases presented in Chapter 4. The tables with that shows the application of the definitions and classification on the cases is shown in Appendix C. The case examples gives some insight into how the proposed definitions can be have in use. The most distinct difference from the other definitions that is applied to the cases is the number of elements that is considered *influencing factors*. Several of the elements that in the other definitions are barrier elements, or parts of the barrier system, is with the proposed definitions influencing factors. Especially the elements related to formalities and checks offs of work conducted in Case A, differentiates the new definitions. A procedure that became difficult to place in the new set of definitions, for Case A, was the labeling of for instance valves. Here it

can be argued that the labeling is an influencing factor, that influences the operator in a positive way. Another interpretation is that the act of labeling is an barrier function, in the same sense that disconnecting safety systems are, in order to avoid unwanted events. The latter is chosen in this case, but the lack of practical experience from the author is in general a source of error.

In the results of Case B and C the outcome for the proposed definitions, were more similar to the other definitions, though it can be argued that the proposed definitions and classifications is more detailed and for some elements give a more accurate description of the actual elements in question. That there are less differences between the proposed definition in the last two cases is not unexpected, especially Case C that have a high degree of technical elements. This shows that the definitions work for the basic technical elements, as well as being able to incorporate the operational elements.

5.3 Possible Framework for Barrier Identification

The definition and classification opens the possibility of a framework that can be used to structure the process of barrier identification, both in the design phase, and in an operational phase or during modifications. For a generic barrier identification process the process can be described in the following nine steps:

1. Perform hazard identification or risk analysis
2. Identify what hazards or hazardous events that can occur where allocation of risk reducing measures are needed.
3. Identify the barrier objectives by asking *why* you need a barrier for the specific situation, or event in the accident sequence.
4. Identify what functions are needed in order to achieve a barrier objective that have been identified, by asking *how* the barrier objective can be achieved. (The six basic functions can act as *guidewords*, for instance by using the worksheet (see Figure 5.3))
5. Identify what barrier elements are needed by asking *what* is needed to perform the functions that are identified in Step 4.

6. Confirm the ability of the barrier element to perform it intended function (for instance by using the barrier evaluation criteria presented by Rausand (2011)), to check that the risk reduction is adequate.
7. Identify factors that will influence the barrier elements ability to perform it intended function
8. If the risk reduction is not adequate, repeat Steps 4-7 to add additional functions, or additional elements for redundancy.
9. Repeat Steps 4-8 for all barrier objectives

In order to structure the process, a worksheet have been developed. The worksheet is shown in Figure 5.3. The worksheet is generic, and can and should be modified to the needs of the user. For instance, a barrier function can be realized by several barrier elements. The worksheet provides an overview of the possible barrier functions that can be applied, and thereby makes it harder to forget or overlook a barrier function that could be needed. The next subsection gives an example of how this framework can be applied to a accident scenario.

	Barrier Objective 1		...		Barrier Objective n	
	Barrier Function	Barrier Element	Barrier Function	Barrier Element
Monitor						
Detect						
Decide						
Activate						
Confine						
Take Action						

Figure 5.3: Example of worksheet for barrier identification

5.3.1 Case Example - Leak Scenario

In order to better explain the barrier definitions, classification scheme and barrier identification method, a case example is used to do this. The system in question is based on the same scenario used in Case B in Chapter 4. The scenario has the seven stages of escalation that is described by Brandsæter (2002); (1) *Isolation failure*, (2) *Ignition inside area*, (3) *Ignition outside area*, (4) *Strong explosion*, (5) *Fire water*, (6) *Spread to other equipment* and (7) *Spreads to other areas*. This list then constitutes steps 1 and 2 in the framework for barrier identification presented in Section 5.3. The next step is then to identify the barrier objectives. In this case '*minimize leakage*', and '*detect leak*' would be an obvious barrier objective for the initial stages of the gas leak. Other barrier objectives could be '*raise awareness of gas leak in leak area*', '*lower gas concentration in area to non-dangerous level*', and '*prevent gas ignition*'. If there is an ignition of the HC gas, there would be several other barrier objectives that is needed, but for this example the focus is on pre-ignition barriers.

Step 4 is to identify the functions needed in order to achieve the barrier objective. This is done with the help of the guide words, and the worksheet. This is shown for this example case for the '*minimize leak*' and '*prevent ignition*' barrier objectives. The barrier elements needed to realize these barrier functions are then identified in Step 5 of the framework. The application of these steps on the case example is shown in Table 5.1. From the table it is shown that there might be possibilities of several barrier elements performing the same barrier function, and in some cases, several barrier elements are needed to perform a needed function.

The next step in the proposed framework is the confirmation of the barrier elements ability to perform its intended function. This step is not performed in this example. Here some calculations, and expert judgement can be used, in combination with experience data.

Step 7 is focused on identifying influencing factors. These are of course case specific, but some general influencing factors, such as the safety influencing factors presented by Schönbeck et al. (2010), such as *maintenance management*, *procedures*, *housekeeping*, *communication* and *training*, as presented in Chapter 2.3. For human operations and human machine interactions (HMI), PSFs can be used. These would depend on the HRA modeling method used. The last two steps are not included in this example, since they only are repeating the previous steps.

Table 5.1: Example of use for the barrier identification worksheet for the barrier objective *minimize leak* and *Prevent Ignition*

Minimize leak		
	Barrier Function	Barrier Element
Monitor	Observe pressure changes in vessel	Pressure sensor Operator Mechanical pressure sensitive device
	Monitor HC gas level in given area	Gas sensors Operator
Detect	Detect ruptures in vessels	Operator vessel integrity sensors(?)
	Detect high levels of HC gas	Gas detectors
Decide		
Activate	Activate shutdown valve leading in to area	Logic solver Operator CCR Operator
Confine	Seal of given area	Doors Hatches
Take Action		
Prevent Ignition		
	Barrier Function	Barrier Element
Monitor	Monitor HC gas in areas with ignition sources	Gas sensors Operator
Detect	Detect HC gas in vicinity of possible ignition source	Operator Gas detector
Decide	decide whether or not to shut down processes that may cause ignition	Operator CCR operators
Activate	Activate shutdown procedures	Operator SIS
Confine	Isolate hot surfaces that can lead to ignition	Isolating material Heat sink
Take Action	Shut down possible ignition sources if alarm is activated	Operator SIS CCR operator

5.4 Discussion of the Proposed Definitions and Classification

One of the clear characteristics of the proposed set of definitions and classification, is the separation of all organizational aspects of the operation of the barrier are considered influential factors, rather than barrier elements. The organizational elements, such as procedures on a low level, and rules and guidelines on a higher level, are separated from the barrier functions realization, since they does not perform the action that detects, monitors, decides, activates, confines, or takes action on an undesired event. That does not mean that the procedures or guidelines are less important, or that less focus should be on these factors when working with safety and risk reduction on a installation. Procedures, rules, regulations, and guidelines lay the foundation of which actions and measures that are to be taken, and when they should be performed. But the quality of a procedure does not assure the quality of an action, it only influences it.

An example of this may be that a procedure states that if a ship infringes the safety zone of an offshore oil rig, the ship must be contacted and measures such as activating an alarm must be take. However, it is logical to assume that if a ship is registered as being on a collision course with the oil rig, the natural response to this would be to try to contact the ship, and take measures to notify the people on offshore oil rig. And it is this action that serves as a barrier, not the procedure. A procedure will influence when and what measures are to be carried out, but not execute the necessary actions, and is therefore not considered a barrier element.

There are some challenges with the proposed definition. The use of the basic functions *monitor*, *detect*, *decide*, *activate*, *confine*, and *take action*, may in some ways be too constricting and, in some situations, ambiguous to the user. The constrictions are intended, but it may in some cases be too much. Especially in cases where elements performs several functions, as a SIS does, or a human might do. This is counteracted by specifying that one barrier element can perform one or more functions.

Some actions may also be difficult to place. An example of this can for instance be monitoring of a flow measure, in the kick detection example in case B. The operator are supposed to detect signs of kicks. This can then be categorized as a detecting - function. In the case

studies, especially Case B however, the comparison have been categorized as a decide function, and the the monitoring technical input from the sensors have been categorized as a technical-monitoring, since the detection of signs of kicks is, based on the Bartlit et al. (2011) report, a continuous process that is different, depending on type of equipment used and type of drilling that is conducted. The detect-function is meant more or less as an equivalent of a sensor-function, but also including human senses, such as it is used in case C, where detection of a gas leak or a fire can be done by either a sensor or a human. There are therefore definitely some ambiguity related to these terms.

Another element of the proposed definition that might be somewhat confusing is the introduction of a new term, barrier objective. Since the term barrier function is somewhat established as a near-equivalent to the barrier objective definition that is presented, there might be some ambiguity, and misunderstanding of the differences of the two terms. The term is introduced in addition to barrier function, to give a clearer distinction between the goal and the performed function. Other terms, such as *barrier function and barrier sub-functions*, and *barrier system-function and barrier element-function*, have been considered during the development of the definitions.

In relation to the barrier performance characteristics presented by Rausand (2011)¹ and barrier properties presented by Hollnagel (2004)², both described by Torgauten (2012), the proposed classifications and definitions seems to be applicable. Both focus on the ability to perform the intended function. The intent of the proposed definitions and classification is indeed to highlight the functions, and make the measures and assessment of the barriers abilities focused on the barriers function.

A element that the Hollnagel (2004) definition has, that the new proposed definition does not have, is the focus on how the barrier is perceived. An example of this is an alarm activation. An alarm can in the classification presented by Hollnagel (2004) be an *symbolic barrier system*. It

¹Specificity, Adequacy, Independence dependability, Robustness, Auditability

²Efficiency and adequacy, Robustness (reliability), Delay in implementation, Applicability to safety critical tasks, Availability, Evaluation, Dependence on humans

focuses on what the barrier does, rather than the act that engages it, as the proposed definition in this thesis does.

The proposed definitions and the proposed classification does however seem to be a good fit for several of the possible modeling methods that are available such as HRA methodologies and models that are academical, and under development and not tested in large scale such as FRAM and to some degree BBNs. BBNs are a available methods of modeling, but within the field of risk assessments and especially with regards to human and organizational factors, it is still a model that is under development.

In the proposed model, the barrier elements function is not included as a separate level. There is definitely possibilities of including this, but here the question is here whether or not this contributes to a better understanding of the barrier function, or only confuses the user of the definitions. On the element level, the barrier element function and the hardware function becomes more intertwined.

Even though this set of definitions and the classification scheme are focused on the function of barriers, rather than the hardware itself, there are, and will be in the future, specific requirements to some of the standard barriers or barrier element, especially when they are related to specific standards. Examples of possible specific requirements are the NORSOK D-001 standard and the NORSOK S-001 standard (NORSOK standards, 2012, 2008). The NORSOK D-001 is specific towards drilling operations, while the NORSOK S-001 is more general regarding design and operational requirements to technical safety. It is worth noting that these established specific requirements does not seem to conflict with the barrier definitions and classification that is presented in this thesis, but that it is not necessarily a direct equivalence between the requirements in the standards and the barrier function or the barrier objective in the definitions.

It is also important to note that this is not a reversal of the barrier strategies that are in place. The focus on barrier functions are in many cases already there, but this classification and definition scheme attempts to take it one step further, and by that ease the integration of human/operational elements, while still giving some boundaries.

With regards to future improvements and trends within the safety and risk reducing methods, such as resilience and system thinking, the proposed definitions will not be outdated if such models should be introduced. The fundamental concept of resilience engineering, as described by Hollnagel (2012), is *'a description of characteristic functions, and look(s) for ways to enhance the systems ability to respond, monitor, learn and anticipate*. This coincides with the functional view of barriers as presented by the proposed set of definitions and classification.

Chapter 6

Summary

In this chapter a summary of the thesis, and the findings of this thesis. A brief discussion on the results of the thesis is conducted, and also possible areas of further work are suggested.

6.1 Summary and Findings

The thesis have addressed some important elements on risk reducing measures, and the relation to operational and organizational factors. In Chapter 2, the literature survey and review is described. The focus of the survey is both the barriers in general, in addition to the human and organizational aspects of risk reducing measures. The review is wide, and gives a brief overview of the general barrier concepts, such as the Reason model (Reason, 1997), the definitions and classification presented by Sklet (2006), the layers of protection principle and the layers of defense principle. There are also a review of the ARAMIS definitions and classifications of barriers (H.Andersen et al., 2004), which arises from the chemical process industry. Some methods and models that integrates human and organizational elements, that was not covered by Torgauten (2012) is also reviewed, and summarized. The regulatory authorities proposed definitions and guidelines have been emphasized, since these give some ground rules on what the authorities demands of the oil and gas industry. There are also reviewed some literature regarding safety instrumented systems, and their relation to human and organizational elements, since these are an important part of the safety systems that are in place in the industry today.

The literature survey and review confirmed that there are inconsistencies in the way human

and organizational elements are treated. There are however some trends that arises. There is a stronger focus on barrier functions, rather than hardware. There are however not a obvious consensus on how human and organizational elements are to be treated with regards to barrier functions.

Chapter 3 is focused on the main modeling methods that have a focus on human and organizational elements, and is giving a brief summary of the main aspects of these models. The main focus is on human reliability analysis (HRA), but also other methods and models are briefly reviewed. HRA methods is a well established way of including human and organizational factors in risk analysis, in other industries, especially the nuclear power industry. There are however research done on utilizing HRA in the oil and gas industry, such as the work done by van de Merwe et al. (2012), attempting to utilize the Spar-H methodology on oil and gas operations. There is however several challenges when doing so, both with regards to the methods themselves, and with regard to the lack of data available on human and organizational factors and errors. HEP data, which is an important part of the HRA methodologies, are also used in other methods, modeling human contributions to errors. Risk_OMT (Vinnem et al., 2012), a modeling method using BBNs to model influential factors to human action uses HEP data in combination with expert judgement to quantify the human contributions. One of the main limitations in the Risk_OMT project was the lack of data on human error and influencing factors.

Some other modeling methods are also described, such as the FRAM method presented by Hollnagel (2012). This method constitutes a fundamentally different approach to modeling, as the main goal is to identify the influence between different functions, and how the functions varies based on different influences. The FRAM method is also a qualitative method, where the variation in the functions are to be described verbally, and not by probabilities. Though not focused on the energy-barrier-asset paradigm the FRAM method focuses on functions and variability, that could be used to analyze barriers as well.

The fourth modeling method that is described in Chapter 3, is based on the system theoretical approach presented by Leveson (2011), called STAMP. This model is also focused on *normal operations*, but is structured around control loops. Here the possibility of including human elements, either as sensors, controller or as actuators, are evident. This interpretation of the

modeling method might fit some barriers quite well, although this might not be the intention of Leveson (2011).

Chapter 4 is divided in three case studies. The the example cases are chosen to represent different cases where barriers are considered and used. Four barrier definitions is then applied to the elements in the cases, to see what elements are considered barrier elements, barrier functions or influential factors, and observe the differences between the four barrier definitions in applied situations. This is in order to uncover differences that are unapparent when just assessing the wording of the different barrier definitions. The four definitions chosen was; the *Principles of Barrier Management in the petroleum industry*(PSA, 2013), the ARAMIS definitions and classifications (H.Andersen et al., 2004), the barrier definitions and classifications presented by Sklet (2006) and the barrier definitions presented by Hollnagel (2004).

The first case is based on a maintenance operation, that was used in the BORA project. This case is a clear pre-event (or pre-hazardous event) situation, in the Reason (1997) event sequence. The differences between the four definitions was most evident in this case, compared to the other two cases. Both the definition by Sklet (2006) and by PSA (2013) define a larger amount of the elements in this case as barrier elements or parts of the barrier system, then the ARAMIS definitions (H.Andersen et al., 2004) does. This is especially regarding the checking of work and other procedural elements. The definition by PSA (2013) also stands out in this case, because of the use of performance influencing factors, which allows for a more differentiated selection.

The second case is a kick detection process, in relation to a drilling operation. Here there are more technical elements, where there are a higher degree of consistency between the different definitions. Here the set of definitions that deviated the most from the rest, was the ARAMS definition. This can in some degree be contributed to the fact that the ARAMIS definition is focused on the process industry, where this kind of operations are non existing. There are also some differences in the treatment of knowledge and training.

The last case example is a leak scenario, where the definition and classification that stands out is the definition presented by Sklet (2006) in relation to detection and activation activities for operators.

The trends that are evident, with regards to operational and organizational aspects, in the case

examples are that Sklet (2006) focuses on checking procedures and control functions, that the ARAMIS definition focuses on actions, and that the Hollnagel (2004) definition focuses on normal operations and warnings. The definitions presented by PSA (2013) stands out as less specific, trending to wage on operational and organizational aspects, where most elements in the cases could be considered barrier elements.

Chapter 5 discusses the previous chapters, and presents a new set of barrier definitions and a new classification scheme based on these definitions. The definition set is based on a functional view of the barrier term. This means that the barrier function becomes the most important part of the barrier. The function is however somewhat different from the barrier function definitions presented previously in the thesis. The barrier functions are low level functions that realizes the barriers objective, which is the higher level goal in relation to a specific hazardous event. There are provided some guide words for describing the barrier function needed; *detect, monitor, decide, activate, confine, and take action* these basic functions can then be realized by either a technical system, a human or a physical structure. The barrier elements are then limited to the those that are realizing the barrier function directly. This means that for instance procedures, rules, regulations, maintenance, and environmental conditions are defined as influencing factors. This is in order to differentiate between the acts and conditions that actually realizes the barrier function from the elements that influence the ability of the barrier elements to realize the barrier function. This distinction is made to make it easier to understand what functions are needed to prevent, control or mitigate a hazardous event, and then in turn make it easier to communicate what these functions do, in order to raise the awareness on what is needed in order to prevent, control or mitigate an event.

The following definitions is proposed in Chapter 5:

☞ **Barrier Objective:** *The intended purpose of the barrier, in order to prevent, control or mitigate the risk of a specific undesired event, disclosed by hazard analysis.*

☞ **Barrier Function:** *A function that is required in order to realize the barrier objective, and is performed by one (or more) barrier element(s).*

■ **Barrier Element:** *A physical structure, a technical system, or a human that is intended and implemented to perform one or more barrier functions, or a specific part of a barrier function.*

■ **Influencing factors:** *Factors that influence the barrier elements ability to perform the intended function, either in a positive or a negative manner.*

The barrier definitions are then compared to the three cases used in Chapter 4. The definitions and classification is incorporated into a proposed framework for barrier identification purposes, and this framework is then used to give an example of the use of the barrier definitions.

6.2 Discussion

The main goal of this thesis is to highlight the challenges in implementing non-technical elements into barrier thinking, clarify the terms and definitions, and propose a possible solution of how this can be done. There are some main challenges that are in need of consideration. The first is the line between what is considered a barrier element and what is not. The various definitions found in the literature survey has different ideas of where this line should be drawn. In the opinion of the author, there is a logical distinction between the elements physically performing a function that reduces risk, and the elements that supports the functional elements. This is not to say that supporting elements, such as procedures and maintenance management, are not important in order to reduce risk, however, it does not perform the risk reducing action, it only facilitates the action.

This is also the reasoning behind the focus on the *barrier function* as the most important element of the barrier, which is the second aspect of this thesis. It is the ability to perform this functions that prevents, controls or mitigates a hazardous event. On the other side, it can then be said that all normal operation actions that prevents the process from going outside its intended area of operation, are to be considered barriers. This might be true, and normal operation elements are important to maintain a safe operation, however, the energy-barrier principle

implies the occurrence of unwanted events, and the planning of handling such unwanted scenarios, and it is in this principle the barrier term must be founded.

The third aspect of this thesis is the ability to model and monitor the performance of the non-technical barrier aspects. Though several modeling methodologies have been reviewed, it is difficult to assess the suitability of them without an comparison, both to today's methods and to each other. Because of this lack of actual comparison, especially quantitative comparison, it is not given any specific recommendation on what modeling methods that should be used. However, the HRA methodologies seem to be the basis for the barrier modeling methods that has its basis in the energy-barrier principle. If the challenges of applicability of the model and the amount of data available are solved, HRA, and in particular HEP data seem to be a valid way of modeling human factors in relation to the functional barrier view the proposed barrier definition set is providing. This is though something that should be reviewed more thoroughly.

It can be argued that the proposed barrier classification and definition set are only another one in the large amount of barrier definitions available. Though, from the authors point of view, the proposed solution is not a final solution, but hopefully a step in the right direction in order to be able to include human actions and organizational factors in risk assessments, and clarify the distinction between function and hardware.

6.3 Further Work

Some of the areas that this of particular interest for further research, based on the findings of this thesis, are the use of HRA in both QRAs and in operational modeling. This will be comprehensive, and will probably be part of larger research projects.

Also, if the proposed barrier definitions are to be used in any real applications, third party reviews should be performed. Here weaknesses and improvements of the definitions can be highlighted.

The differences in application for functional versus hardware focused barrier definitions should also be studied. This should be done in order to explain and highlight practical differences between these two perspectives.

In addition, the relation between performance standards, influencing factors and barrier elements is in need of further study, especially in relation to quantification of human and organizational barrier aspects. The author believes that a more real-world case based test of the different modeling methods would be beneficial in order to actually be able to conclude in some way on that modeling methods that are possible to use, given a specific definition is used. This would require a higher degree of participation from the industry and in particular those operating the offshore vessels.

Appendix A

Acronyms

ARAMIS Accidental risk assessment methodology for industries
in the framework of the Seveso II directive

BOP Blowout Preventor

BORA Barrier and Operational Risk Analysis

BBN Bayesian Belief Network

CCPS Center for Chemical Process Safety

CCR Central Control Room

ET Event tree

ETA Event tree analysis

FMEA Failure mode and effect analysis

FT Fault tree

FTA Fault tree analysis

HAZOP Hazard and operability study

HC Hydro Carbon

HEP Human Error Probability

HFR Human Failure Ra

HRA Human reliability analysis

IF Influencing Factor (Similar to RIF, PIF and PSF)

IPL Independent protection layers

ICAO International Civil Aviation Organization

INSAG International Nuclear Safety Advisory Group

LC Level of Confidence

LOPA Layer of protection analysis

MTTF Mean time to failure

MTO Human, technological and organizational

PFD Probability of failure on demand

PHA Preliminary hazard analysis

PSA Petroleum Safety Authority (PSA is also known as Probability Safety Assessment, see QRA)

RAMS Reliability, availability, maintainability, and safety

RIF Risk Influencing Factor (Similar to IF, PIF and PSF)

Risk_OMT Risk modeling - Integration of Organizational, Human and Technical factors

RT Responce Time

SIL Safety integrity level

SIS Safety instrumented systems

Spar-H Standardized plant analysis risk - Human Reliability Analysis

STAMP System-Theoretic Accident Model and Process methodology

TRA Total Risk Assessment (Similar to QRA)

P&ID Pumps and Instrumentation Diagram

V&B Valves and Blindings

PIF Preformance Influencing Factor

PSF Performance Shaping Factor

QRA Quantitative Risk Assessment / Analysis (Treated equal to PSA, TRA, etc.)

Appendix B

List of operation

Descriptions of the operation taken from the BORA studies, from the description given in Halseth (2012)

Table B.1: Description of maintenance operation tasks

	Work description	Executor	Demands	Possible Faults
Planning				
1	Receives Work Order (WO)	Planner	Piping and Instrumentation Diagram (P&ID) + Activity and control form (AC-form)	
2	Draw up work description	Planner		
3	Requisite resources, materials etc. after need	Planner		
4	Draw up plan for shutdown/start-up	Area-/ operator manager		

5	Draw up valves and blindings-package (V&B)	Planner	V&B drawn up based on WR0218	V&B- list not drawn up, V&B-list is wrong
6	Split point marked in the P&ID	Operations system manager	All connections mounted/demounted must be marked in the P&ID	Split position not noted, Wrong split position noted
7	Draw up V&B list		V&B must include a V&B-list	V&B list not drawn up, V&B list is wrong
8	Valve position marked in P&ID		Valve position described and marked in P&ID	Valve position not scribed and marked in P&ID
9	Mark blindings on P&ID	Area-/ operator manager	Blindings described and marked in P&ID	Blinding not noted, Wrong blinding noted
10	Draw up AC-form	Planner	Moment values for flange assembly, type of seal and relevant tool info included in the AC-form	AC-form not drawn up Wrong seal type specified, Wrong pump pressure specified, Wrong moment specified
11	Identify and mark common barriers		Common barriers should be marked with ref. to V&B- package and be identified with orange rectangular labels	Common barriers not marked

12	Control and sign V&B package	Area-/ operator manager	Independent QA on the plan with the Operations and maintenance (O&M) operator	(Quality Assurance) QA not performed, Fault in V&B package not identified
13	Draw up Work Permit (WP), level 1	Planner	WP must be at level 1	WP not drawn up, Inadequate WP
14	Pre-approval of WP	Area-/operations manager, 1st manager, Platform manager	WP at level 1 must be approved by: Manger (on-shore) and area manager or the person in place of the area manager. The WP must be treated at the on-shore daily meeting before coordination of WP and other simultaneous activities	WP not pre-approved
15	Coordinating with (Central Control Room) CCR and other activities	Area-/ operations manager, CCR		Inadequate coordination, No coordination

Preparing equipment/system

16	Provide the necessary tools, etc.	Technician	The person responsible for the execution is also responsible for the provision of necessary equipment for splitting and assembly, lifting tools and jigs, tools for flange assembly and lubrication	Hydraulic tool not calibrated
----	-----------------------------------	------------	---	-------------------------------

17	Finds the correct seal	Technician	The person responsible for the execution must see too that the right seal is available	Chooses the wrong seal
18	Perform operation and maintenance preparation according to the WP	Area technician	Necessary operation and safety preparations must be done according to the WP and procedures	
19	Process shut down	CCR		
20	Isolate equipment using shutdown valves	CCR / Area technician	Isolate the equipment by closing the specified shutdown valves	Closes the wrong valves, Valve in wrong position
21	Pressure release to flare or other system	CCR	Reduce the pressure by ventilating to the flare	Opens the wrong valve
22	Drain fluid to closed system (including all low points and instrumental pipes)	Area technician	Drain fluid to closed system and drain all low points/inst. Pipes of oil/condensate too closed system and flush with N2 and/or steam	No draining, Inadequate draining, Contact with other HC systems (valve in wrong position/ opens wrong valve/ inadequate procedures)
23	Freeing gas	Area technician		No gas freeing, Inadequate gas freeing
24	Isolation with blindings	Area technician	Requirements for isolation: P<10 Barg: closed and locked, P> Barg: DB&B or blinding	

25	Lock/disconnect valves	Area technician, Instrument technician	Valves are locked where this is necessary	Valve not locked/disconnected, Inadequate locking
26	Disconnect pumps, heat cables etc.	Electro		El. equipment not disconnected, Wrong el. equipment disconnect
27	Label valves	Area technician	All unlabelled valves should be marked in the field. The need of labelling tagged valves in the field is evaluated by the operation system manager. All valves used for isolation shall be durable, clearly and unambiguously labeled	Valve not labelled, Wrong valve labelled
28	Label blindings	Area technician	All blindings affected in the field must be labelled. All blindings used for isolation shall be durable, clearly and unambiguously labeled	Blinding not labelled, Wrong blinding labelled
29	Label flanges to be split	Area technician, Technician	All flanges shall be labelled with WO nr and P&ID nr as a minimum	Flange not labelled, Wrong flange labelled

30	Sign WO form	Area technician		WO form not signed, WO form signed without the equipment being prepared WO form signed without the equipment being prepared
31	Draw up SJA	Area/ operation manager, Area Technician, CCR, Technician	Evaluate the need of a SJA	SJA not performed, Inadequate SJA, Inadequate involvement
32	Perform operation and maintenance preparations according to the WP	Technician	Technician must perform operations and safety preparations according to the WP and procedures	
33	Work place control and sign WP	Technician	Perform control and through sign confirm that orders will be/ are done	Shortcomings not found
34	Approve work location and sign work permit	Area technician	Control work permit	
35	Authorize WP (activate in SAP)	CCR	CCR evaluates if the work can be started in relations to ongoing activities. The authorization to start is given by activating the WP in SAP	

36	Before work call/ re-view WP	Area technician, Technician	Check that one is on the right equipment, System manager must control draining and that the system is pressure free, Approved WP must be in the work location and a review of this must be done with the personnel involved before the work is started.	
37	Handover between shifts		Requirements in relation to shift change. Communication and coordination meeting held and important decisions documented. Review of planned and on-going activities performed. Ensure that the new shift gets all information on status	Inadequate communication
38	Disconnect safety system	Area technician, CCR	Disconnection of safety system and disconnection/ locking of electric equipment must be registered on the WP form or isolation document	Safety system not disconnected
39	Sign splice log			Splice log not signed

40	Keep V&B-list in central space		Updated V&Bs are kept in central place of the plant. Changes in status in V&B are continuously reported in the V&B	
41	Control of spark and ignition sources			Inadequate control of spark and ignition sources

Conduction of maintenance

42	Control that the flange is the one in question, and that the system is emptied of HC	Area technician, Technician	Operational system manager and technician should ensure that WO is approved, the flange in question is the correct one, that isolation/binding is performed correctly and that there is no pressure or HC left in the system etc.	
43	Disassembly of flanges	Technician		Work done on wrong system, The system opened still contains pressure
44	Supervision of opening flanges	Area technician	Area tec. should be present when splitting of HC systems is performed. Work in adjacent areas should be stopped.	
45	Sign AC-form	Technician	AC-form signed	

46	Venting tank	Production technician		Inadequate venting, No venting
47	Gas measurement	Area technician		
48	Control of flanges, seal surfaces and tracks.	Technician	Flanges, seal surfaces and tracks are controlled for injuries, corrosion and wear. Control that bolts and nuts are the right material and tagged according to specifications	Damages not discovered on flanges, seal surfaces or tracks.
49	Work performed according to WO	Technician		Work not performed according to WO, Wrong operation of valves
50	Sign form for "work performed"	Technician	If the tank or drum has been opened, the form "internal inspection" must be filled out and approved before the tank is closed.	
51	Control seal, bolts and tracks	Technician	Control that the right type of seal is used and the quality of the material	Wrong seal not discovered, Damages on bolts and tracks not discovered

52	Assembly of flanges	Technician	Skills required: - 3 day course in flange assembly, - Experience with supervision, - > 1 yr since the last course, if its more than 1 yr since the last course, an E-course may be taken	Flange not assembled, Preload to low, Preload to high, Askew assembly, Bolts not locked, Missing seal in flange, Wrong seal in flange, Damage on seal in flange, Inadequate or wrong lubrication of metal gasket
53	Label assembled flanges	Technician	Old labelling is removed and replaced by a new tag on the flange connection with the WO nr. Moment, date, name and sign.	Flange not labelled, Flange wrong labelled
54	Fill inn AC form	Technician	The person responsible for the assembly should fill inn and sign the AC form continuously as the flanges are assembled.	AC form not filled out, AC form inadequately filled out.
55	AC-form saved for a week at minimum.	CCR	The AC-form must be saved for at least a week after the system is in operation	
56	Clean work area	Technician		

57	Sign form “check out before returning equipment after completed work”		The responsible person should fill in the form	Form not filled in, Form wrongly filled in
58	Perform final inspection, sign WP	Technician	Technician should perform a final inspection in the work place and by signing this confirm that the workplace is cleaned and secure	Wrong assembly not discovered
59	Connect safety system	CCR, Area technician	CCR should perform a reconnection with disconnected safety functions where this is relevant and register this in the WP form	Safety system not connected
60	Sign splice log	CCR		Splice log not signed

Resetting system and production start up

61	Removes blindings	Technician		Forgets to move blindings
62	Resetting valves	Area technician		Valves not reset
63	Removes labelling on valves and blindings	Area technician	All labels in the field should be removed	Labels not removed
64	O ₂ -freeing	Area technician	O ₂ must be removed to achieve inert atmosphere before tank or equipment is ready for start up, N ₂ used as flushing gas	O ₂ not removed, Wrong valve operated

65	Leak test performed	Area technician, CCR	Leak testing should always be performed according to approved specifications/ procedures	Leak test not performed, Wrong assembly not discovered in leak test (ex. Wrong seal used)
66	Connect hoses	Area technician	Requirements to standard couplings, labelling, inspection, pressure testing	Use of un approved hoses, Hose not correctly connected
67	Reset valves	Area technician		Valves not reset
68	Disconnect hoses	Area technician		Hoses not disconnected
69	Log possible leakages	CCR	All leakages during	Leakages not logged
	in relation to the leak test		testing should be logged in a separate system	
70	Unlock border valves	Area technician, Instrument technician		Valves unlocked before system is cleared, Valve in wrong position, Transmitters not calibrated
72	Connect pumps, heat exchangers etc.	Electrician		Electric equipment not connected
73	Open border valves			Border valves not opened
74	Remove labels on border valves		Labels must be removed	Labels not removed, Labels removed without valve being opened

75	Perform final control	Area technician	The area technician should perform the final control on the work place after the work is done. By signing he/she confirms that the work place is acceptable, in addition to the tagging, locks and equipment being removed and is ready for operation	Final control not performed, Inadequacy not discovered
76	Authorize work, sign WP, complete SAP	CCR	CCR will by signing, confirm the completion of the work is authorized by the CCR	Work authorized without being completed, Work completed without being authorized
77	Debriefing			Debriefing not performed
78	Start-up of normal production	Area technician, CCR		Start-up not according to procedures.

Appendix C

Comparison of Proposed Barrier Definitions and Classification

This appendix contains the description of the events and work descriptions used in the cases in Chapter 4 with the addition of the new proposed barrier definition also is applied.

C.1 Case A

Table C.1 lists the work process in a maintenance operation, from the BORA research project. The list of operation is based on Halseth (2012). The results of the case is commented on in Chapter 5.2.2.

Table C.1: Procedures related to maintenance operation, based on BORA.

	Work description	Sklet Classification	ARAMIS Classification	PSA Definitions	Hollnagel Definitions	New proposed classification
Planning						
1	Receives Work Order (WO)			Performance Influencing Factor		
2	Draw up work description			Performance Influencing Factor		Influencing Factor (quality of work description)
3	Requisite re-sources, materials etc. after need			Performance Influencing Factor		
4	Draw up plan for shutdown/start-up			Performance Influencing Factor		Influencing Factor (Quality of plan)
5	Draw up valves and blindings -package (V&B)			Performance Influencing Factor		Influencing Factor (accuracy og V&B package)
6	Split point marked in the P&ID			Performance Influencing Factor		Influencing Factor (accuracy of marking)

7	Draw up V&B list				Performance Influencing Factor			
8	Valve position marked in P&ID				Performance Influencing Factor		Influencing Factor (quality of markings)	
9	Mark blindings on P&ID				Performance Influencing Factor		Influencing Factor	
10	Draw up AC-form				Performance Influencing Factor			
11	Identify and mark common barriers				Performance Influencing Factor	Symbolic Barrier?	Influencing factor (quality of id and marking)	
12	Control and sign V&B package	Active Human & Operational			Performance Influencing Factor		Influencing factor	
13	Draw up Work Permit (WP), level 1				Performance Influencing Factor		Influencing factor (Quality of WP)	
14	Pre-approval of WP	Active Human & Operational			Performance Influencing Factor			

	Coordinating with (Central Control Room) CCR and other activities	Active Human & Operational		Performance Influencing Factor		Influencing factor (organizational cooperation)
15						
Preparing equipment/system						
16	Provide the necessary tools, etc.			Performance Influencing Factor		
17	Finds the correct seal					
18	Perform operation and maintenance preparation according to the WP			Barrier Element		Influencing Factor
19	Process shut down	Active Human & Operational	Activated Procedural	Barrier Element	Functional Barrier	Barrier Function Take Action (Performed by Operator or CCR)
20	Isolate equipment using shutdown valves	Active Human & Operational	Activated Procedural	Barrier Element	Functional Barrier	Confine - Physical, Take Action Human
21	Pressure release to flare or other system	Active Human & Operational	Activated Procedural/ Activated Assisted	Barrier Element	Functional Barrier	Barrier Function, Human and Technical Barrier Elements

22	Drain fluid to closed system (including all low points and instrumental pipes)	Active Human & Operational	Activated Procedural	Barrier Element		Barrier Function, Take action Human and Technical Barrier elements
23	Freeing gas	Active Human & Operational	Activated Procedural	Barrier Element		Barrier Function, Take action Human and Technical Barrier elements
24	Isolation with blindings	Active Human & Operational + Passive Physical	Temporary - Passive	Barrier Element	Physical Barrier	Barrier Function, Take action Human and Technical Barrier elements
25	Lock/disconnect valves	Active Human & Operational + Passive Physical	Temporary - Passive	Barrier Element	Functional Barrier	Barrier Function, Take action Human and Technical Barrier elements
26	Disconnect pumps, heat cables etc.	Active Human & Operational + Passive Physical	Temporary - Passive	Barrier Element	Functional Barrier	Barrier Function, Take action Human and Technical Barrier elements

27	Label valves	Active Human & Operational	Activated Warned			Symbolic Barrier	Barrier Function Technical/Physical and Human Barrier Element
28	Label blindings	Active Human & Operational	Activated Warned			Symbolic Barrier	Barrier Function Technical/Physical and Human Barrier Element
29	Label flanges to be split	Active Human & Operational	Activated Warned			Symbolic Barrier	Influencing Factor
30	Sign WO form	Active Human & Operational					Influencing factors
31	Draw up SJA	Active Human & Operational		Barrier Element		Incorporeal barrier	Influencing Factor
32	Perform operation and maintenance preparations according to the WP					Incorporeal barrier	Influencing Factors (Quality of work, quality of WP)
33	Work place control and sign WP	Active Human & Operational					Influencing Factor
34	Approve work location and sign work permit	Active Human & Operational					Influencing Factor

35	Authorize WP (activate in SAP)	Active Human & Operational					Influencing Factor
36	Before work call/ review WP	Active Human & Operational					Influencing Factor
37	Handover between shifts						Influencing Factor
38	Disconnect safety system	Active Human & Operational	Temporary - Passive	Barrier Element	Functional Barrier	Barrier Function, Technical and Human Barrier elements	
39	Sign splice log	Active Human & Operational		Barrier Element	Functional Barrier	Influencing Factor	
40	Keep V&B-list in central space						Influencing Factor
41	Control of spark and ignition sources	Active Human & Operational		Barrier Element		Barrier Function, Detect and/or Take action Human Barrier element	

Conduction of maintenance

42	Control that the flange is the one in question, and that the system is emptied of HC	Active Human & Operational		Performance Influencing Factor	Incorporeal Barrier	Barrier function, Detect Human and/or sensor
43	Disassembly of flanges				Incorporeal barrier	
44	Supervision of opening flanges	Active Human & Operational				Influencing factor
45	Sign AC-form					Influencing Factor
46	Venting tank		Activated Precedural	Barrier Element		Barrier Function Take Action Technical and Human Barrier Element
47	Gas measurement			Barrier Element		Barrier Function - Monitor / Detect, Human and/or Technical
48	Control of flanges, seal surfaces and tracks.	Active Human & Operational		Barrier Element	Incorporeal barrier	Barrier Function Detect, Human Barrier Element

49	Work performed according to WO							
50	Sign form for “work performed”	Active Human & Operational						Barrier Function Defect, Human Barrier Element
51	Control seal, bolts and tracks	Active Human & Operational		Barrier Elements				
52	Assembly of flanges							
53	Label assembled flanges	Active Human & Operational	Activated Warned			Symbolic Barrier		Influencing Factor
54	Fill inn AC form							
55	AC-form saved for a week at minimum.	Active Human & Operational						Influencing Factor
56	Clean work area							Influencing Factor (Local work environment)
57	Sign form “check out before returning equipment after completed work”	Active Human & Operational						Influencing Factor

58	Perform final inspection, sign WP	Active Human & Operational				Barrier Function - Detect, Human Barrier element
59	Connect safety system	Active Human & Operational	Activated Processual/ Activated Assisted		Functional Barrier	Technical barrier elements
60	Sign splice log	Active Human & Operational				Influencing Factor

Resetting system and production start up

61	Removes blindings	Active Human & Operational	Activated Processual			
62	Resetting valves	Active Human & Operational	Activated Processual			
63	Removes labeling on valves and blindings	Active Human & Operational				Influencing Factor
64	O2-freeing					Act - Human & Technical

65	Leak test performed	Active Human & Operational				Barrier function - De- tect/ Monitor - Techni- cal and Human Barrier Elements
66	Connect hoses	Active Human & Operational	Activated Proce- dural	Barrier Element		Barrier Function - Technical barrier element
67	Reset valves	Active Human & Operational	Activated Proce- dural	Barrier Element		Barrier Function Acti- vate Technical and Hu- man
68	Disconnect hoses	Active Human & Operational	Activated Proce- dural			
69	Log possible leakages in relation to the leak test	Active Human & Operational				
70	Unlock border valves					
72	Connect pumps, heat exchangers etc.	Active Human & Operational + Active Technical		Barrier Element		Technical Barrier Ele- ments
73	Open border valves					

74	Remove labels on border valves							
75	Perform final control	Active Human & Operational						Barrier Function De-tect, Human
76	Authorize work, sign WP, complete SAP							
77	Debriefing							
78	Start-up of normal production			Activated Procedural				

C.2 Case B

Table C.2 shows the elements related to kick detection used in Case B, in Chapter 5, where the proposed elements are based on a description of kick detection barriers by Hauge et al. (2012) in the SINTEF report 'Barriers to prevent and limit acute releases to sea | Environmental barrier indicators', and Chief Counsel's Report (Bartlit et al., 2011) description of kick detection, regarding the Macondo accident.

Table C.2: Description of kick detection operational elements

Element description	Sklet classification	ARAMIS Classification	PSA classification	Hollnagel classification	New proposed definition/ classification
Pit gain	Active Technical		Barrier Element	Incorporeal barrier system	Barrier Function Monitor - Technical, Detect and decide - Human Barrier elements
Flow out measurement	Active Technical	Activated warned	Barrier Element	Functional barrier system	Barrier Function Monitor - Technical Barrier element
Flow in measurement	Active Technical	Activated warned	Barrier Element	Functional barrier system	Barrier Function Monitor, Technical Barrier Element
Flow in/out comparison	Active Human & Operational	Activated warned / assisted	Barrier Element	Incorporeal barrier system	Barrier Function Detect and Decide - Human Barrier Element
Operator knowledge			Performance influencing factor	Incorporeal barrier system	Influencing Factor

Visual inspection of flow line (video)	Active Human & Operational		Barrier Element	Incorporeal barrier system	Barrier Function Delect - Human Barrier Element
Mudlogging	Active Technical		Barrier Element	Incorporeal barrier system	Barrier Function Delect - Human
Drill pipe pressure measurement	Active Technical	Activated warned	Barrier Element	Incorporeal barrier system	Barrier Function - Delect Technical
Gas content measurement	Active Technical	Activated warned	Barrier Element	Incorporeal barrier system	Barrier Functions - Monitor Technical & Decide, Human Barrier elements
Overboard valve	Active Technical	Activated Hardware on demand	Barrier Element	Functional barrier	Barrier Function Activate - Technical, Barrier Function Delect Human Barrier Element
Drilling operation					
Drilling supervision	Active Human & Operational		Barrier Element	Incorporeal barrier system	Influencing Factor
Emergency response manual			Barrier Element	Incorporeal barrier system	Influencing Factor

Driller Training			Performance Influencing Factor		Influencing Factor
Emergency disconnect system (ESD)	Active Technical	Activated - manual / automated / emergency	Barrier element	Functional Barrier	Barrier Function, De-activate and Take Action - Human and/or Activate Technical Barrier Elements
BOP blind shear ram	Active Technical (/ Barrier System)	Activated - manual / automated / emergency	Barrier Element / Barrier	Functional Barrier	Barrier Functions, De-activate and Take Action - Human and/or Activate Technical Barrier Elements

C.3 Case C

Table C.3 is the basis of Case C, presented in Chapter 4. Case C is based on a leak scenario, and the information that is used to construct the elements of the case is based on the elements in NORSOK standard S-001 (NORSOK standards, 2008), and based on the leak scenario described in the paper *'Risk assessment in the offshore industry'* by Brandsæter (2002)

Table C.3: Description of elements in the leak scenario with different barrier classifications

Element description	Sklet classification	ARAMIS Classification	PSA classification	Hollnagel classification	New proposed definition/ classification
Isolation of HC gas	Passive Physical	Permanent Passive	Barrier Element	Physical Barrier system	Barrier Function Component - Physical or Technical Barrier Element
Detection of HC gas in leak area (Sensor)	Active - Technical	Activated - Automated	Barrier Element	(Functional Barrier System)	Barrier Function Element - Technical Barrier Element
Detection of HC gas in leak area (Human)		Activated Procedural	Barrier Element	Incorporeal Barrier System	Barrier Function Element - Human Barrier element
Detection of fire in leak area (Sensor)	Active - Technical	Activated - Automated	Barrier Element	(Functional Barrier System)	Barrier Function Element - Technical Barrier Element
Detection of fire in leak area (Human)		Activated Procedural	Barrier Element	Incorporeal Barrier System	Barrier Function Element - Human Barrier element

Detection of fire in other area (Sensor)	Active - Technical	Activated - Automated	Barrier Element	(Functional Barrier System)	Barrier Function De- tect - Technical Barrier Element
Detection of fire in other area (Human)		Activated Procedural	Barrier Element	Incorporeal Barrier System	Barrier Function De- tect - Human Barrier Element
HC to flare/ vent	Active Technical	Activated - Automated	Barrier Element	(Functional Barrier System)	Barrier Function Activate - Technical and/or Human
Ventilation of leak area (evacuate gas or seal off)	Passive Physical / Active Technical	Permanent Active	Barrier Element	(Functional Barrier System)	Barrier Function Take Action and/ or Activate - Technical Barrier Element
Separation of leak area (seal of area for humans)	Passive Physical / Active Technical / Passive Human	Activated Emergency	Barrier Element	Physical Barrier System	Barrier Function Con- fine, Physical and/or Technical
Alarm activated (Technical)	Active Technical	Activated - automated	Barrier Element	Symbolic Barrier System	Assess& Barrier Function Activate - Technical Barrier Element

Alarm activated (Human)		Activated - manual	Barrier Element	Functional Barrier System	Assess & Barrier Function Activate - Human Barrier Function
Alarm activated (CCR)		Activated - assisted	Barrier Element	Functional Barrier System	Assess & Barrier Function Activate - Human Barrier Element
Activation of ESD (automatic)	Active Technical	Activated - automated	Barrier Element	(Functional Barrier system)	Barrier Function Activate - Technical Barrier Element, Barrier Function Confine - Physical Barrier Element
Activation of ESD (manual)		Activated manual	Barrier Element	Functional Barrier System	Barrier Function Activate - Human Barrier Element, Barrier Function Confine - Physical Barrier Element
Activation of ESD (CCR)	Active Technical	Activated assisted	Barrier Element	Functional Barrier System	Barrier Function Activate - Human Barrier Element, Barrier Function Confine - Physical Barrier Element

Activation of Firewater in leak area (Activator)	Active Technical	Activated automated	Barrier Element	(Functional Barrier System)	Barrier Function Activate - Technical Barrier Element
Activation of Firewater in leak area (Human)		Activated manual / emergency	Barrier Element	Functional Barrier System	Barrier Function Activate - Human Barrier Element, Barrier Function Confine - Physical Barrier Element
Activation of water curtains	Active Technical	Activated - hardware on demand	Barrier element	Functional Barrier System	Barrier Function Activate - Technical Barrier Element, Barrier Function Confine - Technical Barrier Element
Firewalls	Passive Physical	Permanent Passive barrier	Barrier Element	Physical Barrier System	Barrier Function Confine - Physical Barrier Element
Evacuation procedure	Active Human & Operational		Barrier Element	Incorporeal Barrier system	Influencing Factor
Evacuation	Passive Human & Operational	Activated emergency			Barrier Function Take Action - Human Barrier Elements

Bibliography

Bartlit, F. H., Sankar, S. N., Grimsley, S. C., Eaton, J. J., Harris, B. C., and adn Sarita K. Tice, J. I. M. (2011). Macondo | the gulf oil disaster. Technical report, Chief Counsel.

Brandsæter, A. (2002). Risk assessment in the offshore industry. *Safety Science*, 40:231–269.

CCPS (2010). Guidelines for safe and reliable instrumented protective systems. page 1 online resource (431 s.).

Gould, K. S., Ringstad, A. J., and van de Merwe, K. (2012). Human reliability analysis in major accident risk analyses in the norwegian petroleum industry. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 56(1):2016–2020.

Guttmann, H. E. and Swain, A. D. (1983). Handbook of human reliability analysis with emphasis on nuclear power plant applications - final report. Technical report nureg/cr-1278, Nuclear Regulatory Commission.

Halseth, I. K. (2012). Modeling process leaks using fram. Master's thesis, Norwegian University of Science and Technology.

H.Andersen, J.Casal, A.Dandrieux, Debray, B., Dianous, V., N.J.Duijm, C.Delvosalle, C.Fievez, L.Goossens, R.T.Gowland, A.J.Hale, D.Hourtolou, B.Mazzarotta, A.Pipar, E.Planas, FPrats, O.Salvi, and J.Tixier (2004). *ARAMIS User Guide*. European Commission.

Hauge, S., Håbrekke, S., Kråkenes, T., Lundteigen, M. A., and Merz, M. (2012). Barriers to prevent and limit acute releases to sea | environmental barrier indicators. Report, safety report, SINTEF Teknologi og samfunn.

- Hauge, S. and Onshus, T. . (2009). *Reliability data for safety instrumented systems: PDS data handbook*, volume SINTEF A13502. SINTEF, Trondheim.
- Hollnagel, E. (2004). *Barriers and accident prevention*. pages XVI, 226 s. : ill.
- Hollnagel, E. (2012). *FRAM: Modelling Complex Socio-technical Systems*. Ashgate Publishing Ltd, Farnham.
- INSAG (1999). *Basic Safety Principles for Nuclear Power Plants*. International Nuclear Safety Advisory Group, 1 edition.
- ISO (2002). *NS-EN ISO 17776:2000 standard for Petroleum and Natural Gas Industries | Offshore production installations | Guidelines on tools and techniques for hazard identification*. Standards Norway.
- ISO (2009). *Risk Management | Principles and Guidelines*. Standards Norway.
- Leveson, N. (2004). A new accident model for engineering safer systems. *Safety Science*, pages 237–270.
- Leveson, N. (2011). *Engineering a safer world : systems thinking applied to safety*. pages XX, 534 s. : ill.
- NEA (2004). *Human reliability analysis in probabilistic safety assessment for nuclear power plants*. CSNI Technical Opinion Papers 4, NUCLEAR ENERGY AGENCY.
- NEK-IEC (2003a). *NEK IEC 61511-1, Functional safety | Safety instrumented systems for the process industry sector | Part 1: Framework, definitions, system, hardware and software requirements*. International Electrotechnical Commission, 1 edition.
- NEK-IEC (2003b). *NEK IEC 61511-3, Functional safety | Safety instrumented systems for the process industry sector | Part 3: Guidance for the determination of the required safety integrity levels*. International Electrotechnical Commission, 1 edition.
- NEK-IEC (2010). *Functional safety of electrical/electronic/programmable electronic safety-related systems | Part 1: General requirements*. Norsk Elektronisk Komite, 2 edition.

- NORSOK standards (2008). *Technical safety*. Standards Norway, Strandveien 18, PO Box 242, N-1326 Lysaker, 4 edition.
- NORSOK standards (2012). *Drilling Facilities*. Standards Norway, Strandveien 18, PO Box 242, N-1326 Lysaker, 4 edition.
- PSA (2010a). Guidelines regarding the management regulations. <http://www.ptil.no/management/category406.html>.
- PSA (2010b). Regulations relating to management and the duty to provide information in the petroleum activities and at certain onshore facilities (the management regulations). <http://www.ptil.no/management/category401.html>.
- PSA (2012a). *Prinsipper for barrierestyring i petroleumsvirksomheten*. Petroleum Safety Authority.
- PSA (2012b). *Risikonivå i petroleumsvirksomheten*. Technical report, Norwegian Petroleum Safety Authority.
- PSA (2013). *Prinsipper for barrierestyring i petroleumsvirksomheten*. Petroleum Safety Authority, 2 edition.
- Rasmussen, J. (May-June 1983). Skills, rules, and knowledge; signals, signs, and symbols, and other distinctions in human performance models. *Systems, Man and Cybernetics, IEEE Transactions on*, SMC-13(3):257–266.
- Rausand, M. (cop. 2011). *Risk assessment: theory, methods, and applications*. Wiley, Hoboken, N.J.
- Rausand, M. and Høyland, A. (c2004). *System reliability theory: models, statistical methods, and applications*. Number 2nd ed. Wiley-Interscience, Hoboken, N.J.
- Reason, J. (1990). Human error. pages XV, 302 s. : ill.
- Reason, J. (1997). *Managing the risks of organizational accidents*.

- Reason, J. (2008). *The human contribution: unsafe acts, accidents and heroic recoveries*. Ashgate, Farnham.
- Schönbeck, M., Rausand, M., and Rouvroye, J. (2010). Human and organisational factors in the operational phase of safety instrumented systems: A new approach. *Safety Science*, 48(3):310–318.
- Sklet, S. (2005). *Safety Barriers on Oil and Gas Platforms | Means to Prevent Hydrocarbon Releases*. PhD thesis, NTNU.
- Sklet, S. (2006). Safety barriers: Definition, classification, and performance. *Journal of Loss Prevention in the Process Industries*, 19(5):494–506.
- Sklet, S., Ringstad, A. J., Steen, S. A., Tronstad, L., Haugen, S., and Seljelid, J. (2010). Monitoring of human and organizational factors influencing risk of major accidents. spe international conference on health, safety and environment in oil and gas exploration and production, rio de janeiro, brazil.
- Torgauten, A. O. A. (2012). Risk assessment. Project assignment, NTNU, S.P. Andersensvei 5.
- U.S. NRC (2005a). Good practices for implementing human reliability analysis | final report.
- U.S. NRC (2005b). *The SPAR-H Human Reliability Analysis Method*. U.S. Nuclear Regulatory Commission, Office of Nuclear Regulatory Research Washington, DC 20555-0001, nureg/cr-6883 edition.
- U.S. NRC (2006). *Evaluation of Human Reliability Analysis Methods Against Good Practices*. NUREG.
- van de Merwe, K., Øie, S., and Gould, K. (2012). The application of the spar-h method in managed-pressure drilling operations. In *Human Factors and Ergonomics Society 56th annual meeting*. Statoil and Det Norske Veritas.
- Vinnem, J. E., Bye, R., Gran, B. A., Kongsvik, T., Nyheim, O. M., Okstad, E. H., Seljelid, J., and Vatn, J. (2012). Risk modelling of maintenance work on major process equipment on offshore petroleum installations. *Journal of Loss Prevention in the Process Industries*, 25(2):274–292.

Curriculum Vitae



Arve Olaf Alvik Torgauten

Stadsing. Dahls Gate 9, 7015 Trondheim

Født: 24.02.1988

Sivilstatus: Ugift

Tlf: 905 966 22

E-post: arveolaf@stud.ntnu.no

Epost 2: arve@torgauten.com

UTDANNING

2008 – d.d.	Student ved 5-årig masterprogram for Produktutvikling og Produksjon: Studieretning: RAMS, Institutt for Produksjon- og Kvalitetsteknikk (IPK) Prosjektoppgave: Risk Assessment (Major Accident modeling)	NTNU - Trondheim
2004 – 2007	Videregående skole (Allmenne fag) Retning; Matematikk, Fysikk og Kjemi	Danielsen Videregående Skole - Bergen

RELEVANT ERFARING

Høst 2011	Institutt for Produksjon og Kvalitetsteknikk <i>Risikoanalyse av laboratorieutstyr ved instituttet. PHA/HAZID, FMECA, BOWTIE m.m.</i>	NTNU - Trondheim
-----------	---	---------------------

ANNEN ERFARING

Sommer 2010	Renholdsassistent ISS Renhold	Ålesund Sjukehus - Ålesund
2007-2008	Førstegangstjeneste Grensejeger ved Garnisonen i Sør-Varanger (GSV)	Høybuktknoen/ Svanvik grensestasjon – Sør-Varanger

VERV

08.2010 – **Ingeniører Uten Grenser NTNU,** NTNU
02.2012 **Styremedlem**
PR-ansvarlig. Web-ansvarlig.

09.2010 – **Ingeniører Uten Grenser Norge**
02.2011 **Medlem i vedtekts-utvalg**

SPRÅK

- **Engelsk:** Muntlig; meget god, Skriftlig; god
- **Tysk:** Grunnleggende muntlig og skriftlig

IT-KUNNSKAPER

Generell god IT-kunnskap

- **Excel,** god kunnskap
- **Visual Basic,** noe kunnskap
- **LaTeX,** god kunnskap
- **Matlab,** grunnleggende kunnskap
- **Maple,** grunnleggende kunnskap
- **Javascript, HTML, CSS**

