University of
Stavanger

Faculty of Science and Technology

MASTER'S THESIS

Study program/ Specialization:

Master in Risk Management / Offshore Safety

Spring semester, 2013

Open / ~~Restricted access~~

Writer:

Igor Eliassen

…………………………………………
(Writer's signature)

Faculty supervisor: Eirik Bjorheim Abrahamsen (University of Stavanger)

External supervisor(s): Stig Berg (Odfjell Drilling and Technology)

Title of thesis:

Management of change - with the main focus on Safety Instrumented Systems

Credits (ECTS): 30 SP

Key words:

Safety Instrumented Systems
Safety Instrumented Functions
Probability of Failure on Demand
Modifications
Management of Change
MoC procedure

Pages: 86

+ enclosure: 18

Stavanger, 14.06.2013

Preface

This thesis was written at the Department of industrial economics, risk management and planning at University of Stavanger (UiS). This master thesis represents the final work of my master degree in Risk Management - Offshore Safety at the UiS

This thesis treats the topic of “Management of change – with the main focus on Safety instrumented systems” and was written in collaboration with Odfjell Drilling and Technology (OD&T). This thesis is based on literature study and discussions with my supervisors.

I want to thank my supervisor at UiS, Professor Eirik Bjorheim Abrahamsen, for advices, guidance and constructive feedback throughout this thesis. I would also like to thank my other supervisor at OD&T, Stig Berg, for providing me with this topic and taking the time to provide explanations and discuss the problems along the way. In addition, I would like to thank Bjarne S. Jakobsen for feedback and discussion throughout this thesis.

Stavanger, June 2013

Igor Eliassen

Abstract

Safety instrumented systems (SISs) are implemented in the oil and gas industry to detect the onset of hazardous events, and/or to mitigate their consequences. As with any system, for different reasons, modifications are necessary. If the modification is poorly executed, or if the risk is poorly understood, the modification may have undesired consequences.

The main objective of this master thesis was to identify potential pitfalls that may result from poor change management of modifications, and propose recommendations on how to handle these pitfalls. In addition to the main objective, two sub-objectives were supplemented to contribute to discussion and recommendations for the main objective.

For the first sub-objective, a case was presented. The main purpose of this case was to illustrate how different modifications might affect the calculated PFD, and if the calculated values are sufficient to express the extent of the modification. As it became apparent in the discussion chapter, one cannot rely solely on the calculated PFD value. These values can provide useful insight for the decision maker; however, it is important to look beyond the assigned probabilities, since the probabilities may camouflage uncertainties. The circumstances should always be assessed in addition to the calculated PFD.

The second sub-objective was to propose a simple alternative approach on how to classify the modifications to SIS in modification project. The main findings suggest that there is a need for an alternative description on what should be considered as minor and major modifications in SIS modification projects. This thesis proposes an alternative way of categorizing modifications, where four categories are used to express the safety significance of the modification. To aid in the categorization, a checklist consisting of several conditions (questions) is presented. The main purpose of this checklist is to provide an overview of the impact the proposed modification has on the system, and the risk level before the categorization.

To cover the latent functional relationships, failure modes and impacts of modifications, the modification process should be well structured and documented. Several risk and safety assessments should be included as early as possible to ensure that potential problems are identified, and appropriate measures implemented as early as possible. This thesis proposes a management of change procedure in form of a flowchart. This flowchart is based on the identified issues and the requirements in the ISO-9001 standard. The main purpose of the proposed procedure is to ensure that the modifications to SIS, or any other part of the facility are under control, and that the safety is not compromised. Furthermore, the procedure aids in providing traceability during, and after the modification process.

Table of Contents

List of Figures

List of Tables

1. Introduction

Safety instrumented systems (SIS) are widely used for controlling and mitigating risk in many sectors of society. Numerous safety systems are implemented in the oil and gas industry and they are used to detect the onset of hazardous events and/or to mitigate their consequences to humans, material assets, and the environment (Lundteigen, 2009). These types of systems are often implemented to reduce the risk to an acceptable level. The amount of risk reduction depends on the reliability level of the SIS, where safety integrity level (SIL) is used to describe the reliability of different safety functions.

During the lifetime of an offshore facility, changes will be introduced to respond and adapt to varying conditions. Manufacturers aim to improve their components/parts (introducing new technology), the owners try to improve the efficiency of their process and to make it easier to operate and to improve the safety of the installation (NEA, 2005). In addition, the need for change may arise from external parts, such as regulatory bodies.

1.1. Background

According to a study conducted by HSE executive – UK, the main cause of 20 % of the accidents are caused by control and safety systems were to changes made to the system after the system was put into service. Their findings illustrate that if a change is technically inappropriate, poorly executed or its risk is poorly understood the change may have undesired consequences and may lead to accidents (American Berau of Shipping, 2013). A formal and effective change management approach is therefore needed to prevent such consequences. To ensure that the system will not be affected by the modification, the IEC 61508 and 61511standards include a phase on modification in their life cycles. The SIS modification phase addresses the necessary analyses of the modification, with emphasize on an impact analysis. After the impact analysis, one returns back to an appropriate phase in the life cycle for the implementation, thereafter, all subsequent phases have to be performed again.

The benefits of the modifications can be jeopardized if modifications are not subject to a structured change management approach throughout the lifetime of the facility. In practice, especially for older offshore facilities that do not practice a SIL-regime (do not comply with the IEC standards), such structured approach is often neglected or not existing. If the impact of the modification is not properly considered or understood, the ability of the SIS to perform its intended functions may be affected.

1.2. Objectives

1.2.1. Main Objective

Since an offshore module operates in a dynamic world it is subject to continuous change. Changes are often made in process equipment to increase the productivity or to reduce the risk level by modifying safety barriers. Systems that initiate automatic actions on demand are often complex, and are thus vulnerable to modifications. If a thorough change management process does not exist, or is not good enough to capture the mains issues, these changes may have a significant impact on the system and/or the working personnel. The main objective of this thesis is to:

> Identify potential pitfalls that may result from poor change management of SISs, and propose a procedure that can be used to handle these issues in SIS modification projects.

Based on literature study, typical pitfall and best practice in management of change will be presented. This information will be used as the basis for the proposed management of change procedure. It is further important to find out if a formal change management approach should apply for every single modification or not?

In addition to the main objective, two sub-objectives are presented. These sub-objectives are a part of the main objective, and their main purpose is to contribute to the discussion and recommendations to the main objective.

1.2.2. Sub-objective 1

The first sub-objective is to:

> Illustrate how typical modifications may affect the calculated reliability level (PFD) for safety instrumented functions (SIFs), and if the calculated values are sufficient to express the extent of the modification.

To illustrate how different modifications might affect the calculated PFD, a case regarding a F&G-system on an offshore facility will be presented. The purpose of this case is to provide a better understanding of:

- Safety instrumented systems (SISs) and their functions (SIFs)
- How the reliability (PFD) is calculated.
- How the system can be modified.
- How much a typical modification might affect the reliability (PFD).

To provide an adequate answer to the other part of the objective, the information from the literature study and the case will be used as an input to the discussion chapter.

1.2.3. Sub-objective 2

In the oil & gas industry, modification projects may range from a simple modification, where a component is replaced with a similar one, to major modification projects, where for instance large parts of the technical system are rebuilt. It is important to divide the modification intro discrete categories to determine the level of necessary planning and administration, and how the resources should be allocated,

The next sub-objective is to:

> Propose a simple alternative approach on how to classify the modifications in a typical SIS modification project.

To provide an adequate solution, a literature study will be conducted.

1.3. Limitation

- In general, the IEC 61508 and OLF 070 state that three main types of requirements need to be fulfilled in order to achieve a given SIL. These three types are: quantitative, semi-quantitative and qualitative requirements. All three types will be presented; however, the focus during the thesis will mainly be on the quantitative requirements (PFD).
- Human and organizational factors in modification projects are not a part of this thesis.

- The main focus of this thesis is:
  - On the modifications to the hardware part. Discussion about modification to the software part of SISs is not a part of this thesis.
  - On management of change in modification projects.
  - The earlier phases of a modification, from identifying the need for a modification to the design phase.
- Limitations of the case
  - The constructed reliability block diagram is a simplified representation of the real system. Only the components that were presented in the functional description documents for the system were used. Including every single component and cables in the reliability calculation will lead to an increase in the SIFs PFD.
  - Approximate formulas that are presented in PDS-handbook will be used to calculate PFD.

1.4. Thesis Structure

This thesis consists of 10 chapters, including the reference list and an appendix chapter.

Chapter 1 presents the background information, objectives, limitations, definitions and abbreviations. Chapter 2 presents important theoretical background, necessary to understand the case, with main focus on elements such as risk, uncertainty and safety instrumented systems. Chapter 3 contains a short introduction to important standards for SIS: IEC 61508, 615011 and OLF-070. Chapter 4 focuses on the modifications to SIS, the requirements for modifications and a short presentation of the management of change procedure. Chapter 5 presents general background information for the F&G system, followed by the presentation of typical F&G functions (based on OLF-070). The system considered in the case study will be illustrated and the SIFs for the case will be presented. The selection of data source, model, calculation approach and classification of modifications is explained. The case concerning the modifications is then conducted to study how different modifications will affect the calculated PFD. The main focus in Chapter 6 is to provide a discussion around the objectives for this this thesis. Chapter 7 contains recommendations related to the objectives and chapter. Chapter 8 presents closing comments to the objectives stated in chapter 1.2.

Most of these chapters will contain a summary at the end.

1.5. Abbreviation and definitions

ALARP	As Low As Reasonably Practicable
C&E	Cause and Effect
E/E/PE	Electrical, electronic, or programmable electronic
EUC	Equipment Under Control
F&G	Fire & Gas
HVAC	Heating, Ventilation, and Air Conditioning
IEC	International Electrotechnical Committee
ISO	International Organization for Standardization
I/O	Input/output
NORSOK	Competitive position for the Norwegian continental shelf
OLF	The Norwegian Oil Industry Association
OREDA	Offshore Reliability Data
PFD	Probability of Failure on Demand (average)
PSA	Petroleum Safety Authority in Norway
QRA	Quantitative Risk Assessment
RBD	Reliability Block Diagram
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SRS	Safety Requirement Specification

2. Theory

This chapter presents important concepts related to safety instrumented systems, risk and uncertainty. The theoretical basis presented in this chapter will form the basis for the case and the discussion chapter.

2.1. Barriers

The Petroleum Safety Authority Norway (PSA) is the regulatory authority for safety in the petroleum sector on the Norwegian continental shelf. They have developed a set of regulations and guidelines to govern all petroleum activities, which offshore and onshore oil and gas installations in Norway must adhere to. PSA state that the harm or danger to people, the environment or material assets shall be prevented or limited and the risk shall be reduced to a level as low as reasonably practicable. Based on PSA's regulations, the responsible party shall select technical, operational and organizational solutions to reduce the probability that harm, errors/hazard and accident situations occur. Furthermore, safety barriers shall be established to:

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

2.1.1. Definition of safety barriers

According to Sklet (2006), it is recommended to distinguish between; safety barriers, barrier elements, barrier functions and barrier systems. He proposes the following definitions of these terms.

"Safety barriers are physical and/or non-physical means planned to prevent, control, or mitigate undesired events or accidents"(Sklet, 2006).

In this definition a physical safety barrier (e.g. fire-walls, fire doors, fences, drain) are continuously functioning and are often implemented in the design. Non-physical barriers are often referred to as organizational barriers. These barriers are often in form of procedures, risk assessments, safety culture, training and so on.

"A barrier function is a function planned to prevent, control or mitigate undesired events or accidents" (Sklet, 2006).

Barrier functions describe their purpose and the tasks of the safety barriers. Different barriers have different roles, some barriers main role is to prevent that the unwanted events escalate to accidents, while others is to control, or mitigate these events or accidents.

"A barrier system is a system that has been designed and implemented to perform one or more barrier functions." (Sklet, 2006).

A barrier system describes how a barrier function is realized or executed. Such a system may have several functions, and in some cases there may be several systems that carry out a barrier function. A barrier system may be passive or active, and may consist of physical and technical elements (hardware and software), operational activities executed by humans, or a combination thereof (Sklet, 2006).

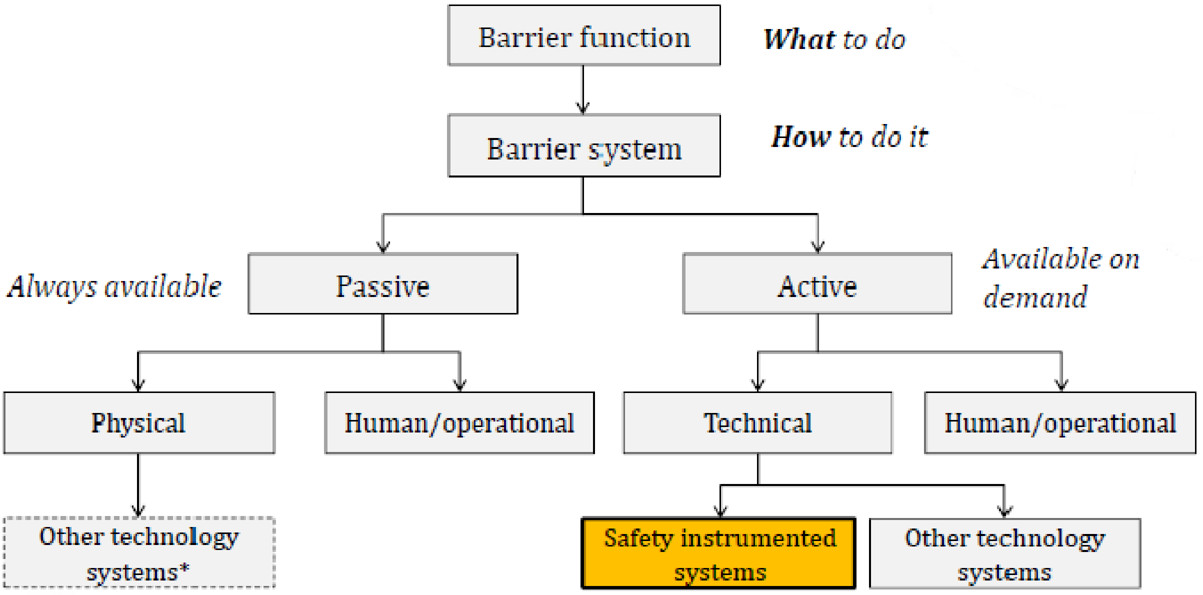


Figure 1: Barrier classification based on Sklet (2006) (Lundteigen, 2011)

Figure 1 is a based on recommendation by Sklet (2006) on how to classify barrier systems. The only difference is that 'other technology systems' are seen as passive-physical barriers and not as active-technical. In this classification, SISs are seen as active barriers that are activated on demand, meaning they perform their required functions in response to certain events.

2.2. Risk reduction

Absolute safety without risk cannot be achieved; however, the risk can be reduced to an acceptable level by implementing the ALARP principle. This means that the risk should be reduced to a level that is as low as reasonably practicable. This reduction is achieved by the implementation of various safety-related systems. These different systems provide safety barriers, also called protection layers, which are independent of each other, meaning that failure in one layer does not lead to failure in others.

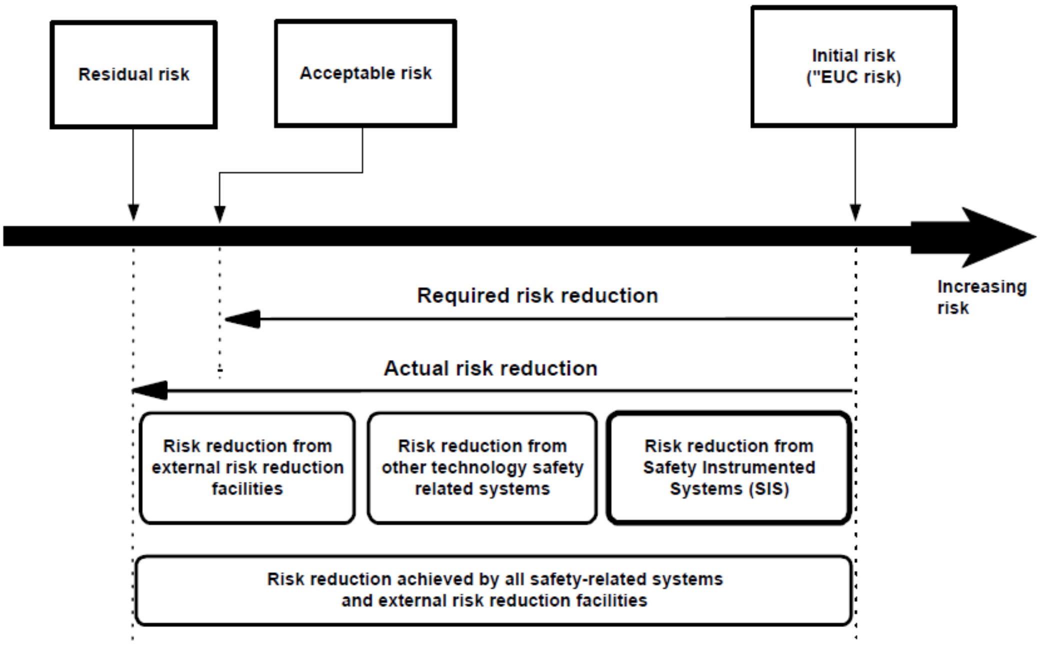

Residual risk
Acceptable risk
Initial risk ("EUC risk)
Increasing risk
Required risk reduction
Actual risk reduction
Risk reduction from external risk reduction facilities
Risk reduction from other technology safety related systems
Risk reduction from Safety Instrumented Systems (SIS)
Risk reduction achieved by all safety-related systems and external risk reduction facilities

Figure 2: Framework for risk reduction (OLF-070, 2004)

Most process facilities contains a lot of different equipment, each contributing to the inherent risk, also called the initial risk. It represents the risk that exists because of the nature of the process, the inherent material and equipment.

As seen in the framework in Figure 2, the amount of risk reduction needed is dependent on the equipment under control (EUC). Based on the IEC 61508 definitions, the EUC could be a piece of equipment, machinery, part of an offshore installation, or even the entire installation. The EUC is then considered as the source of hazard and hence shall be protected (OLF-070, 2004). It is considered as the initial risk of the system without any safety measures, and is often determined by historical data, expert judgments, and /or reliability analysis.

Acceptable risk is a criteria set by authorities, company requirements or by the stakeholders during the risk analysis. This criterion is often represented as a numerical statement or as a quantity which expresses the level of risk that is acceptable. EUC risk is then compared with the acceptable risk to find the required/necessary risk reduction. This risk reduction can be achieved by either external risk reduction facilities, other technology safety related systems, safety instrumented systems, or as combination of these systems.

Achieved risk reduction by other safety related measures and systems are compared against acceptable risk and a residual risk is found. If the residual risk is seen as unacceptably high, a risk reduction factor (RRF) is determined. This factor expresses by how much the risk should be reduced. The risk is then allocated to the SIS and the associated safety instrumented functions (SIFs), where the reliability target of the functions is expressed as SIL. Higher RRF yields higher SIL. Figure 3 illustrates how different barriers influence the risk reduction.

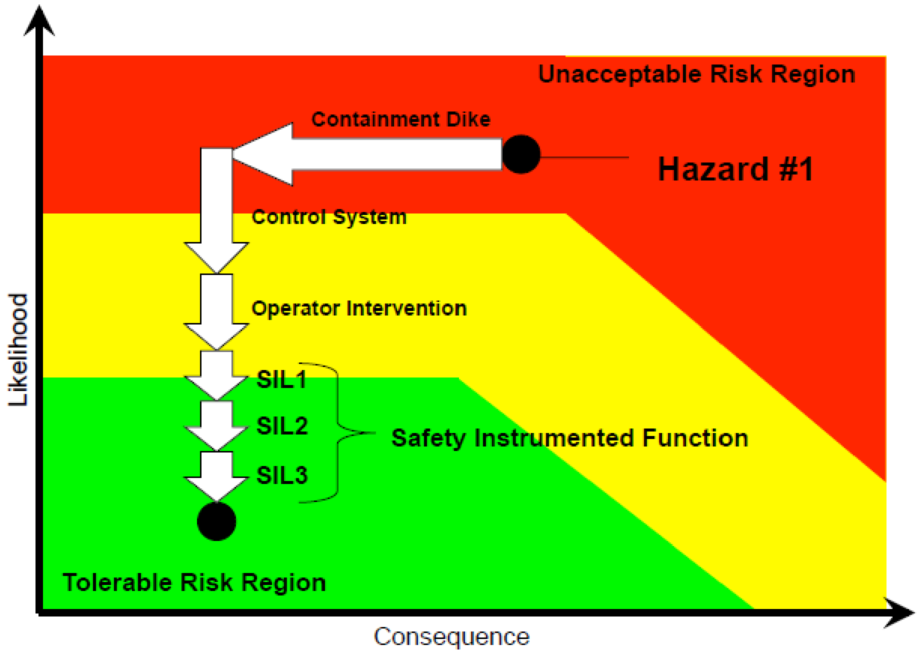


Figure 3: Risk reduction achieved by SIS (Sveen, 2012)

As seen from the figure, the risk reduction achieved by SIS is lower than the risk reduction achieved by other means. However, it is the risk reduction that ensures that the risk exposure is within the tolerable region at all times.

2.3. Safety Instrumented System (SIS)

A SIS provides an independent protection layer used for controlling and mitigating risk in many sectors of society. In the oil and gas industry it is used to detect the onset of hazardous events and/or to mitigate their consequences to humans, material assets, and the environment. A SIS is installed to detect and respond to the onset of hazardous events by the use of electrical, electronic, or programmable electronic (E/E/PE) technology (Lundteigen, 2009). Emergency shutdown (ESD), Fire and gas detection (F&G), Process shutdown (PSD) and High integrity pressure protection system (HIPPS) are some of the SISs that have a crucial role in maintaining the overall safety in the oil and gas industry.

SIS is often split into three main subsystems, which are illustrated in Figure 4. The input elements are used to detect the onset of hazardous events, the logic solver for deciding what to do, and the final elements[1] to perform according to the decision (Lundteigen, 2009). All three components have to be present, and working, for the system to carry out the specified tasks.

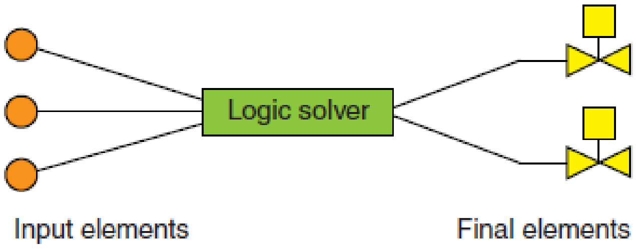


Figure 4: Simplified illustration of a SIS (Lundteigen, 2009)

Input elements may be pressure transmitters or different detectors with the main task of detecting dangerous conditions. A logic solver may be a digital computer such as a programmable logic controller (PLC) or just a signal converter that reacts to a dangerous condition, by activating counter measures. The final element is a type of equipment that has the main purpose of averting the dangerous condition. A final element in a F&G system may for instance be deluge valves, electric fans and other extinguishing systems.

The main requirements for SIS are found in the PSA activity regulations, the management regulations, and the facility regulations.

[1] May also be called actuating devices.

2.3.1. Safety instrumented function (SIF)

IEC standard 61511 defines a safety instrumented function as a "safety function with a specified safety integrity level which is necessary to achieve functional safety." Furthermore, a safety function is defined as a "function to be implemented by a SIS, other technology safety-related system, or external risk reduction facilities, which is intended to achieve or maintain a safe state for the process, with respect to a specific hazardous event."

The terms SIS and SIF are often used almost interchangeably. It should be noted that a SIS is a combination of one or more SIFs, as illustrated in Figure 5. This can be put into context by applying the definitions from chapter 2.1., such that a SIF may be considered as a barrier function, while the SIS may be considered as a barrier system (Lundteigen & Rausand, 2006).

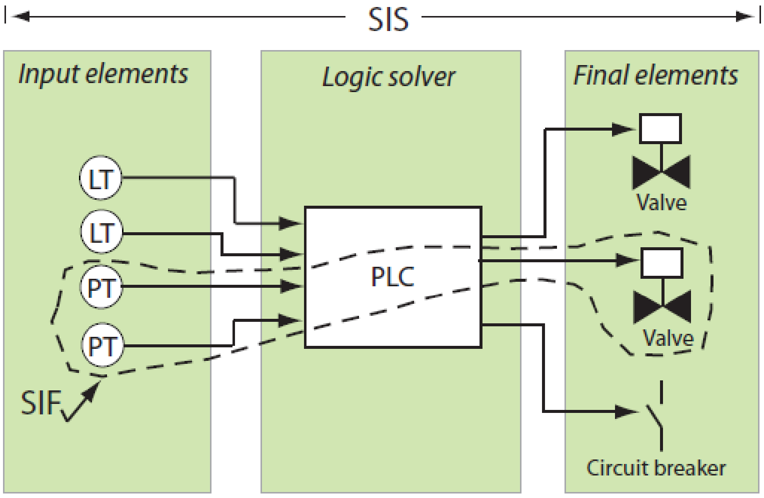


Figure 5: The distinction between SIS and SIF (Lundteigen, 2009)

A SIF is made up of input elements, logic solvers and final elements that act upon dangerous conditions in order to bring the system (EUC) into a specified state, often referred to as a safe state (ref. chapter 5.1.1.). Safe state is often achieved when the SIS performs the intended SIFs.

Safety instrumented functions are divided in two types; SIFs with a protective function that are activated on demand and SIFs with instrumented control functions that are operating in continuous mode. If the SIS fails to perform these intended functions, the hazardous event may escalate and result in an accident. Each safety function implemented into a SIS is therefore required to have a high reliability. As mentioned earlier the reliability is expressed as a safety integrity level (SIL).

2.3.2. Safety Integrity Level (SIL)

Safety integrity is defined as "Probability of a safety-related system satisfactorily performing the required safety function under all the stated conditions within a stated period of time" (IEC-61508, 2004) In general the IEC 61508 and OLF 070 state that three main types of requirements need to be fulfilled in order to achieve a given SIL. These three types are: quantitative, semi-quantitative and qualitative requirements. If one of the three categories fails to meet a specific SIL, say 3, the SIF cannot be classified as a SIL 3 function, even if SIL 3 is supported by the calculated PFD. Only the quantitative requirements will be presented, the other two requirements are presented in appendix B.

2.3.2.1. Quantitative requirements

The IEC 61508 and IEC 61511standards distinguish between four discrete safety integrity levels, which are used as a measure of reliability for SIFs. SIL 4 has the highest level of safety integrity, while SIL 1 has the lowest. The higher the SIL value, the higher is the associated level of safety and the lower is the probability of a failure. This basically means that a high SIL value gives lower tolerance of dangerous failures.

The IEC 61508 standard makes a distinction between low demand and high demand systems. Low demand safety systems are activated on demand to respond to abnormal situations, not more than once per year. Typical examples are Process- and Emergency shutdown system (PSD and ESD). High demand systems may be systems that are subject to frequent demand, or continuous operation mode. Typical examples are dynamical positioning system or a ballast system (Hauge, Lundteigen, Hokstad, & Håbrekke, 2009). This thesis is limited to low demand systems, for it is common to calculate the average probability of failure on demand (PFD_{avg}). PFD_{avg} is a reliability measure which is often used for passive systems (e.g. F&G) that take action when dangerous conditions are detected. (Abrahamsen, 2012).

Table 1: Safety Integrity Levels (IEC-61508, 2004)

Safety Integrity Level (SIL)	Demand Mode of Operation Average probability of failure to perform its design function on demand
4	$\geq 10^{-5}$ to 10^{-4}
3	$\geq 10^{-4}$ to 10^{-3}
2	$\geq 10^{-3}$ to 10^{-2}
1	$\geq 10^{-2}$ to 10^{-1}

Each SIL has a specified target range for the PFD, where each level corresponds to a risk reduction factor (RRF). If the RRF has a factor of 1000 it means that the PFD of the safety function should be lower than 10^{-3}, to fulfill the SIL 3 requirement. To verify that the necessary risk reduction is achieved, all components in the safety function have to be included in the PFD calculation. To satisfy the quantitative requirement, all PFD calculations need to be documented. Since the PFD does not cover all relevant aspects that may cause a SIS to failure, the calculated value may indicate a better performance than will be experienced in the operation phase (Lundteigen, 2009). To compensate for this, the IEC 61508 standard introduces semi-quantitative and qualitative requirements (ref. Appendix B).

2.4. Risk and Reliability analysis

Analysis of reliability and risk is an important and integrate part of planning, construction and operation of all technical systems. Some of the main objectives of risk and reliability analysis are to (Aven, 2006):

- Provide a basis for prioritizing between alternative solutions and actions
- Provide a basis for deciding whether reliability and risk are acceptable
- Systematically describe unwanted events and consequences of these events

Risk and reliability analysis is a tool used to express and reduce the uncertainty regarding future events, often expressed in terms of probabilities.

2.4.1. Interpretation of probability

There are basically two ways of interpreting a probability of an event (A): as a relative frequency or as knowledge based probabilities.

2.4.1.1. *Relative frequency interpretation*

The relative frequency interpretation is defined as the fraction of times an event would occur if the situation analyzed were hypothetically "repeated" infinite number of times under similar conditions. This is difficult to achieve in practice, especially for situations where the studied events rarely occur, such as the failure of SISs. In this interpretation, the probability $P_f(A)$ is unknown and need to be estimated. Since the estimates could be more or less close relative to the "true" underlying probability, estimation uncertainty is introduced. This means that there could be large differences between the estimates and the “correct” value. In statistics, estimation uncertainty is often expressed through measures such as variance and confidence intervals (Aven, 2010).

2.4.1.2. Subjective probability

Knowledge based probability, also called subjective probability, is a measure of uncertainty about future events and consequences, seen through the eyes of the assessor and based on some background information and knowledge. Probability is expressed as the assessors’ “degree of belief” of the occurrence of the event (A). This probability is denoted by P(A|K) to show that this probability is conditional on some background knowledge, K. For knowledge based probabilities it is recommended to use the urn standard. For instance, the probability P(A) = 0.1 means that the assessor compares his/hers degree of belief (uncertainty) about the occurrence of the event (A) with the standard of drawing a specific ball from an urn containing 10 balls. In this interpretation, uncertainty arises from the lack of knowledge (Aven, 2010).

2.4.2. Definition of risk

The concept of risk is defined in many ways. In engineering context risk is often linked to the expected loss, and many different definitions exist. What is common for these definitions is that the concept of risk comprises events (A), consequences (C), and probabilities (P). These probabilities are often referred to as frequency-interpreted probability, meaning that they represent a parameter, for instance expected number of occurrences of the event A per unit of time. The probability is used as a “tool” to express the uncertainties. However, according to Aven (2010), the probabilities do not capture the main essence of risk. This is illustrated by two examples below. These two examples present the typical misconceptions of risk.

2.4.2.1. Risk is equal to the expected value.

One can not specify the future outcome, but one can express how likely this outcome is. In probability theory the expected value is obtained by multiplying each possible outcome with the associated probability, and summing the possible outcomes. The expected value can be interpreted as the average value “in the long run” of the outcome of the experiment, if the experiment is repeated over and over again. According to Aven (2010), expected value can provide good prediction of the actual future quantities in gamble-like situations, but not so often in other situations.

The reason is that the expected values could deviate strongly from the actual outcomes. There are mainly two reasons for this (Aven 2010):

- The consequences or outcomes could be so extreme that the average of a large population of activities is dominated by these extreme outcomes.
- The probability distribution could deviate strongly from the future observed outcome distribution.

Example (Aven, 2010): Risk and expected value

Consider a dice game where a player wins 24 $ if the dice shows 6, otherwise he/she will lose 6$. The expected value is calculated below.

$$E(X) = -24 * \frac{1}{6} + 6 * \frac{5}{6} = 1$$

Consider a situation where the player is not informed about the details of the game, just that the expected value is 1$. Is it enough information to make a decision on whether one should play or not?

$$\boldsymbol{Risk \neq Expected\,Value}$$

2.4.2.2. Risk is a probability or probability distribution

Aven (2008) argues that probabilities alone would not fully capture the essence of the concept of risk. It is important to look beyond assigned probabilities, since the probabilities may camouflage uncertainties. The estimated or assigned probabilities are conditioned on a number of assumptions and suppositions, which depend on the background knowledge of the assessor. The uncertainties may be hidden in the assessors’ background knowledge. In addition, by restricting attention to the estimated or assigned probabilities, factors that could produce surprising outcomes may be overlooked.

By restricting risk to the probability alone, aspects of uncertainty and risk may be hidden. There is a lack of understanding about the underlying phenomena, but the probability assignments alone are not able to fully describe this status.

Example: Risk and probability distributions.

If we consider an undesirable event A, *machine failure*. P (machine failure) describes the probability of a failure, and nothing more. The consequences or outcomes could range from negligible to catastrophic depending on the availability and performance of a set of barriers. In addition, other aspects are also overlooked, such as the extent of exposure of human lives, and other objects that humans value (Aven, 2010).

$$\boldsymbol{Risk \neq probability\ \ or\ probability\ distributions}$$

This is obviously an inadequate description of risk as you do not relate this probability to the possible outcomes. In general there could be many possible outcomes and the restriction to one undesirable event means that the extent or significance of the loss is not reflected.

2.4.2.3. (A,C,U) – perspective

This observations presented above are important for risk management, as the management is not very well informed by the expected values and probabilities alone. The risk management needs to consider uncertainties beyond the expected values and probabilities to provide a sufficient broad characterisation of risk. Aven (2008) argues that uncertainty is a more fundamental concept than probability and should be the pillar of risk. Based on the argumentation above, he introduces a risk-definition that is based on the knowledge-based probability perspective, meaning that the risk does not exist independently of the assessor, as the uncertainties are based on his/hers background knowledge.

Aven (2008) defines risk as the two-dimensional combination of:

i) Events (A), and consequences of these events, (C)

ii) And the associated uncertainties, (U)

Risk is related to future events A and their consequences C. The associated uncertainties mean that we do not know if these events will occur, and if they occur, what the consequences will be. The main features of this risk perspective are illustrated in the figure below.

2012).

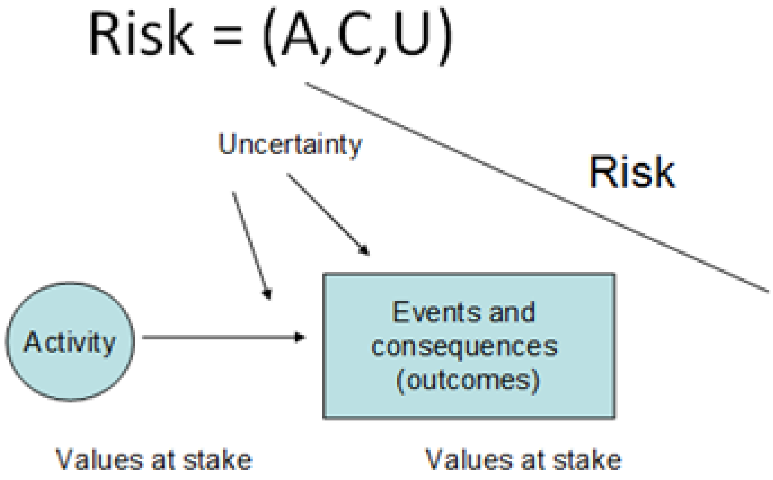


Figure 6: Illustration of the risk definition (Aven, 2010).

A risk description based on (A,C,U) - definition covers the following five components: (A, C, U, P, K). Component A represents future events (initiating events, scenarios), C is the consequences of A, P is the knowledge-based (subjective) probabilities expressing uncertainties about A and C, U expresses the uncertainties beyond what is captured by P, and K the background knowledge that P and U are based on (Aven, 2008). When this perspective is adopted, risk reduction also means uncertainty reduction.

2.5. Uncertainty

Uncertainty can arise from two main causes, natural variation and the lack of knowledge. These two categories of uncertainty are commonly referred to as aleatory and epistemic uncertainty in the literature. Aleatory uncertainty is the uncertainty arising from or associated with, the inherent, irreducible, and natural randomness of a system or process. Epistemic uncertainty is the uncertain arising from the lack of knowledge about the performance of a system or process. The epistemic uncertainty will be reduced when new knowledge becomes available, while the aleatory uncertainty cannot, in principle be reduced. However, several types of uncertainty, which in the past was classified aleatory, are now considered epistemic. This indicates that the uncertainty classification is not fixed (Jin, Lundteigen, & Rausand, 2012).

Based on Aven’s (2008) (A, C, U) – framework, the uncertainty is the same as epistemic uncertainty. The uncertainty is then lack of knowledge about A and C. There is an uncertainty about the occurrence of the event and the associated consequences if this event occurs. According to Avens definition; if uncertainty cannot be properly treated in risk assessment, the risk assessment itself fails to perform as intended, and can therefore not be considered as an informative tool for decision making (Zio & Aven, 2013).

The uncertainty is often expressed through an uncertainty analysis. The analysis may take several forms; quantitative, qualitative or semi-qualitative. Most of the quantitative methods view the uncertainty as aleatory, while qualitative methods view it as epistemic. In many cases it may be enough to use a qualitative approach, which is considered as a more simplified method than quantitative. Since the results are expressed qualitatively, advanced knowledge about statistics is not required.

2.5.1. Uncertainties in the Traditional approach

The quantitative parts of the requirements from the IEC standards require that the PFD is calculated and compared with the criteria in Table 1 . This approach for verification of a quantitative SIL seems intuitively appealing, but is lacking any discussion about uncertainty, which according to Aven (2008) is one of the main components in risk (Abrahamsen & Røed, 2011).

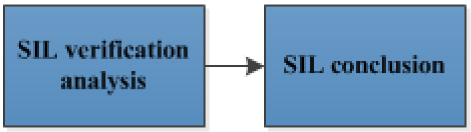


Figure 7: Traditional approach

2.5.2. Uncertainties in the calculated PFD

The calculated PFD plays an important role in the design of SIS design. The associated uncertainties will be briefly described below. According to Lundteigen (2009), PFD is influenced by three main factors:

i) The model.
ii) The data.
iii) The calculation approach.

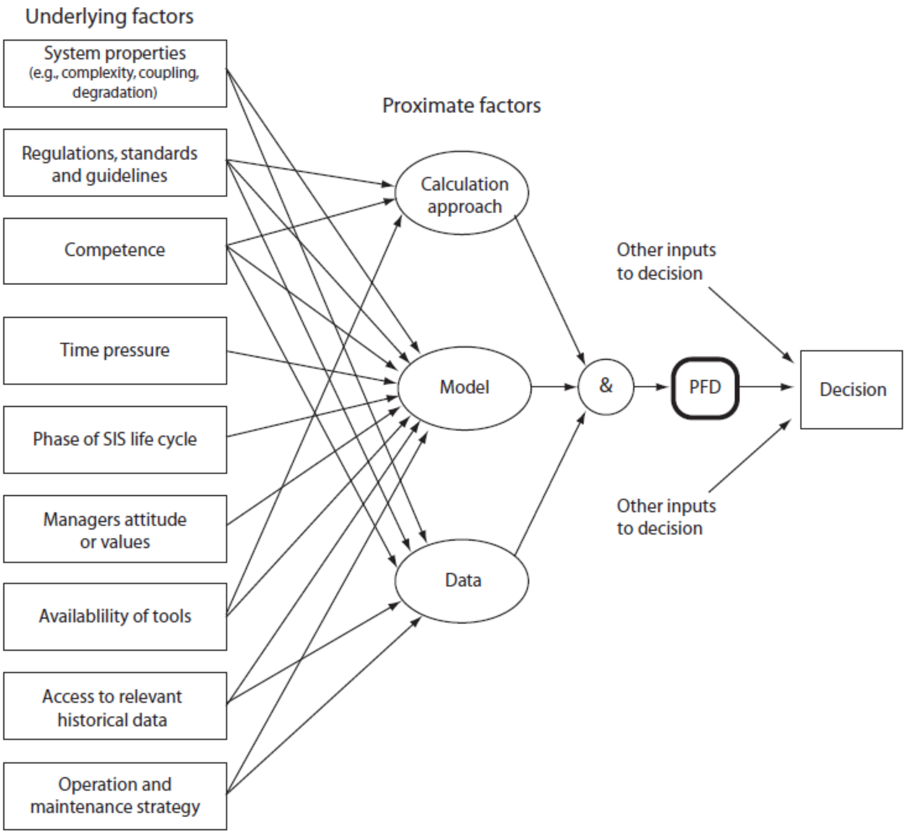


Figure 8: Factors that influences the PFD (Lundteigen, 2009)

Figure 8 illustrates that the uncertainty associated with the PFD depends on whether or not the model, the data, and the calculation approach reflect the main properties of the SIS in question.

2.5.2.1. Model uncertainty

The model constitutes a simplified representation of the real system, reflecting the causal relations that produce the events focused on by the decision-makers (Nilsen & Aven, 2003). A system model may be developed in two steps: first the construction of a functional and/or architecture model and second the development of one or more reliability models (Lundteigen, 2009). The complexity of the model will depend on several factors, such as the amount of information that are considered sufficient for the decision making, the available resources, the complexity and the knowledge of the system. The model is dependent on the competence of the analyst and the properties of the system. There will therefore always be a trade-off between the need for simplicity and accuracy when choosing a model. In addition, there will be several other underlying factors that will influence the choice of the model. The performance of a model must, however, always be seen in light of the purpose of the analysis. A crude model can be preferred instead of a more accurate model in some situations, if the model is simpler and it is able to capture the essential features of the system performance (Zio & Aven, 2013).

Uncertainties related to the calculation approach

The PFD may be calculated by using approximation[2] or exact formula. The results of these two methods are often similar, but minor differences may be introduced. These two formulas are based on the assumption that the units lifetime distribution is exponential with constant failure rate, meaning that lifetime distribution does not depend on the age of the unit. It is also assumed that after a test or repair the unit is as good as new (Aven, 2006). It is referred to appendix A for more information about calculation of PFD.

The IEC 61508 and PDS methods provide somewhat different approaches, which may give different results. The only difference between these two approaches is a configuration factor, CMooN, which is introduced in the PDS method.

2.5.2.2. Uncertainties in the data

The input data in a reliability analysis will have a huge impact on the end result. The level of uncertainty associated with the input data may be influenced by the relevance, quality and amount of available data. The extent to which relevant, high quality and sufficient amount of data can be achieved will depend on several underlying factors (Lundteigen, 2009). These are illustrated in Figure 8

2.5.3. Completeness uncertainty

Completeness uncertainty is another main source of epistemic uncertainty that is introduced in the assessment of reliability. This uncertainty is about facts, either known or unknown, that is not properly included in the analysis. Known completeness uncertainty arises when the analyst is aware of the relevant issues, but has deliberately omitted them from the analysis for different reasons, i.e. lack of understanding of the system, lack of competence, lack of model, lack of data to support the model, outside the scopes of the assessment and so on. Such simplifications reflect the analysists assumptions and suppositions made during the assessment. Unknown completeness uncertainty on the other hand is due to lack of

[2] Approximation may for instance be that a physical phenomenon is replaced by a simple model. In reality, any modeling implies some degree of approximation. Approximation is often used when analyst does not have enough data and/or information to describe the phenomena of interest in detail. Another reason may be that the analyst deliberately would like to simplify the analysis (Zio & Aven, 2013)

knowledge, meaning that the facts are truly unknown, either because they are not yet identified or that they are not known. It is therefore difficult to take them into account when conduction a reliability assessment (Jin et al., 2012).

Failing to include all relevant factors in the analysis will give an incorrect estimate of the reliability, even if the data and model selection is close to perfect (Jin et al., 2012).

2.6. Sensitivity

Both uncertainty and sensitivity are two topics that are commonly referred to in the concept of reliability engineering. Sensitivity analysis is often mentioned in the same context as uncertainty analysis, but the two types of analysis have slightly different meaning (Lundteigen, 2009) A sensitivity analysis in a risk analysis context is a study of how sensitive a calculated risk index is with respect to changes in conditions and assumptions. A sensitivity analysis does not include any assessment of uncertainties, but provides a basis for an uncertainty analysis (Aven, 2010). It shows how sensitive the end result (output) is with respect to changes in input data. By changing one element at a time, while other remains fixed, it is possible to compare the results. By varying assumptions or other quantities, for example such as probabilities it is possible to determine which elements have low or high sensitivity. Elements that have a low sensitivity have an insignificant impact on the end result, and should not be focused on. Elements with high sensitivity should be investigated further. Thereby a sensitivity analysis may be used as a tool to identify critical elements/components. This may provide valuable information for risk reducing measures, resulting in that the resources are allocated more efficiently.

2.6.1. Difference between uncertainty and sensitivity

The main difference between uncertainty and sensitivity is that a sensitivity analysis focuses on how variations in the input parameters may affect the final result/output, while uncertainty analysis is a tool for evaluating the degree of knowledge or confidence in the results. In the context of safety and reliability assessment of SIS, uncertainty may be defined as the degree of doubt in our ability to capture the relevant factors in model, the data, and/or the calculations (Lundteigen, 2009).

3. Standards (Requirements in relation to SIS)

According to the PSA management regulations (section 4 and 5), performance requirements shall be defined with respect to the technical, operational and organizational elements necessary for the individual barrier to be effective. For SIS, references are made to IEC 61508 and OLF-070 as the recommended standards.

3.1. IEC 61508 and 61511

The IEC 61508 is the international standard for E/E/PE safety related systems. It provides requirements for ensuring that systems are designed, implemented, operated and maintained in accordance with the required SIL. A primary objective of this standard is to serve as a guideline for development of sector specific, tailored, standards that at the same time comply with the requirements in the IEC 61508. In addition to the IEC 61508, there are some industry specific standards, such as IEC 61511.

The IEC 61511 has been developed by the process industry, based on the framework provided in the IEC 61508. The IEC 61511 standard provides good engineering practice of the safety instrumented systems. It is based on proven technology, meaning that the components that are used in the SIS are well proven or certified in accordance with IEC 61508.

3.1.1. IEC 61508 Life cycle

The IEC 61508 uses a safety life cycle[3] to structure its requirements. This life cycle provides an approach that can be used to identify the hazards of a system, determining the necessary risk reduction, implementing safety related systems and determine their required reliability. Furthermore, it ensures that this is maintained throughout the lifetime of an installation. The life cycle is divided into 16 phases, as illustrated in Figure 9. Each phase has a specified and detailed set of requirements, inputs and outputs. After completion of each phase, verification shall be performed to confirm that the required output is as planned.

[3] IEC 61511 uses a similar life cycle model.

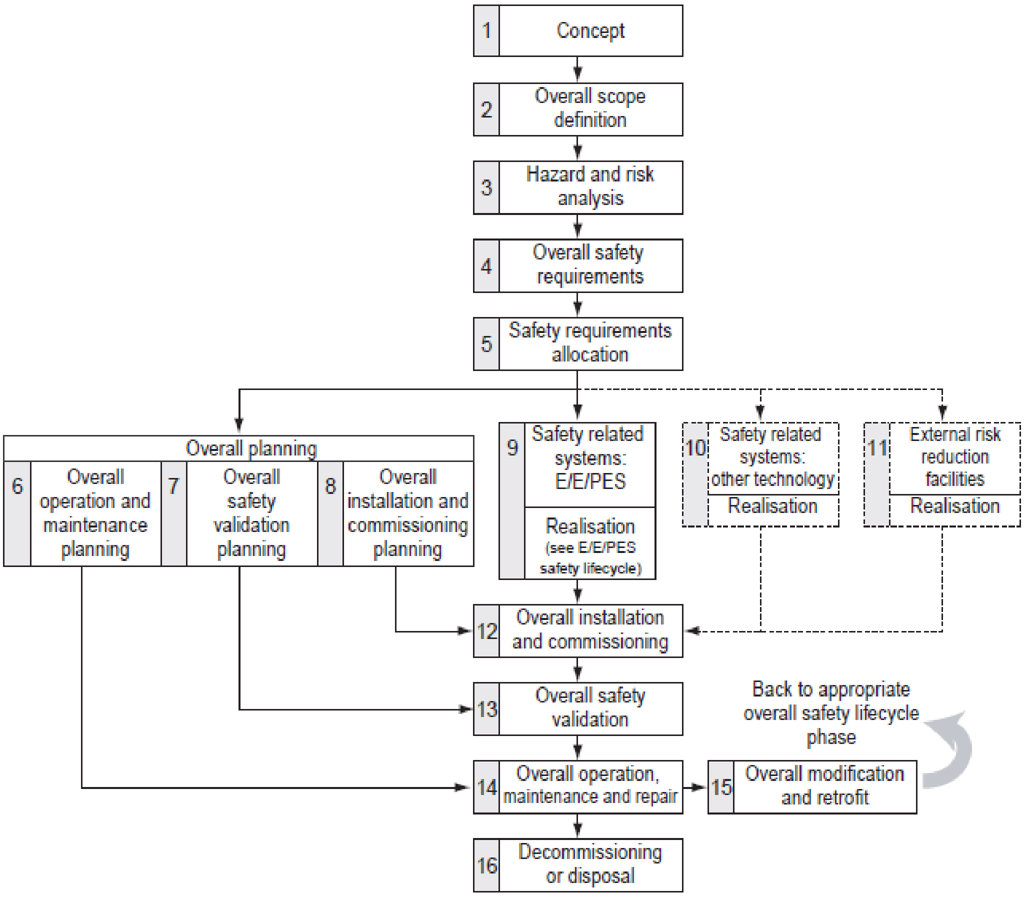

1 Concept
2 Overall scope definition
3 Hazard and risk analysis
4 Overall safety requirements
5 Safety requirements allocation
Overall planning
6 Overall operation and maintenance planning
7 Overall safety validation planning
8 Overall installation and commissioning planning
9 Safety related systems: E/E/PES
Realisation (see E/E/PES safety lifecycle)
10 Safety related systems: other technology
Realisation
11 External risk reduction facilities
Realisation
12 Overall installation and commissioning
13 Overall safety validation
14 Overall operation, maintenance and repair
15 Overall modification and retrofit
Back to appropriate overall safety lifecycle phase
16 Decommissioning or disposal

Figure 9: IEC 61508 Life cycle (IEC-61508, 2004)

The safety life cycle starts off with an initial concept, definition of the EUC, followed by the preparation of the overall scope of the safety analysis. Thereafter, hazard and risk analysis is conducted to find the associated hazards and risks to the EUC. Based on this analysis, the required safety functions are specified. The required risk reduction by these safety functions is determined by comparing risk arising from each hazard with the tolerable risk level. Each safety function is then specified in terms of its functionality and the associated SIL.

The required safety functions may be realized by SIS (E/E/PE technology), other technology or other risk reduction facilities. (Lundteigen, 2009). Only SISs are covered in the IEC 61508 life cycle framework, the latter two are outside the scope, represented with dotted lines. Maintanance, validation, installation and commissioning planning is conducted in parallell with the realization of the SIS. In the operation and maintenance phase, IEC 61508 focus on how to operate and maintain the SIS in accordance with the functional safety and safety integrity requirements (Lundteigen, 2009). The SISs should be installed in a proper manner, according to the overall installation and commissioning plan. Thereafter, an overall safety validation should be performed to ensure that the overall safety requirements and required safety integrity are met. The last phases in the life cycle deal with operation, maintenance, repair, modifications and decommissioning. The requirements for operational phases are based on the procedures for operation and maintenance, that have been developed in parallel with the realization of SIS (Shönbeck, 2007). The SIS modification phase addresses necessary analyses of modifications to the SIS. This phase is of the main interest for this thesis and will be presented in more detail in the next chapter.

3.2. OLF-070

The OLF 070 is a simplification of the IEC 61508 and 61511 standards developed by the Norwegian Oil and Gas Association. The overall purpose of the document is to issue a guideline on the application of the IEC 61508 and the IEC 61511 in the Norwegian Petroleum Industry. This guideline provides various aspects of how the IEC requirements should be adopted (OLF-070, 2004) . The OLF-070 guideline does not take a full risk based approach like the IEC 61508. This is because the Norwegian PSA requirements states that any new approach to the SIS design, should be at least as good or better, than current practices (Lundteigen, 2009).

The difference between the IEC 61508 and OLF 070 is the approach for determining the SIL requirements. The IEC 61508 describes a risk-based approach, while the OLF 070 includes calculations of PFD_{avg} for the most common SIFs, and proposes corresponding minimum SIL requirements for these functions. Use of predefined SILs may ensure a minimum safety level, and could enhance the standardization across the industry. The predefined requirements can also be used to avoid time-consuming calculations, risk analysis and documentation for typical safety functions.

3.3. Safety Requirement Specification (SRS)

In order to fulfill the requirements of the IEC standards a safety requirement specification (SRS) is needed. The SRS plays a vital role in the IEC life cycles, it captures all of the safety requirements from the analysis phase of the lifecycle, forms the basis for the realization phase and is the key document against which the validation of the SIS is performed. A SRS is a document that shall be established for all safety instrumented systems, and shall contain the relevant key information for specifying and operating the instrumented safety functions. The

SRS shall provide a basis for the design, and the document shall be further developed and maintained through all lifecycle phases of the SISs. The SRS shall contain three main types of requirements (OLF-070, 2004):

- Functional requirements that describe the logic of the system,
- Integrity requirements that describe the needed performance for each function
- Operating prerequisites and constraints.

An example of content for SRS for F&G and ESD systems is presented in OLF-070 (Appendix E).

4. Modifications (Changes) to SIS

This chapter provides information on modifications and how they are handled. The information presented in this chapter will form the main basis for the discussion chapter.

4.1. Changes in Safety Instrumented Systems

A change is the result of a continuous decision to exchange, substitute, convert, alter, add, modify or vary a component of an existing process, its equipment and/or control and management systems. Change can be administrative, technical and/or organizational (S.E.A.L International). The latter one is not of interest for this thesis and will therefore not be mentioned further. Administrative changes are modifications to work procedures, for instance by increasing or decreasing the time interval between maintenance/tests. Technical changes will affect the operating process. These changes are often made by adding or removing equipment or materials. The main point of these changes is to increase safety, production and/or profit. However, if these changes are not properly managed they may also increase the risk. For instance a modification may have an effect on:

- Creating hazards that has not previously been identified
- Increasing the probability of incidents that have negative consequences for health and safety.
- Compromising the safety and/or availability of the safety system.

An offshore module operates in a dynamic world and is thus a subject to continual change. Changes to offshore facilities are often made to increase the productivity or to reduce the risk level. Considering a SIS, required modification may arise from various reasons, such as; a need to reduce the downtime, keeping the SIS up-to-date, to comply with regulatory changes etc. These modifications may be introduced through changes to hardware, software, procedures and work practices. All these modifications have the potential to affect the SISs ability to perform their intended functions.

4.2. Modifications in standards

The IEC 61058 and 61511 standards provide a phase on modification in their life cycles. The purpose of the modification phase is to ensure that modifications to any SIS are properly planned, reviewed and approved prior to making the change; as well as ensuring that the required SIL is maintained despite of any changes made to the SIS (IEC-61511, 2003).

Handling of changes is thus an important aspect of the process life cycle to avoid dangerous incidents and accidents. The modifications should be carefully analyzed with respect to the impact the change has on the system. Changes to SIS should consider the impact on the EUC, the EUC risk, the SIS hardware and software, the operation and maintenance procedures, tools, and practices. In the IEC 61508 life cycle; the impact analysis of the proposed modification, will determine which phase to return to for proper implementation. If planned changes to the system have a negative effect on safety, one should return to the beginning of the safety life cycle. As stated in IEC 61508, if the modification affects the functional safety or safety integrity it is required to return to hazard and risk analysis phase (Lundteigen, 2009).

4.2.1. Impact analysis

An impact analysis is a systematic approach for evaluating changes to a system. According to the requirements in IEC 61511, an impact analysis shall be carried out to demine the impact the modification has on the functional safety. This analysis is used to provide justification for or against the change. An impact analysis considers (Yozallinas, 2013):

- new features, enhancement, or problems to be fixed,
- the underlying reason for change or the root cause,
- and the proposed solution in terms of the existing system and its constraints and requirements.

An impact analysis is a formal way of documenting the discussions and informal reviews that take place to provide traceability for the modification (Yozallinas, 2013).

4.2.2. Requirements for modifications

The requirements for modification are stated in IEC 61511:

- Prior to carrying out any modification to a SIS, procedures for authorizing and controlling changes shall be in place. These procedures shall include a clear method of identifying and requesting the work to be done and the hazards which may be affected.
- An impact analysis shall be carried out to demine the impact the modification has on the functional safety. Based on this analysis, one should return back to an appropriate phase in

the life cycle for implementation. Thereafter, all subsequent phases should be performed again.

- The modification activity shall not begin before the proper authorization is received.
- All appropriate information and documentation shall be maintained for all changes to the SIS, the information shall include:
    - description of the modification and the reason for the change
    - an impact analysis of the modification activities
    - hazards that may be affected
    - all approvals required (collected along the way)
    - tests used to verify that the change was properly implemented
    - configuration history
    - tests used to verify that the change has not adversely impacted parts of the SIS which were not modified.
- The modification shall be performed by qualified and trained personnel. All affected and appropriate personnel shall be notified about the change and receive the necessary training (when necessary).

4.2.3. Management of change (MoC)

Handling of SIS modifications is referred to as Management of Change (MoC) in OLF-070, and several other standards. The main focus of the MoC is to prevent catastrophic accidents and to properly evaluate the concerns of safety and health, and to accomplish review of the change in a timely manner (Shinkle, 2001). MoC is a process used to evaluate and properly manage any modification to the design, control, or operations of a covered process. During a modification, one of the main tasks of the MoC is to evaluate the potential impact of a proposed change. The main task of this evaluation is to study how a change may affect the modified system, including how the change may affect other systems which were not modified.

4.2.3.1. The MoC procedure

A MoC is a procedure that shall be in place to initiate, review, approve and execute changes to the SIS. The main task is to maintain safety when changes are introduced to the facility and/or documentation. The MOC procedure could be required as a result of modifications in the following areas (OLF-070, 2004):

- component(s) with different characteristics;
- new proof test interval or procedures;
- changed set-point due to changes in operating conditions;
- changes in operating procedures;
- a new or amended safety legislation;
- modified process conditions;
- changes to the Safety Requirement Specifications;
- a correction of software or firmware errors;
- correction of systematic failures;
- as a result of a failure rate higher than desired;
- due to increased demand rate on the SIS;
- software (embedded utility, application).

A MoC procedure should address (Hauge & Lundteigen, 2008):

- Criteria for when a modification shall be initiated.
- A method for analyzing the impact of modifications, for the SIS, and other systems. The impact analysis should address new hazards that may arise from the modification
- Documents that must be updated as part of the modification. Typical documents are C&E-charts, different drawings, operation and maintenance procedures etc.
- Who have the authority to approve SIS modifications, and which departments must be involved have to be clarified.
- Upon which types of modification are new competence and/or training needed?

Offshore experience has shown that many major incidents occur when changes are made to procedures, equipment, activities or approved practice without an evaluation of the potential impacts it has on the system (IMCA, 1999). It is therefore essential that the proposed changes are thoroughly considered to avoid implementing unnecessary or ill-considered modifications. MoC is thus necessary for keeping track of changes in a process, equipment or documents. The main steps of a MoC procedure are presented in the Figure 10. As mentioned earlier, the main task is to address the potential impact of the proposed change. Furthermore, it aids in reducing the risks, to avoiding badly planned implementation, and that the changes are well documented. The IEC 61511 standard states that in order to achieve these objectives, modifications must be made in a way that ensures that; all changes are properly planned, reviewed, and approved in advance, and that the required safety integrity of the SIS is maintained in spite of any changes (Emerson Process Management, 2005).

4.2.3.2. Replacement in kind (RIK)

If the proposed modification is "replacement in kind", the change does not require a full formal MoC process. Keep in mind that a "RIK" may in fact not be an in-kind replacement, if it does not meet the following criteria (S.E.A.L International):

- Same specification: The components have the same technical specifications as the original equipment (material, dimensions, weight, etc.)

- Same service: The service for equipment remains the same, meaning that inspection and maintenance requirements should not change. In addition, the process conditions must be the same as for when the original equipment was in service.

- Procedural replacement: The replacement is a part of routine maintenance, where the component is replaced due to its known life span by maintenance workers with sufficient level of training and experience. In case of component failure; investigation is required and MoC applies.
- Replacement - not improvement: The new component is the same as the original one; meaning that it should not be an improved component or from a new supplier. Even seemingly minor. Change in any of the specifications may impact some aspects of the process in some way.

4.3. Typical modification process

In nuclear industry it is typical to divide the modification process into distinct phases, as illustrated below.

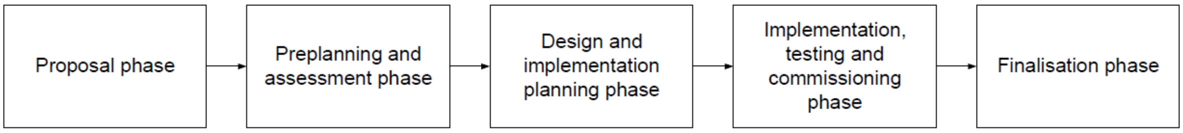

Proposal phase
Preplanning and assessment phase
Design and implementation planning phase
Implementation, testing and commissioning phase
Finalisation phase

Figure 10: Phases in a typical modification process (NEA, 2005)

All phases will to some degree include design, planning, assessment and documentation activities. In this process, modifications will go through several decisions and check points, during which additional analysis (information) may be needed or where the modification may be returned to an earlier stage in the process. A proposal for modification comes from internal or external sources where the main focus is on safety or production. In the preplanning and assessment phase, the project team considers modification proposals, where cost and benefit assessment is conducted. In the design and implementation planning phase are the resources allocated. During the next phase, the plans are finalized, assessed and implemented. The last phase includes reporting and documentation activities (NEA, 2005).

4.3.1. MoC flowchart

The flowchart below presents the main steps of a good MoC procedure; this illustration can be seen as a more detailed representation of the five phases in Figure 10.

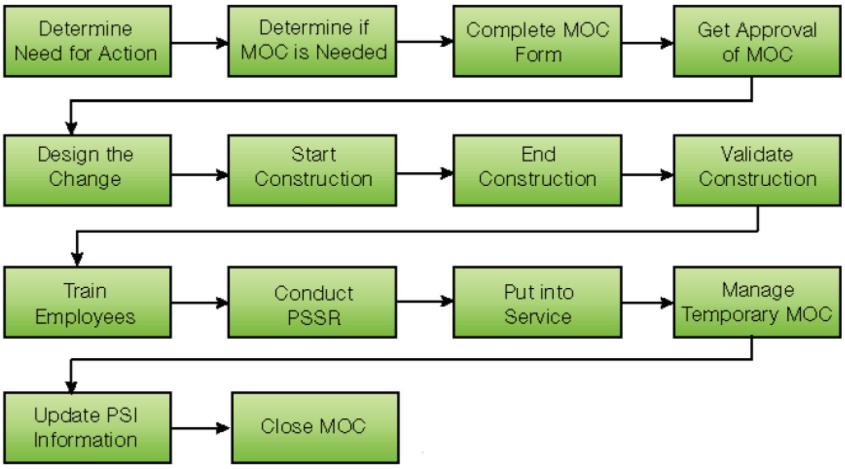


Figure 11: Flowchart of a good MOC procedure (Garland, 2012)

The first step is to identify the need for a change and put it in writing. The change should be sufficiently described, including the technical basis for the change and the impact the change may have on the risk level (safety). In the second step, engineering and safety personnel analyze and evaluate the proposed change, followed by an approval process. In the engineering design step, engineers from different disciplines participate in detailed engineering of change, to develop a design solution. The construction personnel implements the proposed changes in the design (when necessary) of the facility. The MoC process continues with a verification process, during which several critical activities are carried out. The change has then to be clearly communicated to all relevant personnel and necessary training has to be received before the system is put into service. During the closing phases it is essential that all information and documents are updated (Garland, 2012).

4.4. MoC in offshore oil and gas industry

A typical modification covers three main phases:

1. The objectives should be thoroughly considered. The proposed situation should be compared to the existing situation, and the change should be highlighted. A risk assessment is conducted to assess the change and provide mitigating actions. As an example, an additional gas leak is introduced to an area. The effect on the risk level is considered and actions are proposed. Typical actions will be to install additional gas detectors to maintain the risk within an acceptable level.
2. Another main task is to verify that the modification does what it is set out to do, and ensures compliance with all relevant rules and regulations.
3. The focus is on humans, and how they can be affected (direct and indirect) by the modification.

Even though OLF-070 recommends the use of an IEC 61508 life cycle and the use of MoC procedure to handle modifications, this approach is not widely used in the oil and gas industry. However, several other techniques and analysis methods are used to analyze the proposed change.

4.4.1. Typical methods to analyze the proposed change

Hazard identification (HAZID) is a typical brainstorming process that is used to reveal challenges that may be introduced by the proposed modification. The end result of this structured process is a list of actions that shall be initiated to ensure that the risk level is not affected by the modification. Hazard and Operability (HAZOP) study uses guidewords to identify scenarios that may result in hazards or operational problems, for instance, how the modification may lead to operation or maintenance failures.

In addition, different analysis methods such as Change- and constructability analysis are used to ensure that the modification fulfills the requirements and regulations. These techniques and methods reveal the main issues relating to safety and compliance. However, these analysis are just a part of the big picture, other aspects have to be included to provide a broad evaluation.

5. Case - Fire and gas (F&G) system

This chapter is presented to aid the first sub-objective, which focuses on how typical modifications may affect the calculated PFD. A case study is introduced for an F&G-system on an offshore installation, to illustrate how a modification may affect the PFD.

- Chapter 5.1 and 5.2 introduce the F&G case, where the main purpose is to provide a better understanding of SISs (F&G) and safety functions (SIFs).
- Chapter 5.3 presents the approach used for the case, more specific for the calculation, selection of data and model.
- Chapter 5.4 presents the calculated PFD of the original SIFs (before modifications).
- Chapter 5.5 presents typical modification that will be used to illustrate how the PFD is affected.

The results obtained from the case are provided to supplement the main objective, and clarify potential pitfalls that may be introduced by a poor management of change.

5.1. Typical F&G functions.

A F&G-system is one of the main components contributing to the overall safety in the oil and gas industry. The purpose of fire and gas detection system is to continuously monitor for the presence of flammable/toxic gases and fire, to alert personnel and allow control actions to be initiated manually or automatically to minimize the probability of personnel exposure, explosion and fire (NORSOK-S-001, 2008).

The F&G system activates its safety functions upon detection of abnormal situations, to get the area into a safe state. These actions are often described in the areas cause and effect (C&E) chart. For the system to take automatic actions, predefined criteria have to be met. Voting philosophies are often used to reduce the number of false alarms. Consider a 2oo4 detector configuration, where 2 out-of-4 detectors need to be activated before a low alarm for a confirmed fire is achieved. If the voting is not necessary, a single detector (1oo1) may release a confirmed fire/gas signal.

5.1.1. Cause and Effect (C&E) chart and safe state

NORSOK-standards recommend the use of C&E-charts. The typically used for a cause-and-effect representation of F&G and ESD systems (Norsok-S-005, 2005). A cause-and-effect (C&E) diagram is a matrix, illustrating the relationship between all inputs (causes) into a system and all corresponding outputs (effects). It can be used to describe the safety functions, and the actions necessary to get the system into a safe state upon detection of hazardous events. A safe state is often defined as "state of the process when safety is achieved"(IEC-61508, 2004). This definition does contain a note stating that in order to get a process to a safe state the knowledge of the proses is important. Some processes may have to go through a number of states (actions) before a safe state is achieved. Description of the safe state should be included in a SRS, including details regarding how the SIS takes the process to a safe state (OLF-070, 2004).

5.1.2. Typical F&G functions presented in OLF-070

As mentioned, OLF-070 presents typical F&G functions with a proposed minimum SIL. Recommendations from OLF 070 state that SIL-2 requirement should be applicable for F&G-functions. To achieve a SIL 2 for the F&G system, the PFD must be less than 0.01, meaning that at 100 demands the systems statistical probability of failure is 1 of 100.

5.1.2.1. The Fire & Gas detection system

The fire and gas detection system consists mainly of gas and fire detectors that are connected to F&G logic solvers. The safety function of F&G detection system is to generate an alarm signal, interpret the information and transmit the appropriate action.

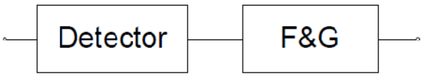


Figure 12: RBD for fire/gas detection sub-function (OLF-070, 2004).

In this case, the safe state for the process will be a signal from the F&G node. It is assumed that the F&G logic is a single system. According to OLF a SIL2 requirement is obtainable for both fire and gas detection.

5.1.2.2. Electrical isolation

Electric isolation is initiated from the F&G detection system. This action is typically initiated upon HC gas detection and confirmed fire detection. Different actions are performed relative to where the gas is detected.

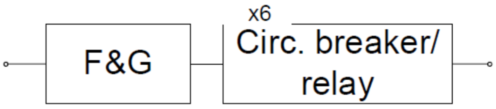


Figure 13: RBD for electrical isolation (OLF-070, 2004).

The safe state for the process will be to isolate electric ignition sources. The calculations in OLF-070 illustrate that it is not straightforward to achieve a SIL2 requirement for this function. To satisfy these requirement no more than three circuit breakers should be included in the function. Nevertheless, they conclude that SIL 2 requirements may be achieved if this function consists of only a few circuit breakers. If more circuit breakers have to be activated the test interval should be reduced.

5.1.2.3. Firewater Supply

Firewater supply is initiated from the F&G detection system. The system boundaries include the fire water demand signal processed in the fire pump logic, start of fire pumps and opening of one deluge-valve (given confirmed fire).

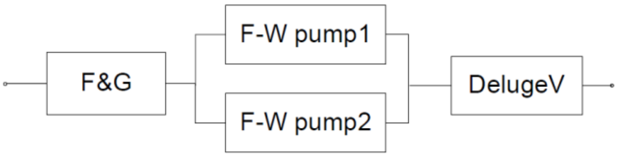


Figure 14: RBD for deluge function (OLF-070, 2004).

Safe state for the process will be that fire water is released. The calculations show that SIL 1 is obtained, but OLF concludes that the SIL 2 requirement is achievable.

5.1.2.4. Others

Final elements such as PA /dedicated alarm system, ESD, HVAC and BD are not part of the F&G function in OLF 070.

5.2. Introduction to the case

Based on the description in the functional documents and C&E-chart (Appendix C) for the area under consideration, an overview of the system and actions is illustrated below.

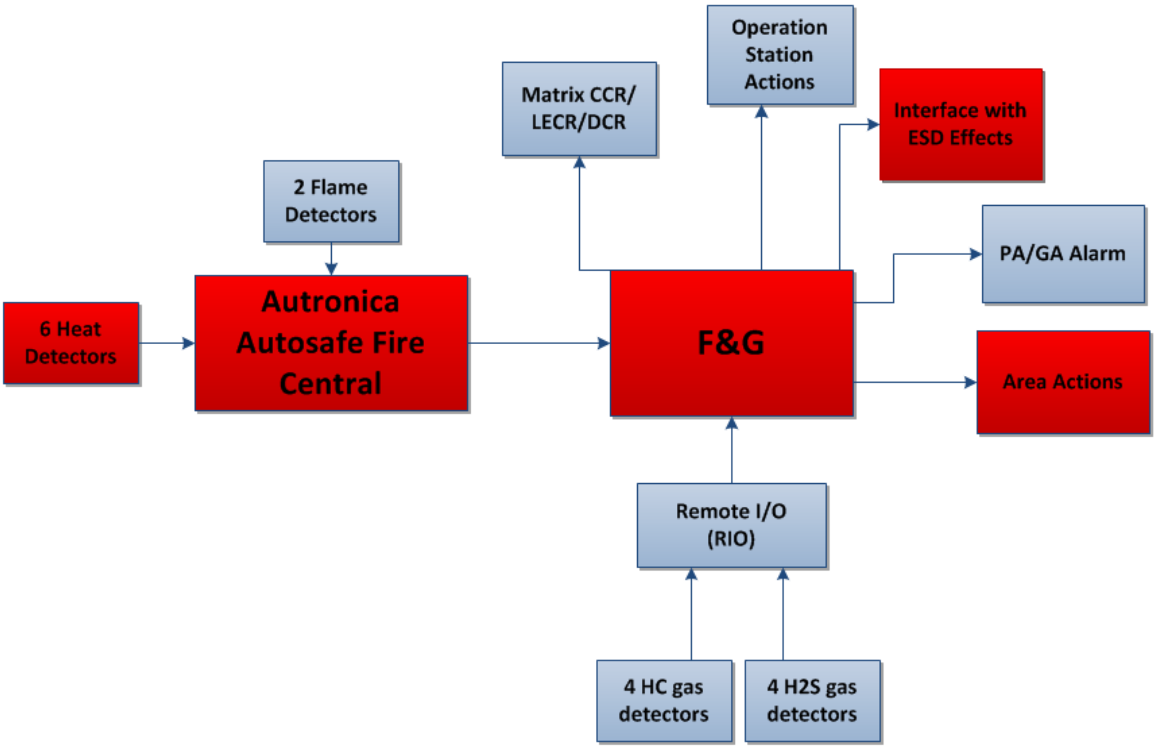


Figure 15: Overview over the F&G system (Based on C&E and functional description).

The gas and/or fire are detected, and the signal is sent to the F&G. The F&G node decides whether actions are required. The components and functions marked in red are of the main interest for this thesis. The two chosen actions for this thesis are: area actions (deluge) and the interface with ESD-effects (shutdown of HVAC). These actions are presented later and used as basis for the case.

5.2.1. Fire detection function

The fire detection system monitors the smoke, flame and heat throughout the installation. The purpose is to detect fire at an early stage and to signal the danger, by audible and visual means. All fire detectors are connected to the F&G system through the Autronica fire central. All alarms, status and actions will be carried out by the F&G system (DSME, 2008a). The following voting philosophy generates a confirmed signal (DSME, 2008a):

- 1 heat detector
- 2 smoke detectors
- 2 flame detectors
- 1 smoke and 1 flame detectors

F&G detection system interpret inputs from detectors. The signals are then controlled by the F&G system using different software loops. Based on the configuration, the Software loop activates an output signal according to the applicable C&E-chart

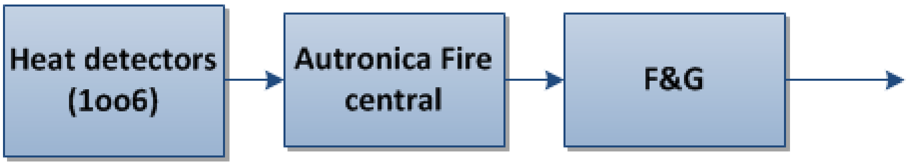


Figure 16: Heat-detection function, based on C&E and functional descriptions

5.2.2. Deluge and Fire pumps (Area actions)

The deluge system shall provide adequate coverage of the relevant fire and explosion scenarios, with respect to both volume and area coverage (NORSOK-S-001, 2008). The main purpose of deluge system is to keep equipment and hull structure at low temperature in case of hydrocarbon fire.

The deluge water is supplied by the Fire water system, consisting of four main fire pumps, 4 x 50%. Two pumps are installed in each pump room, with separate supply lines from each of the pump rooms. One pump is in stand-by mode while the other pump is on maintenance in each pump room. Pumps that are in standby mode are automatically opened up when the F&G system detects a confirmed fire condition. The suction valves are located prior to the fire water pumps, meaning that before the fire pumps receive signals from F&G system, a signal is sent to the corresponding suction valve to open. After it is confirmed by the F&G system that the valve is open, a signal is sent for the fire pumps to start (DSME, 2008b).

The area under consideration is covered by two deluge valves. These valves are automatically opened by the F&G system upon confirmed fire in the area. Valves can also be opened manually by the local deluge release push button, from F&G workstation or by manually operating the valves. Only the automatically actions are of interest for this thesis.

Activation of the fire-pumps and opening of deluge valves is another important action, which is also activated upon heat-detection. Safe state is achieved when both deluge valves are closed. See figure below for illustration of fire-water and deluge function.

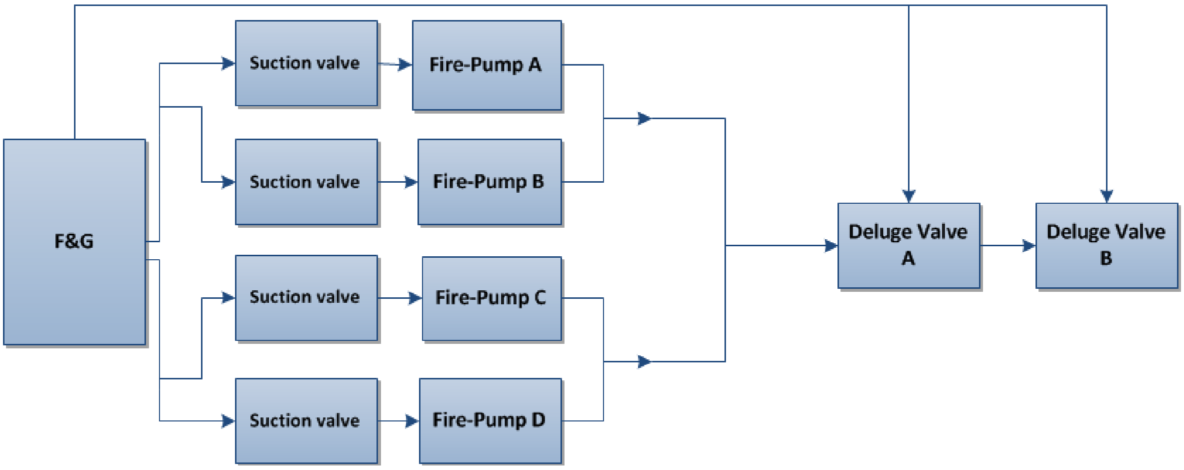


Figure 17: Fire-water (Deluge) function (Based on C&E) and functional descriptions

5.2.3. Interface with ESD effects (HVAC)

ESD is activated either manually or automatically with the main purpose of minimizing the consequences related to an emergency situation and to ensure that conditions are as safe as possible for the installation and the equipment.

The ESD system receives and processes input signals from manual pushbuttons or confirmed gas/fire from the F&G system, and then sends shutdown / stop signals to the power sources, equipment and ventilation devices (DSME, 2010). Upon confirmed fire in the area the automatic F&G actions, through ESD, are to shutdown intake fans, exhaust fans, intake dampers and exhaust dampers. In order to close the damper from ESD, an interposing relay is installed in the relay panel to make the interface between the dampers and the ESD system. When the ESD system has to close the dampers, it de-energizes its output to open the contact on the power supply to the dampers actuator. When intake or outlet dampers close, the dedicated fans will automatically be stopped via interlocks.

Upon heat-detection, the F&G system informs the ESD system to shut-down the ventilation in the related zone, meaning to stop fans and dampers. The safe state is achieved when both HVAC ducts are closed; see the figure below for illustration.

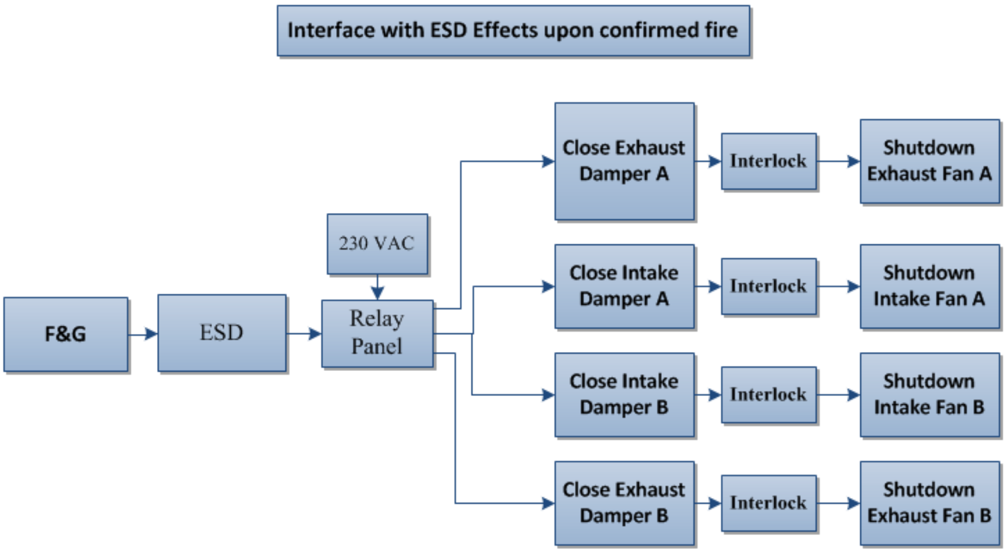


Figure 18: HVAC function (Based on C&E) and functional descriptions

5.3. Case approach

This sub-chapter explains the selection of data, model and the calculation approach. The main aim of this case is to study how different modifications will affect the reliability level for the three functions, presented above, and how much the original reliability will be affected by different modifications.

5.3.1. Data Collection

Most reliable calculations of PFD is achieved when sufficient amount of data from one source are available, preferably site specific data. Due to various restrictions, this is not possible. Therefore, laboratory (vendor) data or data from generic sources are often used in determination of SIL for an SIF. Figure 19 illustrates the compromise that has to be made between the need for failure data and the relevance of the data. The generic data is more available, but it is also less relevant for the component under consideration

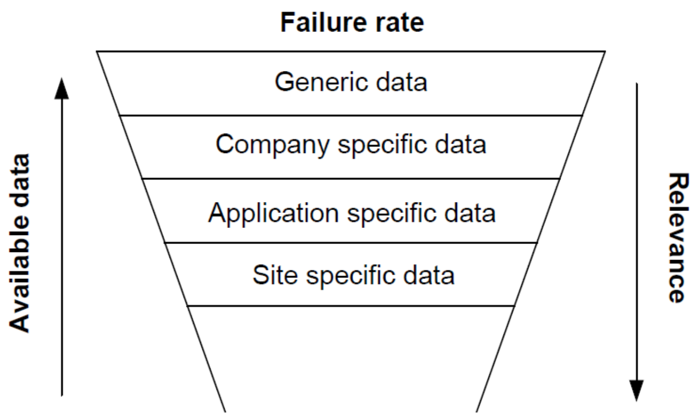


Figure 19: Failure rate data, availability and relevance (Hauge, Håbrekke, & Lundteigen, 2010).

Data from generic sources are often based on operational experience from a number of installations and a number of comparable equipment types. The generic data reflects some kind of average expected field performance for different types of components. It can therefore be argued that using generic data can often be considered as a fairly robust approach in reliability quantification. (Hauge et al., 2010). It is important to keep in mind that due to lack of field experience, generic data do not exist for new type of equipment, and only vendor data is available. This data is often based on laboratory testing, in some cases also field experience. Compared to generic data, data from vendors often show a "significantly" higher reliability for components. (Hauge et al., 2010).

Since the main objective of this thesis is to observe how different modifications affect the reliability of the F&G system, it is appropriate to use the combination of vendor and generic data. Generic data will be mainly gathered from table A.3 in OLF 070. For components where generic data is not available, data will be gathered from vendors.

5.3.2. Model selection

Since the components either functions or not, the F&G-system is assumed to have a static behavior. The focus of the assessment is on how different modification may affect the original PFD, an advanced model is thus not necessary. Due to the complexity of the assessment, a reliability block diagram (RBD) is considered as a suitable model for this case. A RBD shows the functional blocks of the system in a sequential and/or parallel structure, and describes the dependencies between components necessary for the system to carry out its intended functions. These functional blocks describe the configuration of components, making it easier to calculate the overall reliability. This model makes it easy to identify how to achieve a specific function. Another advantage with this method is that it may be used as input for other analysis methods. This model is however only useful when reliability values for the component in the system are known.

5.3.3. Calculation approach

The formulas presented below are approximations and should not be interpreted as absolutely correct. They are rather intended to capture the main contributors to PFD.

5.3.3.1. Single failure

Based on the information presented in appendix A, the following approximate formula for a single component (1-out-of-n) may be applied.

$$PFD_{1oo1} \approx \lambda_{DU} * \frac{\tau}{2}$$

Where λ is used to express the reliability of simple items and components, measured in units of time, such as failures per million hours. Failure rate for dangerous undetected (DU) failures are expressed by λ_{DU}. Dangerous undetected failures may occur at any time and can only be discovered by inspection and proof tests. Performing a proof test is the only method to discover the failures which cannot be revealed by diagnostic measures. The time interval between proof tests is represented by τ (in hours).

For identical components in parallel system, the formula may be written as:

$$PFD_{1ooN} = \frac{(\lambda_{DU}\tau)^N}{N+1}$$

5.3.3.2. Common cause failure (CCF)

To increase the reliability/ and or availability of a system, such as SIS, redundancy is often introduced. Unfortunately, the intended gain in system reliability can be considerably reduced due to common cause failures (CCF). A CCF is a failure where two or more (redundant) components fail of the same cause, occurring simultaneously or within a rather short time interval (Hauge et al., 2010). For common CCF the PFD for an M-out-of-N system can be calculated from:

$$PFD_{MooN} = \beta * \lambda_{DU}\frac{\tau}{2}$$

The standard beta-factor model, consisting only of a parameter, β, is the most commonly used CCF model; is the preferred model in IEC 61508. This factor indicates the fraction of failures of a single component that causes both components of a redundant pair to fail “simultaneously” or within a short time interval. A limitation of the standard model is that it does not reflect the different voting configurations of the system. Hence, the same result is obtained for e.g. 1oo2, 2oo3 and 1oo5 voting systems (Hauge et al., 2009). In order to make a comparison between voting meaningful, there should be different $\beta's$ for different voting configurations (OLF-070, 2004). To reflect this OLF-070 proposes the use of the multiple beta factor model upon which the PDS method is based on. This model introduces a configuration factor C_{MooN} that distinguishes between the effects of various voting configurations. For a system with an M-out-of-N configuration the β-factor is represented with.

$$\beta_{MooN} = C_{MooN} * \beta$$

C_{MooN} is then a modification factor for various voting configurations, and β is the factor which applies for a 1oo2 voting. By using this model, the parameter β is maintained as an essential parameter whose interpretation is now entirely related to a duplicated system. Furthermore, the effect of voting is introduced as a separate factor, independent of β (Hauge et al., 2009). Typical values of β-factor for different components can be found in OLF-070, table A.3. These apply to dangerous undetectable random hardware failures. CCF configuration factors for typical voting configurations can be found in PDS method handbook 2009, and are presented below.

Table 2: Numerical values for CCF of a MooN voting (Hauge et al., 2009)

Voting M/N	**C_{MooN} - factor**				
	N=2	**N=3**	**N=4**	**N=5**	**N=6**
M=1	1	0.5	0.3	0.21	0.17
M=2	-	2.0	1.1	0.7	0.4
M=3	-	-	2.9	1.8	1.1

The approximate formula used for quantification of common cause contribution to PFD for an M-out-of-N is can now be written as:

$$PFD_{MooN} \approx C_{MooN} * \beta * \lambda_{DU} * \frac{\tau}{2}$$

5.3.3.3. Approximation formulas for calculation of the PFD

In this case, confirmed fire/gas will initiate several automatic actions. To reduce the number of false alarms; m-out-of-n voting configuration is applied. To reflect the different voting configurations for the F&G detection system, it is appropriate to include common cause contribution (C_{MooN}) to PFD. The formula for common cause contribution does not include the contribution from independent failures. Since field equipment may have relatively high failure rates, contribution from independent failures cannot be neglected and should therefore always be estimated (Hauge et al., 2009). By combining common cause failure contribution with the contribution from independent failures, formulas for different voting logics can be constructed as shown in table below.

Table 3: Simplified PFD formulas PDS (Hauge et al., 2009)

Voting	*PFD calculation formulas*		
	Common Cause contribution		**Contribution from independent failures**
1oo1	-		$\lambda_{DU} * \frac{\tau}{2}$
1oo2	$\beta * \lambda_{DU} * \frac{\tau}{2}$	+	$\frac{(\lambda_{DU}\tau)^2}{3}$
2oo2	-		$2 * \lambda_{DU} * \frac{\tau}{2}$
1ooN; N=2,3,…	$C_{1ooN} * \beta * \lambda_{DU} * \frac{\tau}{2}$	+	$\frac{(\lambda_{DU}\tau)^N}{N+1}$
MooN, M<N; N=2,3,…	$C_{MooN} * \beta * \lambda_{DU} * \frac{\tau}{2}$	+	$\frac{N! * (\lambda_{DU}\tau)^{N-M+1}}{(N-M+2)! * (M-1)!}$
NooN; N=1,2,3…	-		$N * \lambda_{DU} * \frac{\tau}{2}$

The first term presents the contribution to PFD from common cause failures. For voted configurations this will often be the main contributor to the total PFD. In the second term, the contribution from independent failures is given. For a MooN voting we get a contribution if at least N-M+1 of the components fail within the same test interval. For NooN voting configurations, the PFD equals the sum of independent failure contributions (Hauge et al., 2009).

5.3.3.4. *Calculation example*

To achieve a low alarm for confirmed fire, a 2-out-of-3 configuration for the HC gas detection is applied. What is the PFD for a single component and for the whole configuration, assuming twelve months between each proof-test, the β –factor is 0.05 and that the λ_{DU} is $0.132 * 10^{-6}$?

Based on the information from Table 2 and Table 3, the PFD for a single component and for the whole configuration is:

Example

$$\boldsymbol{PFD_{1oo1}} = \lambda_{DU} * \frac{\tau}{2} = 0.132 * 10^{-6} * \frac{8760}{2} = \mathbf{5.782 * 10^{-4}}$$

$$\boldsymbol{PFD_{2oo3}} = C_{2oo3} * \beta * \lambda_{DU} * \frac{\tau}{2} + (\lambda_{DU}\tau)^2$$

$$= 2.0 * 0.05 * 0.132 * 10^{-6} * \frac{8760}{2} + (0.132 * 10^{-6} * 8760)^2$$

$$= 5.782 * 10^{-5} + 1.38 * 10^{-6} = \mathbf{5{,}915 * 10^{-5}}$$

As seen from the calculation above, the main contribution to the PFD is from common cause failures. Furthermore, it can be seen that the $\mathrm{C_{MooN}}$ factor clearly has an impact on the calculated PFD.

5.4. Calculation of the original PFD

To be able to compare the result before and after the modification, the first thing to do is to calculate the original PFD. All PFD calculation will be based on the data presented in appendix E

5.4.1. Heat detection

Confirmed fire signal is generated when one heat detector in the room is activated. Safe state for the detection function is achieved when a signal is sent from the F&G node.

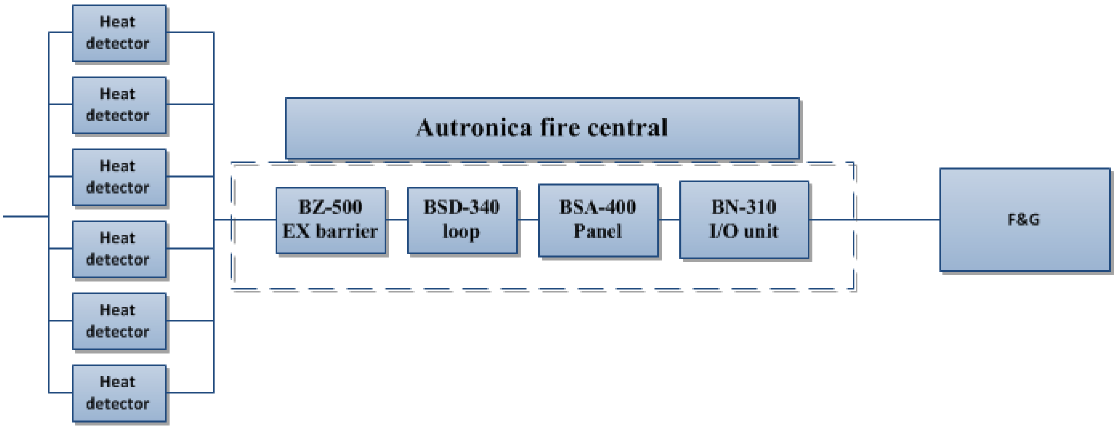


Figure 20: RBD for heat-detection.

Heat detection calculations

$$PFD_{fire\ central} = \mathrm{PFD}_{\mathrm{BZ-500}} + \mathrm{PFD}_{\mathrm{BSD-340}} + = \mathrm{PFD}_{\mathrm{BSA-400}} + \mathrm{PFD}_{BN-310} = 1{,}21 * 10^{-3}$$

$$\boldsymbol{PFD_{total} = PFD_{detectors} + PFD_{fire\ central} + PFD_{F\&G} = 5,60 * 10^{-3}}$$

5.4.2. Fire-water (Deluge) function

The system consists of four main fire pumps, where one pump is in stand-by mode while the other pump is on maintenance in each pump room. This means that only two pumps are available at a time, one in each room. According to the C&E, safe state is achieved when both deluge A and deluge B are activated.

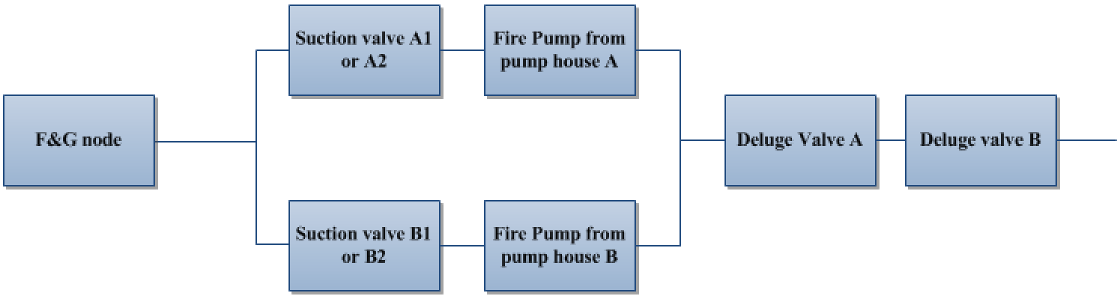


Figure 21: RBD for fire-water (Deluge) function

Comment: it is assumed that the suction valve has the same properties as a deluge valve. The fire pump comprises: electric motor and generator, fire water diesel engine and fire water pump. Based on the method for the parallel system presented in (Häger, 2004) , the reliability of the system may be written as:

FW-Deluge function

$$PFD_{total} = \left[\left(PFD_{suction\ valve\ A} + PFD_{fire\ pump\ A}\right) * \left(PFD_{suction\ valve\ B} + PFD_{fire\ pump\ B}\right)\right] + PFD_{F\&G} + PFD_{deluge\ valve\ A} + PFD_{deluge\ valve\ B} = \mathbf{2,54 * 10^{-2}}$$

5.4.3. HVAC function

According to the C&E chart, all dampers and fans have to close before safe state is achieved. Illustration below shown that both HVAC ducts have to close, meaning that exhaust/intake dampers with the associated fans have to shut down in both ducts before the system is considered to be in a safe state.

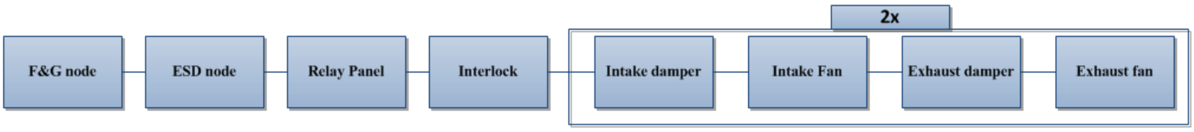


Figure 22: RBD for HVAC function.

Comment: in calculations below, interlock is considered as a standard industrial PLC. In addition, the interlock function is only considered once in the calculations below, such that if the interlock is functioning, all fans will be closed. The reliability data for the HVAC fans were not available in the OLF-070, PDS and OREDA databases. The value is therefore assumed, see appendix E

HVAC-function

$$\boldsymbol{PFD_{total}} = PFD_{F\&G} + PFD_{ESD-Node_{(including\ I\ O)}} + PFD_{relay} + PFD_{interlock} + 2 * \left(PFD_{intake\ damper} + PFD_{(intake\ fan)} + PFD_{exhaust\ damper} + PFD_{exhaust\ fan}\right) = \mathbf{6,88 * 10^{-2}}$$

5.5. Modifications

This sub-chapter presents typical modification projects that will be used to demonstrate the effect the modifications has on the calculated PFD.

5.5.1. Typical modifications to a F&G-system

Some other typical modification projects that are performed in the offshore oil and gas industry are:

- Most typical modifications are replacement of old or failed components.
- Adjustments of time intervals for functional tests
- Deluge system is updated upon introduction of new leak sources.
- Installation of an additional HVAC duct.
- Installation of new equipment, followed by connection to the F&G system.
- Temporary equipment.
- Installation or upgrade of a control rooms.

5.5.2. Results of the modifications to the original system

Based on the typical modifications presented above several modifications will be conducted and the associated PFD will be calculated. The calculation will be conducted in excel and the results will be presented in a table for each function. This table will show the modification, the calculated PFD and how much the original PFD is changed. Keep in mind that these results are limited to the changes in the calculated PFD; other aspects are not considered during this case. They will however, be included in the discussion in the next chapter.

5.5.3. Heat detection function

The original PFD was calculated in chapter 5.4.1

The original PFD: $\mathbf{5,60 * 10^{-3}}$

Table 4: Modifications to heat detectors

Modification (heat detectors)	PFD (modification)	Change in the calculated PFD
Increasing the components failure rate by a factor of 100	6,54E-03	9,40E-04
Maintenance time interval is changed from half year to • each second year	5,63E-03	3,00E-05
Increasing components failure rate by a factor of 100 adjusting the test interval each year	8,46E-03	2,86E-03
Installing a new detector (1oo7)	5,60E-03	0
Changing the voting configuration to 1oo2	5,66E-03	6,00E-05
Changing the voting configuration to 1oo1	6,69E-03	1,09E-03
Test each second year and 1oo3 configuration	5,60E-03	0
Components failure rate is increased by 10 and 1oo1 voting configuration	1,65E-02	1,09E-02

The 1oo6 voting configuration makes the system robust against typical modification. Even if the voting configuration or test interval is altered, the reliability is barely affected. The reason is the high reliability of heat detectors (gas detectors have higher failure rate). When reliability of the components decreases, the PFD increases. One should keep in mind that even if the calculated PFD is not altered, other aspects may be. Another important aspect which should be considered is that these six detectors cover the whole room, meaning that some areas are governed by only one detector.

5.5.4. Fire-water and deluge

The original PFD was calculated in chapter 5.4.2.

Original PFD: $2{,}54 * 10^{-2}$

Table 5: Modifications to the deluge function.

Modifications Deluge	PFD (Modified)	Change in the calculated PFD
Test interval: 2180 Test interval: 8760	1,49E-02 4,58E-02	-1,05E-02 2,04E-02
An extra deluge valve is installed 3oo3 • 3oo3 and 8760 • 3oo3 and 2180	3,55E-02 6,64E-02 2,01E-02	1,01E-02 4,10E-02 -5,30E-03

As seen from Appendix E, the deluge valves have a low PFD. Therefore, installing a new deluge valve to achieve a safe state for the room will result in a higher PFD value. Adjusting the test intervals will also affect the PFD.

5.5.5. HVAC function

The original PFD was calculated in the chapter 5.4.3

Original PFD: $6{,}88 * 10^{-2}$

The results for typical modification to HVAC are given below.

Table 6: Modifications to the HVAC function

Modification (HVAC)	PFD (modified)	Change in the calculated PFD
Fire damper test time is each half year • Each year	1,01E-01 1,65E-01	3,22E-02 9,62E-02
HVAC fan are tested each half year • Each year	7,31E-02 8,19E-02	4,30E-03 1,31E-02
Electric fans failure rate is increased by a factor of 10	1,08E-01	3,92E-02
Both dampers and fans are tested each half year	1,05E-01	3,62E-02
Removing a HVAC duct	5,06E-02	-1,82E-02
Installation of a third HVAC duct	8,69E-02	1,81E-02
Installation of a fourth HVAC duct	1,05E-01	3,62E-02

HVAC are not a part of the F&G function in OLF, and a required SIL is therefore not specified. The HVAC- function in this thesis consists of two HVAC ducts, each including several critical components. The results show that adjusting the test time interval for these components have a big impact on the calculated PFD. Installation of additional HVAC ducts is a typical modification in modification projects. The results show that the PFD will also be affected by these types of modification.

5.6. Summary

The main purpose of this chapter was to illustrate how different modifications might affect the calculated PFD. This chapter focused on providing a better understanding for SIS and their SIFS, how PFD is calculated and how systems can be modified.

The results from this case are as expected. Typical modifications may have effect on the calculated value; some modifications more than others. Modifications, such as installation of additional HVAC duct and deluge valve result in higher PFD values. Modifications such as exchange of similar components will not result in any significant changes to the calculated PFD value. However, it is important to keep in mind that these “typical” modifications may affect other parts of the system. In some cases, it may be important to consider the holistic picture. This will be discussed in the next chapter.

Several assumptions were made during the case. Even if the results were mainly used as an input to the discussion it is important to express the introduced uncertainty. Slightly different modifications or use of other data, models or the calculation methods could have resulted in different results. Assumptions and suppositions made during the case are presented in appendix E1.

6. Discussion

The main objective of this thesis is to identify potential pitfalls that may result from poor management of SISs. The pitfalls will then be used to propose a method on how to handle modifications to SIS. Typical pitfalls are presented in this chapter, while the proposed method following in the next chapter.

As mentioned in chapter 1.2, two sub-objectives are presented to contribute to discussion and recommendations for the main objective. The first part of this chapter focuses on the discussion of these sub-objectives, while the second part has a more detailed discussion related to the main objective. The issues to discuss in this chapter are presented below

Table 7: Main issues to discuss

Chapter 6.2	Provide a discussion relating the first sub-objective. The main focus is on: - How typical modifications may affect the calculated reliability. - Using PFD value to express the extent of the modification.
Chapter 6.3	Providing a discussion relating to the second sub-objective The main focus is on: - Available classification.
Chapter 6.4	Providing a discussion regarding the main objectives. The main focus in on: - Updating of documents and analyses. - Impact analysis.

6.1. Introduction

In 2003, Health & Safety Executive HSE – UK conducted an analysis concerning the reason for the failure of safety and control systems. In this analysis 34 incidents were studied, and 56 causes were identified. The results are presented in the figure below. Their findings suggest that the main cause of 20 % of the accidents are caused by control and safety systems were to changes made to the system after the commissioning (meaning changes made to the system after it was put into service). Due to the small sample size, one may say that these results have low statistical significance and therefore should be used with care. Nevertheless, the results give an indication that modification to SIS may lead to dangerous conditions.

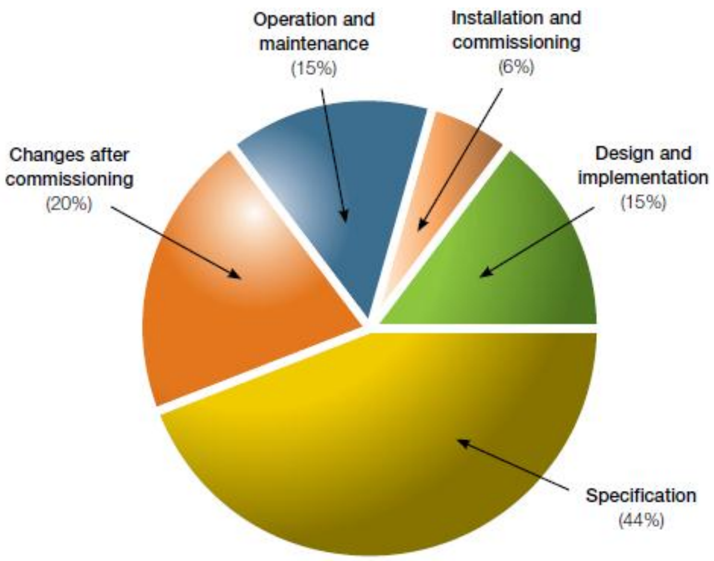


Figure 23: Root causes of failures in control and safety systems (Health and Safety Executive, 2003)

6.1.1. Management of change (MoC)

A MoC is an essential part of the risk management. It is a systematic approach to manage modifications and to reduce the risk that may arise from the modification. MoC is a modification procedure that can be used to ensure consistency, traceability and repeatability. Failure to adequately control, document and communicate changes may lead to unauthorized modifications and deviations from accepted practices and procedures (Houlbrook & Lyon, 2006). History has shown that bad change management process may lead to incidents and accidents. To cover the main issues that might arise during a modification project, a structured management of change method is necessary.

6.2. The first sub-objective.

The purpose of this sub-objective is to:

1) illustrate how typical modifications may affect the calculated reliability level (PFD) for safety instrumented functions (SIFs),
2) and if the calculated values are sufficient to express the extent of the modification.

6.2.1. Case discussion

To provide an adequate coverage of the first part of this objective, a case was presented. The main purpose was to provide a better understanding of:

- Safety instrumented systems (SISs) and their functions (SIFs)
- How the reliability (PFD) is calculated.
- How the system can be modified.
- How much a typical modification might affect the reliability (PFD).

6.2.1.1. SISs and SIFs

The case was used to illustrate three SIFs of a F&G-system Since these systems are often complex, some simplifications were made. SISs may often have many interactions between each other. For instance, in order to shut down the HVAC, a signal has to be sent from the F&G through ESD. These types of systems are often modified and if the changes are not subject to a structured management of change, problems can be introduced.

6.2.1.2. How the PFD is calculated

The PFD may be calculated in two ways, by exact or approximate formulas. In addition, the method in the IEC 61508 standard and PDS method proposes slightly different methods, which may provide different answers. The only difference between these methods is a configuration factor that is presented in the PDS method. Using this factor, results have shown that it has an impact on the calculated PFD. In situations where the CMooN value is higher than 1, the PDS guidelines will result in a higher PFD than using the IEC 61508 guidelines. While if CMooN is lower than 1, PDS will result in a lower PFD than with use of IEC 61508 (Eikeskog, 2012).

Based on the extent and purpose of the case, approximate formulas (including the configuration factor) presented in the PDS method was used. The results from exact and approximate formulas are often similar, but differences may be introduced.

6.2.1.3. Typical modification to the system

This case presented typical modifications that are performed in modification projects to a F&G system. These modifications were used to illustrate the changes in the calculated PFD. The considered modifications were mainly exchange of components, adjustments to test intervals and extension to the safety functions.

The case considered the modifications that are performed on the system. However, as it turns out, the SIS may be affected by sources that may arise as an indirect result of modifications to the facility. Two simple examples are presented below to demonstrate how the SIS may be affected as an indirect result of a modification.

Examples – SIS affected by other modifications

1. Modification to an area where a cabinet is placed in front of a fire detector. This can affect the SIS ability to execute its SIF. That is, to detect the fire.
2. Due to several alterations to an area, the capacity of deluge is no longer enough to protect the equipment

These two simple examples illustrate that the changes from other parts of the facility may be a source of the change, and that the designs prerequisites should always be reflected to obtain a full overview over a modification.

6.2.1.4. *Effect on the calculated PFD*

The modification of safety systems where components are replaced or added-on is of the main interest for this thesis. As seen from the case, the modifications may have different effects on the calculated PFD. Modifications that introduce changes to SIFs, such as installation of additional HVAC or deluge valve, are seen as more critical modifications than replacement of components. This is clear, since these modifications are considered as add-ons, introducing extra components to the PFD calculations.

Even before the illustration, it was evident that the modifications would to some degree have an impact on the calculated PFD value. Based on this, one can state that the results from the case study were expected.

6.2.2. PFD value to express the extent of the modification.

The traditional approach use PFD as a way to demonstrate a SIL level of a function. The higher the SIL, the higher is the expected reliability of the system. If calculations illustrate that the PFD is affected, the modification can be considered as safety significant. These values can therefore provide useful insight for the decision maker. However, the PFD value is a probability. As demonstrated in chapter 2.4:

- The probability could deviate from the future observed outcome distribution.
- The probability of a failure does not describe the consequences of the failure. In general, the consequences may range from negligible to catastrophic. Restricting the

attention to undesirable event means that the extent or significance of the loss is not reflected.

According to Aven (2008), it is important to look beyond assigned probabilities, since the probabilities may camouflage uncertainties. The estimated or assigned probabilities are conditioned on a number of assumptions and suppositions, depending on the background knowledge of the assessor. By varying (sensitivity analysis) the assumptions and suppositions the result may differ. One may therefore see the background knowledge as the frame conditions for the reliability analysis, and the produced probabilities must always be seen in relation to these conditions. This means that different analyst may get different values, if the assumptions and suppositions are different (Abrahamsen & Røed, 2011).

6.2.2.1. Alternative approach

Based on the reasoning above, uncertainties should be taken into consideration more extensively than what is seen in the traditional probabilistic approach. Abrahamsen & Røed (2011) argue that uncertainties should be taken into account before a conclusion is made on the SIL level. This can be done in form of a qualitatively workshop, which is conducted after a PFD is calculated. The main purpose is to reflect the uncertainties in the calculated PFD and the uncertainties that the probability do not capture. They propose an alternative approach, illustrated below.

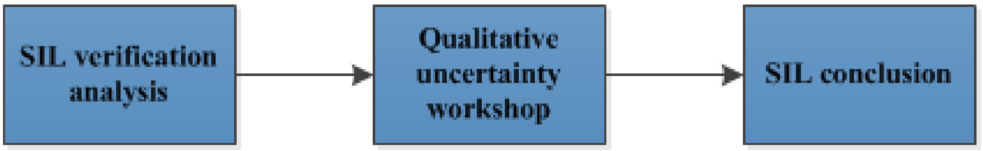


Figure 24: Alternative approach for conclusion of a SIL (Abrahamsen & Røed, 2011)

An example for this approach is presented below:

Example (Abrahamsen & Røed, 2011): SIL verification

Uncertainty not considered:

- PFD calculations imply that the SIL requirement is within the SIL 3 value.

Uncertainty is considered:

- Due to different circumstances, the SIL for the SIF is not considered to be within SIL 3.
- In this case, additional risk reducing measures should be implemented prior to the operation of the SIS. These could be measures in order to reduce the PFD or means to reduce the uncertainty factors to such an extent that an updated evaluation concludes on SIL3.

6.2.2.3. Circumstances of a modification

As argued above, the PFD alone is not enough to capture all aspects of a modification. A review (impact analysis) that considers whether the change affects the system or its functionality is needed. This review should cover the role of equipment in managing hazards, and ensure that the effectiveness of the system is maintained. Another essential element of is this review is to identify any additional hazards or risks that may be introduced inadvertently. For example, a change to an equipment inspection regime may result in that critical items are not checked as often as they should, leading to an increasing likelihood of component failure (Houlbrook & Lyon, 2006).

6.2.3. Summary of the first sub-objective

For this sub-objective, a case was presented. The main purpose of this case was to illustrate how different modifications might affect the calculated PFD, and if the calculated values are sufficient to express the extent of the modification.

A case was used to provide a better understanding for SIS and their SIFS, how PFD is calculated and how SISs can be modified. The case demonstrated that a F&G-system, or any other SISs are subject to continual change and are often rebuild to handle new challenges. The result for the case illustrated that typical modification to SIF, such as additional HVAC and deluge have the potential to effect the calculated PFD, while replacement of components have a negligible effect on the calculated PFD. The results from the case were as expected, however, the focus during the case were only on the calculated PFD value.

Another important issue that appeared from the discussion is that changes to SIS can arise from two main sources:

1. As a direct modification to SIS
2. As the changes to the operating prerequisites. These changes are often introduced as an indirect result from changes to the facility.

During modification project where the modifications may affect the SIS indirectly, interactions are often not fully understood, and/or overlooked. It is therefore necessary that this issue receives more focus.

The focused during the case was on the effect the change has on the calculated PFD. It became apparent in the discussion that these values can provide useful insight for the decision maker; however, it is important to look beyond the assigned probabilities, since the probabilities may camouflage uncertainties. The circumstances should always be assessed in addition to the calculated PFD.

6.3. Categorization of modifications

Categorization of modifications is often used to determine if a formal MoC procedure is necessary. Often, when the modification is considered as RIK or as minor, a strict MoC procedure is not applied. In the oil & gas industry there is a large span of different modification projects, ranging from simple modification. In some projects, a component is replaced with a similar one (RIK). While in others, large parts of the technical system are rebuilt. To determine the necessary level of detail for the modification project it is appropriate to separate the modifications into discrete categories. These categories are used to define the importance of the modification. In several process industries the modifications are divided into two main categories: “minor” and “major”.

6.3.1. Modification in Norwegian Petroleum Safety Authority (PSA) requirements

According to the Norwegian PSA’s requirements, in the event of major rebuilding and modifications of existing facilities, facilities regulations will apply for what is covered by the rebuilding or a modification. Facilities regulation § 82 provides a description on what is considered as a major modification on an offshore facility.

Facilities regulation § 82 (Petroleum Safety Authority Norway, 2010):

"a major modification may be the installation of a new module, major interventions in hydrocarbon-carrying systems or major changes in physical barriers."

Based on the PSA description in § 82, all modification to SIS can generally be considered as "minor", as long as the modification do not affect the hydrocarbon-carrying systems, or introduce a major change to physical barriers. The general description presented by the PSA is the only description regarding categorization of modifications; a clear definition or guideline does not exist. Due to the variety of different modification projects, a clear definition is difficult to achieve.

6.3.2. Alternative description

To simplify decision on how much resources should be spent on a modification projects, alternative description on how to classify modifications of SIS is needed. A clear description is necessary to aid in the categorization of the modification, since it forms the basis for the later stages of the modification process. For an alternative approach, it is proposed that the modifications should be categorized based on their safety significance, meaning their effect on safety. This approach should also consider additional factors:

- The magnitude of the modification.
- The circumstances of the modification.

6.3.2.1. Safety significance

In the nuclear industry, the safety significance and the potential for design errors is taken into account before a modification category is determined. This categorization of safety significance determines the need for safety and risk analysis to be performed and the documents that should prepared. The main information to consider for these safety categories are presented below.

Table 8: Categorization of modifications, based on the safety significance. (Based on:(IAEA, 2012)

Major effect on safety	- The modifications can affect the: • Design function or the ability of the structures. • Systems and components to perform their intended safety functions. - The modification can introduce hazards that have not been previously addressed. - May affect the overall safety analysis, such as QRA.
Significant effect on safety	- Modification may require adaptation of the operational limits and conditions. - Do not affect the overall safety analyses, but might affect documents/analysis on lower level.
Minor effect on safety	- Modification do not affect safety analysis, safety related operational procedures, operational limits and conditions. - No effect on safety system setting.
No effect on safety	- Modification present no hazards and have no impact on safety.

The classification and categorization process for modifications having safety significance should be documented in detail, together with the justification for the proposed safety category (IAEA, 2012).

6.3.3. Summary of the second sub-objective

The purpose of the second sub-objective was to propose a simple alternative approach on how to classify the modifications in a typical SIS modification project

Based on literature study, the PSA provides a description on what should be considered as minor and major modification. According to their description all modifications directly to SIS are considered as minor. It is therefore a need for an alternative description for categorization of modifications. This categorization process should be based on a screening and discussion, at the same time being flexible and allowing for subjective judgment. The main focus should be on the safety significance; however the magnitude and the circumstances of the modification should also be reflected in the categorization process.

6.4. Poor management of change (MoC) in modification projects.

Poor management of change may be result of different reasons. Three of the main reasons are discussed in this sub-chapter:

- Control/ update of documents
- The impact analysis is inadequate
- Indirect changes to SIS

6.4.1. Update of documents and safety analyzes

Norwegian regulations state that the basis for the system shall be continuously updated. This means that one should always be aware of the existing risk picture, and risk reducing measures shall be identified and implemented, to ensure that the risk level is within the acceptable region. This does not necessarily mean that more extensive risk analysis documents, such as QRA should be continuously updated; rather that such documents should be updated, when there is a need for the update. The main argument is that the update should be appropriate for the considered situation. Mostly, it is sufficient to update the less extensive documents. For a SIS it may for instance be enough to update the SRS and SIS loop calculations

Both the SRS and SIS loop calculations (including reliability data dossier) are live design and engineering documents that should be continuously updated (Hauge & Lundteigen, 2008). As mentioned in chapter 3.3, three types of requirements shall be included in the SRS; integrity requirements, required response times and accidental loads. Furthermore, it is necessary to ensure that there is consistency between assumptions and constraints made in the risk analysis and what is stated in the SRS. The reason for this is to ensure that no modification should affect the facilities ability to operate safely in accordance with the assumptions and intent of the design. In situations where the assumptions and constraints change, it has to be clarified and the document should be updated when appropriate (Hauge & Lundteigen, 2008). In some situations, it can be sufficient to update the risk analysis or the SRS. Other times the update of both should be considered. If the SRS is updated, it is important to ensure that the new safety integrity requirements are verified by updating relevant hazard and risk analyses. This can imply that any modification that affects the functional safety or safety integrity requirements may require an update of the hazard and risk analysis (QRA).

Even though the SRS is one of the central elements in the IEC life cycles, this document is often incomplete, not properly implemented or missing in projects where safety is deemed critical (Curtis, 2010). One of the reasons for missing SRS may be that the SIS was designed before the IEC standards were issued and recognized as good engineering practices.

6.4.1.1. Safety Requirement Specifications (SRS) in modification projects

SRS plays a vital role in ensuring the safety of a plant, as well as it is an important resource during modifications. When a SRS is missing, the information may be found in several other documents, for instance in a cause and effect (C&E) diagram. A C&E diagram is used to document the logic associated with the relevant SIFs and may therefore be considered sufficient to form the specifications for SIS. The problem is that the C&E diagrams cannot address all of the requirements of a full SRS specification, and does therefore not provide enough information during modification projects.(Curtis, 2010). Many important SIS aspects, such as details about maintenance (proof-testing), reliability requirements, system specification and other requirements are not mentioned in a C&E.

The IEC 61511 standard does not specify whether the SRS should be a single document, or a collection of documents. According to the requirements presented in this standard, a SRS may be developed by the hazard and risk assessment team or a project team (SafeProd, 2005). Generally, the SRS shall contain the relevant key information for use in specifying, and operating the instrumented safety functions (OLF-070, 2004). The basis for a SRS may be found in other project documents. By combining these documents it is possible to construct a document that comprises the same information as a SRS. Typical documents, not limited to, may be maintenance documents, C&E-charts, different risk analysis (QRA/TRA), functional description of the systems. The result of this may be a “SRS-like” document that includes a list of references (hyperlinks) to all documents providing the necessary information. This will also provide an overview of all documents that may be affected by the modification. If any assumptions and suppositions change, these documents should be updated.

6.4.1.2. Modifications are not properly updated.

For an operating system, especially for the older types, many modifications have been conducted during its lifetime. For instance, if a modification is subject to poor change management, and not properly updated, problems may arise. For the first, several modifications will increase the demand, meaning that the system has to carry out more functions than what was stated in original analyzes. For the second, as a result of this, the reliability of the system and the functions may be lower than what is required. And for the third, the overall risk may be affected.

Experience suggests that poor management of change (update of documents) has repeatedly been found to be a cause of incidents as this has often led to safety systems being operated in conditions different from their original specifications (Ramirez & Walkington, 2012).

6.4.2. Impact analysis

Change to any system has the potential to affect the systems and/or documentation. For SIS, it is important to update how the documents affected the change, to reflect the actual configuration and reliability of the system. The impact analysis is a structured analyses used to identify all possible impacts that the proposed modification might have on the systems and the facility.

Experience suggests that if an impact analysis on the change have not been conducted or been through enough, the safety integrity of the system may potentially be affected. This can also be significantly compounded over time whereby multiple modifications have occurred to SIS without the supporting impact assessment and documentation being available (Ramirez & Walkington, 2012).

If the modification is not subject to a thorough impact analysis, important aspects of the modification may be overlooked. These problems have been thoroughly discussed in the nuclear industry, and some of the main findings are presented below:

6.4.2.1. Modifications are considered to have a small impact on the safety

Experiences from the nuclear industry have shown that modifications considered as having a high impact on safety, generally appear to result in fewer problems than those considered to have small impact. This seems to be as a result of that major modifications are more likely to invoke a structured modification process. The reason for this is that safety significant modifications require higher level of skills and knowledge. Modifications foreseen to have a small impact on safety are often managed with fewer resources, and therefore receive less scrutiny. Operating experience in the nuclear industry has shown that a modification that is not initially considered as safety significant can still lead to safety challenges. For instance, the use of non-identical spare parts in modification may lead to differences in operating or maintaining conditions. Even minor technical modifications may introduce changes to the system, and impact the operators and maintainers roles and tasks (human factors) (NEA, 2009).

6.4.2.2. Cumulative effect of multiple modifications

Even if the modification is recognized and assessed, it is possible that some aspects are overlooked or considered as unimportant (NEA, 2005). There is a possibility that the cumulative effect of several less safety critical modifications may have a major impact on some important parameters in the system. Such problem may arise if multiple modifications are not subject to a detailed impact analysis.

6.4.2.3. Not identified modifications and several

Not-identified modifications to components, materials or spare parts have been shown to cause safety significant events in the nuclear industry (NEA, 2005). Not-identified modification may for instance arise if the manufacturer introduces slightly changes to a component without communicating this to relevant personnel. Change of this component may be categorized as a RIK, when in fact, it is not.

6.4.2.4. Temporary modifications

According to operational experience in the nuclear industry, temporary modifications may have a significant safety impact; this is especially the case for temporary modifications that are considered to have a small impact on safety. Typical problems with such modifications are that it seems as they do not receive the same kind of scrutiny and impact assessment as permanent modifications. This implies that it is easier and less time-consuming to introduce a temporary modification than a permanent change. Even if these modifications are labeled as temporary, they may as time passes become permanent.

6.4.3. Cascade- effect

The SIS can be modified in two ways: by a change to the system and/or change to the operating prerequisites. The effect of the latter on is often not fully understood during modification projects. In modification project where the modifications may affect the SIS indirectly, interactions might be not fully understood, and/or overlooked. It is therefore necessary that this issue receives more focus.

The tricky part of modifying an offshore facility, or any other process facility, is that everything is somehow interrelated. A modification to a system can therefore introduce the need for other modifications. This is often referred to as the cascade-effect. This is especially important to consider during modification for complex systems, where many SISs interfaces with each other and other parts of the facility. In such systems, any modification has the potential to affect the system; if for instance an interaction between components is overlooked.

Modifications, such as installation or upgrade of a control rooms will to some degree introduce a cascade-effect. Due to one modification, other functions may be affected. As a result of this, the description on what is considered as a safe state may be affected, and problems may arise. Due to the extent of these types of modifications, the impact and the effect on safety may be significant. A "cascade-effect" example is presented below. The example considers how a new requirement may introduce a chain of modification.

Example – Modification to a control room

As an example, consider an older control room at an offshore oil rig, where new requirement makes it necessary to install new equipment. A radiator is installed to control the temperature inside the room, this means that a fire source is introduces in a small room, such that a fire detector is necessary. In addition, HVAC duct need to be installed to fulfill the air change requirements and to close the fire dampers in case of a dangerous situation. The installation of new equipment is often followed by connection to the F&G system.

6.4.4. Summary of the main objective

Based on the discussion in this chapter, some of the typical problems that may arise during modification projects where a structured management of change process may be non-existing, insufficient, or lacking are presented below:

- Important documents are not updated.
  - ➢ The actual configuration and the reliability of the system may be different from what is stated in the available documents.
  - ➢ Documents are not properly updated to reflect the actual risk level.

- If an impact analysis on the change have not been conducted or been detailed enough
  - ➢ The safety integrity of the system may potentially be affected.
  - ➢ This effect of several modifications can be compounded over time.
  - ➢ **Modifications considered to have a small impact on the safety may present a threat to safety if some aspects of the modification is overlooked.**
  - ➢ The impact of modifications on SISs are not easy to detect since these system are often complex. Interactions may be overlooked

- The SIS may be modified in two ways: by a change to the system and/or change to the operating prerequisites. The effect of the latter on is often not fully understood during modification projects.
  - ➢ Cascade effect: everything is somehow interrelated and something may be overlooked

- Too much focus on probabilities (PFD)
  - ➢ Uncertainty (circumstances of the modification) is often overshadowed by the calculated PFD.

6.5. Main findings

The main objective of this thesis is to identify potential pitfalls, which may result from poor management of SISs. This sub-chapter presents the main findings of the discussion chapter.

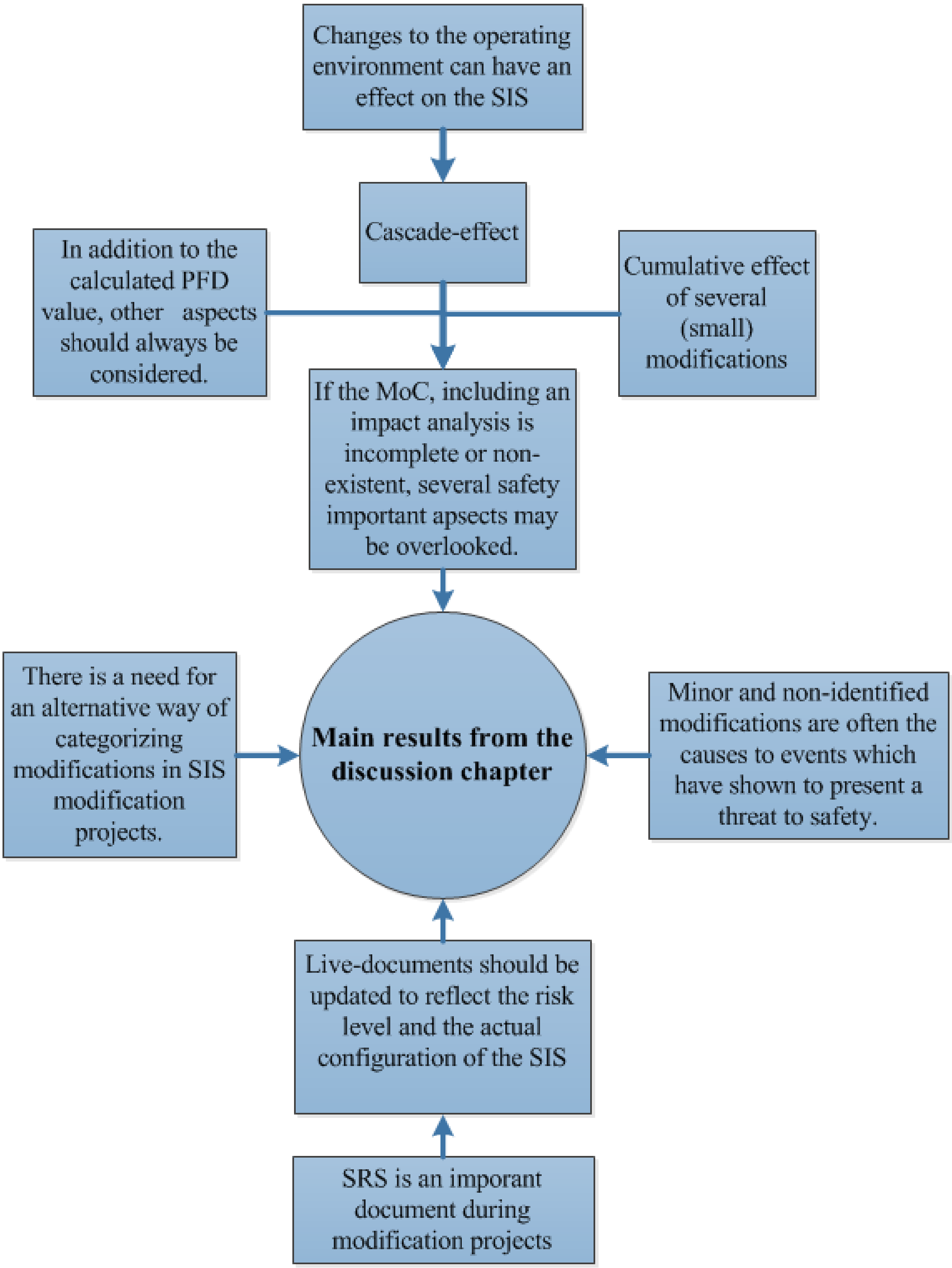

Changes to the operating environment can have an effect on the SIS
Cascade-effect
In addition to the calculated PFD value, other aspects should always be considered.
Cumulative effect of several (small) modifications
If the MoC, including an impact analysis is incomplete or non-existent, several safety important apsects may be overlooked.
There is a need for an alternative way of categorizing modifications in SIS modification projects.
Main results from the discussion chapter
Minor and non-identified modifications are often the causes to events which have shown to present a threat to safety.
Live-documents should be updated to reflect the risk level and the actual configuration of the SIS
SRS is an imporant document during modification projects

Figure 25: Illustration of the main findings

7. Recommendations

Based on the overall impression of the main findings, the likelihood of such events as presented in the main findings can be reduced by a thorough assessment of the proposed modification. To cover all latent functional relationships, failure modes and impacts of modifications a planned an comprehensive installation, testing and commissioning, a structured management of change procedure is necessary (NEA, 2005). The modification process should be structured and well documented. Risk and safety assessments should be included as early as possible in this process, to identify possible problems and implement measures as early as possible. The people involved in these analyses should have a good understanding and knowledge of the problem and the facility as a whole. The classification of modifications will form the scope for the modification process, which later phases will be based on.

This chapter proposes a structured MoC procedure for modification projects that covers the main issues that were identified during the discussion chapter. Before the proposed MoC procedure is presented, SRS in modification projects and the alternative way of categorizing modifications will be presented.

7.1. SRS in modification projects

A basic SRS should have the operating prerequisites and constraints for the system. In a modification project it is necessary to verify these constraints. If the system will be affected by the modification, the change in reliability and other aspects should be studied. By creating a SRS-like document, the project team can get a better overview and understanding of the system. This will simplify the study of the impact the modification has on the system, and contribute to control which documents are affected by the proposed change. To create this document it may be necessary to define system boundaries. This can be done by creating a SRS for each system or each area.

7.2. Categorization of modifications for SIS

Based on discussion in chapter 6, there is a need for a clearer classification of modifications to SIS. A suggestion is to link the alternative descriptions directly to SISs, such that a modification of SISs can be categorized either as a “major”, “medium” or “minor”, independently of the description given by the PSA. From literature study it is evident that the nuclear industry provides the best practice in modification handling. It is therefore proposed to adapt their way of categorizing the modification; with the main consideration to safety significance.

Table 9: Categorization of modifications. Based on(IAEA, 2012)

RIK	This modification presents no hazards and has no impact on safety. This often applies RIK, such that the modification should meet the criteria presented in chapter 4.2.3.2
Minor modification	This modification has minor effect on safety, during and after the modification. The modification does not have any impact on the settings of the safety system.
Medium modification	The modifications include changes to safety related items or systems and in operational approaches and/or procedures. This type of modification will usually necessitate an update of the SIS-loop calculations and SRS. The impact on safety is significant, and the impact on the higher-level documents such as QRA should be minimal (not enough to change the conclusion for the area).
Major modification	Modifications of this type may have a significant impact on the risk level or may involve an alteration of the principles and conclusions on which the design of the system (facility) were based on. These changes may alter the technical solutions implemented for meeting acceptance criteria or lead to changes in the operating rules (Description of what is considered as safe state will be changed).

The proposed approach is to considering the three requirements given in the IEC 61508 (OLF-070): quantitative, semi-quantitative and qualitative requirements. The main factors one should consider for classification are; changes to the PFD, change to the original structure, and changes to what is considered as the safe state.

To aid in the decision making, a checklist consisting of several conditions (questions) may contribute to get a better overview of the impact and safety significance the proposed modification has on the system and the risk level. These questions cover some parts of an impact analysis. The impact on the system, functions and interface with different systems/functions are considered, as well as impact on the human aspect. If any uncertainties arise, a thorough discussion should be performed. The project team, consisting of trained and qualified personnel shall assess the impacts, and make subjective evaluation regarding the severity of the impact. This evaluation can be used as a way to categorize the modification.

Table 10: Checklist for categorization of modifications. Partly based on (Omland, 2008)

Does the solution introduce new technology?	If the modification to the SIS introduces new types of technology or new type of components, the change needs to be analyzed. Until the new component/technology is "proven in use" the change should not be considered as minor.
Will the functionality of the system be affected by the modification?	A review of the change must consider the role of the equipment in managing hazards, and if the effectiveness of the system is maintained. In addition, one should consider hazards or risks that are introduced inadvertently. The discussion should consider the criticality of the modified SIF.
Does the modification affect the existing safety level on the facility, and what is the effect on the safety level?	Any modification that is not "RIK" can to some degree affect the calculated PFD, but seldom change the SIL. Occasionally, the calculation may show that the modification can affect the system to such an extent that the SIL level may change. In situations like this it is important to keep in mind that there is more to a SIL than just the calculated PFD, other aspects such as circumstances and the uncertainty should be discussed.

How will the original assumptions and constraints be affected by the modification?	According to the Norwegian regulations, the basis for the system shall be continuously updated. There should be consistency between assumptions and constraints made in the risk analysis and what is stated in the SRS. If for any reason, the assumptions or constraints change, it has to be clarified and the document should be updated when appropriate. For instance, consider that after several modifications more workers and gas leak sources are introduced in an area. The original number of workers and gas leaks sources in the area formed the basis for risk reduction, and had some influence on the necessary (original) SIL. If the original assumptions and constraints are not updated, the SIL remains the same, however, now there are now more leak sources and humans in the area. The question is then: is the necessary risk reduction still achieved? Introducing more gas leak sources will give a higher probability of a gas leak in that area and introducing more humans will increase the FAR-value. This demonstrates that if assumptions and constraints from the original analysis are changed as a result of the modification; the impact on documents and analysis should be evaluated. The importance of the assumptions and suppositions should be discussed thoroughly before a decision is made on the categorization of the modification.
Will the modification be handled according to relevant standards, such as MoC in OLF-070, or other relevant standards?	Management of change is a central piece in modification handling. This methodology is used to addresses the potential impact of the proposed change. Furthermore, it aids in reducing safety risks, avoiding poorly planned implementations, and that changes are well documented. If the modification is not handled according to the proposed approach in standards (MoC), several aspects may be not identified.

The complexity of the modification (complexity of the system)	The need for competence and technical skills depends on the complexity of the system. Furthermore, the interference between the modified system and the not-modified system should be studied in detail. For instance a change in F&G system may affect the ESD system.
What are the costs associated with the modification?	If the cost associated with the modification is high, it should imply that the modification process should be thoroughly executed.
Will the modification have an impact on human actions (HMI) or practices?	Any changes to work procedures, for instance by increasing or decreasing the time between maintenance should be analyzed and communicated. All relevant personnel that may be affected by the change should be identified.

These questions (issues) do not provide a clear solution whether the modification should be considered as RIK, major, medium or minor. Other aspects should also be considered and a decision making process has to take place, where the entire risk picture is considered. As mentioned several times earlier, one should be careful when the modification is not RIK. Since if the modification is considered as a RIK, a formal MoC procedure is not necessary and the modification can be conducted without any analysis and reviews (S.E.A.L International). Decision on whether the modification should be categorized as RIK is critically important and is the most challenging aspect of managing a change, since an RIK may turn out to be not in-kind. This may have negative consequences.

A minor change will often be a change that can be quickly implemented and do not have a significant impact on SIS. These changes do not require the same rigor as medium and major changes; nevertheless, they should be properly assessed as discussed earlier.

7.3. Management of change procedure

It is important to consider that the changes to SIS are similar to regular changes. Both need a thorough process to control the changes and the impact the changes may have on the system (facility). The flowchart for a modification project presented below is based on the main findings in this thesis and the requirements in ISO-9001.

ISO 9001 is a standard for the quality management of businesses. It applies to the processes that create and control both the products and services an organization supplies. It also prescribes systematic control of activities to ensure that the needs and expectations of the customers are met. This standard is designed and intended to apply to virtually any product or service (ISOQAR). A management of change (MoC) can be seen as a process used to control the modification from the beginning to the end. During this process the modification is the product that has to go through several phases to ensure that the end product satisfies the customer. In ISO-9001, product realization consists of several phases: planning, customer, design and development, provision and control. The main essence of these phases is presented in appendix D. Including these phases in a change management process can contribute to a good MoC procedure.

7.3.1. Presentation of a management of change flowchart

This thesis focuses mainly on the modification projects, where a structured and formal MoC procedure is not present. As seen from the case study and the discussion, modifications may have impact on the SIS in several ways. Even minor modifications may present a threat to safety. A thorough MoC procedure is necessary to ensure that the modifications are carried out and documented in a sufficient manner; this applies for both minor and major modification. The principles for managing modifications in the different categories are the same; the only difference is the depth and breadth of the risk (safety) assessment.

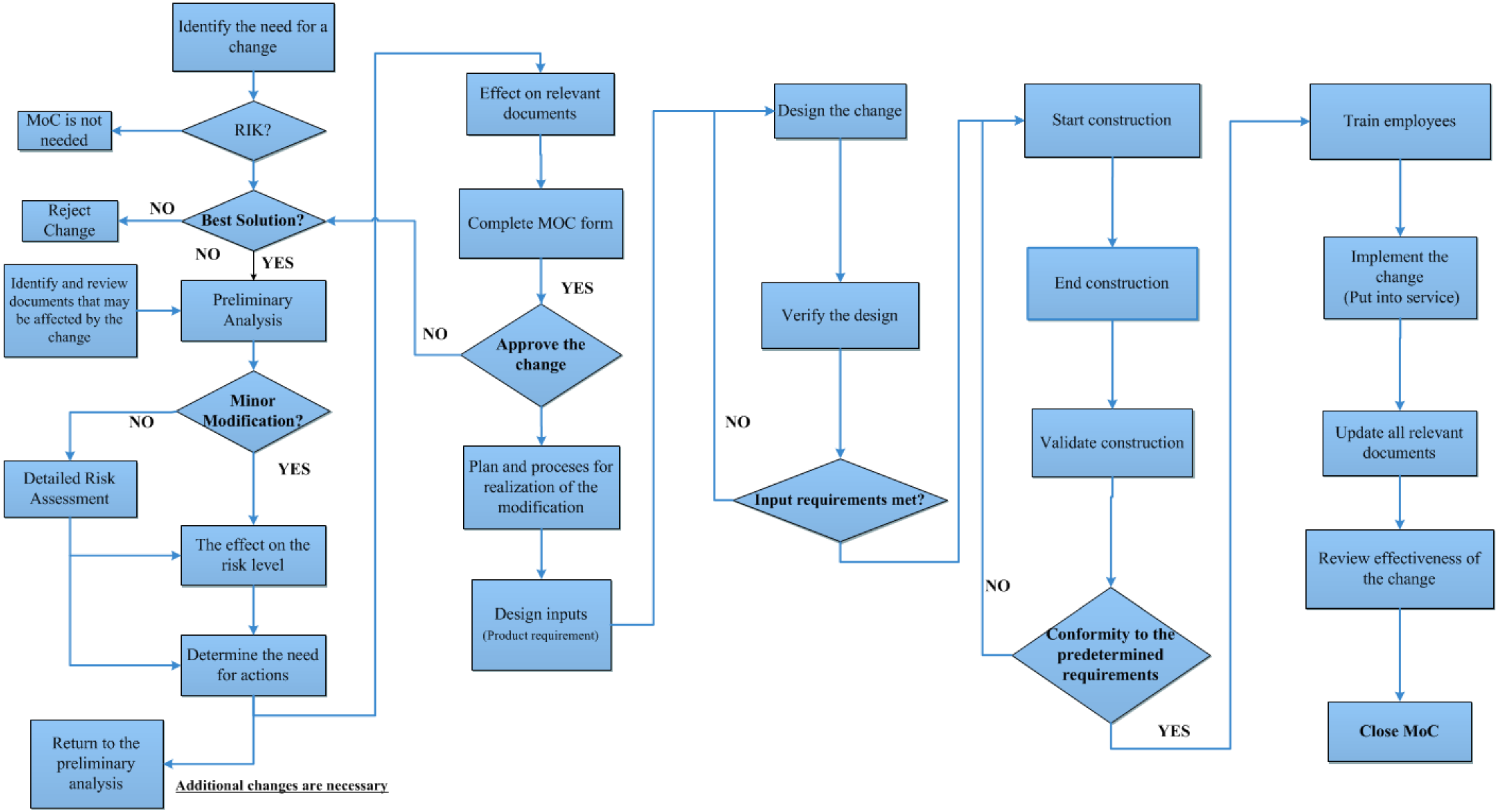

Identify the need for a change
RIK?
MoC is not needed
Best Solution?
NO
Reject Change
NO
YES
Identify and review documents that may be affected by the change
Preliminary Analysis
Minor Modification?
NO
YES
Detailed Risk Assessment
The effect on the risk level
Determine the need for actions
Return to the preliminary analysis
Additional changes are necessary
Effect on relevant documents
Complete MOC form
YES
NO
Approve the change
Plan and proces for realization of the modification
Design inputs
(Product requirement)
Design the change
Verify the design
NO
Input requirements met?
Start construction
End construction
Validate construction
NO
Conformity to the predetermined requirements
YES
Train employees
Implement the change
(Put into service)
Update all relevant documents
Review effectiveness of the change
Close MoC

Figure 26: Proposed procedure for modification projects.

7.3.1.1. Proposal activities

For a number of different reasons, e.g. feedback from operational experience, new technology and new requirements, the need for a change arises. Once it is decided that the modification is not a replacement-in-kind (RIK). The change has to be managed with a formal MoC procedure. The next step is to verify that the proposed modification is the best solution, where one considers cost vs. benefits of the proposed modification(s). When one decides to continue with the proposed modification, the project team may move to the next step.

- The modification should be considered as a not-in-kind replacement, until it can be documented that the change is a RIK. The main purpose is to be sure that the modification is actually an in-kind, at the same time as it reduces temptation in categorizing the change as an in-kind to avoid the whole MoC process.

7.3.1.2. The assessment activities

When a specific modification is determined to be a not-RIK and deemed as the best alternative, full consequences of this modification for the safety of the facility should be reviewed and the physical boundaries of the modification should be defined (IAEA, 2001).

The preliminary assessment, with the use of proposed questions, and detailed assessment of the modified area and/or system will be used as the basis for evaluation of the potential impact associated with the proposed change. This evaluation should be used to classify the modification as minor, medium or major. If the preliminary assessment has clearly demonstrated that the modification have no consequences for safety, during and after the modification, then it can be considered as minor and a more detailed assessment is not necessary. If there are uncertainties on whether the modification is minor or not, a more detailed risk assessment is needed to assess the potential risks. In additional, nuclear industry state that temporary modifications may also be a source of risk. These types of modification are often not subject to an in-depth safety analysis. This is troublesome, since temporary modifications may after a while become permanent, without a sufficient safety assessment. Based on this, it is proposed that temporary modification should go through a detailed risk analysis before implementation.

Before the preliminary analysis is conducted it is necessary to identify and review documents that may be affected by the change. This step is closely related to the creating of the "SRS-like” document. This document will form the background for project work and workshops where the effect the modification has on the risk level will be determined. The data collected during this process will form the basis for the PFD calculations. The PFD should be calculated and the SIL should be verified. As mentioned earlier, the traditional approach lacks any discussion about the uncertainty factors. The calculated PFD values can provide useful insight for the decision maker; however, it is important to look beyond the assigned probabilities, since the probabilities may camouflage uncertainties. The circumstances should always be assessed in addition to the calculated PFD.

Methods such as HAZID may be used to provide a clearer overview over the potential impacts and measures to reduce the risk. A detailed risk assessment often requires higher level of resources, skills and knowledge. When a detailed risk assessment is to be conducted, it is strongly advised to collect all relevant documents that are collected during the preliminary analysis phase. Based on the preliminary/detailed risk assessment, effect on the risk level may be demonstrated. If the risk level is affected, the project team must determine the need for necessary actions; such actions may be derived from a structured HAZID.

As discussed earlier, all modifications should be properly assessed; the cascade-effect of a modification should be understood. If the necessary actions are in form of “a need for other modification”, one should return back to the preliminary analysis. The main purpose of this loop is to assure that all modifications introduced by the cascade-effect are identified.

> The full benefit of a management of change process are only realized when the risk analysis takes a life-cycle approach in identifying issues associated with the change (American Berau of Shipping, 2013).

The ability to recognize and evaluate potential hazards and impact of the change, and proposing effective control measures during a HAZID analysis will depend on the knowledge and experience of the people participating in the analysis. Following steps should take place in a structured HAZID (American Berau of Shipping, 2013):

- Define the change (SIS), including the system, activity and area it is associated with
- Identify every difference between the existing situation and the proposed change.
- Identify the effect of the differences.
- Present necessary actions to control the negative impact associated with the change.

- Use a method to present and characterize the impact of the change.

Further, it should be demonstrated by the detailed risk assessment that the modified facility can be operated safely and complies with the systems specifications and safety requirements. Special consideration should be given to showing the following (IAEA, 2001).

- Compliance with all relevant safety standards and regulations.
- Any adverse effect on the safety characteristics of other systems/areas.
- The modification can be carried out without significantly increasing the risk level.
- The modification will not introduce new hazards.
- Direct and indirect effects on the SISs (facility) should be included in the assessment.
- Potential interactions with other (earlier) changes need to be reviewed.

The main focus in the analysis should be on scenarios where something may go wrong. The proposed actions should be implemented to keep the risk at an acceptable level, during and after the modification. Based on the classification of modification, impact analysis and proposed actions to reduce the risk level, effect on relevant documents should be studied. A major modification will often require update of these documents.

Before the planning for realization phase of the modification(s), the change should be approved. All modifications should have a document describing the main findings of the assessment activity phase. If the solution (modification) is not deemed as acceptable, one should return back and assess if the proposed solution is in fact the best solution. However, if the acceptance can be achieved by a "quick fix", the team should go back to an appropriate phase to assess this solution.

7.3.1.3. Design and implementation planning activities

For modification projects of SIS, planning is an essential part. This part is heavily dependent on the documentation developed in the earlier stages of the safety life cycle, or the development of SRS-like document. Often, a more thorough and well-organized documentation makes the task easier for the project group. Implementation plan shall describe issues discovered prior to this phase and how the change will be executed. Specific actions, time limits, and responsibilities for addressing any quality, health safety and environment issues or any negative impact prior to the change being implemented shall be identified.

Thereafter, inputs relating to the products requirements should be determined. As stated in ISO-9001, these inputs should include the functional and performance requirements, applicable internal and regulatory requirements, information from previous similar designs (projects) and other requirements that are essential for the design and development. The outputs should be in a form suitable for verification against inputs.

7.3.1.4. Implementation, testing and commissioning activities.

During verification of the design, activities such as design review may be conducted to verify if the design fulfills the predetermined requirements. If any non-conformities are identified, they should be addressed and the design updated.

Validate construction step will include different commissioning activities to ensure that the system does what it is set out to do. Commissioning is a well-planned, documented, and managed engineering approach, to the start-up and turnover of facilities, systems, and equipment to the end-user. This results in a safe and functional environment that meets established design requirements and stakeholder expectations (Blackburn, 2012). A well-documented commissioning approach can offer a traceable verification process. During commissioning activities several pre-commissioning activities such as Factory Acceptance Test (FAT) and Site acceptance test (SAT) can be performed. FAT are useful in protecting the business aspect of an investment, by testing the equipment or system at the factory, before it is shipped out. This allows the system to be tested and deficiencies corrected in a manufacturing environment before it arrives on-site. SAT on the other hand verifies proper equipment and operation on-site (Blackburn, 2012).

7.3.1.5. Finalization activities

In every modification project, communication to personnel is essential. The reason for this is to ensure that the operation personnel thoroughly understand their task, and that maintenance workers understand how their work can be affected during or after the modification. The change should be properly communicated, an overview of what is being done, the reason it is being done, and what the outcome is expected to be. After the construction is validated, all affected employees should receive necessary training.

After the system is put into service all relevant documents should be updated (the update should be appropriate for the situation). Different documents that are identified during earlier phases may need to be updated to reflect the change. To demonstrate transparency, any modifications to documentation and risk register should be communicated to all relevant personnel.

A modification should not be closed before all influenced instructions and documents are updated. The effectiveness of change should be reviewed and lessons learned should be documented and communicated. If the change is satisfactory, the MoC can be closed.

7.3.2. Comments to the proposed flowchart

After the proposed flowchart has been used, it is important to get feedback on the strength and weaknesses. This should encourage contribution from all involved departments. This can be done during the review of effectiveness of change. Any suggestions for improvements should be assessed, and if appropriate, the flowchart should be updated.

It is acknowledged that the proposed MoC procedure may be seen as comprehensive. This is done to handle the identified issues in chapter 6. This is also of the reasons of the detailed assessment phase in proposed flowchart.

The main purpose of this procedure is to ensure that the modifications to SIS or any other modifications are at under control at all times, and that the safety is not compromised. At the same time ensure that information is traceable during and after the modification. Based on the experience from nuclear industry, most of the modifications that are not properly assessed may have a negative impact on safety. Since the consequences of a poorly executed modification often are unexpected, the modification should be considered as a risk in itself. The project team should be aware of this, and what can occur if the modifications are not given proper attention. They should also understand the potential impact that minor (small) modification may have on the system (facility). The awareness may for instance be improved by collecting and communicating information about earlier modification-related events (NEA, 2005).

7.3.3. Outputs from the MoC process

Typical outputs from the MoC procedure:

- A list of documents which are affected by the change, and if documents need to be updated.
- Final documentation with a:
  - Description of the modifications
  - Why the change were made
  - Description of how the modification will impact the SIS
    - A list over all calculations
    - Change in functional test intervals?
  - Details of all changes to the configuration
    - List of changed equipment
  - Hazards that might be affected by the modification
  - Descriptions and results of tests during commissioning
  - Approvals collected along the way.

8. Closing comments

This chapter presents the main findings of this thesis and proposes some topics for further work.

8.1. Main objective

The main objective of this thesis was to identify potential pitfalls that may have resulted from poor change management of SISs. Furthermore, the goal was to propose a method on how to handle modifications of SIS in modification projects.

The main findings are presented in chapter 6.5. These are based on the discussion, suggesting that modifications (e.g. minor, temporary and not-identified) not properly assessed may have a negative impact on safety. In addition, the necessary documents should be updated to reflect the actual configuration of the SIS (facility) and the actual (true) risk level after the modification. To cover the latent functional relationships, failure modes and impacts of modifications, the modification process should be well structured and documented. Several risk and safety assessments should be included as early as possible, to ensure that potential problems can be identified, and appropriate measures implemented as early as possible.

The proposed flowchart for management of change is presented in chapter 7.3.1. This chart is based on the identified issues and the requirements in the ISO-9001 standard. The main purpose of this flowchart is to ensure that the modifications to SIS, or any other part of the facility are under control, and that the safety is not compromised. Furthermore, the procedure aids in providing traceability, during and after the modification process.

8.1.1. Sub-objective 1

The purpose of the first sub-objective was to illustrate how typical modifications may affect the calculated reliability level (PFD) for safety instrumented functions (SIFs), and if the calculated values sufficiently expresses the extent of the modification.

A case was used to provide a better understanding for SISs and their SIFs. The case also presented how PFD can be calculated and how the system can be modified. This case demonstrated that a SIS is subject to continual change and is often rebuilt to handle new challenges. The result for the case illustrated that typical modification to SIF, such as additional HVAC and deluge valves have the potential to effect the calculated PFD, while replacement of components have a negligible effect on the calculated PFD. The results from the case were as expected, however, the focus during the case were only on the calculated PFD value. As it became apparent in the discussion, PFD values can provide useful insight for the decision maker; however, it is important to look beyond the assigned probabilities, since the probabilities may camouflage uncertainties. The circumstances of a modification should always be assessed in addition to the calculated PFD.

The case only focused on the modification to the SIS. However, the SIS may also be modified by a change to the operating prerequisites. The effect of this is often not fully understood during modification projects. Everything on an offshore platform is somehow interrelated. Therefore, one modification to SIS or any other part of the facility can trigger a need for other modifications, introducing the so-called cascade-effect.

8.1.2. Sub-objective 2

The second sub-objective was to propose a simple alternative approach on how to classify the modifications in a typical SIS modification project. The main findings suggest that there is a need for an alternative description for categorization of modifications. This categorization process should be based on screening and discussion of the modification, at the same time being flexible and allowing for subjective judgment. The main focus should be on the safety significance; however, the magnitude and circumstances of the modification should also be reflected in the categorization process.

Chapter 7.2 presents an alternative approach for classification of modifications in SIS modification projects. Based on the classification used in the nuclear industry, the modification should be categorized with the main consideration to the safety significance. To aid in the categorization, a checklist consisting of several conditions (questions) is presented. The main purpose of this checklist is to get a better overview of the impact the proposed modification has on the system and risk level. These questions focuses on the impact the modification can have on the humans, system, functions and interface with different systems/functions. The results from the assessment should be evaluated before the modification is categorized.

8.2. Further study

This thesis is written within a limited period of time with limited resources and information. Some topics for further research are presented below.

Human errors in modification projects.

Due to the scope limitations, the human factor was only barely mentioned in this thesis. It is however deemed as necessary to study how, and why human errors may arise during the modification projects. The impact these errors may have on the modification should be studied throughout all phases of a modification project.

Lack of data for components in reliability calculations.

During this thesis and discussion with my supervisors, an additional objective arose.

> Identify a method on how to handle components that are not SIL-certified or lack the necessary reliability data in reliability calculations.

This is an issue that often arises during modification projects. Appendix F presents an attempt to provide an adequate method. The discussion from the appendix suggests that it doesn't matter if a component is citified or not, as long as it can be demonstrated that the safety function achieves the necessary risk reduction. To calculate the risk reduction, the components failure (historical) data are needed. Furthermore, as pointed out the best approach to handle components without reliability data is the use of a structured expert judgment. Since their data is mainly based on their background knowledge, the strength of this knowledge has to be expressed

It is proposed that a more thorough literature study should be carried out regarding this objective. Based on the literature study, one could provide a simple step by step approach that can be used in reliability calculations. That approach should incorporate the uncertainty dimension (strength of knowledge), as discussed in appendix F.

9. Referance

Abrahamsen, E. B. (2012). *Lecture notes in Reliability Analysis (MFDT).* University of Stavanger (UiS).

Abrahamsen, E. B., & Røed, W. (2011). A new approach for verification of safety integrity levels. *Reliability & Risk Analysis: Theory & Applications, 2*, 20-27.

American Berau of Shipping. (2013). Management of Change for the Marine and Offshore Industries.

Aven, T. (2006). *Pålitelighets- og Risikoanalyse* (4 ed.). Oslo: Universitetsforlaget AS.

Aven, T. (2008). *Assessing Uncertainties Beyond Expected Values and Probabilities*. England: John Wiley & Sons Ltd.

Aven, T. (2010). *Misconceptions of risk*. United Kingdom: John wiley & Sons Ltd.

Aven, T. (2013). Practical implications of the new risk perspectives. *Reliability Engineering and System Safety, 115*, 136-145.

Blackburn, T. D. (2012). Commissioning Fundamentals and a Practical Approach *PDHonline Course*.

Curtis, I. (2010). Safety in numbers. *European Oil & gas*(9), 12-15.

DSME. (2008a). Functional Description Fire & Gas System Internal document.

DSME. (2008b). Functional Description of Fire Water and Deluge System. Internal document.

DSME. (2010). Functional Description of Emergency Shutdown System. Internal document.

Eikeskog, K. H. (2012). *Reliability as a decision tool against SIL requirements.* (Master), University of Stavanger (UiS).

Emerson Process Management. (2005) SIS 302 - Modification.

Flage, R., & Aven, T. (2009). Expressing and communicating uncertainty in relation to quantitative risk analysis. *Reliability & Risk Analysis: Theory & Applications, 2,* 9 - 18.

Garland, R. W. (2012). An Engineers's Guide to Management of Change. *CEP*, 49-53.

General Monitors. (2008). SIL 103: SIL Certification Demystified.

Hauge, S., Håbrekke, S., & Lundteigen, M. A. (2010). Reliability Prediction Method for Safety Instrumented Systems – PDS Example collection, 2010 Edition: SINTEF.

Hauge, S., & Lundteigen, M. A. (2008). Guidelines for follow-up of Safety Instrumented Systems (SIS) in the operating phase: SINTEF.

Hauge, S., Lundteigen, M. A., Hokstad, P., & Håbrekke, S. (2009). Reliability Prediction Method for Safety Instrumented Systems - PDS Method Handbook, 2010 Edition. Trondheim: SINTEF.

Health and Safety Executive. (2003). *Out of control - Why control systems go wrong and how to prevent failure* (Second ed.).

Houlbrook, A., & Lyon, A. (2006). Robust Change management - A solution to Many Drilling-Related Accidents and incidents. *Society of Petroleum Engineers*.

Häger, D. (2004). *Implementation of Sil requirements in the Norwegian offshore industry.* (Master), University of Stavanger, Stavanger.

IAEA. (2001). Modifications to Nuclear Power Plants - Safety Guide *Safety Standards Series* Vienna: International Atomic Energy Agency.

IAEA. (2012). Safety in the Utilization and Modiciation of Research Reactors *Specific Safety Guide*. Veinna: International Atomic Energy Agency Safety Standards.

IEC-61508. (2004). Functional safaty of electrical/electronic/programmable electronic safety-related systems. General requirements *IEC 61508-1*. Geneva: International Electrotechnical Commission.

IEC-61511. (2003). Functional safety - Safety instrumented systems for the process industry sector *IEC-61511*. Geneva: International Electrotechnical Commission.

IMCA. (1999). Guidance for the management of change in the offshore environment: The International Marine Contractors Association.

ISO-9001. (2008). Quality management systems requirements: International Organization for Standardization (ISO).

ISOQAR, A. Quality Management Standard- What is ISO 9001? Retrieved 07.05.2013, from http://www.alcumusgroup.com/isoqar/standards/iso9001-quality/

Janbu, A. F. (2009). *Treatment of Uncertainties in Reliability Assessment of Safety Instrumented Systems.* (Master), NTNU, Trondheim.

Jin, H., Lundteigen, M. A., & Rausand, M. (2012). Uncertainty assessment of reliability estimates for safety-instrumented-systems. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*.

Lundteigen, M. A. (2009). *Safety instrumented systems in the oil and gas industry - Concepts and methods for safety and reliability assessments in design and operation.* (Ph.D.), NTNU, Trondheim.

Lundteigen, M. A. (2010). Lecture on reliability analysis of Safety Instrumented Systems - An overview of methods and practises.

Lundteigen, M. A. (2011). *Lectures notes on reliability of safety critical systems.* NTNU.

Lundteigen, M. A., & Rausand, M. (2006). *"Assessment of hardware safety integrity requirements". Proceedings of the 30th ESReDA seminar.* NTNU, Trondheim.

NEA. (2005). Safety of modifications at nuclear power plants - The role of minor modifications and human and organisational factors: Nuclear energy agency - Committee on the safety of nuclear installations.

NEA. (2009). The Role of Human and Organisational Factors in Nuclear Power Plant Modifications *CSNI Technical Opinion Papers*: Nuclear Energy Agency.

Nilsen, T., & Aven, T. (2003). Models and model uncertainty in the context of risk analysis. *Reliability Engineering and System Safety*, *79*, 309 - 317.

NORSOK-S-001. (2008). Technical Safety. Lysaker: Norsk Standard.

Norsok-S-005. (2005). System control diagram. Lysaker: Norsk Standard.

OLF-070. (2004). Application of IEC 61508 and IEC 61511 in the Norwegian petroleum industry. *The Norwegian Oil and Gas Industry Association.* Norway.

Omland, A. (2008). *Challanges in relation to the aplication of IEC 61509 standard and OLF 0-70 and approach regarding modification of F&G detection system on offshore installation.* (Master), University of Stavanger.

Petroleum Safety Authority Norway. (2010). Regulations relating to design and outfitting of facilities, etc. in the peroleum activities (The Facility Regulations).

Ramirez, E. C., & Walkington, J. (2012). *Effective Risk Reduction in Processes: the Contribution of Functional Safety Management Systems*. Paper presented at the Safety Control Systems Conference – IDC Technologies.

Roest, I. (2002). Expert opinion - Use in practice: Vrije University Amsterdam.

S.E.A.L International. Management of Change - NPC Training Program - Student Handout.

SafeProd. (2005). Safety Requirements specification Guideline

Shinkle, J. (2001). Management of Change - An Essential Process Safety Management Element.

Shönbeck, M. (2007). Introduction to reliability of safety systems.

Skjong, R., & Wentworth, B. H. (2001). *Expert Judgement and Risk Perception*. Paper presented at the Offshore and Polar Engineering Conference, ISOPE, Stavanger.

Sklet, S. (2006). Safety barriers: Definition, classification, and performance. *Journal of Loss Prevention in the Process Industries, 19*, 494–506.

Sveen, A. O. (2012). Lecture on Safety Systems by Siemens. NTNU.

Yozallinas, J. (2013). So What’s an Impact Analysis? Retrieved from http://www.exida.com/index.php/blog/indepth/so_whats_an_impact_analysis

Zio, E., & Aven, T. (2013). Industrial disasters: Extreme events, extremely rare. Some reflections on the treatment of uncertainties in the assessment of the associated risks. *Process Safety and Enviromental Protection, 9*, 31-45.

10. Appendix

A. Probability of failure on demand (PFD)

Information in this chapter is gathered from Aven (2006)

For low demand SIS it is common to calculate the average probability of failure on demand (PFD_{avg}). PFD_{avg} is a reliability measure which is often used for systems (e.g. F&G) that take action when dangerous conditions are detected (Abrahamsen, 2012).

Availability

Availability, A_i, can be defined as "the long run proportion of time that component *i* is functioning /operating". Availability is slightly different from reliability in that it takes repair time into account. The difference may be described by an unreliable component that can be quickly repaired when it fails, thus achieving higher reliability.

$$Availability\ A(t) = \frac{Functioning\ time\ (mean\ time\ to\ failure\ )}{Total\ time\ (mean\ time\ to\ failure + mean\ down\ time)} = \frac{MTTF}{MTTF + MTTR}$$

Unavailability

The average unavailability is the mean proportion of time the system is not function. That is why PFD_{avg} sometimes is called the mean fractional dead time (MFDT). The unavailability at time t, A(t),denotes the probability that a system will fail to respond adequately to the demand at time t.

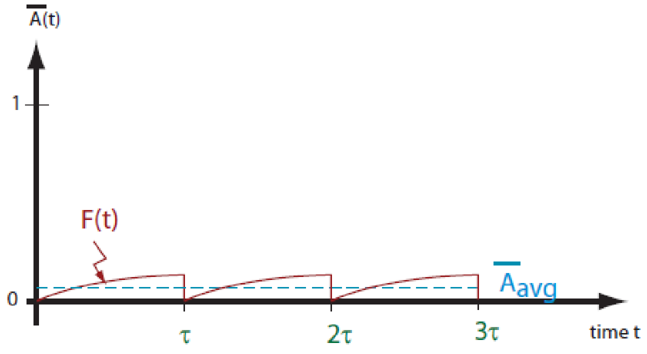


Figure 27: The unavailability of a periodically tested system (Lundteigen, 2010).

In most applications we are not interested in the PFD as a function of time. It is sufficient to know the long run average value of PFD (PFDavg). Because of the periodicity of $\bar{A}(t)$, the long run average PFD is equal to the average value of $\bar{A}(t)$ in the first test interval (0,τ)

$$\bar{A}(t) = P(a\,failure\,has\,occured\,at, or\,before\,time\,t) = P(T \leq t) = F(t) = PFD(t)$$

For A SIS, PFD$_{avg}$ is the unavailability of a safety function. It describes the probability that the safety function has already failed before the demand to act occurs, meaning that the system/function cannot be activated on demand. Assuming exponential distribution, PFD$_{avg}$ can be calculated by:

$$PFD_{avg} = \lambda * MTTR$$

$$\lambda = \frac{Number\ of\ failures}{Total\ operating\ time}$$

Failure rate, λ, is measured in units of time, such as failures per million hours. Failure rate is often used to express the reliability of simple items and components. It is also frequently used to express the reliability of particular functions, for example the dangerous failure rate of a safety system

PFD$_{avg}$

The PFD may be calculated by using approximation or exact formula. The results of these two formulas are often similar, but minor differences may be introduced (Abrahamsen, 2012). These two formulas are based on the assumption that the units lifetime distribution is exponential with constant failure rate, meaning that lifetime distribution does not depend on the age of the unit. It is also assumed that after a test or repair the unit is as good as new. Additional assumptions are:

- The components are put in operation at time t = 0
- The system is tested and, if necessary, repaired after regular time intervals of lengths
- The time required to test and repair the item is considered to be negligible.

Exact formula for PFD$_{avg}$

The average probability of failure on demand is mathematically expressed by:

$$PFD_{avg} = \frac{\int_0^\tau F(t)dt}{\tau} = 1 - \frac{\int_0^\tau R(t)dt}{\tau}$$

$F(t)$is the lifetime distribution, τ is the time between tests and $R(t)$ is called the survivor function, also described as $1 - F(t)$

Approximation formula for PFD$_{avg}$

$$F(t) \approx \sum_{J=1}^{k} \prod_{i\in Kj} q_i(t) = \sum_{J=1}^{k} \prod_{i\in Kj} \left(1 - e^{-\lambda t}\right) \approx \sum_{J=1}^{k} \prod_{i\in Kj} (\lambda_i t)dt$$

$$1 - e^{-\lambda t} \approx \lambda_i t \;\; for\ small\ values\ of\ \lambda_i t\ , typically < 0.1$$

Based on this, the approximate formula of PFD (MFDT) can be described by (Aven, 2006):

$$PFD_{AVG} \approx \frac{\int_0^\tau \Sigma\Pi(\lambda_i\, t)dt}{\tau} = \frac{\int_0^\tau \Sigma(\Pi\lambda_i)\mathrm{t}^{|\mathrm{kj}|}\mathrm{dt}}{\tau} = \frac{\Sigma(\Pi\lambda_i) \int_0^\tau {t_i}^{|kj|}dt}{\tau} \qquad = \frac{\Sigma(\Pi\lambda_i)\left[\frac{t^{|kj|+1}}{|kj|+1}\right]_0^\tau}{\tau}$$

$$= \frac{\Sigma\frac{1}{|kj|+1}\Pi(\lambda_i)t^{|kj|+1}}{\tau} = \sum\nolimits_{i=1}^{M} \frac{1}{|kj|+1} \prod\nolimits_{i\in j} (\lambda_i\tau) \rightarrow PFD_{avg} \approx MFDT$$

$$PFD_{avg}(MFDT) \approx \sum_{J=1}^{M} \frac{1}{[K_j]+1} \prod_{i\epsilon j} (\lambda_i\tau)$$

- M is the total number of minimal cut sets
- K_j is the jth minimal cut set
- $|K_j|$ is the number of components in the minimal cut set K$_j$
- $\tau\ is\ the\ length\ of\ the\ test\ interval$
- $i \in K_j$ is the components in minimal cut set j

B. Semi-quantitative and qualitative SIL requirements

Semi-quantitative requirements

Semi quantitative requirements are called the architectural requirements. These requirements are expressed by the hardware fault tolerance (HWFT). The HWFT are determined by whether the system A or B is considered, the specified SIL and the safe failure fraction (SFF).

Table 11: Hardware fault tolerance for on type A and B safety related subsystems. Adapted from:(IEC-61508, 2004)

Safe Failure Fraction (SFF)	**Hardware Fault Tolerance (HWFT)**					
	Type A			**Type B**		
	0	1	2	0	1	2
<60%	SIL 1	SIL 2	SIL 3	_	SIL 1	SIL 2
60% - 90%	SIL 2	SIL 3	SIL 4	SIL 1	SIL 2	SIL 3
90% - 99%	SIL 3	SIL 4	SIL 4	SIL 2	SIL 3	SIL 4
>99%	SIL 4	SIL 4	SIL 4	SIL 3	SIL 4	SIL 4

SFF is the fraction of failures which can be considered as “safe”. These failures are detected by diagnostic tests or if the failure does not result in loss of the safety function (IEC-61508, 2004). SFF may be interpreted as a measure of the inherent safeness of a component, that is, to what extent the component responds in a safe way when a failure occurs (Lundteigen, 2009).

$$SFF = \frac{\lambda_{SD} + \lambda_{SU} + \lambda_{DD}}{\lambda_{SD} + \lambda_{SU} + \lambda_{DD} + + \lambda_{DU}}$$

Table 12: Different failure types.

Failure types	
Safe Detectable ($\boldsymbol{\lambda_{SD}}$)	This represents safe and detectable failures. These types of failures do not affect the functionality of a SIF.
Safe Undetectable ($\boldsymbol{\lambda_{SU}}$)	This represents safe but not detectable failures. These types of failures do not affect the functionality of a SIF.
Dangerous Detectable ($\boldsymbol{\lambda_{DD}}$)	This represents dangerous but detected failures. For these types of failure the SIF cannot be performed, but the system will quickly go into the safe state.
Dangerous Undetectable ($\boldsymbol{\lambda_{DU}}$)	This represents dangerous failures that can only be revealed by proof tests. For this type of failure the SIS cannot perform the intended SIF on demand.

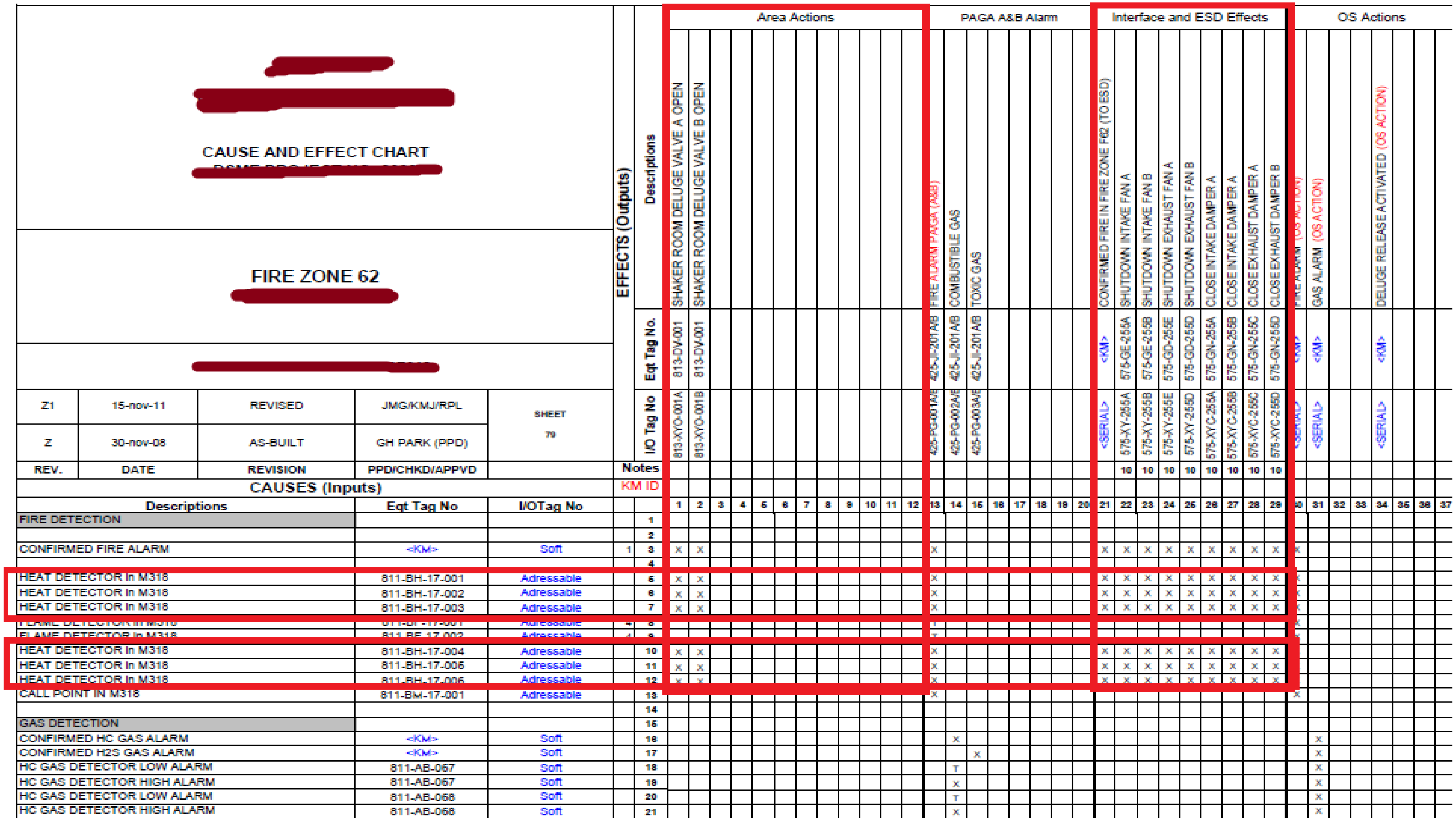
Type A components are characterized by well-defined failure modes, completely determined behaviors and sufficiently documented performance by field experience data. Type B components do not meet one or more of these requirements. Components having application software are often considered as type B (Lundteigen, 2009).

The HWFT describes the way a subsystem behaves in a failure mode and is dependent on the voting structure of the hardware. Without redundancy, the safety function cannot be performed if one failure occurs. If redundancy is introduced, the system can carry out its intended function even when a failure occurs. If two elements are operating redundantly (1oo2-voting structure), one may fail without affecting the performance of the safety function. Since one failure does not impact the safety function, the HWDT is 1.

Qualitative requirements

These requirements concerns which techniques and measures one should use to avoid and control systematic faults. Systematic faults are faults in hardware and software introduced during specification, design, operation or maintenance/testing, which may result in a failure of the safety function under certain conditions (OLF-070, 2004).

C. Cause & Effect chart used in the case



[redacted]

[redacted]

CAUSE AND EFFECT CHART

[redacted]

FIRE ZONE 62

[redacted]

[redacted]

Z1	15-nov-11	REVISED	JMG/KMJ/RPL	SHEET 79
Z	30-nov-08	AS-BUILT	GH PARK (PPD)	
REV.	DATE	REVISION	PPD/CHKD/APPVD	

					Area Actions												PAGA A&B Alarm								Interface and ESD Effects									OS Actions							
			EFFECTS (Outputs)	Descriptions	SHAKER ROOM DELUGE VALVE A OPEN	SHAKER ROOM DELUGE VALVE B OPEN											FIRE ALARM PAGA (A&B)	COMBUSTIBLE GAS	TOXIC GAS						CONFIRMED FIRE IN FIRE ZONE F62 (TO ESD)	SHUTDOWN INTAKE FAN A	SHUTDOWN INTAKE FAN B	SHUTDOWN EXHAUST FAN A	SHUTDOWN EXHAUST FAN B	CLOSE INTAKE DAMPER A	CLOSE INTAKE DAMPER A	CLOSE EXHAUST DAMPER A	CLOSE EXHAUST DAMPER B	FIRE ALARM (OS ACTION)	GAS ALARM (OS ACTION)			DELUGE RELEASE ACTIVATED (OS ACTION)			
				Eqt Tag No.	813-DV-001	813-DV-001											425-JI-201A/B	425-JI-201A/B	425-JI-201A/B						<KM>	575-GE-255A	575-GE-255B	575-GD-255E	575-GD-255D	575-GN-255A	575-GN-255B	575-GN-255C	575-GN-255D	<KM>	<KM>			<KM>			
				I/O Tag No	813-XYO-001A	813-XYO-001B											425-PG-001A/B	425-PG-002A/B	425-PG-003A/B						<SERIAL>	575-XY-255A	575-XY-255B	575-XY-255E	575-XY-255D	575-XYC-255A	575-XYC-255B	575-XYC-255C	575-XYC-255D	<SERIAL>	<SERIAL>			<SERIAL>			
			Notes																							10	10	10	10	10	10	10	10								
CAUSES (Inputs)			KM ID																																						
Descriptions	Eqt Tag No	I/OTag No			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37
FIRE DETECTION				1																																					
				2																																					
CONFIRMED FIRE ALARM	<KM>	Soft	1	3	X	X											X								X	X	X	X	X	X	X	X	X	X							
				4																																					
HEAT DETECTOR In M318	811-BH-17-001	Adressable		5	X	X											X								X	X	X	X	X	X	X	X	X	X							
HEAT DETECTOR In M318	811-BH-17-002	Adressable		6	X	X											X								X	X	X	X	X	X	X	X	X	X							
HEAT DETECTOR In M318	811-BH-17-003	Adressable		7	X	X											X								X	X	X	X	X	X	X	X	X	X							
FLAME DETECTOR In M318	811-BF-17-001	Adressable	4	8													T																	X							
FLAME DETECTOR In M318	811-BF-17-002	Adressable	4	9													T																	X							
HEAT DETECTOR In M318	811-BH-17-004	Adressable		10	X	X											X								X	X	X	X	X	X	X	X	X								
HEAT DETECTOR In M318	811-BH-17-005	Adressable		11	X	X											X								X	X	X	X	X	X	X	X	X								
HEAT DETECTOR In M318	811-BH-17-006	Adressable		12	X	X											X								X	X	X	X	X	X	X	X	X								
CALL POINT IN M318	811-BM-17-001	Adressable		13													X																	X							
				14																																					
GAS DETECTION				15																																					
CONFIRMED HC GAS ALARM	<KM>	Soft		16														X																	X						
CONFIRMED H2S GAS ALARM	<KM>	Soft		17															X																X						
HC GAS DETECTOR LOW ALARM	811-AB-067	Soft		18														T																	X						
HC GAS DETECTOR HIGH ALARM	811-AB-067	Soft		19														X																	X						
HC GAS DETECTOR LOW ALARM	811-AB-068	Soft		20														T																	X						
HC GAS DETECTOR HIGH ALARM	811-AB-068	Soft		21														X																	X						

D. Short summary of ISO 9001 requirements.

During the planning of the product realization phase

During this phase, the organization shall plan and develop the processes needed for product realization. When appropriate, the organization shall determine: the objectives and requirements, the need for processes and documents, verification, validation and monitoring processes. In addition, when appropriate, records needed to provide evidence that the resulting product meet requirements (ISO-9001, 2008).

Customer-related processes

During customer-related processes phase the organization shall determine the requirements related to the product and review these requirements and establish good communication with the customer (ISO-9001, 2008).

Design and development

This phase shall consist of several stages. The first stage considers the design and development, where the organization shall plan and control the design, and further development of the product. The second stage considers the design and development inputs and outputs, where the inputs relating to the products requirements should be determined and necessary documentation maintained. These inputs should include the functional and performance requirements, applicable internal and regulatory requirements, information from previous similar designs (projects) and other requirements that are essential for the design and development. The outputs should be in a form suitable for verification against inputs. In the next stage, systematic reviews shall be performed in accordance with planned arrangements to evaluate the ability of the results to meet the requirements. Any problems shall be identified and the necessary actions should be proposed. To ensure that the design and development outputs have met the design and development input requirements verification shall be performed in accordance with planned arrangements (ISO-9001, 2008).

Purchasing

During the Purchasing phase the organization shall ensure that the purchased product conforms to specified purchase requirements. Any supplier should therefore evaluate based on their ability to supply product in accordance with the organizations requirements (criterias).

Any product from suppliers shall be verified by inspection or other activities that the product meets the specified purchasing requirements (ISO-9001, 2008).

Product and service provision

This phase includes planning, production and service provision under controlled conditions; using quality management plans to control the production process (ISO-9001, 2008).

Control and monitoring

Control of monitoring and measuring equipment phase main task is to determine the conformity of the product to the predetermined requirements. The organization shall establish processes to ensure that monitoring and measurement ban be carried out in a manner that is consistent with monitoring and management requirements (ISO-9001, 2008).

E. Data dossier for the case

Component	λ_{DU}	τ	β	**CCF**	**PDF single**	**PFD total**	**Comments**
Heat detector - 1oo6	5,00E-07	4380	0,05	- 9,31E-06	1,10E-03 1,58E-17	1,10E-03 9,31E-06	
ESD/**F&G** – incl. I/O (single PLC)	1,00E-06	8760	0,01		4,38E-03	4,38E-03	
Standard industrial **PLC**	5,00E-06	8760			2,19E-02	2,19E-02	
Circ. Breakers /relay (6kV–10kV)	2,00E-07	17520	-	-	1,75E-03	1,75E-03	
Fire damper	7,30E-06	2190	0,03		7,99E-03	7,99E-03	β –value from PDS handbook
HVAC fan (failure to stop)	1,00E-06	2190	-	-	1,10E-03		This is an assumed value.
Fire water - Fire pump (fail to start) - Fire water diesel engine - Electric generator - Electric motor Fire water 1oo2	 - - - -	 - - - -	 - - - -	 - - - -	 9,40E-04 1,90E-03 1,40E-03 1,40E-03	5,64E-03 3,18E-05	
Deluge valve incl. actuator, solenoid and pilot valve, fail to open - Suction valve (1oo2)	4,70E-06	4380	0,03	- 3,09E-04	1,03E-02 1,41E-04	1,03E-02 4,50E-04	$\beta - value$ from PDS handbook
Autronica **fire central** - BZ -500 - BSD-340 - BSA-400 - BN-310	 2,00E-09 8,00E-09 2,60E-07 6,88E-09	 8760 8760 8760 8760			 8,76E-06 3,50E-05 1,14E-03 3,01E-05	1,21E-03	Vendor data. Available in appendix E2

E1. Uncertainty in the case

Model uncertainty:

In the sub-chapter about model selection, several assumption and reason for assumptions were mentioned. Furthermore, the constructed RBDs are based on documents that do not contain all relevant information about the design of the system; only the main components are presented. The RBDs are thus simple illustrations of the real system. However, as mentioned earlier, the model must always be seen in the light of the purpose of the analysis and the purpose.

Uncertainties related to the calculation approach:

In this case the calculation of PFD were based on approximated formulas (presented in the PDS method), including the configuration factor, CMooN. This factor has an impact on the calculated PFD, and will in several cases provide different PFD then what is calculated by the method presented in IEC 61508.

To simplify the calculations for the FW-deluge function, the presented approach were not used and the CMooN factor was omitted from the calculations. This has some impact on the calculated PFD value.

Data uncertainty

The assessment in this thesis has mainly used generic data from OLF-070, vendor data is used for the fire central. The data from OLF-070 is often used in PFD calculations. However, it may be argued that this data is too conservative for some components, giving a higher failure rate comparing with vendor data. One important aspect to consider is that the OLF-070 provides typical values up-to 2004, thus the data may be considered as old for some components.

A sensitivity study, performed by Janbu (2009), considered two generic values form OLF-070 and OREDA for a level transmitter. Her study showed that two different generic values may lead to significant differences between the estimated unavailability. One can therefore say that the main data uncertainty stems from the confusion on which data one should use in the reliability calculations.

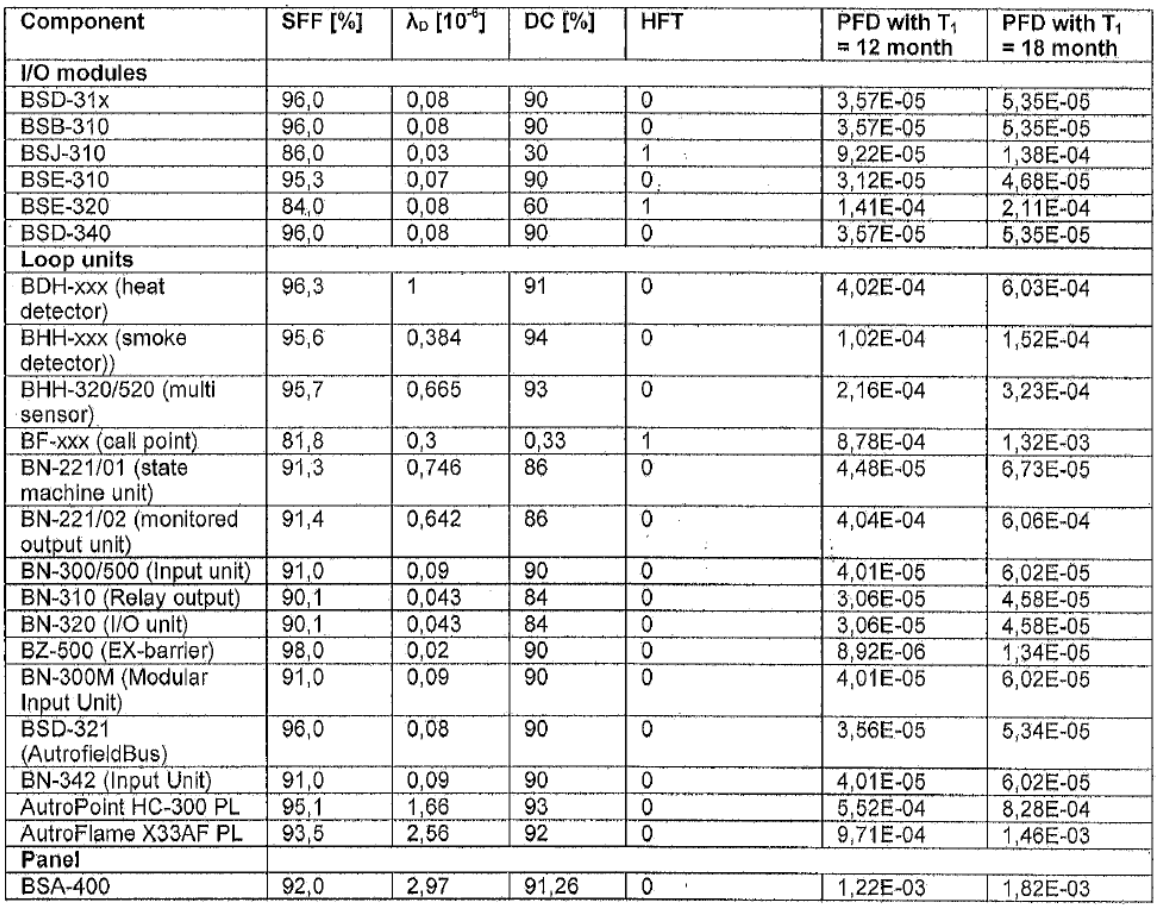
The reliability data for HVAC fans are not available in OLF-070, PDS or OREDA database. An assumption is therefore made to consider the fan as an electric motor with additional parts and the test time is similar to fire dampers. Changes in this components reliability will have a big impact on the total PFD for the HVAC function.

Completeness uncertainty:

This case study contains what is called known uncertainty, meaning that some issues are deliberately omitted from the analysis to simplify the representation and calculations. The reason is that the scope of the assessment is to study how different modifications affect the reliability level, the exact representation and calculation method are thus not necessary. Nevertheless, the result may have been different if the exact representation were used.

Due to lack of knowledge about the fire central system, only heat detectors were modified.

E2. Data for Autronica Fire Central



Component	SFF [%]	λ_D [10^{-6}]	DC [%]	HFT	PFD with T_1 = 12 month	PFD with T_1 = 18 month
I/O modules						
BSD-31x	96,0	0,08	90	0	3,57E-05	5,35E-05
BSB-310	96,0	0,08	90	0	3,57E-05	5,35E-05
BSJ-310	86,0	0,03	30	1	9,22E-05	1,38E-04
BSE-310	95,3	0,07	90	0	3,12E-05	4,68E-05
BSE-320	84,0	0,08	60	1	1,41E-04	2,11E-04
BSD-340	96,0	0,08	90	0	3,57E-05	5,35E-05
Loop units						
BDH-xxx (heat detector)	96,3	1	91	0	4,02E-04	6,03E-04
BHH-xxx (smoke detector))	95,6	0,384	94	0	1,02E-04	1,52E-04
BHH-320/520 (multi sensor)	95,7	0,665	93	0	2,16E-04	3,23E-04
BF-xxx (call point)	81,8	0,3	0,33	1	8,78E-04	1,32E-03
BN-221/01 (state machine unit)	91,3	0,746	86	0	4,48E-05	6,73E-05
BN-221/02 (monitored output unit)	91,4	0,642	86	0	4,04E-04	6,06E-04
BN-300/500 (Input unit)	91,0	0,09	90	0	4,01E-05	6,02E-05
BN-310 (Relay output)	90,1	0,043	84	0	3,06E-05	4,58E-05
BN-320 (I/O unit)	90,1	0,043	84	0	3,06E-05	4,58E-05
BZ-500 (EX-barrier)	98,0	0,02	90	0	8,92E-06	1,34E-05
BN-300M (Modular Input Unit)	91,0	0,09	90	0	4,01E-05	6,02E-05
BSD-321 (AutrofieldBus)	96,0	0,08	90	0	3,56E-05	5,34E-05
BN-342 (Input Unit)	91,0	0,09	90	0	4,01E-05	6,02E-05
AutroPoint HC-300 PL	95,1	1,66	93	0	5,52E-04	8,28E-04
AutroFlame X33AF PL	93,5	2,56	92	0	9,71E-04	1,46E-03
Panel						
BSA-400	92,0	2,97	91,26	0	1,22E-03	1,82E-03

Comment:

Vendor data for the fire central provide failure rate in form of rate of dangerous failure, λ_D. This value comprises: rate of dangerous failures that are detected by the diagnostic function, λ_{DD} , and rate of dangerous undetected failures, λ_{DU}. The relationship is expressed by the formula below.

$$\lambda_{DU} = (1 - DC) * \lambda_D$$

Diagnostic coverage factor (DC) expresses the fraction of the dangerous failures which are detected.

F. Not-Certified components and components that lack reliability data

The problem on what to do with components that are not certified or lack reliability data in reliability calculations arose during this thesis. The purpose of this appendix is to conduct a literature study to:

Identify a method on how to handle components that are not certified or lacks the necessary reliability data.

Introduction

On older systems, one often finds components that are not SIL certified or do not have any reliability data. In situation where reliability data are missing for components, they may be omitted from the PFD calculation. The results may therefore be to some extent misleading. This chapter sets out to propose a simple method on how to handle components that are not certified, or without the necessary reliability data.

SIL-certified components

A functional safety certification may be claimed by a product. Product certificates are issued either by the manufacturers or by other independent agencies to show that the appropriate calculations have been carried out and analysis has been completed on a product to indicate that the product is compatible for the use within a system of given SIL. For full IEC 61508 certification, the manufacturers design and quality processes are also involved. However, a full certification does not mean that the product is more reliable, rather that it adds credibility to the manufacturer's products and processes. Therefore, a certification may be seen as a piece of paper that adds credibility to the analysis conducted, the results obtained and the manufacturer's products and processes (General Monitors, 2008).

Every components in the function needs to provide sufficient reliability to achieve the required SIL. It is therefore important to keep in mind that SIL levels apply for safety instrumented functions (SIFs), i.e. the field sensor, the logic solver and the final element, and not for the individual component (even if they are SIL certified). It has therefore more meaning to say that these components are suitable for use within a given SIL environment, but they are not individually SIL rated (architecture plays an important role). This means that the necessary risk reduction may be achieved, even with uncertified components as long as failure rate for the components are available.

Lack of failure rate for components

If data for components are not available, complete calculations cannot be performed. In some cases these components may be neglected to simplify the reliability analysis, giving misleading results. From the literature search, the best approach that can be used to determine the values of the input parameters is the expert judgment.

Expert judgment

Expert judgment has always played a large role in science and engineering. It has in the last years gathered more acceptances and is now recognized as just another type of scientific data. An expert is defined as a person with background in the subject area and who is recognized by others as qualified as an expert in that subject area (Skjong & Wentworth, 2001). Expert judgment is an approach, based on experts training and experience, used to collect knowledge and informed opinions from individuals with a particular expertise. A defining feature is that experts provide subjective probability distribution that summarizes their beliefs about the value for quantity of interest.

In reliability calculations one often finds components that do not have any historical data, thus making it difficult to calculate the reliability. This motivates the use of expert judgment as a source of information in estimating the unknown variables and parameters. In such situations experts process all available information including their background knowledge. An end result of this process may for instance be a failure rate distribution for a component. The use of experts may thus be seen as valuable approach, especially for situations where there is lack of data or when data is not directly relevant. However, their judgments may significantly affect the results (Janbu, 2009). The use of expert judgments may in some cases introduce even more uncertainty. The judgments are based on their background knowledge, which may be wrong, poor or not updated. In addition, expert judgment may be ruled by motivational aspects. The advantages and disadvantages are presented in the table below.

Table 13: Advantages and disadvantages with expert judgment

Advantages	**Disadvantages**
• Estimates may be provided in situations where there is lack of historical data.	• Expert may have poor background knowledge
• Cheap and quick method.	• One expert may dominate
• Relies heavily on expert's knowledge.	• Heuristics and biases may be introduced, meaning that the assessor may unconsciously put too much weight on insignificant factors
• Several experienced people may combine their knowledge.	

If the expert opinion is in quantitative form, it can be considered as “data”(Roest, 2002). When components lack the necessary data, expert judgment may thus be used as a source of data. Their experiences and knowledge may be used to assign a subjective probability in from of a failure rate or a failure rate distribution.

Subjective probability

Experts subjective probability is denoted by P(A|K) to show that this probability is conditional on some background knowledge, K. This probability reflects their degree of belief of the event A to occur based on the available knowledge. There is therefore no uncertainty in the assigned value P(A|K), as this would presume that there was a correct value of the probability. However, the assigned values are dependent on the available knowledge, meaning that if the background knowledge changes, then the probabilities may also be changed. Even so, for a given background knowledge the probability is not uncertain (Aven, 2013). The background information is therefore the main source of uncertainty in subjective probabilities. Since the uncertainties could be hidden in the background knowledge, it has more meaning to say that the assigned values are dependent on the strength of the knowledge, which reflects the “quality” and goodness” of the assigned probabilities. The strength of knowledge can be described by different rationales and implementation procedures. A simple approach that offers practicality and may serve as a screening of uncertainty factors is presented below.

Assessing the strength of knowledge

Uncertainty in the background knowledge needs to be expressed to the decision maker. With the focus on lack of data for components it is sufficient to provide a simple qualitative methodology to access the level of uncertainty. This can be done by expressing the strength of knowledge upon which the failure rate values or distributions are based on.

One possible approach is to use crude rating of the strength of knowledge, where the strength may take three values; weak, medium and strong. Typical conditions to consider are given in table below. Weak knowledge means large or a high level of uncertainty, while strong knowledge means small or low degree of uncertainty (Aven, 2013).

Table 14: Conditions to determine the strength of knowledge ((Flage & Aven, 2009)

Large uncertainty (Weak) **if one or more of the following conditions in are met**	**Small uncertainty (Strong)** **If all conditions are met**
- The phenomena involved are not well understood; models are non-existent or known/believed to give poor predictions.	- The phenomena involved are well understood; the models used are known to give predictions with the required accuracy.
- The assumptions made represent strong simplifications	- The assumptions made are seen as very reasonable.
- Data are not available, or are unreliable	- Much reliable data are available.
- There is lack of agreement/consensus among experts.	- There is broad agreement among experts.
Moderate uncertainty (Medium) **Cases in between strong and weak strength of knowledge**	
- For instance when some reliable data are available, or when the case is well understood, but the models are considered simple.	

This simple qualitative approach does not provide a straight forward answer on whether the strength of knowledge is small, medium or large. Such approaches should be used with care since it is possible to make some adjustments that may change the result. For instance if there is lack of data, one may consider the experts subjective judgment as representative data and the strength is thus no longer weak.

If expert judgment cannot consider as reliable data, the strength of knowledge may be considered as weak, meaning that the failure rate is based on weak strength of knowledge. As seen from the table above the only condition that leads to weak strength of knowledge is that the data are not available, or unreliable. Expert agreement may be obtained by structural methods for expert elicitation. A typical procedure contains disseminating the assessment problem, the data and all other relevant information. The experts are then required to formalize and document their rationale, followed by an interview process where they are asked to defend their rationale. Thereafter, the experts will specify their own distribution by determining quantities. Another alternative is that the experts provide the analysts with necessary information, giving the analysis background for processing and transforming the information to a probability distribution (Aven, 2010). This approach expresses the result in two forms, both quantitative and qualitative. The quantitative form expresses probabilities, probability distributions, estimates, ratings etc. The qualitative gives a description of the assumptions made and provides rationale used in the deduction of the result (e.g. probability distribution).

Summary

The discussion illustrates that whether the components are certified or not does not matter, as long as it can be demonstrated that the safety function achieves the necessary risk reduction. To calculate the risk reduction, the components failure (historical) data are needed. Furthermore, as pointed out in discussion, the best approach to handle components without reliability data is the use of a structured expert judgment. Since their data is mainly based on their background knowledge, the strength of this knowledge has to be expressed. The strength of background knowledge may be assessed by the use of a simple qualitative method. The purpose is to describe the assumptions made and provide the rationale used in the deduction of the result (e.g. probability distribution). To express the strength of knowledge, the conditions stated in table 15 can be used as the starting point for this assessment.

Keep in mind that these conditions should be considered as a whole and not separate. Assessment should also include circumstances and the analysis problem. Traceability is an important part of this approach.