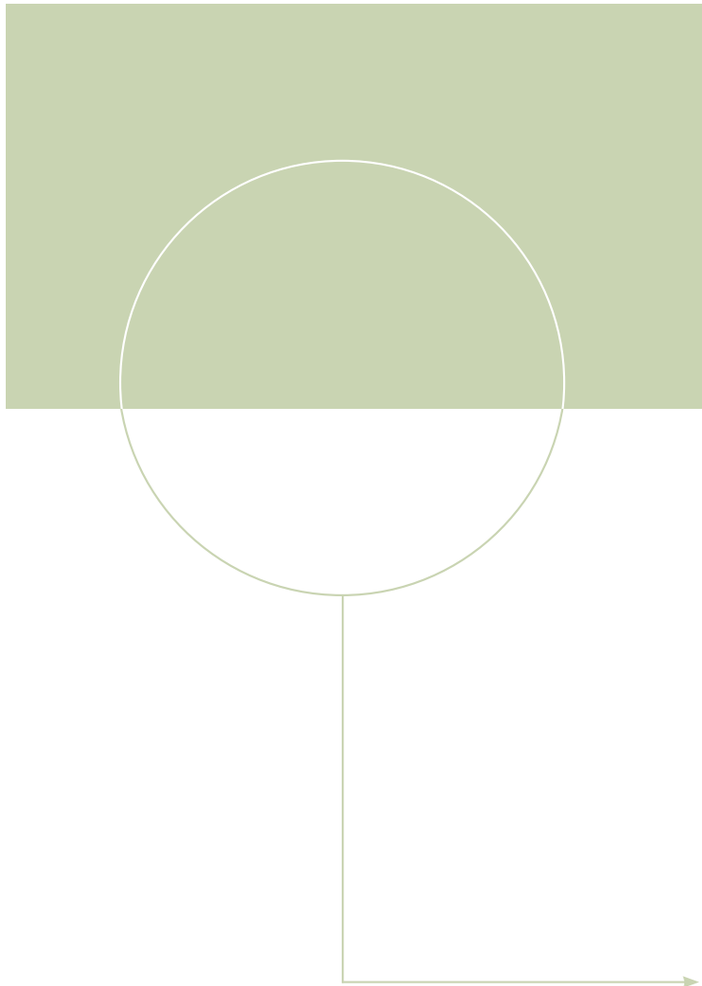


Master's thesis

2019

Gunnar Johannessen

NTNU
Norwegian University of
Science and Technology
Faculty of Engineering
Department of Mechanical and Industrial Engineering

Gunnar Johannessen

Reliability and Safety Assessment of All-Electric Subsea Concepts

June 2019

NTNU
Norwegian University of
Science and Technology

NTNU
Norwegian University of
Science and Technology

NTNU
Norwegian University of
Science and Technology

Reliability and Safety Assessment of All-Electric Subsea Concepts

Gunnar Johannessen

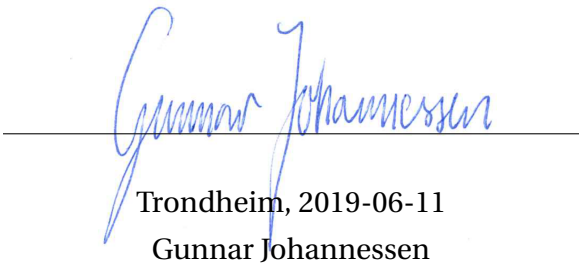
Reliability, Availability, Maintainability and Safety (RAMS)
Submission date: June 2019
Supervisor: Mary Ann Lundteigen

Norwegian University of Science and Technology
Department of Mechanical and Industrial Engineering

Preface

This master thesis was carried out in the spring of 2019, as part of the 2-year Master of Science program, RAMS, at the Norwegian University of Science and Technology. The thesis is written in collaboration with external company Aker Solutions. The topic was proposed by main supervisor Professor Mary Ann Lundteigen and decided in collaboration with Christopher Lassen at Aker Solutions. As part of a summer internship at Aker Solutions, a brief introduction to the all-electric development was made prior to this thesis.

It is assumed that the reader has basic knowledge about safety and reliability assessment similar to NTNU course TPK 4120. It is also considered that the reader has some understanding of subsea production systems, but this is not a requirement.



Trondheim, 2019-06-11
Gunnar Johannessen

Acknowledgment

I would like to thank Professor Mary Ann Lundteigen for great guidance and support throughout this semester. Her insight in both industry and academia has been of great value for this master thesis. I would also like to thank Christopher Lassen at Aker Solutions for the opportunity to collaborate on both the project and master thesis. I am also grateful for valuable inputs from Jone Sigmundstad at Aker Solutions regarding the all-electric project, his knowledge and encouragement has been really inspiring and helpful.

I would also thank my classmates for valuable discussion and inputs, which help to gain better knowledge on various topics within RAMS.

G.J.

Summary

The oil and gas industry investigates to replace existing electro-hydraulic control systems with all-electric solutions for control of subsea valves. The all-electric technology has great potential for utilisation of reservoirs located at greater depths and in longer distances to existing infrastructure. The industry has identified several technological opportunities with all-electric, where lower costs, improved HSE, and reliability are key drivers for the technology.

The objective of thesis is to propose an approach for modelling and elaborate on the reliability and safety performance for all-electric systems. Requirements for design and operation of subsea equipment on the Norwegian Continental Shelf are regulated by the Norwegian Petroleum Safety Authority to ensure that installations are sufficiently reliable. The consequences of an accident in the oil and gas industry might cause serious damage to people, environment and assets, which emphasise the need for reliable barrier systems. The process industry use digitalised safety systems to control and stop the flow of hydrocarbons in the occurrence of hazardous events. The safety system is controlled by using a combination of electric and hydraulic fluids to open and close the subsea valves. By introducing an all-electric control system to challenge the current safety function, the performance needs to be at least as good as the existing electro-hydraulic counterpart.

The Petroleum Safety Authority requires design and implementation of safety-instrumented systems to comply with standards IEC 61508 (2010) and IEC 61511 (2016). These standards present requirements and recommendations for assessment of the safety performance for safety-instrumented systems, both in a qualitative and quantitative manner. Quantitative calculations of the safety performance are based on the expected average downtime within a test interval. Regular proof tests are conducted to verify the functional integrity of the system and detect hidden failures.

The proposed model is based on Petri Net modelling technique, to simulate the lifetime of all-electric actuators and valve system. The model is built in so that a fair comparison to accepted requirements for the safety performance of electro-hydraulic actuators and valve system are made. The system characteristic of an all-electric actuator introduce possibilities for different operational strategies compared to the electro-hydraulic system. Four simulation runs were made with different assumptions about the operational strategy to investigate effects on the average unavailability of the safety system.

The thesis concludes that a safety system with all-electric actuators is compliant with the quantitative requirements in comparison to an electro-hydraulic actuator. There are some uncertainties regarding failure data and assumptions about degraded operation. Further work is recommended to focus on the testing methods that can be utilised in the occurrence of a failure to verify that the risk is sufficiently low.

Sammendrag

Olje- og gassindustrien ønsker å erstatte eksisterende elektrohydrauliske styringssystemer med hel-elektriske løsninger for kontroll av undervannsventiler. Hel-elektrisk teknologi har stort potensial for utnyttelse av reservoarer ved større dybder, med lengre utstrekningsavstander, og med lengre avtandstand fra nye til eksisterende infrastruktur. Olje- og gassindustrien ser flere muligheter med hel-elektrisk teknologi, hvor lavere kostnader, forbedret helse, miljø og sikkerhet, og forbedret pålitelighet er drivere bak teknologien.

Formålet med masteroppgaven er å foreslå en modell og analysere påliteligheten og sikkerhetsytelsen for hel-elektriske systemer. Krav til utforming og drift av havbunnsutstyr på norsk kontinentalsokkel reguleres av Petroleumstilsynet for å sikre at påliteligheten til utstyret er tilstrekkelig. Konsekvensene av en ulykke i olje- og gassindustrien kan føre til alvorlig skade på mennesker, miljø og eiendeler, som understreker behovet for gode og pålitelige barrieresystemer. Prosessindustrien bruker digitaliserte sikkerhetssystemer til å kontrollere og stenge strømningen av hydrokarboner i tilfelle uønskede hendelser inntreffer. Sikkerhetssystemet styres ved å bruke en kombinasjon av elektriske systemer og hydraulikk for å åpne og lukke undervannsventilene. Ved å introdusere et hel-elektrisk kontrollsystem til å overta sikkerhetsfunksjonen, må ytelsenkravet være minst like godt som det eksisterende elektrohydrauliske systemet som brukes i dag.

Petroleumstilsynet krever at utforming og implementering av sikkerhetsinstrumenterte systemer er i overenstemmelse med standardene IEC 61508 (2010) og IEC 61511 (2016). Disse standardene gir krav og anbefalinger til utforming for god sikkerhetsytelse for sikkerhetsinstrumenterte systemer, både på en kvalitativ og kvantitativ måte. Kvantitative beregninger av sikkerhetsytelsen er basert på forventet gjennomsnittlig nedetid i et testintervall. Regelmessige tester utføres for å verifisere systemets funksjonelle integritet, og for å oppdage skjulte feil.

En modell er foreslått basert på en type adferdsmodell kalt Petri Net for å kunne simulere levetiden til en hel-elektrisk aktuator og ventilsystem. Modellen er bygget på en slik måte at en sammenligning til aksepterte krav til sikkerhetsytelse av elektrohydrauliske aktuatorer og ventilsystem er gjort rettferdig. Systemkarakteristikken for en hel-elektrisk aktuator åpner opp muligheter for ulike operasjonelle strategier i forhold til det elektrohydrauliske systemet. Fire simuleringscenarier ble laget med forskjellig antagelser for å se effekter av sikkerhetssystemets gjennomsnittlige utilgjengelighet.

Oppgaven konkluderer med at et sikkerhetssystem med hel-elektriske aktuatorer samsvarer med de kvantitative kravene sett i forhold til en elektrohydraulisk aktuator. Det er noen usikkerheter knyttet til feildataene og antagelsene for drift med nedsatt ytelsesevne. For videre arbeid anbefales det å fokusere på testmetodene som kan benyttes ved nedsatt ytelsesevne å verifisere at risikoen er tilstrekkelig lav.

Contents

List of Figures

List of Tables

Abbreviations

AMV	Annulus Master Valve
AWV	Annulus Wing Valve
CAPEX	Capital Expenditures
DC	Diagnostic Coverage
DD	Dangerous Detected
DHSV	Downhole Safety Valve
DU	Dangerous Undetected
E/E/PE	Electrical/Electronic/Programmable Electronic
EPU	Electronic Power Unit
ESD	Emergency Shutdown
EUC	Equipment Under Control
FMECA	Failure Modes, Effects and Criticality Analysis
HFT	Hardware Fault Tolerance
HIPPS	High Integrity Pressure Protection System
HPU	Hydraulic Power Unit
IEC	International Electrotechnical Committee
MDT	Mean Down Time
MTTF	Mean Time to Failure
MTTR	Mean Time to Repair
MRT	Mean Repair Time
NCS	Norwegian Continental Shelf
OPEX	Operational Expenditures
PFD	Probability of Failure on Demand
PMV	Production Master Valve
PSD	Process Shutdown
PWV	Production Wing Valve
RAMS	Reliability, Availability, Maintainability, and Safety
RBD	Reliability Block Diagram
ROV	Remotely Operated Vehicle
SAS	Safety Automation System
SC	Systematic Capability
SD	Safe Detected
SFF	Safe Failure Fraction
SIF	Safety-Instrumented Function
SIL	Safety Integrity Level
SIS	Safety-Instrumented System

SPS	Subsea Production Systems
SU	Safe Undetected
XMT	Subsea tree
XOV	Crossover valve

Chapter 1

Introduction

The oil and gas industry has shown an increasing interest to reduce CO_2 emissions from their production facilities while at the same time meet the increasing world energy demand. The International Energy Agency (IEA) recognise a higher demand of energy, particularly from emerging countries like China and India. Norwegian oil companies are shifting investments strategies to meet the energy demand and at the same time reduce production costs and emissions. Together with investments in renewable energy, electrification of the Norwegian Continental Shelf (NCS) is introduced as a solution to reduce carbon emissions from production (NTNU, 2018).

1.1 Background

A part of the electrification process on the NCS, oil and gas companies shows an increasing interest to replace subsea electro-hydraulic technology with all-electric technology. This means to change technologies that have been developed through decades of operational experience. Aker Solutions is currently developing all-electric solutions for subsea applications such as production trees (XMT) and manifolds. There are many challenges to face in the development of new technology, one being to build a reliable and safe system that are able to perform as intended when needed.

All-electric solutions have been in development for quite some time, but are still pending to become the industry standard for subsea systems. The first all-electric subsea production system was claimed by Cameron in 2008 on the K5F field outside the Netherlands. The system was designed for improved reliability and enhance the environmental performance[1]. All-electric systems have occasionally emerged in different subsea installation throughout the last decade, and Aker Solutions is now looking into full field all-electric deployment. The technology is still

[1]Total press release https://www.total.com/en/media/news/press-releases/first-gas-k5f-netherlands-field-using-innovative-subsea-technology

considered premature for such installations, and further studies have to be carried out (Johannessen, 2018).

1.2 Problem Formulation

The theoretical framework will consist of a review of different literature such as standards, research papers, articles and books. The thesis will investigate and elaborate on reliability and safety parameters for all-electric concepts, and compare to existing system solutions.

Replacing electro-hydraulic actuators with all-electric actuators involves some major modifications concerning reliability and safety. A subsea XMT will no longer require hydraulic fluids to operate valves, i.e., all functionality is provided by a combination of electronics and mechanical parts. New fail-safe solutions, retrievability, and all-electric control modules are all subject to changes that impact RAMS parameters.

The master project will be a continuation of the specialisation project, where the purpose is to suggest an approach for modelling and calculating reliability and availability of all-electric XT valves, which allows optimising design parameters in light of constraints posed by safety, maintenance and operational philosophies. The basis for analysis is concepts developed in Safety 4.0 as they are not subject to confidentiality. Reliability and availability performance is part of the technology qualification process needed for all-electric technology to be implemented in the industry.

1.3 Objective

The main objective of this master thesis is to suggest an approach for modelling and calculating reliability and availability for all-electric XMT valves. The results allows for optimising design parameters in light of constraints posed by safety, maintenance and operational philosophies. The following sub-objectives are made:

- Propose an approach, including model(s) for the analysis of reliability and availability, and relevant data and assumptions to be made to support the analysis. The model should consider necessary detailing of the XMT valve itself and the system in which it is installed.
- Suggest a way to utilise the model to optimise the design parameters of the XMT valve within the boundaries of safety and reliability, and requirements.
- Elaborate on the level of uncertainty associated with the analysis, considering the scope of the analysis, the model, and relevance of data, and suggest possible strategies to present uncertainty and possible reduce it.

1.4 Limitations

A subsea system comprise in many different modules and subsystems working together, but the thesis is limited to only consider XMT valves and associated equipment needed to operate them. Due to confidentiality of specific design solutions, for example internal design of an actuator, a more high-level system approach has been considered. From a modelling point of view, this means that the system is considered to be built up by larger items than what is considered in an actual development project.

Only failures in hardware equipment is considered, meaning the analysis does not consider reliability and safety of entities like software and organisational procedures.

1.5 Actors Involved

This thesis is written in collaboration between Norwegian University of Science and Technology (NTNU), and company Aker Solutions.

- **NTNU:** The thesis is written in collaboration with the RAMS research group at NTNU, where Professor Mary Ann Lundteigen is the main supervisor. Her contribution is to provide help and guidance on writing a thesis
- **Aker Solutions:** Aker Solutions is the industry partner for the thesis. Aker Solutions is a global engineering company located in 20 countries with more than 15 000 employees. The company delivers products and solutions for the energy market from early design studies, to implementation, operation, and decommissioning. Engineer Christopher Lassen from Aker Solutions is main contact for the thesis and contributed to align the research problem and industry related problems. From the Aker Solutions all-electric team, RAMS engineer Jone Sigmundstad contributes with guidance and help on more technical aspects of the thesis.

1.6 Approach

The main scope of the thesis is to elaborate on reliability for all-electric solutions for subsea applications. The work is based around a literature review of current all-electric subsea technology introduced by the industry and academic research. In addition to a literature review, Aker Solutions provide guidance based on the internal development project, but due to the confidentiality of the project, only non-confidential topics are considered for the thesis.

1.7 Structure of the Report

A brief description of the chapters are provided in the following:

Chapter 1 Chapter 1 presents an overview of the topic for this thesis, background, objectives, and context for topic.

Chapter 2 A brief introduction to subsea systems is given in the context of the topic. A literature review has been conducted for the all-electric subsea technology.

Chapter 3 An introduction to safety-instrumented systems and reliability allocation methods is presented here. This chapter presents the theoretical framework for the thesis which is used in further chapters.

Chapter 4 Elaborates on requirements and operation of safety-instrumented systems on the NCS in light of the literature review on all-electric technology.

Chapter 5 The previous chapters, a system familiarisation, and a model is presented in this chapter. The basis for the results and how they are obtained is explained in this chapter.

Chapter 6 Presents the results of from the simulations conducted by the model.

Chapter 7 Conclusions and recommendations on further work are given in this last chapter.

Chapter 2

Subsea Production Systems

Subsea Production Systems (SPS) are installed on the seabed to allow for economic recovery of oil and gas [1]. The first SPS on the NCS was installed on the Ekofisk field in 1971 (Zhang et al., 2017), and subsea technology has seen great growth since. Operators are constantly looking into developing technology to utilise fields at greater water depths, and with longer tie-back distances to topside platforms. This requires improved systems that can handle ultra-deepwater production systems (Bell et al., 2005). Improvements for better recovery and exploration of oil and gas reserves has introduced other technologies such as subsea processing alongside subsea production, for example, subsea compression systems (Lima et al., 2011). The subsea domain of the industry are still expanding, and Ramberg et al. (2013) discuss the steps towards entire factories deployed on the seabed.

Subsea wells can be configured as either satellite wells or clustered wells. Satellite wells are stand-alone and individual wells that are either connected to a central manifold, or directly to a topside facility. Clustered wells are wells that share the same structure. The Ormen Lange field (Bernt and Smedsrud, 2007) and the AKPO fieldNelson (2010) are examples of subsea productions systems built in a clustered configuration.

A SPS is built around the subsea wellhead where the main building blocks are subsea trees, manifolds, flowlines, and control systems. Figure 2.1 illustrates that the typical topology is to have an XMT on top of each well, from here the flow is directed to a manifold. Each manifold have several XMTs either deployed in a satellite configuration, or as an integrated part of the manifold template.

[1] `https://akersolutions.com/what-we-do/products-and-services/subsea-production-systems/`

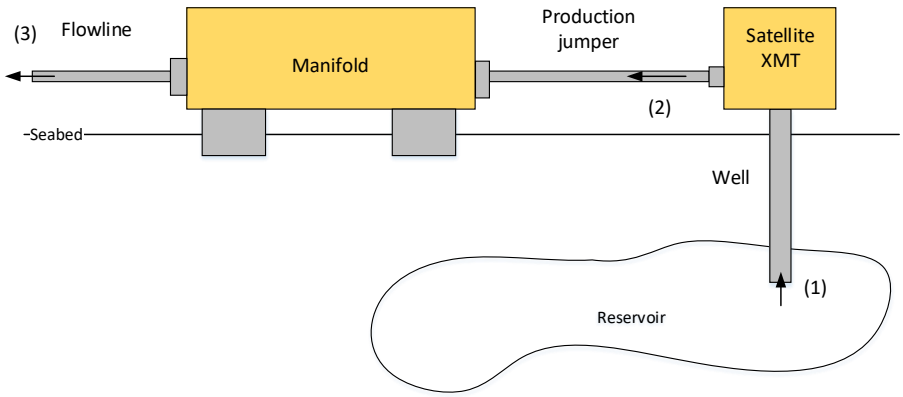


Figure 2.1: Production flow from reservoir (from Johannessen (2018)).

2.1 Subsea Trees

Subsea Trees (XMT) are installed onto the wellhead on the seabed. It forms the physical interface between well and manifold/production pipeline. On the Norwegian Continental Shelf (NCS), a XMT serves several important functions for both control and safety in the production process. The main functions are:

- Control and regulate flow of hydrocarbons;
- Act as safety barrier towards environment;
- Allow for injection of chemicals to well or flowline;
- Control downhole safety valve (DHSV), and other downhole valves;
- Bleed of excessive pressure from annulus;
- Allow for well intervention.

Figure 2.2 shows a simple schematic sketch for a XMT. There are two production valves located on the production wing block, the production master valve (PMV) and the production wing valve (PWV). Similarly, there are two valves on the annulus block, the annulus master valve (AMV) and the annulus wing valve (AWV). These valves are used for access to the annulus area. In addition, there is a cross-over valve (XOV) going straight from annulus to the production bore. A more detailed schematic can be found in the guideline NOG 070 (2018).

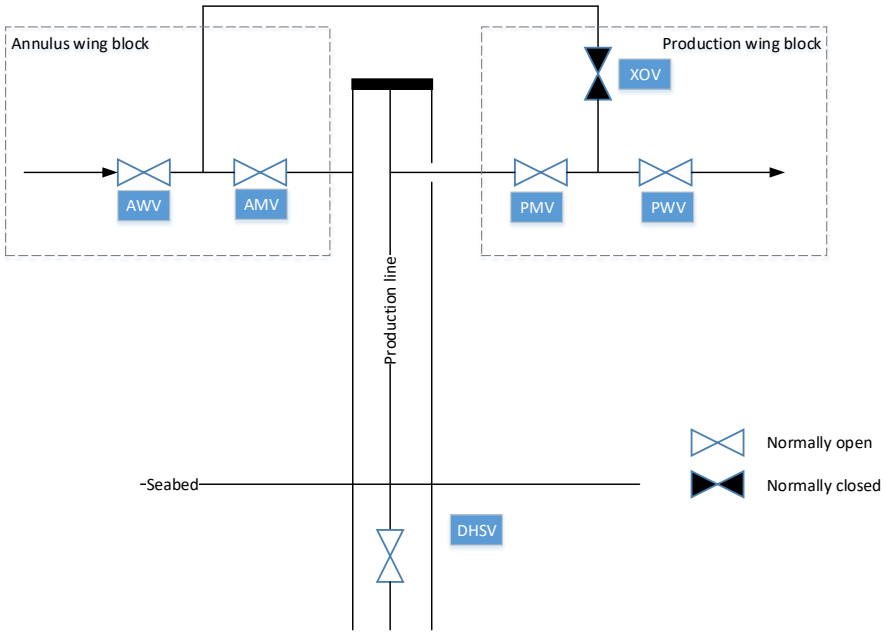


Figure 2.2: Simplified XMT schematic (Johannessen, 2018)

The XMT valves are operated through an electro-hydraulic multiplex control system. Electric power is provided by the electrical power unit (EPU) and hydraulic power is provided by the hydraulic power unit (HPU). These units are located topside and fed through an umbilical to the SPS on the seabed. Hydraulic pressure is also stored in subsea accumulators to decrease response time for opening and closing of the valves. To control the direction of hydraulic pressure, a set of directional control valves are installed. These valves are electronically controlled from topside and allows for individual control of each XMT valve (Zhang et al., 2017).

It is recognised by companies that the current electro-hydraulic systems have some limitations, and Abicht et al. (2017) lists some key challenges associated with the electro-hydraulic control system. Increased step-out and tie-back distances (i.e. distance from exisiting or future fields to platform), greater water depths, size and complexity of HPU and hydraulic lines, costs, and reliability are seen as limiting factors for the current control system. Some of these challenges can potentially be overcome by utilising all-electric technology.

2.2 All-Electric Subsea Technology

All-electric subsea technology has been discussed in the industry for quite some time. It is mentioned that the technology was discussed already in the early 1990s (Bouquier et al., 2007). However, companies hold back on the technology as the industry in general are conservative about

implementing new technology. Well-proven and qualified technology is first in line when selecting equipment in a new field development. Other industries such as automotive and aviation have already accepted all-electric solutions for their safety application, where components such as batteries and electrical motors are utilised (Moe et al., 2018).

Potential reduction in capital (CAPEX) and operational expenditures (OPEX) is a driver for enabling all-electric technology, and Moe et al. (2018) mentions that the potential cost reduction for SPS development is around 5 – 15%, while umbilical cost reduction is around 25 – 50%. Removal of hydraulic related equipment is recognised as a large contributor to reducing costs. The HPU, and a large number of control cabinets and other control related equipment, can be removed from the topside facility. This can not only save costs, but also free up space, which can contribute to a safer working environment (Winther-Larssen and Massie, 2017). Subsea equipment can be made more compact and savings can be done through removal of hydraulic components, especially for control equipment.

Winther-Larssen and Massie (2017) compares the cost of an electro-hydraulic and an electric actuator. It is found that due to the increased complexity of an electric actuator, the added cost is likely to be comparable to the savings. In an earlier study for all-electric systems, made by Rivenbark et al. (2001), an illustration (Figure 2.3) shows a complexity comparison of hydraulic and electric valve actuation.

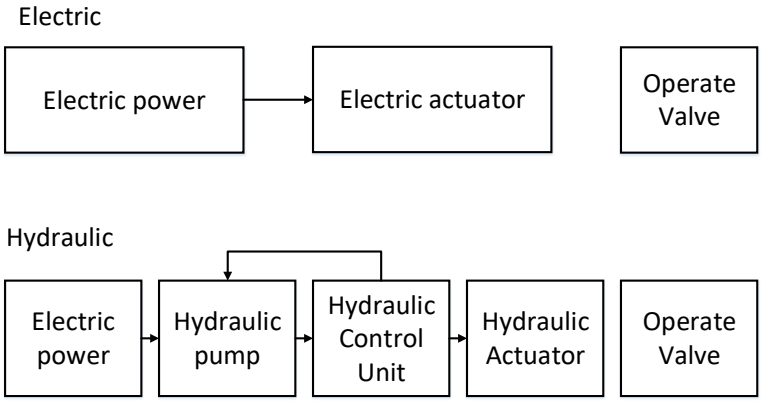


Figure 2.3: Complexity comparison. Adapted from Rivenbark et al. (2001).

Despite the illustrated simplicity of an electric actuator, the internal complexity is rather different. The actuator itself goes from a rather simple spring to an electro-mechanical system, this is illustrated both by Winther-Larssen and Massie (2017), and Moe et al. (2018).

Cost reduction is not the only driver for enabling all-electric technology. Abicht et al. (2017) mentions that both HSE and technical improvements are drivers for enabling all-electric, in addition to cost. As mentioned above, HSE improvements can be made by freeing up space in the personnel working area. Additionally, it removes the possibility of exposing highly pressurised hydraulic fluids to personnel and environment.

Technical improvements can be made through better condition monitoring capabilities, as electronic equipment is favoured over mechanical equipment for monitoring (no conversion of the analogue signal is needed). More precise valve control allows for simplified testing methods like partial stroke test, which means to stroke the valve a small portion of the travel distance (Abicht et al., 2017). Partial stroke testing and the effects of it are further discussed in chapter 3.8.2.

Electronics are often kept in smaller and separately retrievable modules, which makes it easier to retrieve with a smaller vessel (Moe et al., 2018). This feature is shown in Figure 2.4, where electric actuators can be retrieved separately from the fixed valve.

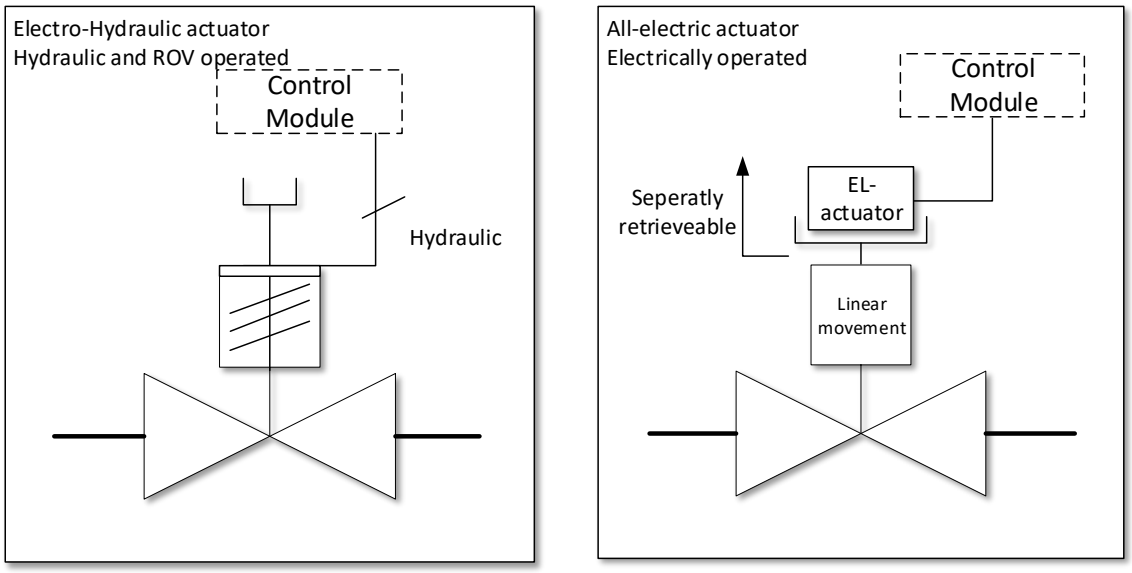


Figure 2.4: Comparison of electro-hydraulic actuator and all-electric actuator (Adapted from Winther-Larssen and Massie (2017)).

Upon failure of any component necessary to operate the valve, the failure shall be in such manner that the valve is able to close (NORSOK S-001, 2018). This is called a fail-safe mechanism. The fail-safe mechanism used in conventional electro-hydraulic systems has a de-energize-to-trip principle, meaning loss of energy results in closure of the valve. The advantage of a de-energize-to-trip design is that the system is not dependent on an energy source to function.

There are two possible options to achieve fail-safe operation for an all-electric actuator, either spring return or return powered by a local energy source such as a battery. Halvorsen and Koren (2008) argues that a battery has several advantages for use in an XMT actuator, this is also supported by Moe et al. (2018). No failure modes of broken springs, no power consuming latchback mechanism for the spring, and no need for high power cables from topside are some advantages mentioned.

Chapter 3

Reliability of Safety-Critical Systems

This chapter presents the theoretical background for design and reliability assessment of safety applications in the oil and gas industry.

3.1 Petroleum Safety Authority

The Petroleum Safety Authority (PSA) is the regulator for technical, operational and organisational safety on the NCS. The role of the PSA is to supervise safety, emergency preparedness and the working environment in Norwegian petroleum activities offshore and on land (PSA, 2019). The PSA provides several regulations concerning operation and design of facilities on the NCS. The most relevant for this thesis is the management regulation, and the facilities regulation. The management regulation relates to the duty of providing information about facilities, while the facilities regulation relates to design of facilities in the Norwegian petroleum industry.

The two regulations refers to some key standards to use as basis when implementing safety systems for Norwegian offshore petroleum activities. The main standards covered in this thesis are given in table 3.1 below.

Table 3.1: Applicable Standards for functional safety

Standard	Description	PSA regulation
IEC 61508	Generic standard on functional safety	Management §5 Facilities §8 Activities §26, §47
IEC 61511	Functional safety in the process industry	Management §5
NOG 070	Guideline on application of IEC 61508 & 61511	Management §5 Facilities §8 Activities §16, §26, §47

3.2 Barrier Management

The consequence of an accident in the oil and gas industry might cause serious harm to people, environment or assets. The probability of accidents is regarded to be quite low, but if an accident occurs the consequence is severe. In case an undesired event occurs, it could be sufficient to have some mitigating measures in place. Cockshott (2005) introduced the bow-tie model, which can illustrate the use of mitigating measures in order to reduce consequences. For example, the airbag system in a car is deployed after a collision to protect people inside the car.

These mitigating measures may be referred to as safety barriers. A safety barrier is defined as "a physical and/or nonphysical means planned to prevent, control, or mitigate undesired events or accidents" (Sklet, 2006).

Section 5 of the PSA management regulation[1] describe requirements for barriers in the Norwegian petroleum industry. Barrier elements are categorised into three different categories: technical, operational or organisational. Technical barrier elements are "equipment and systems that are included in the realisation of a barrier function", for example a valve. Operational barrier elements are "actions or activities the personnel must take/perform to realise a barrier function", for example, push a button to initiate a shutdown. Organisational barrier elements are "personnel with defined roles or functions and specific competence that are included in the realisation of a barrier", for example, a safety engineer. A practical guideline on barrier management in accordance to the PSA requirements is provided by Hauge and Øien (2016).

3.2.1 Barriers in Relation to XMT

A SPS has several safety barriers, and barrier systems. A barrier system is "a system that has been designed and implemented to perform one or more barrier functions" Sklet (2006). The XMT can be regarded as a safety barrier system with several valves installed in the production bore to make sure that a failure in one does not compromise the safety. In some situations, additional barrier systems might be added in addition to the XMT. This can for example be a high integrity pressure protection system (HIPPS), which are installed to protect the pipeline if pressure exceeds an acceptable level (Aruo et al., 1995).

Considering the valves only, following barrier elements belong to the XMT barrier envelope:

- DHSV is part of the primary barrier;
- PMV, PWV, AMV, AWV, and XOV belongs to the secondary barrier.

The terms primary and secondary barrier are used in relation to well integrity. Well integrity is defined as "application of technical, operational and organisational solutions to reduce risk

[1] https://www.ptil.no/en/regulations/all-acts/the-management-regulations3/II/5/

of uncontrolled release of formation fluids throughout the life cycle of a well" (NORSOK D-010, 2013).

The NOG 117 (2008) for well integrity introduces the well categorisation system based on well condition. There are four different categories; red, orange, yellow and green, from worse to best respectively.

Table 3.2: Well categorisation system (Reproduced from NOG 117 (2008))

Category	principle
Red	One barrier failure and the other is degraded/ not verified, or leak to surface.
Orange	One barrier failure and the other is intact, or a single failure may lead to leak to surface.
Yellow	One barrier degraded, the other is intact.
Green	Healthy well, no or minor issue.

Safety barriers are the main concern for well integrity as it consists of both passive and active systems working to prevent an uncontrolled flow of hydrocarbons. Passive systems are system that are always available to perform a safety funciton, while active systems are systems designed to respond to certain events (Rausand, 2014).

3.3 Safety-Instrumented Systems

Subsea safety systems are digitalised, i.e., they use a combination of sensors, logic solvers, and actuating items to ensure safety when required. Electrical/electronic/programmable electronic (E/E/PE) technology is central for active safety systems.

In the process industry E/E/PE safety-related systems are called safety-instrumented systems (SIS). An SIS use a combination of one or several safety-instrumented functions (SIF) to ensure safety for the protected system. The system in which safety-instrumented systems are installed to protect are called equipment under control (EUC) (IEC 61508, 2010). In other words, a SIF is a safety function performed by the SIS (IEC 61511, 2016). The terms SIS and SIF are used in the international standard IEC 61511 (2016), while the term E/E/PE safety-related systems are used in IEC 61508 (2010). These standards are further discussed in chapter 3.4.1.

A subsea SIS typically consists of process sensors which monitor pressure and temperature. The signal is monitored by a logic solver located topside, depending on information from the sensors, the logic solver sends signals to activate the barrier valves subsea. For example, if fire or gas is detected in a hazardous area, the logic solver initiates closure of all necessary valves to prevent the fire or gas leakage from escalating. An automatic shutdown of the system in case of an emergency such as fire and gas is called an emergency shutdown (ESD) (NORSOK S-001, 2018).

3.4 Applicable Standards and Guidelines

Table 3.1 shows some standards referenced by the PSA to use for design and implementation of safety systems in the Norwegian petroleum industry. In following, a further elaboration of these are provided.

3.4.1 IEC 61508 & IEC 61511

IEC 61508 (2010) and IEC 61511 (2016) are standards developed by the International Electrotechnical Committee (IEC) as guidelines for design of E/E/PE safety-related systems. IEC 61508 is a generic standard meant to be applied for any industry, while IEC 61511 is a specific standard made for E/E/PE safety-related systems in the process industry. IEC 61511 was made to make it easier to apply requirements and principles for implementing prior use equipment within the process industry (NOG 070, 2018). In oil and gas projects the application of IEC 61511 is more common, as these projects concern well-proven or prior use equipment. Main difference of the two is that IEC 61508 is more directed towards vendors, while IEC 61511 is more directed towards end users and system integrators (IEC 61511, 2016, p.10). The relationship between the two standards is shown in Figure 3.1.

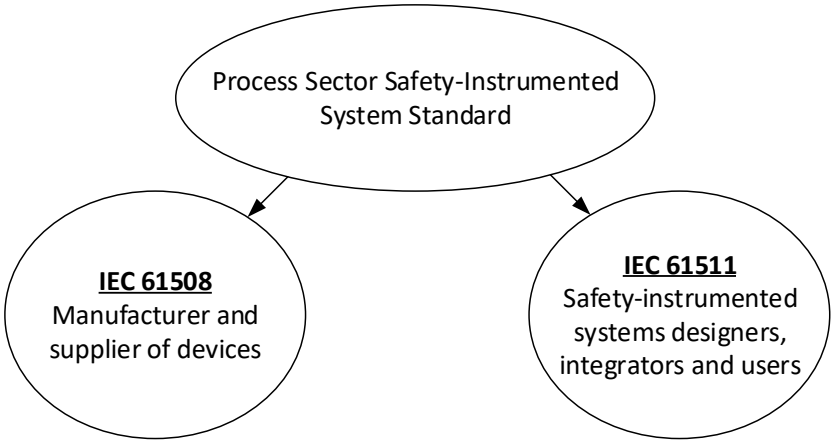


Figure 3.1: Relationship between IEC 61508 (2010) and IEC 61511 (2016) (adapted from IEC 61511 (2016)).

3.4.2 Norwegian Oil and Gas Association Guideline 070

NOG 070 (2018) is a guideline made on the application of IEC 61508 (2010) and IEC 61511 (2016) in the Norwegian petroleum industry. The purpose of the guideline is to ease the work related to safety applications in the Norwegian Petroleum industry. As an example, it provides minimum performance criteria for selected functions identified by oil and gas comapnies and regulators on the NCS.

3.5 Safety Integrity

Safety systems are implemented to reduce the risk of a hazardous event to occur. To quantify the risk reduction that is needed, IEC 61508 introduces the concept of safety integrity level (SIL). Safety integrity is a performance measure of how well the safety function or system shall perform, the measure is then split it into four levels. The performance measure for low-demand systems are given as the probability of failure on demand (PFD). Table 3.3 shows the four levels of safety integrity and the corresponding PFD range.

Table 3.3: SIL table for low-demand systems (adapted from IEC 61511 (2016))

Safety Integrity Level	Probability of failure on demand
SIL 1	$\geq 10^{-2}$ to $< 10^{-1}$
SIL 2	$\geq 10^{-3}$ to $< 10^{-2}$
SIL 3	$\geq 10^{-4}$ to $< 10^{-3}$
SIL 4	$\geq 10^{-5}$ to $< 10^{-4}$

IEC 61508 (2010) classifies the cause of SIS failures as either random hardware failures or systematic failures. Random hardware failures are quantified through calculations and qualitative limitations, while systematic failures follow qualitative principles on avoidance of such failures. The failure classification is as follows and Figure 3.2 shows examples for each type of failure.

- **Random hardware failures:** Random hardware failures are defined as failures that occur due to natural degradation mechanisms (IEC 61508, 2010).
- **Systematic failures:** Systematic failures are failures that can be related to a certain cause and only eliminated by a modification of the design, manufacturing process or operational procedure (IEC 61508, 2010).

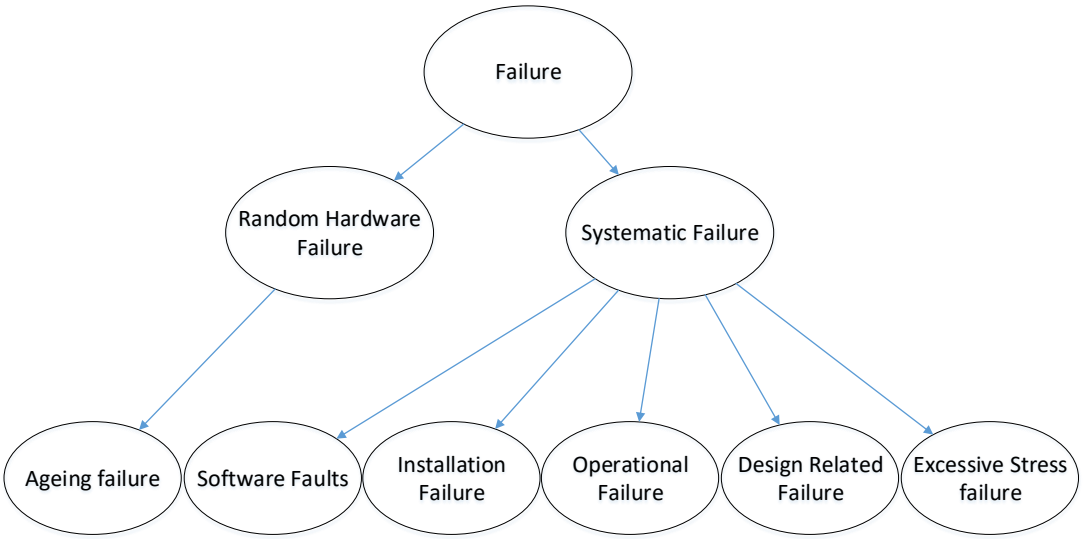


Figure 3.2: Failure classification by cause (from SINTEF (2013))

IEC 61508-6 (2010) suggests formulas for calculating PFD that are based on random hardware failures only. To calculate the PFD there are several parameters that should be assessed. For the calculation, information about system architecture and a classification of dangerous and safe failures are needed.

Dangerous and safe failures are classified as either detected or undetected. Detected failures are failures detected more less instantly after occurring, while undetected failures remain hidden until the system is needed (e.g. a demand occurs) or tested. Dangerous detected (DD) and dangerous undetected (DU) failure rates are needed to quantify the effects from random hardware failures by the formulas given in IEC 61508-6 (2010). Assessment of DD and DU failures are further discussed in chapter 3.8. Formulas and quantification methods are further discussed in chapter 3.6.

Hardware failures are also limited by some qualitative requirement. These requirements are referred to as architectural constraints, which limits the highest SIL that can be claimed for an element. NOG 070 (2018) suggests to follow route 1_H in development of new technology. When following this route, architecural constraints are determined based on two parameter: Hardware Fault Tolerance (HFT) and Safe Failure Fraction (SFF). HFT is the number of faults tolerated before system failure. SFF is the fraction of known failures and described in IEC 61508-2 (2010) as

$$\text{SFF} = \frac{\lambda_S + \lambda_{DD}}{\lambda_S + \lambda_{DD} + \lambda_{DU}} \tag{3.1}$$

Table 3.4 is for type B components, in which behaviour under faulty conditions is not completely determined.

Table 3.4: Architectural constraints for Type B components

SFF	HFT		
	0	1	2
< 60%	-	SIL 1	SIL 2
60% - 90%	SIL 1	SIL 2	SIL 3
90% - 99%	SIL 2	SIL 3	SIL 4
>99%	SIL 3	SIL 4	SIL 4

Lundteigen and Rausand (2006) elaborates on the qualitative requirements addressed in IEC 61508, and highlights that reliability calculations might not capture system complexity that well. Other uncertain parameters such as failure rates, average value for PFD, misinterpretation of failure modes, and the fact that only hardware failures are considered in the calculations argue in favour for the need of some qualitative requirements as well. Architectural constraints are introduced to achieve a more robust architecture, at all subsystem levels (IEC 61508-2, 2010).

The distinction between the two types of failures is important when assessing the overall safety integrity of an SIS. A SIL is obtained based on quantification of random hardware failures alone. There might be other causes to why a safety function fails, which is the reasoning for having requirements about systematic safety integrity.

The parameter for systematic safety integrity is systematic capability (SC). *"Systematic capability relates to the ability to ensure low enough contribution from systematic faults, so the SIL requirement is not compromised"* (IEC 61508-2, 2010). SC is not quantified, but follows the strategy on how to avoid and control the occurrence of systematic faults. Requirements on how to achieve this is given in IEC 61508-2 (2010).

Like HFT for random hardware failure, SC also sets limitations for the maximum SIL an element can claim. For an element that has SC = N, where N = $1,2,3,...$, and failure of the element does not result in failure of the safety function, systematic capability for the element is SC = N + 1. That means if the element is used as single (HFT = 0), and calculations on PFD gives SIL 3, SC needs to be at least SC = 3 for SIL 3 to be claimed for the element (Creech, 2014). A more thorough description on systematic capability is provided by Creech (2014).

The best way to avoid systematic failures is to avoid introducing them in the first place. Note that a systematic fault (i.e. a state) is the result of systematic failure (i.e. an event) (Rausand, 2014). IEC 61508-2 (2010) provides requirement for both avoidance and control of systematic faults. In general, it takes more effort to control systematic faults as higher the SIL is.

3.6 SIS Quantification Methods

IEC formulas

As discussed previously, formulas for calculating PFD are suggested in IEC 61508-6 (2010). The formulas are based on finding the average unavailability (MDT) in a test interval $[0,\tau]$. $\text{PFD}_{\text{avg,i}}$ of an item i is found by dividing MDT_i by τ. For series structures, PFD_{avg} is found by the sum of $\text{PFD}_{\text{avg,i}}$ for all items. PFD values are very similar to values found by probabilities when compared to 1, hence the addition (IEC 61508-6, 2010). For parallel structures this assumption is no longer valid.

Formulas are suggested for different k-out-of-n ($k$oo$n$) voted architectures with maximum three channels. The main idea of the formulas is to calculate a voted group as a single channel (Rausand, 2014). PFD calculations are based on the average dangerous group failure frequency, $\lambda_{\text{D,G}}$, and the group-equivalent mean down time, t_{GE}.

$$\text{PFD}_{\text{avg}} = \lambda_D t_{GE} \tag{3.2}$$

For a 1-out-of-1 (1oo1) structure, the group-equivalent mean down time is equal to the channel-equivalent mean down time, t_{CE}. The PFD_{avg} is then calculated as

$$\text{PFD}_{\text{avg}} = \lambda_{DU}\left(\frac{\tau}{2} + \text{MRT}\right) + \lambda_{DD}\text{MTTR} \tag{3.3}$$

Rausand (2014) states that many relability analysts find the IEC formulas confusing. There are no derivation or justification of the formulas in the standard. A general formula for the equivalent mean down time for a $k$oo$n$ structure has been proposed (Rausand, 2014)

$$t_{\text{GE}} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{\tau}{n-k+2} + \text{MRT}\right) + \frac{\lambda_{DD}}{\lambda_D}\text{MTTR} \tag{3.4}$$

Simplified Formulas

Rausand and Høyland (2004) introduces the simplified formulas for calculation of PFD. These formulas only consider the down time due to DU failures, and the repair time is assumed to negligible. These formulas are easy to derive and can, for example, be used to verify results of simulations. PFD_{avg} for some $k$oo$n$ structures are provided by Rausand and Høyland (2004), for example, a 1oo1 structure is

$$\text{PFD}_{\text{avg}}^{\text{1oo1}} = \frac{\lambda_{\text{DU}}\tau}{2} \tag{3.5}$$

These formulas can be difficult to derive and calculate once systems get more complex. One modelling technique that can be used is a state/transition model called Petri Nets.

3.6.1 Petri Nets

Petri Nets is a graphical and mathematical modelling technique applicable for modelling system behaviour (Murata, 1989). It is an emerging technique for reliability modelling, but still one of the less preferred tools amongst reliability engineers. Signoret et al. (2013) highlights that due to the rapidly increasing graphical complexity of rather simple systems, can be a reason for resisting to use Petri Nets. The graphical representation consists of *places*, represented as circles, and *transitions*, represented as boxes, which are connected by arcs. Places can be seen as system conditions or states, while transitions represent events. The transition has input and output places, precondition and post-condition respectively (Murata, 1989; Rausand, 2014). Terminology and guidance on the application of Petri Nets for reliability modelling is given in the standard IEC 62551.

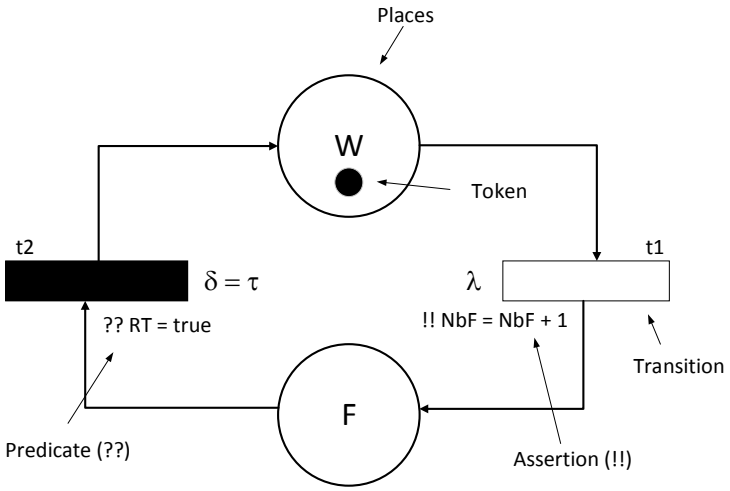


Figure 3.3: Petri Net Example

The use of predicates and assertions is a way to model repeated places in a Petri Nets. A predicate is a conditional statement that needs to be valid for enabling a transition. An assertion is a formula used to update one, or more, variables when a transition is fired (Signoret et al., 2013). In Figure 3.3 an assertion is used to update the variable NbF to count the number of failures every time the transition is fired. Likewise, the Boolean predicate RT has to be true to enable firing of the transition. This variable can be determined by another sub-Petri Net, for example if the repair team is working on another component, the variable RT becomes false, i.e. the transition in Figure 3.3 cannot be fired. Note that one transition is black, which indicate a deterministic distribution with parameter δ, while the white transition indicate an exponential distribution with parameter λ.

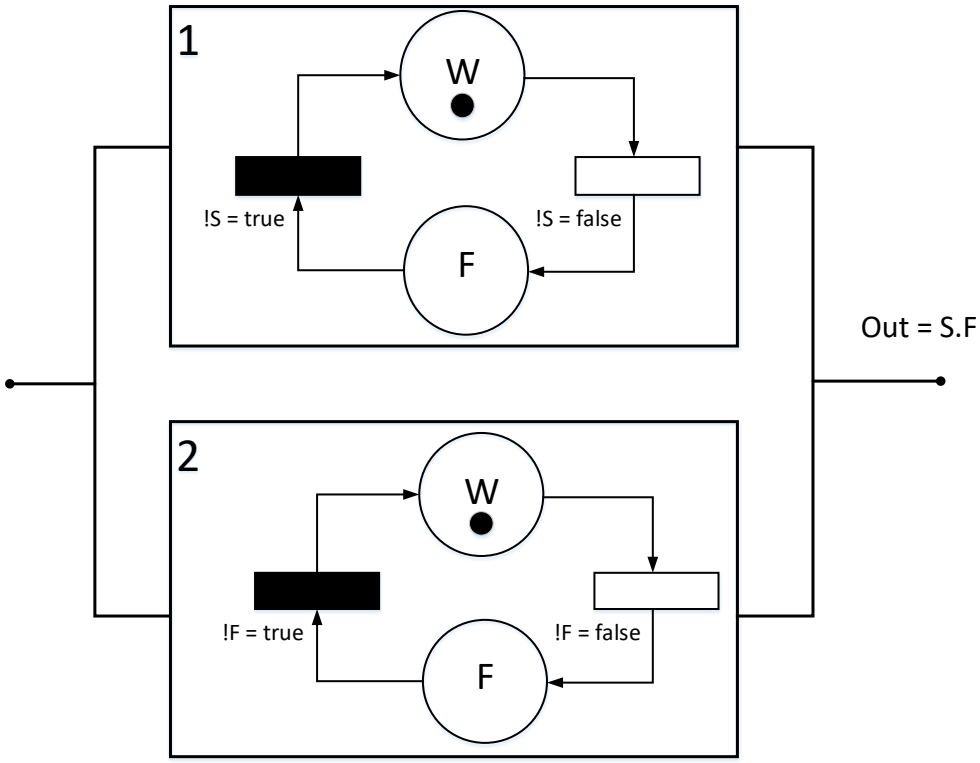


Figure 3.4: Example of RBD driven Petri Nets

3.6.2 Reliability Block Diagram Driven Petri Nets

A reliability block diagram (RBD) is a success-oriented network describing connections between components and how they fulfil a certain system function. RBDs are commonly used in reliability engineering as they are easy to read and communicate. There are two possible structures describing the relationship between components, series or parallel. A series structure can be referred to as a logical OR (.) operator, meaning component 1 or component 2 may fail for the system to fail. In contrary, a parallel structure indicate that both component 1 AND (+) component 2 have to fail in order to have system failure, i.e. a logical AND operator. An example of an RBD driven Petri Nets is shown in Figure 3.4, where either variable S or F (notated "S.F") needs to be true for the system to work. IEC 61078 (2016) is the international standard for RBDs and describe both symbols and calculation methods. The disadvantage of an RBD is that it may be difficult to capture more complex systems and repair strategies. If a system has more than one function, an RBD has to be made for each function (Rausand and Høyland, 2004). IEC 61508 (2010) often refer to different RBD architectures as $koon$, for example 1oo1 and 1oo2. This means that k-out-of-n components needs to function for the system to deliver its output.

In an effort to reduce complexity and increase readability of PNs, Signoret et al. (2013) describes an approach called "Reliability Block Diagram Driven Petri Nets". The approach is based

on the logic of an RBD where AND and OR operators are realised through predicates and assertions in the Petri Nets. System behaviour of each block is modelled as a Petri Net, and transitions are enabled through predicates dependent on sub PNs. A detailed approach on the use of Petri Nets for reliability calculations is given in the standard ISO TR 12489 (2013).

3.6.3 Simulation Method

Monte Carlo and discrete event simulation is a methodology for simulating real life problems and relies on repeated computations of stochastic events occurring within a specified time frame. The Monte Carlo method is a preferred methodology in reliability analyses due to its ability to handle complex repair strategies (Rausand and Høyland, 2004; Billinton and Peng Wang, 1999; Lei and Huang, 2017).

Monte Carlo Simulation starts by letting the system start at time $t = 0$. The first event is generated from a statistic distribution, typically a lifetime distribution that has been made for each component in the system. The time to this first event is then recorded, and stored as an observation. This process is repeated a number of times and statistics are obtained from each run. When the number of events increase, the advantage of this method is that it provides uncertainty estimation. Lei and Huang (2017) use a simple flow chart to describe the general idea of the Monte Carlo Simulation. The flowchart has been reproduced in Figure 3.5.

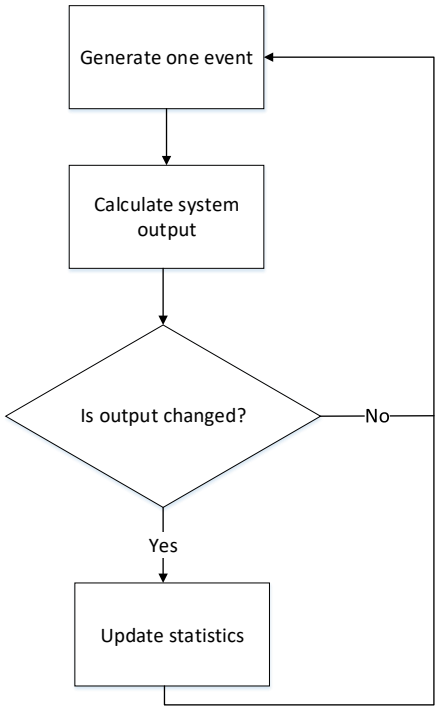


Figure 3.5: Monte Carlo Simulation mainloop. Adapted from Lei and Huang (2017)

The Monte Carlo simulation principle for Petri Nets is described briefly by IEC 61508-6 (2010). With basis in Figure 3.3 the simulation can be explained as follows

1. The token starts in the place W. Time spent in this state is stochastic and governed by an exponential distribution with parameter λ.
2. Transition $t1$ is the only next event available. A random number from the distribution enables the transition.
3. When transition $t1$ has fired, the token is removed from place W and added to place F.
4. Transition $t2$ is valid after the deterministic delay δ.
5. The token is now removed from place F and added to place W.

The transition are able to fire as long as the firing time is within the observation time $[0, T]$. When the observation time is up, one history is recorded. Relevant parameters, such as mean time spent in each place and firing frequencies, is recorded. Monte Carlo simulation consists of obtaining a great number of histories. The results are obtained by statistical calculation on parameters from every history.

To present the uncertainty of the Monte Carlo simulation, the standard deviation and confidence interval can be used. Considering a parameter x_i is recorded from every history N, the

mean value ($\bar{x}$) and variance (σ^2) is calculated as

$$\bar{x} = \frac{\sum_{i=1}^{N} x_i}{\mathrm{N}} \quad \text{and} \quad \sigma^2 = \frac{\sum_{i=}^{N} (x_i - \bar{x})^2}{\mathrm{N}} \tag{3.6}$$

When these statistics are obtained from the simulation, the confidence interval around the true parameter x and significance level α can be found by

$$P[x \in \left(\bar{x} - z_{\frac{\alpha}{2}} \frac{\sigma}{\sqrt{\mathrm{N}}}, \bar{x} + z_{\frac{\alpha}{2}} \frac{\sigma}{\sqrt{\mathrm{N}}}\right)] = 1 - \alpha \tag{3.7}$$

It is assumed that for a sufficiently large number of histories, the true parameter x belongs to a standard distribution, hence the statistic $z_{\frac{\alpha}{2}}$. For a two-sided 90% confidence interval, $z_{\frac{\alpha}{2}} = 1.645$.

As discussed previously, probability of failure on demand can be calculated as the expected down times D_i in the time interval t (Rausand and Høyland, 2004).

$$\mathrm{PFD}_{\mathrm{avg}} = \frac{E(D_i)}{t} \tag{3.8}$$

The same logic can be applied to the Monte Carlo simulation. By observing the mean time a token spends in a failed state, the average unavailability is obtain.

3.6.4 Failure Modes and Effects Analysis

A failure modes and effects analysis (FMEA) is a systematic approach to identify how items or processes might fail and what the corresponding effects are (IEC 60812, 2018). An FMEA is typically conducted in early design phases by members of the design team. It is preferable for the team members to have good knowledge about the system and hardware design for a good quality FMEA process. An FMEA is based on failure modes and failure effects which are defined as follows (IEC 60812, 2018):

- **Failure Mode:** Manner in which a failure occurs.
- **Failure Effect:** Consequence of a failure, within or beyond the boundary of the failed item.

Details about the FMEA process are provided by Rausand and Høyland (2004), and the standard IEC 60812 (2018). Typical elements of a FMEA worksheet is presented in table 3.5.

Table 3.5: Typical columns of a FMEA worksheet

FMEA Column	Description
Item	Item or element of the system
Function	The function(s) for the item
Operational mode	The item may perform under various operational modes
Failure mode	Possible failure modes of the item
Failure cause	Possible failure causes of the item
Detection	How the failure mode can be detected
Effect of failure	Effects of the failure mode, on local and system level

An FMEA can be applied to large and complex systems with several required functions. Not all functions are equally important to the analyst. Rausand and Høyland (2004) propose a way to classify functions for identification and analysis purposes. The main classification categories are described in the following:

- **Essentials functions:** Are functions required to fulfil the purpose of the functional block.
- **Auxiliuary functions:** Are functions in place to support the essential function. Might not be an obvious function, but important for the essential function. This can, for example, be the housing or container mechanism.
- **Protective functions:** Are functions intended to protect environment, equipment or people. Safety functions, environment functions and hygiene functions are sub-classes of protective functions.
- **Information functions:** Are functions that provide the user with information, for example, sensors, condition monitoring, gauges, and alarms.
- **Interface functions:** Are functions that connect the functional blocks together.
- **Superfluous functions:** Are functions often associated as "nice to have" functions. These functions might never be used.

A good understanding of the system functionality could be a good starting point for identification of failure modes for the FMEA procedure.

There are different adaptations of an FMEA. If the analysis include an analysis of criticality, the analysis becomes an FMECA. For criticality analysis including diagnostics, it is often referred to as an FMEDA (IEC 60812, 2018). Grebe et al. (2018) elaborates on the development of the FMEDA. Two new sections were added to the inital FMEA. One was quantitative failure rates for every component, and the other was the probability of the system to detect failures via automatic diagnostics.

3.7 Reliability Data

Failure data can be provided either by a manufacturer, or found in generic data sources. Generic failure data are often derived and published by organisations who collect data from various equipment groups (Rausand, 2014). The oil and gas industry has collected data for a long time. The most relevant publications are OREDA (2015), PDS handbook (SINTEF, 2013) and Exida handbooks (Exida, 2015).

- **OREDA Handbooks:** OREDA is an organisation sponsored by oil and gas companies to collect and exchange reliability data. The first handbook was published in 1984 followed by five new publication including the last one in 2015. The handbooks cover both offshore topside and subsea data. The OREDA handbook does not cover safety specific failure rates, but provide failure rate for a wide range of equipment groups used the NCS.
- **PDS handbook:** The PDS handbook is reliability database for control and safety systems made by Norwegian research organisation SINTEF. Compared to OREDA, it is more tailored towards safety-instrumented systems where data for input devices, logic contollers, and final elements are provided. The format of the handbook is suitable for reliability analysis in line with IEC 61508 (2010) and IEC 61511 (2016) (SINTEF, 2013).
- **Exida Handbook:** Exida handbooks are similar to PDS handbooks and covers specific data for safety applications in the process industry.

3.7.1 Data Uncertainty

Generic data bases derive failure rates from a large population of failure data. Statistical methods are applied to find an approximate failure rate for a component. This means that failure rates are not treated as deterministic values, but belongs to some distribution (e.g. exponential distribution).

Rausand (2014) discuss the uncertainty of failure rates and highlights that data found in handbooks like OREDA (2015) might come from equipment installed a long time ago. The technology used for those equipment groups might be different to what is being used today. Also, some equipment might be used in application where they initially where not intended. To overcome such problems, Brissaud et al. (2010) suggests a method to adjust failure rates based on influence factors. This can be a suitable approach if, for example, failure data for a component does not match the environmental conditions it is meant for.

In 2013, all Boeing 787 Dreamliner aircraft was grounded due to a safety concern regarding backup batteries. Investigations showed that the batteries was not as reliant as initially estimated. The actual failure rate was experienced to be three orders of magnitude greater than initially estimated (Williard et al., 2013). Failures may arise not only from natural degradation,

but also flaws or mistakes during the manufacturing process. This emphasise the relevancy for systematic capability in design, which is not required for quantification in reliability analyses in IEC 61508 (2010).

3.8 SIS Testing

Testing and maintenance are activities carried out to ensure that the safety system performs adequately. The documentation describing how to install, operate and test the equipment is called the safety manual. This manual shall contain any proof test and/or maintenance requirements (IEC 61508-2, 2010, Annex D). Rausand (2014) splits testing into three main categories: proof-testing, diagnostic testing and partial testing.

3.8.1 Proof-testing

A proof test is a test carried out at predetermined intervals to detected DU failures. Such tests are carried out to lower the risk of failures upon demand (Zio et al., 2013). The proof test scheduling can be categorised into three main strategies (Rausand, 2014):

- **Simultaneous testing:** This is where all components in a subsystem is tested simultaneously. During such a test, the EUC is left unprotected by SIF in question.
- **Sequential testing:** Testing is performed in sequence. All components are tested after each other and restored to a functional state before the next test is initiated. During a sequential test, the EUC is never left fully unprotected.
- **Staggered testing:** Staggered testing is where redundant components or systems are tested at different times, but the test interval is kept constant.

Liu and Rausand (2016) investigate effects of different proof-testing strategies induced by DD failures. The paper considers the term "insert tests" which are tests performed outside the regular proof test interval. The different strategies are (1) repair the system and do not perform a test, (2) perform an insert test and keep the scheduled test interval, and (3) perform an insert test and postpone the following proof test. Results show that insert tests are more effective as the DD failure frequency increases. Furthermore, there is minimal difference between strategy 2 and 3.

Testing is performed to verify that equipment is performing as intended. Hidden failures are detected (i.e DU) during conditions where the failure can be isolated and not bring harm to EUC. However, it is discussed if tests are perfect and all failures are detected during the test period.

3.8.2 Partial Test

Partial test is a type of "insert test" performed in between full proof tests. The purpose is to detect one or more specific DU failure without disturbing the EUC (Rausand, 2014). Partial testing of valves can be done by performing a partial stroke test (PST). This is done by stroking the valve a small portion of the travel distance. The effectiveness of a partial test is described by the partial test coverage, given by the fraction of DU failures detected by PST divided by all DU failures

$$\theta_{PST} = \frac{\lambda_{\text{DU,PST}}}{\lambda_{\text{DU}}} \tag{3.9}$$

Lundteigen and Rausand (2008) propose a methodology to determine the test coverage. Some arguments for introducing partial stroke test is to (i) improve safety, and (ii) reduce costs. Safety is improved when PST is added to scheduled full proof test, as it leads to a reduction in the calculated PFD. Savings in costs are realised through fewer production stops. When utilising PST, the PFD may be expressed as (Lundteigen and Rausand, 2008)

$$\text{PFD} \approx \text{PFD}_{\text{FT}} + \text{PFD}_{\text{PST}} = (1-\theta_{PST})\frac{\lambda_{\text{DU}}\tau_{FT}}{2} + \theta_{PST}\frac{\lambda_{\text{DU}}\tau_{PST}}{2} \tag{3.10}$$

3.8.3 Diagnostic Testing

Rausand (2014) defines diagnostic test as “an automatic partial test that uses built-in self-test features to detect failures”. When dangerous faults are detected by a diagnostic test, they are classified as DD failures. DU and DD failures are important to distinguish when determining the diagnostic coverage of an element. IEC 61508-2 (2010) annex C.1 formulates diagnostic coverage as

$$\text{DC} = \frac{\lambda_{\text{DD}}}{\lambda_{\text{D}}} \tag{3.11}$$

The diagnostic coverage can be used to find the DU failure rate.

$$\lambda_{\text{DU}} = (1-\text{DC})\lambda_{\text{D}} \tag{3.12}$$

In subsea oil and gas applications safety systems are often designed in a way that upon DD failures, the system goes to safe state. This means that the unavailability contribution induced by DD faults are neglected in calculations as the EUC is in safe state. Here, the nature of a reliable safety system and production availability experience conflicting interests. The system designer might want to design a system with a high SFF to enable a lower HFT as this is more cost efficient. One argument which favours all-electric is that it enables better monitoring capabilities. The valve and actuator used in electro-hydraulic systems consists mainly of mechanical components, which are hard to monitor or test without a full proof test.

Nadir et al. (2016) presents an overview of the effect of diagnostic coverage on different architectures presented in IEC 61508-6 (2010). These architectures are 1oo1, 1oo2, 1oo2D, 2oo2, 2oo3 and 1oo3, where D means diagnostic. This architecture is normally a 2oo2, but in case a fault is detected in either channel, the voting is changed to a 1oo1 (IEC 61508-6, 2010, clause B.3.2.2.4). The study shows that the 1oo2D architecture gives a decreasing PFD_{avg} for an increasing DC compared to 1oo1 and 2oo2, but not as good for the other architectures. It is stated that when designing a system with high DC, it might be more effective to have 1oo2 than a 1oo2D if redundancy is required (e.g. for availability).

Chapter 4

Requirements and Framework

In the previous chapter, the concept of SIS are introduced. In this chapter, the objective is to present some key requirements to consider when implementing a SIS or SIF for subsea.

Demonstrating safety for novel subsea technology is currently in discussion both within the industry and academia. As mentioned, all-electric subsea valve actuation have been in development for quite some time where, according to Bouquier et al. (2007), the first development programs were initiated in the early 1990s. It is also mentioned that these programs fell short due to lack of addressing the overall system reliability.

4.1 Framing Requirements

The rationale for implementation of new technology is that the performance is assumed to be at least as good as the old. According to NORSOK S-001 (2018), design and realisation of SIS shall be in accordance to principles given in IEC 61508 (2010) and IEC 61511 (2016). For implementation of standardised solutions, NOG 070 (2018) can be used as an alternative.

4.1.1 Well Isolation Requirements

An electric actuator can not be regarded as a standardised solution due to the increased complexity compared to a hydraulic actuator. Thus, it can be discussed if NOG 070 (2018) is a relevant standard to use as a benchmark for safety performance of an all-electric actuator. Most requirements are given in relation to hydraulic components, which are not always comparable to the electric counterpart. Though components are not the same, the intended functions are the same and can be transferred to all-electric control.

Isolation of a subsea well can be realised through closure of one or several XMT valves. NOG 070 (2018) have developed specific performance requirements for the ability to isolate a well. The following requirements apply for isolation of the production bore:

- SIL 2 with three XMT valves
- SIL 3 with three XMT valves and the DHSV

The XMT valves belongs to the secondary well barrier, where PMV, PWV, and XOV are located in the production bore. The isolation requirement can be achieved either by closing the PMV or the PWV and the XOV. The DHSV is not part of the Aker Solutions product portfolio, thus not considered further in the analysis.

Further design on how to achieve these isolation functions are provided by NOG 070 (2018), but this is where the standard is mostly applicable to standardised hydraulic solutions.

4.1.2 System Design Requirements

As mentioned, design and realisation of SIS shall be in accordance to IEC 61508 (2010) and IEC 61511 (2016). Meeting requirements about both random hardware failures and systematic failures ensures a well designed SIS. Route 1_H should be followed for hardware safety integrity and route 1_S for systematic safety integrity for new equipment.

Effects of random hardware failures are calculated to find the claimed SIL, for comparison to the required SIL discussed in previous section. Note that claimed SIL is based on analyses of the system before it is installed. IEC 61508-2 (2010) suggests to start by defining the architecture of the system. Requirements about HFT set limitations for highest SIL claimed. For example, for a type B component installed as single (i.e. HFT = 0) and SFF between 90% and 99%, the highest SIL that can be claimed for the component is SIL 2. The SFF is reflected in the ability to detect failures. A greater diagnostic coverage makes a greater SFF as the portion of DD failures increase.

There are various parameters needed to be able to conduct a quantification of random hardware failures. As seen from equation 3.1 about SFF, an assessment of dangerous and safe failures are needed. All elements or components might not be fully independent of each other, so IEC 61508-2 (2010) suggests to determine the effects and probability of common cause failures.

An assessment of DD and DU failures are needed to determine the SFF for element to be used in the safety application. For such an assessment it is suggested by IEC 61508 (2010) to use an FMECA where failure modes are identified and a failure classification is made for each component in the system.

If the system goes to safe state upon a DD failure, the equipment is protected and the effect of a DD failures are not considered in the calculations. If it is assumed that the equipment is as good as new after a test, the proof test interval is needed for the quantification.

4.2 Maintenance & Operation of Subsea SIS

Different maintenance strategies might have impact on the safety performance of an SIS. The remote location of a subsea system makes traditional maintenance strategies more difficult to apply. For larger subsea installations, it might take several months to deploy and mobilise for a retrieval vessel. This puts greater pressure on the reliability performance of a subsea installation. Methods like proof-testing and diagnostic testing can be utilised to ensure adequate performance of the remote safety system.

It is highlighted by several industry suppliers that electric equipment features better condition monitoring (Bouquier et al., 2007; Winther-Larssen and Massie, 2017; Moe et al., 2018). Better monitoring can give a greater rate of DD failures, or the ability to monitor degradation over time to plan in advance of a DD failure. In any case, a repair must be performed.

One particular feature of the all-electric actuator system, is the possibility to retrieve a single actuator from the XMT without losing control of other valves. Compared to the control module on a conventional electro-hydraulic XMT, control of other valves are lost upon failure of the control module. An ROV can be used to override the valves in this situation, but it still takes time to mobilise an ROV.

Considering the main production bore with the two main isolation valves PMV and PWV. If a failure occur in either of them, the other is still able to function. Assuming there are two options for repair of the actuator: (1) continue operation with one valve while the other is being repaired, or (2) bring EUC to safe state and perform repair. In option (1) the SIS is operating in degraded mode. Degraded mode of operation is when an SIS (or SIF) is operating with "reduced performance or reduced ability to perform its indented function" (NOG 070 (2018), section 10.4.2). There can be many reasons for why degraded mode occurs, but common for all failure modes is that degraded mode may result in an increased risk and requires compensating measures. NOG 070 (2018) suggest such measures to be

- Proof testing
- Start-up and/or shutdown
- Preventive maintenance activities
- Field equipment malfunction and repair
- Field equipment replacement

For this option, it should be paid attention to the repair time assumptions made in calculations for PFD. Requirements for system behaviour upon fault detection is provided by IEC 61508-2 (2010). Depending on the HFT the requirements are as followed

- For HFT > 0

  - Isolation and repair of faulty part. Repair should be performed within the mean repair time assumed in calculations for PFD. If not, an action to achieve safe state shall take place.

- For HFT = 0
  - Repair shall be performed within mean repair time assumed in calculations for PFD. Additional compensating measures and constraints shall be provided during the repair. These measures shall be as least as good as the SIS in normal operation.

Option (2) is the second alternative to both these requirements. The drawback of a shutdown, is the stop in production. Loss of production can be costly and oil companies want to avoid this if possible.

4.2.1 Partial Testing

Testing of subsea SIS is performed to make sure that the functional integrity of the SIS is maintained. In addition to regular proof tests and diagnostic testing, partial testing is introduced as the last SIS testing method. Partial stroke testing is discussed as a testing feature for all-electric as the valve is easier to control. It is mentioned by NOG 070 (2018) that partial tests should not replace the need for full proof tests.

In calculations it is assumed that equipment is as-good-as-new (AGAN) after testing, though this is often not the case. It is also assumed that the test is perfect, where all DU failures are detected if present. The approach for considering imperfects tests is mentioned by IEC 61508-6 (2010), and is based on splitting the DU failure rate. The effectiveness of a proof test is expressed by the proof test coverage (PTC). The rate of revealed and non-revealed failures can be expressed by using the PTC and DU failure rate (Rausand, 2014). This thesis does not consider imperfect testing.

Chapter 5

Modelling of All-Electric Actuator

This chapter introduces modelling methods and approaches used for modelling a high-level all-electric actuator concept. Methods for quantification of safety performances, industry requirements and possible strategies are used as input for the analysis.

5.1 System Familiarisation

The starting point for analysis is to get familiar with the system. Through the literature review in chapter 2.2, the outline for all-electric technology is established. Several different configurations and system solutions are proposed by suppliers and oil companies. Aker Solutions has made a reference architecture for a shutdown system which utilise a battery for fail-safe operations (see Figure 5.1). The system comprises in a topside ESD, (e.g. a logic solver, or a push-button), an electrical power unit (EPU), and a power distribution unit. The main functions are shown as part of the secondary well barrier in Figure 5.1. The shutdown system communicates and controls the electronics (e.g. batteries and electrical motor). The final elements are all mechanical parts that make sure the gate valve is closed properly.

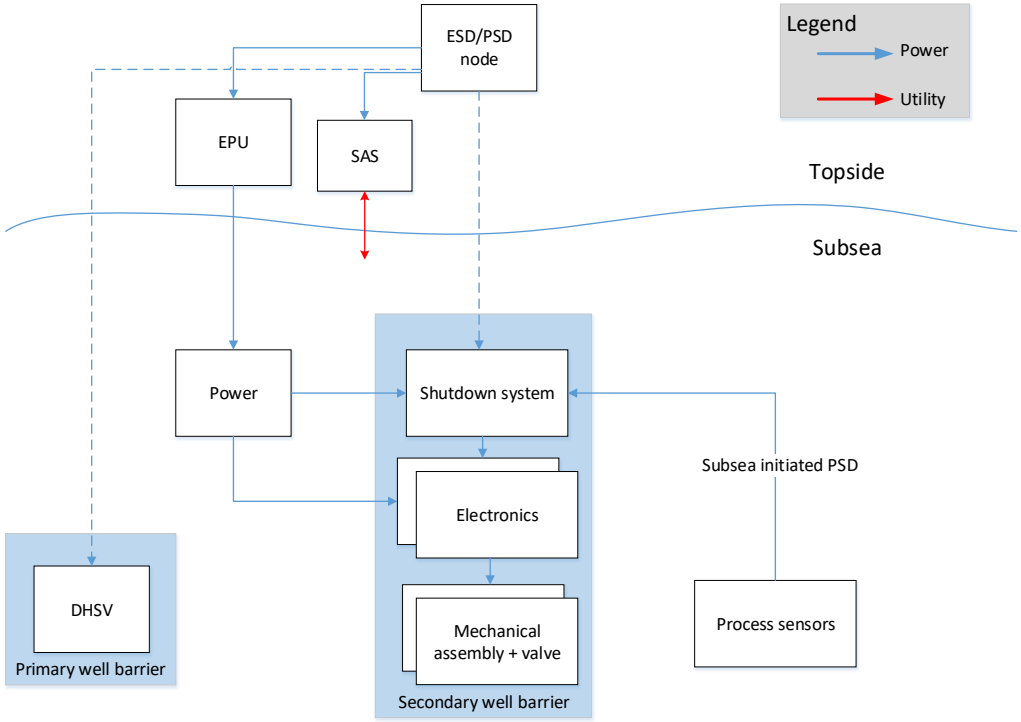


Figure 5.1: All-Electric Safety architecture. Adopted from DNV GL (2018) project

The RBD for the electric actuator is shown in Figure 5.2. The electric actuator is separately retrievable from the XMT, meaning that upon failure of an actuator the whole XMT does not need to be replaced. For the maintenance strategy, this is quite different from the conventional electro-hydraulic actuator where the whole XMT have to repaired upon actuator failure.

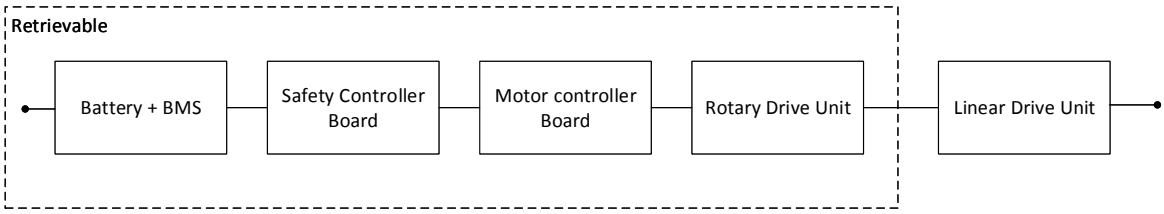


Figure 5.2: Electric actuator RBD

5.2 Failure Modes, Effects and Criticality Analysis

An FMECA was conducted to get a better understanding of the system behaviour. FMECA is normally the first step in reliability analysis to understand how components can fail and determine

effects and criticality upon such failures. The analysis began by identifying all components that are included in the safety application. The boundary is sat to include actuator and valve, which means that topside logic and the push button is outside the scope of the FMECA. The FMECA sheet is attached in appendix A.

The FMECA was conducted in accordance with IEC 60812 (2018), from a high-level hierarchical viewpoint, where the items represent sub-systems and not components. Different operational modes are considered for the whole system:

- *Normal operation:* This is when the safety system is in a "stand-by" mode and no demand has occurred. The process isolation valves are in an open position and the process fluids are flowing through the XMT.
- *Under demand:* This is after a demand has occurred and the system has performed its safety function. The process isolation valve(s) is in a closed position stopping the process fluids from reaching further in the production line.
- *Restart:* This is when the system can restart, and the valve is brought back to an open position.

The FMECA process was performed in a different way than typically performed. A normal approach is to identify all possible failure modes and assess a failure rate for each failure mode. Due to uncertainty about failure rates for the equipment and failure modes identified for each operational mode, the process was reserved. As illustrated in Figure 5.3, for each component a dangerous failure rate was obtained. This failure rate was then assigned as the sum of all failure modes for that particular component. Based on an assumption about diagnostic coverage, the dangerous failure rate was split into either DD or DU according to the detection ability of each failure mode. The classification of each failure mode was marked by an "x" in the FMECA worksheet.

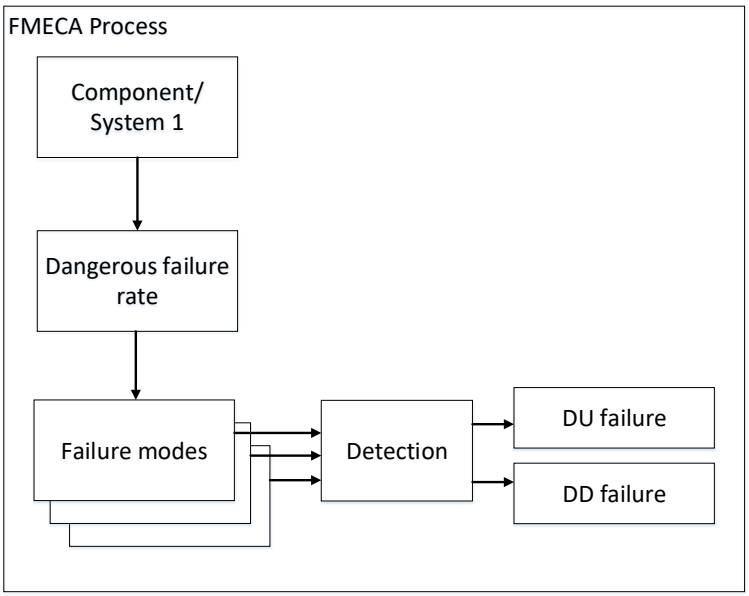


Figure 5.3: The FMECA process

As support for identifying failure modes for each item, the functional classification system was applied. For example, the essential function of the battery is to provide electric power to the electronics. The battery is placed subsea, so an important auxiliary function is the housing, which the battery is placed inside. The battery management system is serving as a protection system for the battery (Lu et al., 2013; Chin et al., 2019). Though this is treated as a separate item, it can be seen as a protective, information and interface function for the battery pack as a whole. During normal operation, the battery is connected to an external power source from topside.

The safety controller is assumed to be similar to a logic solver. For emergency shutdowns, the power signal topside is cut, and the safety controller initiates closure of the valve. After a shutdown signal has occurred, the safety controller is assumed not needed for a restart.

The motor and motor controller provides the torque needed to move the valve stem.

5.2.1 Failure Data Assessment

Failure data have been collected from various sources such as OREDA, PDS and Exida. Failures classified as *Critical* in OREDA is not safety specific, meaning some safe failures are included. These OREDA failure rates are used as a reference for equipment that uses the same technology, for example, the process isolation valves. PDS and Exida are also generic databases, meaning that the item failure rates might not be projecting the actual product performance.

The most challenging part of the failure rate assessment were assumptions about the diagnostic coverage for each item. Equation 3.11 and 3.12 can be used to assess the diagnostic

coverage if the DU failure rate is not provided in the failure data handbooks.

The battery is protected and monitored by the BMS, and through the FMECA process, it was decided that most of such failures are detected by the BMS. The same logic was applied to the controllers. These are electronic items with high potential DC, so it is assumed a diagnostic coverage of 80% for both battery pack and controller units.

Table 5.1: Data Dossier

Item	Failure Rates[1]		Source	Comments
	DD	DU		
Motor	0.24	0.14	Exida	Topside motors
Controller	8.00	1.60	PDS	ESD logic from PDS
Battery pack	1.00	0.20	Approximation	Based on literature
Isolation Valves	0.26	0.18	PDS 2013	Gate Valve and Actuator

[1] Failures per 10^6

Repair and mobilisation times are based on industry judgement. There are many factors that go into the availability of vessels and personnel who perform repairs on subsea equipment. In table 5.2, the assumed mobilisation times are presented. The electric actuator is assumed to be a light and simple system to retrieve from the XMT, where fewer resources are required for the repair. The gate valves are not separately retrievable, meaning the whole XMT needs to be replaced in case of a failure. It is assumed that a lot more resources are needed for retrieval and replacement of the XMT.

Table 5.2: Mobilisation times

Item	Mobilisation time
Electric actuator	168 hours
Isolation valves	1440 hours

5.3 Modelling Method and Approach

There are several methodologies available to perform an analysis on the safety performance. The Petri Nets modelling technique was chosen as the preferred method. Müller et al. (2009) compares the use of analytical approaches suggested in IEC 61508-6 (2010) and stochastic nets, like Markov and Petri Nets. The analysis concludes that Petri Nets are more suited to analyse real industrial systems. Petri Nets modelling is also suggested as a suitable modelling technique in IEC 61508-6 (2010). Compared to analytical formulas, like the once proposed in IEC 61508-6 (2010) and the simplified formulas, the Petri Net has a better ability to handle more complex assumptions about repair strategies. It is mentioned by Signoret (2007) that the IEC 61508-6

(2010) formulas have the underlying assumption that a safe state is reached when performing maintenance and testing, which might not always be the case.

There are several approaches to build a Petri Net model for the safety system. It is difficult to identify all possible states of a component or system. It could be a starting point to assess possible failure states. For a safety system, DU and DD faults are states of interest. DU failures contribute to unavailability of the SIS but is not detected before the component is tested. Some analytical methods like an RBD cannot consider such an assumption. This is also discussed by Signoret et al. (2013), where RBD driven Petri Nets are introduced. The concept of RBD driven Petri Nets is also discussed in chapter 3.6.2.

ISO TR 12489 (2013) provides examples of how to use Petri Net for reliability calculations. To obtain the probabilistic parameters of interest, ISO TR 12489 (2013) present an auxiliary Petri Net for unavailability, reliability and frequency calculations. The following two standards on Petri net modelling for reliability and system modelling were used as a reference to build a Petri Net model for the all-electric actuator system.

- IEC 62551 (2012) provide general techniques for Petri Net modelling
- ISO TR 12489 (2013) is a more specific technical report on reliability calculation methods for safety systems in the process industry

Due to the authors limited knowledge in computer programming, the Petri Net model and simulation is built using the GRIF software[1] package. GRIF is a software package developed by SATODEV who provides several simulations and Boolean modelling tools. The Petri Net simulation module uses a Monte-Carlo simulation engine called MOCA-RP, developed by French oil company Total. Signoret et al. (2013), Signoret (2007), Liu and Rausand (2016), and Wu et al. (2018) have used the GRIF software for Petri Net modelling in these respective papers.

Generic safety functions provided in NOG 070 (2018) are used as a basis to create the all-electric safety functions. Isolation of a subsea well starts when an emergency shutdown (ESD) is initiated topside followed by a power cut in the electrical power unit. When signals are no longer present subsea, the controllers initiate closure of the valve to reach a safe state. The RBD in Figure 5.4 are made for the all-electric actuator system. Failure rates and PFD values are provided by NOG 070 (2018), where fire and gas detection logic and ESD logic has a proposed $\text{PFD}_{\text{avg}} = 1.9\text{e}{-}04$. The initiating push button has $\lambda_{DU} = 0.3 \times 10^{-6}$ according to PDS handbook 2013 (SINTEF, 2013).

[1] `http://grif-workshop.com`

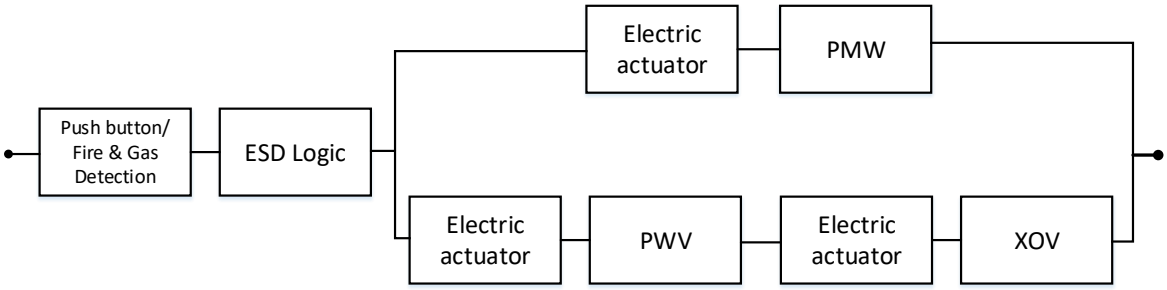


Figure 5.4: RBD for secondary well barrier isolation

The basis for the model of the electric actuator is illustrated in a basic flowchart shown in Figure 5.5. The actuator starts in a working condition. When a failure occurs, it is either DD or DU failure. DD failures are detected immediately and an ROV is called to do the retrieval and repair. DU failures are not detected before a proof test is initiated. Once a failure is detected by a proof test, the ROV is called to retrieve and replace the actuator. When the repair/replacement is done, the system goes back to a working state.

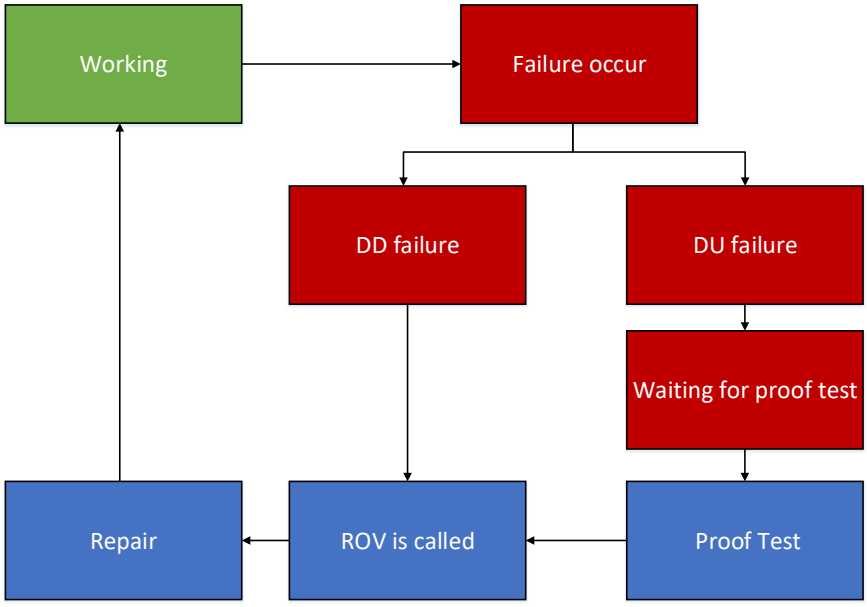


Figure 5.5: Flowchart of the electric actuator Petri Nets model

The following assumptions were made for the Petri Net model

- Failures are exponentially distributed
- All components are as good as new after proof testing and repair
- A functional test is perfect, meaning all hidden failures are detected

- No common cause failures are considered

The electric actuator is modelled with two possible states; working or, failed (see Figure 5.6). The transitions are under Dirac law meaning that it takes a deterministic value. One token is placed in place `Act_W` indicating that the system starts in a working state. For the first transition, `Act_failure`, to fire, some conditional arguments need to be realised. These are modelled as guards. Here, the guards are the Boolean variables `B_state`, `SC_state` and `M_state`. After firing, transition `Act_failure` updates the Boolean variable `Act_state` to false (i.e. not working).

When the failure transition is fired, the token reaches the place `Act_F`. It remains in this place until the repair is finished. The guard `?Act_state==true` must be fulfilled for the actuator to return to a working state.

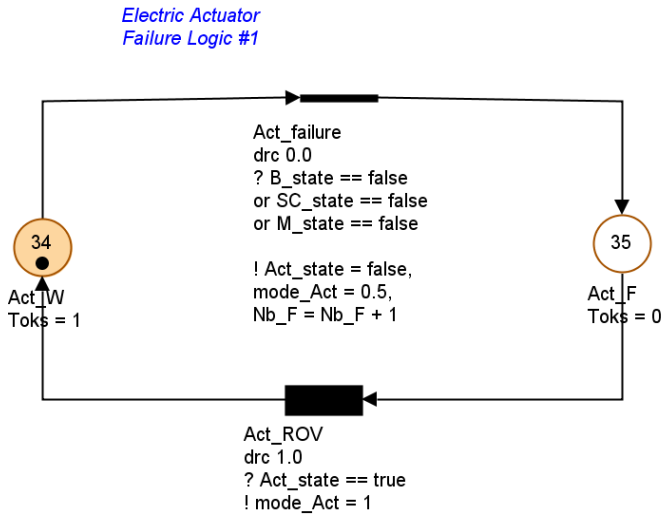


Figure 5.6: Electric actuator Petri Net

All the Boolean variables in Figure 5.6 are updated by other PNs. For the actuator to fail, either the battery, the controller or the motor has to fail. Figure 5.7 shows the Petri Nets for the battery. It is assumed that the battery can either have a DD failure or DU failure, both assumed to be exponentially distributed. Upon DD failure, the system goes straight to `Battery_F`, and the variables `B_state` is updated to false. This enables firing of the transition `Act_failure` from the previous figure (Figure 5.6). The electric actuator is now in a failed state. The same approach is used for DU failures, but since DU failure remains unknown until the subsequent test, a place `Battery_DU` is added. This place allows for calculating the average time with a DU failure.

Once either DD or DU failures are detected, the repair action is initiated. The variable `callROV` becomes true, and the actuator is retrieved and replaced.

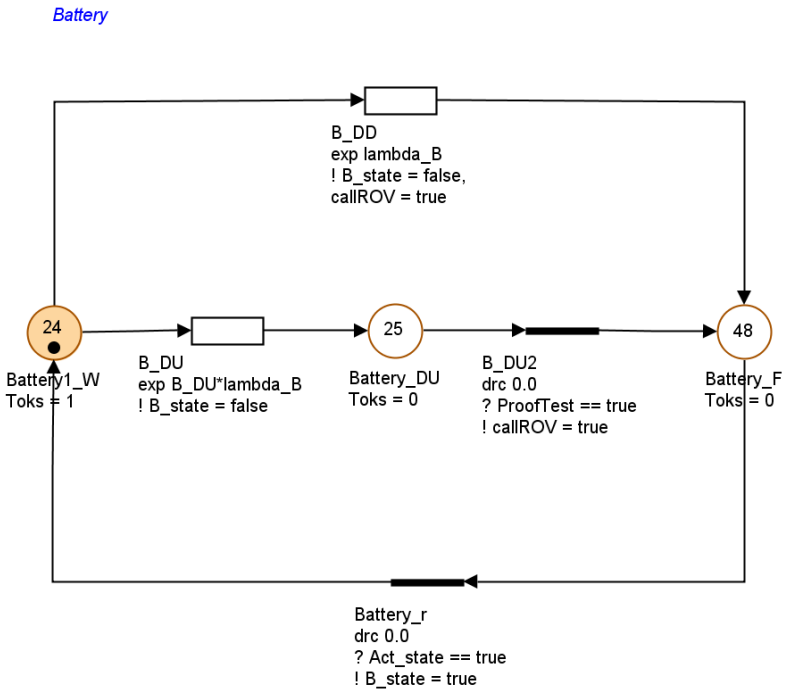


Figure 5.7: Petri Nets for battery failure

The ROV operation is a quite simple Petri Net. Once the variable `callROV` becomes true, the ROV will be in operation for a specific time given by the deterministic parameter ROV_Repair.

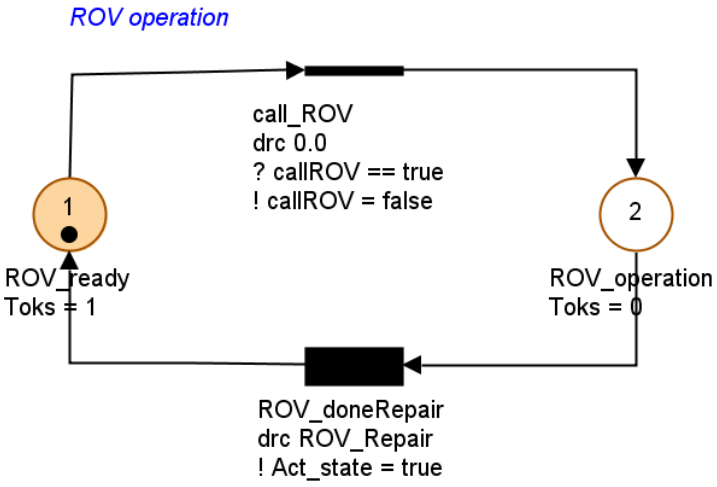


Figure 5.8: Petri Nets for ROV operation

The valve does not have the possibility to be retrieved and replaced separately. This means that the repair time cannot be assumed to be as short as for the actuator part. Thus, the valve

part is modelled as a separate system with the same approach. The difference is that when both valves are failed, a vessel is called for retrieving and repair of the XMT. Figure 5.9 shows the Petri Nets for PMV valve. Both PMV and PWV are modelled this way, with the conditional argument that both have to fail before a vessel is called.

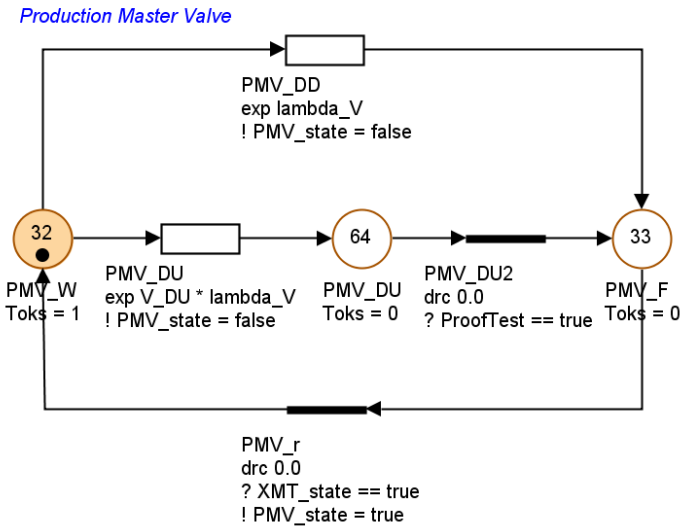


Figure 5.9: Petri Nets for XMT valve

The basis for the calculation of average unavailability of the system is the RBD presented in Figure 5.4. The methodology for RBD driven Petri Net was used to build a sub-Petri Net which calculates the average down time of the system. As seen by the RBD, the system becomes unavailable when a failure occurs in both the upper and lower path. A sub-Petri Net for calculation of the mean unavailability was made, and seen in Figure 5.10. When the conditions given by the guard are fulfilled, the transition is enabled and a token is placed in the place `Unavailability`. It remains in this place until the necessary repairs are performed. The variable `pfd` is used to observe the unavailability per time unit. Both ISO TR 12489 (2013) and Signoret et al. (2013) propose to observe MTTF and unreliability in an auxiliary Petri Net for calculation. The places `MTTF` and `Unreliability` are added to the Petri Net in Figure 5.10.

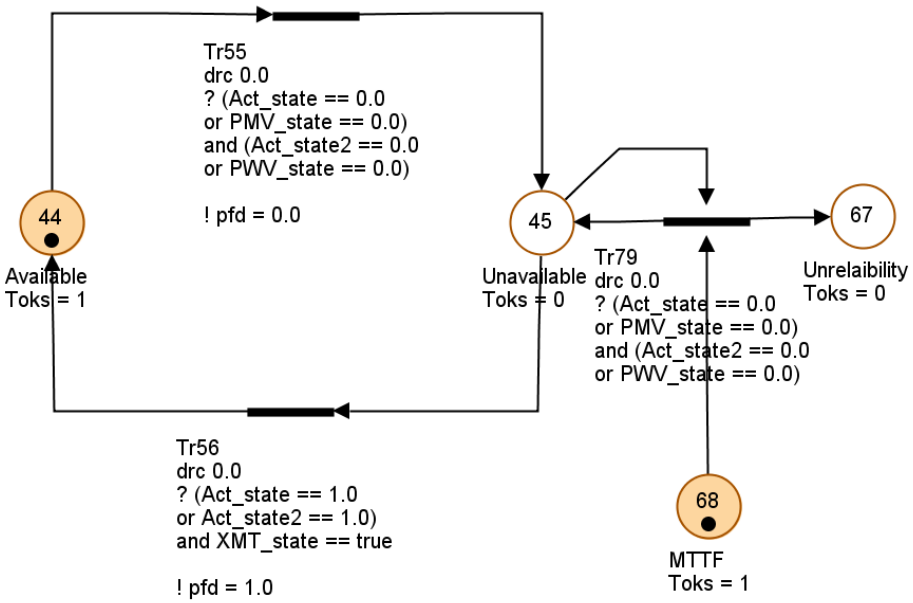


Figure 5.10: Auxiliary Petri Net for unavailability calculation

5.4 Modelling cases

To see the effects of different maintenance and repair strategies, different modelling cases were made. These cases have a different assumption and the Petri Net variables were modified accordingly.

The base case for the study is operation with testing once every year. In the case of an actuator failure, it is assumed retrieved by an ROV and replaced with a new available spare actuator. Operation is continued while the repair is ongoing.

Case 1 shares many similarities with the base case, but here it is assumed that all components are tested once a DD failure occur (i.e. outside the regular test interval). This approach is similar to the "insert test" strategy discussed by Liu and Rausand (2016). In this case the proof test interval is constant, meaning that a failure can occur right before the proof test. From a production availability point of view, this assumption is less suited due to stop in production. The production availability is not considered in the model, and the availability of the SIS is not affected.

Case 2 assumes that the repair time can be extended upon DD failures of the actuator. Repair time upon DU failure is unchanged due the practical assumption that repair resources are already available on the location during a proof test. This case is expected to give a very similar result as base case. If considering the IEC 61508 (2010) formula in equation 3.3, the down time due to DU failures is on average much longer than down time due to DD failures. The objec-

tive of this case is to discover the effect of postponing the repair upon a failure in the proof test interval to give more time to plan the repair.

For case 3 it is assumed that repair due to DD failure can be postponed to the subsequent proof test. This assumption might be conflicting with some operational requirements about degraded operation. According to requirements, other risk reducing measures shall be realised to justify this assumption.

5.5 Uncertainty handling

Simulations are performed by utilising the Monte Carlo simulation method. In order to obtain a result with minimal uncertainty, the model should be ran with a satisfying number of histories. The average unavailability of the system was found by observing the mean time spent in the unavailable state. The mean and standard deviation was obtained from simulation results. From chapter 3, equation 3.7 for calculation of the confidence interval was used to present the uncertainty of the Monte Carlo simulation.

Chapter 6

Results And Analysis

This chapter presents and discusses the results from the different modelling cases. The Petri Net model and RBD for isolation of production bore presented in chapter 5 are used as a basis for the analysis.

6.1 Results

The calculations have been performed by observing the mean time a token spends in each place. The simulation software utilises the Monte Carlo method to observe variables and mean markings of tokens (i.e. the time a token spends in a place). The following settings were used for the Petri Net simulation:

- Life time = 25 years (219 000 hours)
- Proof test interval = 8760 hours
- Number of histroies = 100 000
- Confidence range at 90%

Normal life time of a subsea field is around 20 to 30 years, thus a 25 year life time with a proof test once every year has been chosen for the simulation. Different number of histories have been evaluated to see where the model started converging, and 100 000 histories gave the best results within an acceptable computation time. Due to some uncertainty about the failure rates, a confidence level of 90% has been chosen.

The four different cases was considered in four simulation runs, each with two different repair times for the ROV operation, 168 hours and 720 hours. A longer repair time of 720 hours was chosen to see effects of a more conservative approach. The simulation is based on the Figure 5.4, excluding the push button and ESD node and the results are shown in table 6.1.

- Base case: Normal operation

- Case 1: Proof test upon DD failure
- Case 2: Delayed repair upon DD failure (168 hours)
- Case 3: Delayed repair upon DD failure (subsequent proof test)

Table 6.1: Case Results

	PFD_{avg}			
Repair time	Base Case	Case 1	Case 2	Case 3
168	2.37e-4	1.87e-4	2.52e-4	3.28e-3
720	4.13e-4	3.51e-4	4.41e-4	3.71e-3

Compared to the base case, both case 1 and case 2 shows similar results for PFD_{avg}. Case 1 gives the lowest PFD_{avg} which is reasonable due to the assumption that a proof test is run if a DD failure occurs. Case 2 gives a marginal higher PFD_{avg} as the downtime induced by DD failures is extended by one week, while the repair time upon DU failures is unchanged. Case 3 has the most conservative assumption by deferring the repair to the subsequent proof test. This reflects the radical different result compared to the other cases.

From chapter 3.5, the PFD values correspond to a certain SIL ranging from SIL 1 to SIL 4. Case 3 is more than one SIL higher than the other cases, meaning the safety performance is not as good as for the other cases. While the base case, case 1, and case 2 are in the lower range of SIL 3, case 3 is in the lower half of SIL 2.

The results provided above are average values within the proof test interval. Figure 6.1 shows the values obtained from the simulation for the base case with ROV repair time of 168 hours only. Due to the properties of the model, the curve is not as smooth as those typically obtained by other methods, for example, the Markov approach. The data points are calculated once every 24 hours, throughout the simulation lifetime, for every history. A regression line is fitted to the calculated values for illustrative purposes only. The curve peaks at around 6.5e-4, which still is within the SIL 3 range. Note that for this particular figure, the x-axis shows the number of days, not hours.

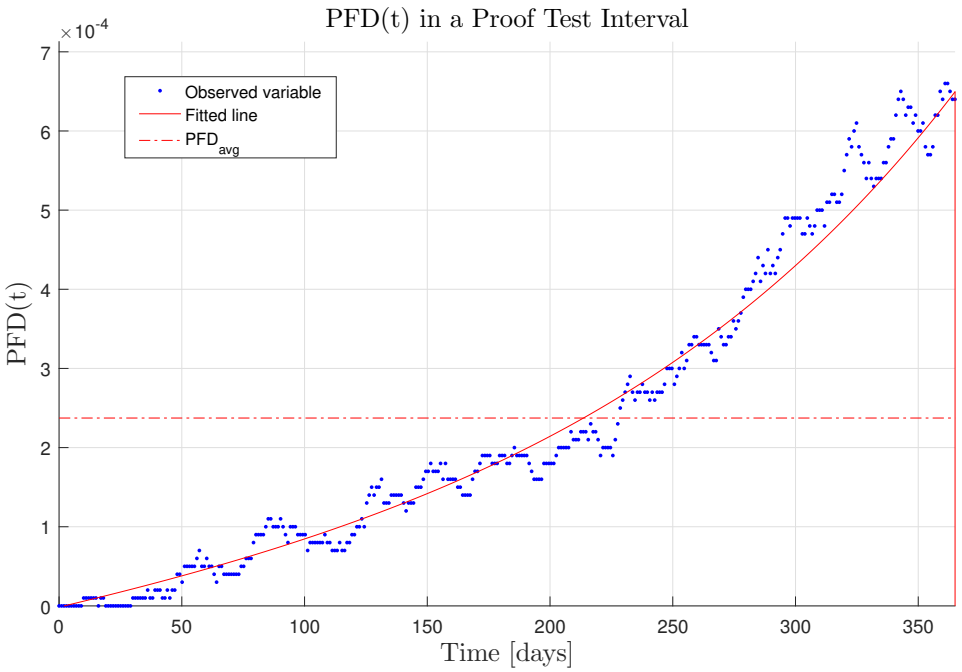


Figure 6.1: Unavailability per time unit for base case

Figure 6.2 shows the comparison between base case and case 1. The first four proof tests are shown in the graph, where the PFD(t) goes back to zero after each proof test due to the assumption about as good as new. The difference is marginal, but the peak values of case 1 reflect the difference in the PFD_{avg} values.

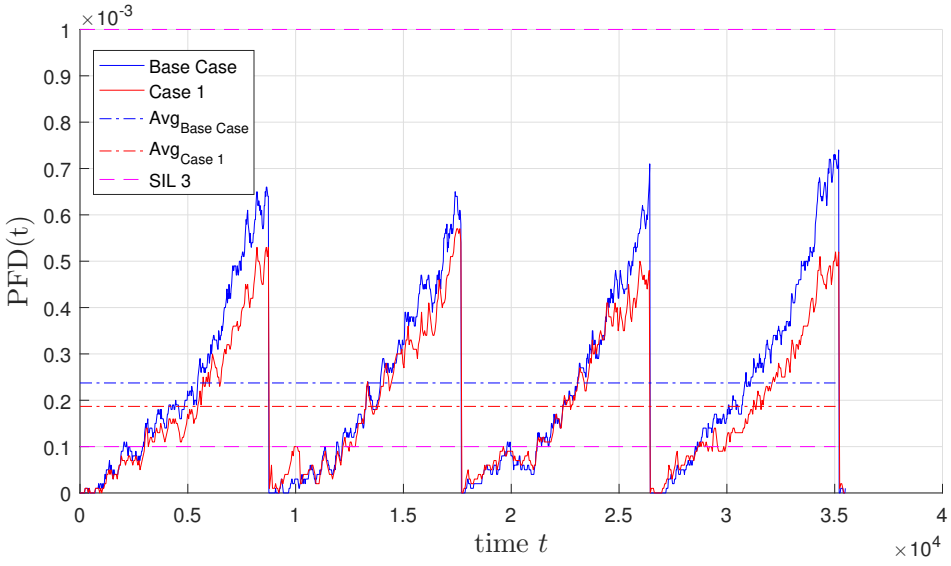


Figure 6.2: Base case versus case 1

Similar to Figure 6.2 above, the difference between the base case and case 2 is shown in Figure 6.3. The difference is even smaller for these two cases, as indicated by the average values.

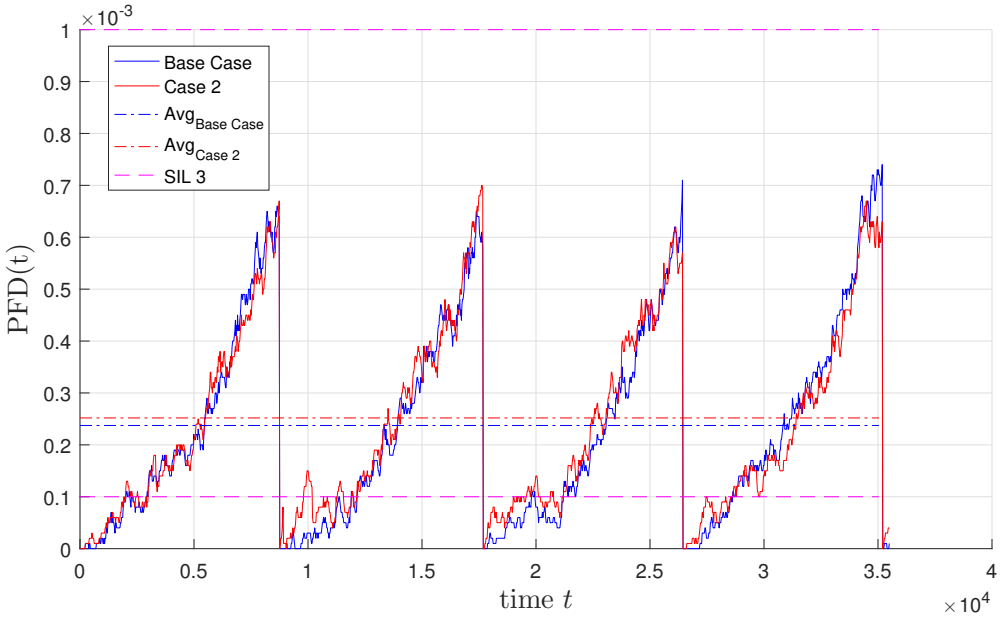


Figure 6.3: Base Case versus Case 2

The difference between base case and case 3 is the most evident. The PFD(t) is climbing quite fast into the SIL 2 region shown by the black dotted lines in Figure 6.4. Possible actions to prevent the fast climbing can be to decrease the proof test interval or introduce partial stroke testing, which has not been investigated in this thesis. Due to the improved control of the electric actuator movement, partial stroke testing is a testing method that can be utilised for case 4.

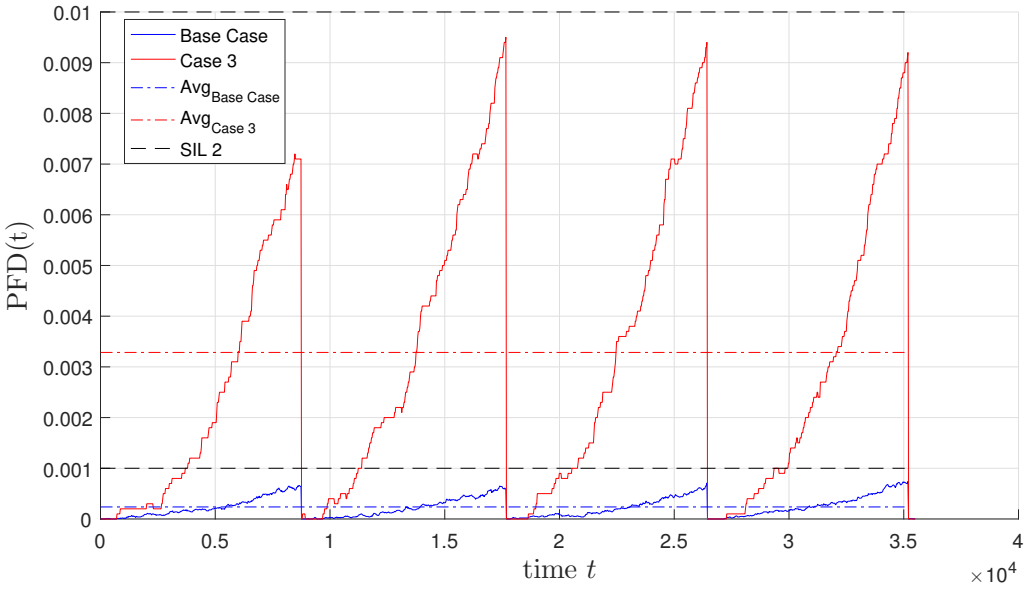


Figure 6.4: Base Case versus Case 3

The simulation results were obtained by studying the actuators and XMT gate valves only. For comparison to the SIL requirements discussed in chapter 4, the ESD logic, and push button are added to the calculation.

Table 6.2: SIF for secondary barrier isolation of subsea XMT

	PFD_{avg}			
Item	Base case	Case 1	Case 2	Case 3
Valves	2.37e-4	1.87e-4	2.52e-4	3.28e-3
ESD logic	1.90e-4	1.90e-4	1.90e-4	1.90e-4
Push button	1.30e-3	1.30e-3	1.30e-3	1.30e-3
Sum	1.73e-3	1.68e-3	1.74e-3	4.77e-3

Table 6.2 shows that the PFD_{avg} for all cases are within the SIL 2 requirement for secondary barrier isolation of the production bore.

6.1.1 Results Compared to Analytical Approach

To check the validity of the simulation results, a comparison to an analytical approach has been made. Simulation results might deviate from analytical results once system complexity increases. The results presented in Figure 6.3 are from simulation of the base case and shows the PFD_{avg} for the internal components of the actuator. This corresponds to the RBD made for the actuator in Figure 5.2. The analytical results has been calculated based on IEC 61508 (2010) formulas and the simplified formulas discussed in chapter 3.6.

Table 6.3: Comparison of Simulation and Analytical Approach

	Simulation		Analytical	
Item	PFD_{DU}	PFD_{DD}	PFD_{DU}	PFD_{DD}
Battery	9.00e-4	1.99e-4	8.79e-4	1.68e-4
Motor	6.27e-4	6.40e-5	6.31e-4	4.03e-5
Controller	6.92e-3	1.60e-3	7.01e-3	1.08e-3
Sum	8.44e-3	1.86e-3	8.51e-3	1.55e-3

The PFD_{avg} due to DU failures is quite similar for both simulation and analytical methods. The difference between DD failures is more evident than those for DU failures. This might be due to how DD failures have been calculated in the model. Once a DD failure occurs, the token is placed in the failure state of the component. This state is shared with tokens from the DU failure, meaning that the a small portion of the down time for DD failures are due to DU failures. This does not have impact on the overall PFD_{avg} for the system.

6.1.2 Uncertainty

The Monte Carlo simulation was run with a 90% confidence range. Table 6.4 shows the confidence measures from the simulation runs for the base case, case 1 and case 2. The mean and standard deviation are obtained from the simulation, and the 90% confidence range was calculated by using equation 3.7. Due to the high number of histories in the simulation is it assumed that the calculated values of PFD_{avg} is normally distributed according to the central limit theorem.

Table 6.4: Simulation uncertainty parameters

Case	PFD_{avg}	σ	90%CI
Base case	2.37e-4	2.11e-3	[2.26e-4, 2.48e-4]
Case 1	1.87e-4	1.67e-3	[1.78e-4, 1.95e-4]
Case 2	2.52e-4	2.14e-3	[2.41e-4, 2.63e-4]

Figure 6.5 shows the probability density function for the base case, case 1 and case 2. From the figure it seems like the results from case 1 are more accurate than the other two.

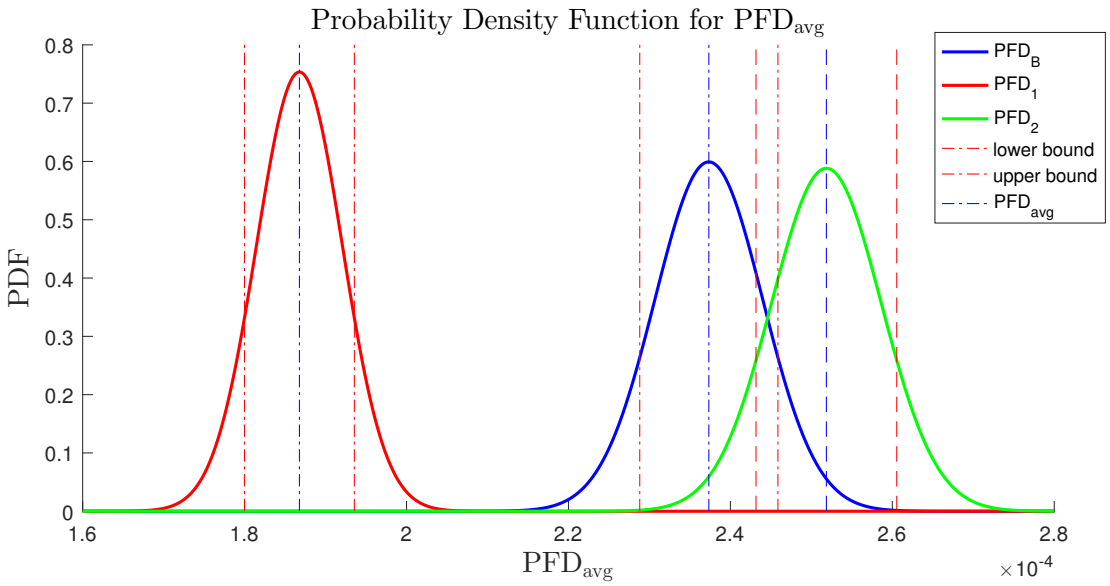


Figure 6.5: 90% Confidence Interval for PFD$_{avg}$

6.2 Remarks and Discussion of Results

The industry requirements and framework were discussed in chapter 4 to use as a benchmark for the performance of the electric actuator system. Results show that the quantitative performance is within the requirement of SIL 2 for secondary barrier isolation of the production bore.

In the analysis, it is assumed that production can continue even if one barrier valve is failed. As discussed in chapter 3.2.1, operation with a degraded barrier is allowed as long as other risk-reducing measures are introduced, such as proof testing or partial testing. Effects from partial stroke testing are not considered in the analysis but recognised to have a positive effect on the PFD$_{avg}$. Proof tests were assumed to have no impact on the degradation of the equipment, though this is not likely to be the case. Considerations regarding the degradation of equipment should be made if more frequent proof tests or partial tests are introduced when operating in degraded mode. During the FMECA process, it was recognised that diagnostic testing of batteries is performed by the BMS, and the literature states that such a system detects many potential failure modes. In normal operation, the battery is connected to a power source and it is not clear whether or not this is the case during proof tests. A single 1oo1 battery configuration was assumed in the proposed model though redundant configurations are discussed in the literature. A redundant battery configuration opens the possibility to utilise other test scheduling methods like sequential or staggered testing, which allows at least one battery to be fully charged and tested within the one-year test interval.

The actuator goes from being a mechanical spring system to an electro-mechanical system which enables failure monitoring of individual actuators. Due to long mobilisation and repair

times for subsea equipment, easily retrievable and individually controlled actuators add flexibility to repair strategies compared to electro-hydraulic actuators. The results show that requirements are met even when DD failures are considered in the calculations. DD failures are often associated with production losses due to shutdown and repair. In operation, DD failures require some action to be made to compensate for the increased risk, where proof tests or partial tests were suggested as measures if the repair is deferred.

For subsea in general, fewer resources are required upon failures of electronic modules which means that repair actions can be accomplished faster. In comparison to the isolation functions provided by NOG 070 (2018), the electronic modules and controllers can be placed inside each actuator. The functionality previously found in the control modules are distributed onto each valve which allows for control of individual valves. This reason was used when assuming that production can continue upon loss of an actuator. For isolation of the production bore by only utilising the XMT valves, this flexibility is an advantage. For example, if the control module of an electro-hydraulic actuator fails, and the DHSV is not utilised, control of the XMT valves are lost and a shutdown is initiated.

The failure rates are collected from generic databases of equipment that has existed in operation for quite some time. It is difficult to assess if such an approach reflects the actual product performance as the actuator internals might use components with other failure characteristics than those from the generic database. A more detailed analysis of the internal components of the actuator could have given a more accurate estimate to be used in a development project. The model seems to provide results similar to analytical approaches when basic repair strategies are considered. The Petri Net modelling approach can easily be adapted to suit other, more advanced strategies. For the comparison to the electro-hydraulic counterpart presented in NOG 070 (2018), the model seems to be comparable regarding the functional level.

Chapter 7

Conclusion

This chapter presents a summary and conclusion of the work that has been done for this thesis. A discussion is added which presents strength and weaknesses of the results, and how they might be utilised for further work. The objective for a discussion part is to discuss the contribution of the thesis in a larger context.

7.1 Summary & Conclusions

The objective of this thesis is to propose an approach for modelling and calculation of the reliability and safety performance of an all-electric subsea actuator. This is done by studying the advantages and challenges for the development of all-electric subsea equipment in relation to the safety performance it is required to perform. Regulations on the NCS require an adequate level of safety to be documented before equipment is installed.

Subsea XMTs are installed on the seabed to prevent an unintentional flow of hydrocarbons to reach the environment. The XMT is an assembly of valves and fittings which acts as barrier elements towards the environment. The valves are controlled by an SIS to make sure the valves are closed in the presence of any hazardous events that might occur during production. The standard solution for subsea SIS is based on a combination of electric and hydraulic power to control the valves, but challenges associated with hydraulics are addressed by the industry. As fields are developed at greater depths, and with longer distances to existing infrastructure, electric control is suggested as a replacement for hydraulic-based control systems. The reliability of hydraulic-based solutions has, through many years of development and operational experience, wide acceptance in the industry. Demonstrating safety and reliability with an all-electric solution requires documentation that the safety performance is at least as good as for the existing electro-hydraulic system.

Methods and requirements for reliability and safety assessment of SIS are established by the standards IEC 61508 (2010) and IEC 61511 (2016). These methods are utilised to create a model

for quantification of random hardware failures of a proposed all-electric actuator system. Necessary components and functions for the all-electric system are identified through a literature review of relevant papers mostly conducted by the industry. Battery powered fail-safe mechanism is considered as the best options due to the system simplicity compared to a spring solution. Batteries are not commonly used in safety application on the NCS, which is reflected in the lack of available failure data. This results in some uncertainty regarding battery failure characteristics and applicability for proof testing. The other components are assumed to be similar to existing components that are found in generic failure databases.

The modelling approach proposed in this thesis are made considering a comparison to existing requirements for safety performance. The actuator is installed as part of a SIF for isolation of the production bore. The boundary for the model was made to make a fair comparison with existing requirements suggested by guideline NOG 070 (2018). This is identified to be an ESD node, a push button for manual shutdown, the control system, actuators and the gate valves. The model proved to be accurate for calculations of simple and more complex operational strategies compared to analytical approaches suggested by IEC 61508 (2010).

The results show that the proposed system is compliant with the industry requirements for secondary well barrier isolation of the production bore. It was assumed that production continued as long as one barrier valve, including actuator, was functional, which proved to have benefits for different repair strategies. The PFD_{avg} was improved if a proof test was initiated upon DD failure of one actuator, compared to the normal case where a proof test was run only once a year. It was also considered that the repair could be extended from one to two weeks, which had a marginal impact on the PFD_{avg} within the one-year test interval. A less conservative approach was tested by assuming that repair of DD failures was deferred to the subsequent proof test. Although the PFD_{avg} was within the requirement of SIL 2 when considering the whole SIF, such an assumption should not be considered without further investigation of the effects of partial tests or an increase of the proof test frequency.

7.2 Discussion

This thesis have elaborated on the reliability and safety performance of an all-electric subsea actuator. It challenges operational strategies by testing the effects of reduced performance upon a failure in the safety system. Production down time is directly connected to lost revenue and a production shutdown is avoided if possible. The results might show weakness is terms of level of abstraction, where a more high level approach were used. A deeper analysis of the internal components of the actuator could have improved the PFD estimate of it. No common cause failures, or systematic failures are considered for the results.

7.3 Recommended Further Work

Recommendations for further work are suggested in the following bullet points:

- Effects of partial testing as a risk-reducing measure that can allow for operation in degraded mode. Through the thesis is was identified that all-electric actuators have great potential for control of partial stroke test.
- Investigation of different configurations of internal components in the actuator. Compare the safety performance of a spring solution to a battery solution.
- A detailed assessment of the battery safety integrity. A question might be if the battery needs to be safety rated, and how can this be done? The automotive industry use ASIL rated batteries, but how reliable is this compared to SIL as presented in this thesis?

Bibliography

Abicht, D., Halvorsen, G.-R., and Ramberg, R. M. (2017). *Subsea All-Electric*. Offshore Technology Conference.

Aruo, R., Lund, B., and Onshus, T. (1995). *Subsea HIPPS Design Procedure*. Offshore Technology Conference.

Bell, J., Chin, Y. D., and Hanrahan, S. (2005). *State-Of-The-Art Of Ultra Deepwater Production Technologies*. Offshore Technology Conference.

Bernt, T. and Smedsrud, E. (2007). *Ormen Lange Subsea Production System*. Offshore Technology Conference.

Billinton, R. and Peng Wang (1999). *Teaching distribution system reliability evaluation using Monte Carlo simulation*, volume 14, pages 397–403.

Bouquier, L., Signoret, J. P., and Lopez, R. (2007). *First Application of the All-Electric Subsea Production System-Implementation of a New Technology*. Offshore Technology Conference.

Brissaud, F., Charpentier, D., Fouladirad, M., Barros, A., and Bérenguer, C. (2010). *Failure rate evaluation with influencing factors*, volume 23, pages 187–193. Elsevier.

Chin, C. S., Jia, J., Hay King Chiew, J., Da Toh, W., Gao, Z., Zhang, C., and McCann, J. (2019). *System design of underwater battery power system for marine and offshore industry*, volume 21, pages 724–740. Elsevier.

Cockshott, J. (2005). *Probability Bow-Ties: A Transparent Risk Management Tool*, volume 83, pages 307–316. Elsevier.

Creech, G. (2014). *IEC 61508 Systematic Capability*, volume 47, pages 125–128. SAGE PublicationsSage UK: London, England.

DNV GL (2018). Safety 4.0. `https://www.dnvgl.com/technology-innovation/oil-gas/safety40/index.html`. [Online; accessed 21-05-19].

Exida (2015). *Safety Equipment Reliability Handbook*. Exida, 4 edition.

Grebe, J. C., Goble, W. M., and Chalupa, R. P. (2018). *FMEDA Development Paper*. EXIDA, Sellersville, PA.

Halvorsen, V. S. and Koren, E. (2008). *All Electric Subsea Tree System Development*. Offshore Technology Conference.

Hauge, S. and Øien, K. (2016). Guidance for barrier management in the petroleum industry. `https://www.researchgate.net/publication/309319877_Guidance_for_barrier_management_in_the_petroleum_industry`.

IEC 60812 (2018). *Failure Modes and Effects Analysis (FMEA and FMECA)*. International Electrotechnical Commission, Geneva.

IEC 61078 (2016). *Analysis Techniques for Dependability: Reliability Block Diagrams*. International Electrotechnical Commission, Geneva.

IEC 61508 (2010). *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*. International Electrotechnical Commission, Geneva.

IEC 61508-2 (2010). *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems: Part 2: Requirements for Electrical/Electronic/Programmable Electronic Safety Related-Systems*. International Electrotechnical Commission, Geneva.

IEC 61508-6 (2010). *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems: Part 6: Guidelines on the Application of IEC 61508-2 and IEC 61508-3*. International Electrotechnical Commission, Geneva.

IEC 61511 (2016). *Functional Safety: Safety Instrumented Systems for the Process Industry Sector*. International Electrotechnical Commission, Geneva.

IEC 62551 (2012). *Analysis techniques for dependability: Petri net technique*. International Electrotechnical Commission, Geneva.

ISO TR 12489 (2013). *Petroleum, petrochemical and natural gas industries: Reliability modelling and calculation of safety systems*. International Organization for Standardization, Geneva.

Johannessen, G. (2018). Reliability and Safety Assessment of All-Electric Subsea Concepts.

Lei, Y. and Huang, A. Q. (2017). *Data center power distribution system reliability analysis tool based on Monte Carlo next event simulation method*, pages 2031–2035. IEEE.

Lima, F. S., Storstenvik, A., and Nyborg, K. (2011). *Subsea Compression: A Game Changer*. Offshore Technology Conference.

Liu, Y. and Rausand, M. (2016). *Proof-testing strategies induced by dangerous detected failures of safety-instrumented systems*, volume 145, pages 366–372. Elsevier.

Lu, L., Han, X., Li, J., Hua, J., and Ouyang, M. (2013). *A review on the key issues for lithium-ion battery management in electric vehicles*, volume 226, pages 272–288. Elsevier.

Lundteigen, M. A. and Rausand, M. (2006). Assessment of Hardware Safety Integrity Requirements. *Proceedings of the 30th ESReDA Seminar*.

Lundteigen, M. A. and Rausand, M. (2008). Partial stroke testing of process shutdown valves: How to determine the test coverage. *Journal of Loss Prevention in the Process Industries*, 21(6):579–588.

Moe, S., Monsson, O. S., Rokne, y., Kumar, A., and Johansen, C. (2018). *Electric Controls Technology: The Role in Future Subsea Systems*. Offshore Technology Conference.

Müller, J. R., Ständer, T., and Schnieder, E. (2009). *Improving System Safety Modelling in accordance to IEC 61508 by using Monte Carlo Simulations*, volume 42, pages 193–197. Elsevier.

Murata, T. (1989). *Petri nets: Properties, analysis and applications*, volume 77, pages 541–580.

Nadir, F. E., Baraka, I. H., Bsiss, M., and Amami, B. (2016). *Influence of failure modes and effects analysis on the average probability of failure on demand for a safety instremented system*, pages 867–871. IEEE.

Nelson, S. G. (2010). *AKPO: The Subsea Production System*. Offshore Technology Conference.

NOG 070 (2018). *Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry*. Norwegian Oil & Gas Association.

NOG 117 (2008). *Recommended guidelines for well integrity*. Norwegian Oil & Gas Association.

NORSOK D-010 (2013). *well integrity in drilling and well operations*. Norsk Standard.

NORSOK S-001 (2018). *Technical Safety. Edition 5, June 2018*. Norsk Standard.

NTNU (2018). *NTNU BRU21: Strategy for Oil and Gas*. Norwegian University of Science and Technology, Trondheim. [Online; accessed 20-05-19].

OREDA (2015). *OREDA handbook; Offshore Reliability handbook*, volume 2 - Subsea Equipment. OREDA Participants, 6th edition.

PSA (2019). Norwegian Petroleum Safety Authority. `https://www.ptil.no/en/about-us/role-and-area-of-responsibility/`. [Online; accessed 25-04-19].

Ramberg, R. M., Davies, S. R. h., Rognoe, H., and Oekland, O. (2013). *Steps to the Subsea Factory*. Offshore Technology Conference.

Rausand, M. (2014). *Reliability of Safety-Critical Systems : Theory and Applications*. Wiley, Hoboken, NJ, 1st edition.

Rausand, M. and Høyland, A. (2004). *System Reliability Theory: Models, Statistical Methods, and Applications*. Wiley, Hoboken, NJ, 2nd edition.

Rivenbark, M., Khater, S., Dietz, W., and Barnes, S. (2001). *An Innovative All Electric Well Production System*. Society of Petroleum Engineers.

Signoret, J. P. (2007). *High-Integrity Protection Systems (HIPS): Methods and Tools for Efficient Safety Integrity Levels Analysis and Calculations*. Offshore Technology Conference.

Signoret, J.-P., Dutuit, Y., Cacheux, P.-J., Folleau, C., Collas, S., and Thomas, P. (2013). *Make your Petri nets understandable: Reliability block diagrams driven Petri nets*, volume 113, pages 61–75. Elsevier.

SINTEF (2013). *Reliability Data for Safety Instrumented Systems*. PDS data handbook 2013 edition.

Sklet, S. (2006). *Safety barriers: Definition, classification, and performance*, volume 19, pages 494–506. Elsevier.

Williard, N., He, W., Hendricks, C., Pecht, M., Williard, N., He, W., Hendricks, C., and Pecht, M. (2013). *Lessons Learned from the 787 Dreamliner Issue on Lithium-Ion Battery Reliability*, volume 6, pages 4682–4695. Multidisciplinary Digital Publishing Institute.

Winther-Larssen, E. and Massie, D. (2017). *All-Electric as an Enabler for More Cost Effective Developments on Cluster Systems*, page 15. Offshore Technology Conference, Houston, Texas, USA.

Wu, S., Zhang, L., Lundteigen, M. A., Liu, Y., and Zheng, W. (2018). *Reliability assessment for final elements of SISs with time dependent failures*, volume 51, pages 186–199. Elsevier.

Zhang, Y., Tang, W., and Du, J. (2017). *Development of subsea production system and its control system*, pages 117–122. IEEE.

Zio, E., Baraldi, P., and Liu, Y. (2013). *Testing Strategies of Redundant Safety Instrumented Systems with Dangerous Detected Failures*, volume 33.

Appendix A

FMECA worksheet

(inserted on next page)

Description of unit				Description of failure			Effect of failure		Failure Classification				Comments
Item ID	Item name	Function	Operational mode	Failure mode	Failure cause	Detection	Local effect	Global effect	DD	DU	SD	SU	
1	Battery	Provide power to electronics	Normal operation	Fail to function	Ageing, cell short circuit	Detected by BMS	Not able to power electronics if other power source not available	Loss of redundant power source Power from topside	X				
					Excessive discharge	No detection	Not able to power electronics	Not able to power electronics upon demand		X			Power cut topside upon ESD. If power requirement is greater than what the battery can delivery.
			Under demand	Fail to function	Excessive discharge requirement on demand	Detected by BMS	Battery lifetime shortended	Not able to power electronics				X	
			Restart	Fail to function	Battery discharged	Detected by BMS	No able to power electronics	Not able to open valve upon restart				X	
2	Battery Management system	Monitor and communicate battery status Protection of battery cells	Normal operation	Fail to function	Loss of communication	Detected by no monitoring status	No protection of battery	No control of battery status	x				Assumed part of battery failure rate
	SUM								1,00E-06	2,00E-07			
3	Safety Controller	Controller unit for safety application	Normal operation	Fail to function	Loss of connection to motor	Detected by internal diagnostics	No safety signal to motor	Not able to close gate valve	x				
				Spurious activation	Wrong input signal	No detection	Safety signal sent to motor	Valve will close				x	
	SUM								8,00E-06	1,60E-06			
4	Motor controller	Controller unit for motor operations	Normal operation	Fail to function	Loss of connection to motor	Detected by internal diagnostics	No signal to motor	Not able to close gate valve	x				Assumed part of motor assembly
5	Motor	Generate torque to move linear drive unit	Normal operation	Reduced torque	Increased friction due to bearing failure, contamination, or misalignment.	Partial Stroke Test or upon demand	Reduced ability to move linear drive unit	Worst case not able to close gate valve		x			Failure rate source exida EMCRH O2

				No rotation	Damage to stator or rotor	Internal diagnostics. Or partial stroke test	Not able to move linear drive unit	Not able to close gate valve	x				
			Restart	Fail to start	Damage to stator or rotor or loss of communcation	Valve does not open	Motor will not provide rotational force	Loss of production				x	
	SUM								2,70E-07	1,62E-07			
6	Linear Drive Unit	Convert rotational movement to linear movement	Normal operation	Breakage	Fracture or contamination	Possibly detected by increased motor torque	Not able to move linear drive unit	Not able to close gate valve		x			PDS failure rate. This is conservative assumptions as the this valve also incl. The hydraulic actuator. Linear drive unit assumed part of valve assembly
7	Production Master/Wing Valve	Process/ Production isolation	Normally open Electric & ROV operated	Fail to close	Stuck valve	Detected by position sensors or process flowmeter	Not able to close valve	Loss of one barrier element		x			
			Under demand Closed position	Fail to open	Stuck valve	Detected by no flow	Not able to open valve	Isolation of well. Production loss from well				x	
	SUM								2,60E-07	1,80E-07			

Appendix B

Matlab Code

The matlab code used to generate figures

```
% parameters
n = 100000;
mean = 0.0002373481518903;  % Base Case, Normal Operation MRT = 168
mean1 = 0.00018677;         % Case 1, Inserted Proof test
mean2 = 0.0002518569145604; % Case 2, delayed repair


std = 0.0021054/sqrt(n);
std1 = 0.0016745/sqrt(n);
std2 = 0.002144588624223/sqrt(n);

alpha = 0.1;

x1 = linspace(0.00016,0.00028,1000);
pdf = normpdf(x1,mean, std)/n;
pdf1 = normpdf(x1, mean1, std1)/n;
pdf2 = normpdf(x1, mean2, std2)/n;

xmin = norminv(alpha, mean, std);       % lower bound of 90% CI
xmax = norminv(1-alpha, mean, std);     % upper bound of 90% CI

xmin1 = norminv(alpha, mean1, std1);    % lower bound of 90% CI
xmax1 = norminv(1-alpha, mean1, std1); % upper bound of 90% CI

xmin2 = norminv(alpha, mean2, std2);    % lower bound of 90% CI
xmax2 = norminv(1-alpha, mean2, std2); % upper bound of 90% CI

% Plots
figure(1)
hold on
plot(x1, pdf,'b','LineWidth',1.5)
plot(x1, pdf1, 'r', 'Linewidth',1.5)
plot(x1, pdf2, 'g', 'Linewidth',1.5)

ylim = get(gca, 'ylim');
plot([xmax xmax],ylim, 'r-.', 'LineWidth', 0.5)
plot([xmin xmin],ylim, 'r-.', 'LineWidth', 0.5)
plot([mean mean],ylim, 'b-.', 'LineWidth', 0.5)

plot([xmax1 xmax1],ylim, 'r-.', 'LineWidth', 0.5)
plot([xmin1 xmin1],ylim, 'r-.', 'LineWidth', 0.5)
plot([mean1 mean1],ylim, 'b-.', 'LineWidth', 0.5)

plot([xmax2 xmax2],ylim, 'r--', 'LineWidth', 0.5)
plot([xmin2 xmin2],ylim, 'r--', 'LineWidth', 0.5)
plot([mean2 mean2],ylim, 'b--', 'LineWidth', 0.5)

title('Probability Density Function for $\mathrm{PFD_{avg}}$',↙
'interpreter','latex','FontSize',14)
ylabel('PDF','interpreter','latex', 'FontSize',14)
xlabel('$\mathrm{PFD_{avg}}$', 'interpreter','latex','FontSize',14)
legend('PFD_B', 'PFD_1', 'PFD_2','lower bound','upper bound', 'PFD_{avg}')
```

```
clear all
clc
% Table input
var1 = readtable('PFD_t_curveTS3.csv'); % csv file from GRIF
var2 = readtable('PFD4_t_curveTS3.csv');
t = var1.Time;
t2 = var2.Time;
value = 1 - var1.Value;
value1 = 1 - var2.Value;

n = 4*370;
reg = value(1:n);
t1 = linspace(0, 380, 380);

figure(1)
hold on
plot(t(1:n),value(1:n), 'b')
plot(t(1:n),value1(1:n), 'r')
plot([0 4*8760], [0.0002373381518903 0.0002373381518903],'b-.', 'LineWidth', 0.5)
plot([0 4*8760], [3.28E-03 3.28E-03],'r-.', 'LineWidth', 0.5)

xlabel('time $t$', 'FontSize', 14, 'interpreter', 'latex')
ylabel('$\mathrm{PFD(t)}$', 'FontSize', 14, 'interpreter', 'latex')
legend('Base Case', 'Case 3', 'Avg_{Base Case}', 'Avg_{Case 3}')
grid on

% Regression fit
function [fitresult, gof] = createFit(t1, reg)
%% Fit: 'untitled fit 1'.
[xData, yData] = prepareCurveData( t1, reg );

% Set up fittype and options.
ft = fittype( 'exp2' );
opts = fitoptions( 'Method', 'NonlinearLeastSquares' );
opts.Display = 'Off';
opts.Normalize = 'on';
opts.Robust = 'LAR';
opts.StartPoint = [0 0.5 -3.88155175269093e-05 -0.493888349750389];

% Fit model to data.
[fitresult, gof] = fit( xData, yData, ft, opts );

% Plot fit with data.
figure( 'Name', 'untitled fit 1' );
hold on
h = plot( fitresult, xData, yData);
plot([0 xData(end)], [0.0002373381518903 0.0002373381518903],'r-.', 'LineWidth', 0.5)
plot([365 365], [0 6.5e-4], 'r')
legend('Observed variable', 'Fitted line','PFD_{avg}', 'Location', 'NorthEast' );
% Label axes
title('PFD(t) in a Proof Test Interval', 'interpreter', 'latex', 'FontSize', 14)
xlabel('Time [days]', 'interpreter', 'latex', 'FontSize', 14)
ylabel('PFD(t)', 'interpreter', 'latex', 'FontSize', 14)
ylim([0 inf])
xlim([0 365])
```

```
grid on
```