NTNU

Norwegian University of
Science and Technology

Testing of Safety Systems: Bad Effects and Their Modelling with Comparative Studies

Guilherme de Azevedo Vale

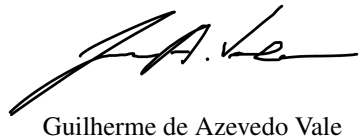
Reliability, Availability, Maintainability and Safety (RAMS)
Submission date: July 2018
Supervisor: Anne Barros, MTP

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

Preface

This master's thesis is written during the fall semester of 2018 in Reliability, Availability, Maintainability and Safety (RAMS) at the Department of Mechanical Engineering. This thesis is the final step of the two years international master program in Mechanical Engineering at the Norwegian University of Science and Technology (NTNU).

The title of the thesis is *Testing of safety systems: bad effects and their modeling with comparative studies* and is written with the guidance of my supervisor professor Anne Barros at NTNU and my co-supervisor Luiz Fernando Oliveira from DNV-GL. The topic motivation was to develop the knowledge on safety-instrumented systems, proof test incompleteness and the degradation effect due to the proof test, which is an industry concern. The thesis is mainly written for people with basic knowledge on reliability theory. However, the author tried to make the thesis in an understandable manner for people with no prior expertise in reliability.



Guilherme de Azevedo Vale
Trondheim, 23rd July 2018

Acknowledgment

First of all, I would like to thank my supervisor Professor Anne Barros (NTNU) and my co-supervisor Luiz Fernando Oliveira (DNV-GL). Professor Anne Barros supported me since my first semester at NTNU in TPK4120 Safety and Reliability, and then during my summer job in SUBPRO under her supervision, and also in TPK4450 Condition Monitoring and later on, in my master thesis. Her intelligence and availability to discuss all the topics in the reliability framework, provided me interesting thoughts and she always was pushing me to go further.

Luiz Fernando Oliveira, R&D Manager at DNV-GL Brazil, accept to guide me as a master student in January 2018. Since this time, his guidance was extremely important for the completeness of this master thesis. With more than 45 years of experience in safety and reliability, Luiz Oliveira encourage me to develop different reliability approaches rather than following the same topics as every student. Moreover, his models were the basis for this master thesis.

I also would like to thank my family for all the support. Without them, I wont be able to go abroad and do my master at NTNU. I am extremely grateful to them.
During these 2 years, my wife, Giovanna, was always by my side, supporting and encouraging me to continue. Thanks, my love!

Summary

Safety systems are used in the process industry for many years. The application of these system is based on IEC 61508 standard. In this standard, proof testing is recommended in order to achieve the required SIL. It is common to assume that all the proof tests are complete and all the failure modes are covered. However, it is not always true.

The main objetive of this thesis is to assess the impact of degradation due to proof test and also evaluate the impact of incomplete testing. In order to do that the ATSV and MTSV failure rate models are proposed based on DNV-GL papers. Another approach using multi state models are used. The Multiphase Markov model is used to reflect the effect degradation due to proof testing and test incompleteness.

The BOP and the HIPPS valves were used as example to PFD assessment since there are historical data that theses system can face degradation if a complete test is performed.

Table of Contents

List of Tables

List of Figures

Abbreviations

ATSV	=	Additive Step Vary Model
API	=	American Petroleum Institute
ALARP	=	As Low as Reasonable Possible
BSR	=	Blind Shear Ram
BOP	=	Blowout Preventer
CCPS	=	Center for Chemical Process Safety
CSB	=	Chemical Safety and Hazard Investigation Board
DU	=	Dangerous Undetected
DHSV	=	Downhole Safety Valve
ESD	=	Emergency Shutdown
ETA	=	Event Tree Analysis
EUC	=	Equipment Under Control
E/E/PE	=	Electrical / Electronic / Programmable Electronic
FMECA	=	Failure Mode, Effect and Criticality Analysis
FTA	=	Fault Three Analysis
HIPPS	=	High Integrity Pressure Protection System
HFT	=	Hardware Fault Tolerance
IEC	=	International Electrotechnical Commission
MATLAB	=	Matrix Laboratory
MTSV	=	Multiplicative Step Vary Model
MTTF	=	Mean Time to Failure
NTNU	=	Norwegian University of Science and Technology

O&G	=	Oil and Gas
OLF	=	Norwegian Oil Industry Association
PFD	=	Probability of Failure on Demand
PFDavg	=	Average Probability of Failure on Demand
PFH	=	Probability of a Dangerous Failure per hour
PTC	=	Partial Test Coverage
PSA	=	Norwegian Petroleum Safety Authority
PSD	=	Process Shutdown
RBD	=	Reliability Block Diagram
RUL	=	Remaining Useful Lifetime
SIF	=	Safety Instrumented Function
SFF	=	Safe Failure Fraction
SIL	=	Safety Integrity Level
SIS	=	Safety Instrumented System

Chapter 1

Introduction

The oil and gas industry operates complex and hazardous technologies which have the potential to generate undesired hazard events that can lead to harm to people, asset and environment. In order to deal with these unexpected events, a high level of operational safety is required. The implementation of Safety Instrumented Systems (SIS), which are based on E/E/PE technologies, are vital in the oil and gas industry since they are responsible to provide risk reduction and make operations safer and more reliable.

1.1 Background

During the last decade, it was possible to see the volatility of the energy market, especially in the Oil and Gas industry. From 2000 to 2008, the oil price went from $25 to $150 per barrel. The reason for this relevant increasement was the high energy demand from emerging countries such as China and India. By the end of 2008, a global recession restricted the demand for energy and the oil dropped again to $40. The following year, the economy was recovered again, and the oil price was back to the $100 baseline. This price fluctuates with a low variance between 2008 and 2014, and due to worldwide problems, such as lower expand of China economy, India and Brazil faced economy and political issues, the investment of shale oil/gas production in U.S and Saudi Arabia which decide to keep the oil in a low baseline. Nowadays, the brent oil price starts to ramp-up again from $35 to an average of $74 (June/2018) per barrel. It is expected that the world energy demand will expand by 30%, with the consumption of all modern fuels continuing to grow until 2040. Oil consumption will continue to grow (by 12%) between 2015 and 2040 (NTNU, 2018).

Along the history, the oil and gas market had cycles like the ones described above since its beginning. Since the last decade, the oil and gas industry realized that a process optimization analysis was necessary to ensure the business continuity for the future operation. The oil price cycles are expected along time, but the business needs to continue. This optimization process can cover from better operational procedures, Enhance Oil Recovery (EOR) techniques, reduce man-hours and salaries, establish a spare parts philosophy,

perform better project management, to project design/configuration, equipment reliability, availability, maintainability and safety (RAMS).
The optimization process part which covers the operational safety shall take into consideration that all industrial activities are associated with a potential hazard which the consequences are undesirable. Therefore, the operational safety shall be maintained. Unfortunately, no activity is free of the hazards. Although the equipment failures cannot be avoided, they could be tolerated until a certain level where the operation can continue within an acceptable level of risk. The concept of As Low As Reasonable Practical (ALARP) is used to define the boundaries between a Not Tolerable and Tolerable risk. It is always important to consider the gain of a safety equipment and the cost of the equipment and the impact if the undesirable event occurs.
The concept of reliability engineering and how it is applied into the optimization process is the key in the oil and gas industry. According to (Blischke and Murthy, 2011), the equipment reliability depends on a variety of complex interactions of the laws of physics, engineering design, manufacturing processes, management decisions, random events and usage (degradation). The reliability theory is applicable in the design phase as well as in the operational phase. The international standard IEC 61508 (IEC 61508, 2016b) provides guidance on how to manage the reliability of the safety-related systems during the overall safety life cycle of a EUC (Equipment Under Control).

1.2 Motivation

Across the history, some major oil and gas accidents were responsible for the turning points in safety management improvement. These lessons-learned were important in a matter to identify what can go wrong and how it can be improved. Moreover, these accidents highlighted the necessity that new safety systems shall be installed in order to avoid hazards events. An example of a recent major accident is the Deep Horizon Blowout in 2010, which 11 workers died and 17 were seriously injured by an explosion in the Deep Horizon offshore rig. It has been the largest oil spill in U.S. history. The CSB (Chemical Safety and Hazard Investigation Board) conducted a technical investigation to identify what could contributed to the accident. During the investigation, it was identified a failure in a key part of a safety equipment, the BOP (Blowout Preventer) which has failed to seal the well during the emergency situation.
The BOP is a complex electrically and hydraulic powered device located subsea which it is essential to controlling the well and act in an emergency situation to protect the platform. It is designed to prevent flammable oil and gas from travelling up the riser to the drilling rig. A blowout can be catastrophic since oil and gas reaching the drilling rig can quickly find an ignition source leading to a fire or explosion with possible harm to people and the asset. During the emergency, some parts (annular, solenoid valves, etc) of the BOP were activate by the operators but the safety equipment did not act as intended. Would this accident been avoided if the components of the BOP have been tested correctly or more often?
Another example of safety-critical equipment from subsea is the Downhole Safety Valve (DHSV). The DHSV is a final element of a production well and it is responsible to isolate the wellbore in case of uncontrolled oil flow from the well. Marvin Rausand mentioned in his book (Rausand, 2014a) the DHSV testing procedure. Normally, the DHSV is proof-

tested with a testing interval of 6 months. Due to its location subsea and the high cost of repair, a failure on this valve is critical to oil production. Provide the full test of the DHSV is not economically visible, since the valve test consider its closure against a flowing well. This test is called slam-shut and the valve cannot withstand more than few tests like this one without mechanical degradation. It is the explanation of why the DHSV testing is incomplete. According to the book (Rausand, 2014a), the common test is performed stopping the flow from the well downstream the valve, and the DHSV is closed against a static well, not reflecting the actual operation scenario. Some questions can be raised based on the description of these two safety-critical equipment examples: Are the equipment being tested correctly? How often is the test interval? Is it according to the SIL requirement? Is it a complete test? If not, which failure modes are covered? Is there any inherent degradation associated to the test? Which lifetime models can be used to predict this equipment behavior? Many OG installation systems which have safety-critical equipment installed have these equipment subjected to ageing mechanisms which can lead to deterioration of their condition with potential impact on its required function and safety purpose. Every equipment is expected to face degradation. However, the point here is how can we address this issue in the reliability quantification because nowadays, it is not taking into account. Normally, the calculations considered a constant failure rate during the equipment lifetime and it is not always true. The lack of real data is a limitation regarding the degradation modelling since condition monitoring technologies are not well established in the market yet.

1.3 Objetive

The objective of this master thesis is to rationalize and compare methods for reliability quantification using different lifetime models. This comparison will take into account the incompleteness of the proof test. Moreover, this thesis will also provide alternative methods to evaluate the impact of the degradation caused by proof testing. Valuable discussion will be presented to assess the pros and cons for each model and its combination between incompleteness and degradation effect. For this purpose, the following tasks shall be performed:

1. Give an overall overview about the main concepts and approaches for reliability assessment related to safety-critical equipment.

2. Introduce how incomplete testing is taking into account in reliability lifetime and multi-states models.

3. Discuss and model the degradation effect related to proof testing.

4. Combine incomplete testing and degradation effect due to proof test into the same model.

5. Carry out case studies using the subsea High Integrity Pressure Protection System (HIPPS) and the Blowout Preventer (BOP) blind shear ram as examples, using MATLAB as a software tool.

6. Discuss the key findings based on results and address the pros and cons regarding each model.

7. Provide suggestions to further studies in the area of reliability, incomplete testing and degradation related to proof testing.

1.4 Delimitations

The main objective of this thesis is to evaluate and quantify the reliability of SIS operating in low demand mode. During the analysis, only the undetected failures were considered, assuming that this kind of failures are the major contributor to the SIS unavailability. The safe and detectable failures were not included since their failures were going to lead the SIS to a safe state or be detectable by automatic diagnostic coverage.
Moreover, the thesis is limited to analyze physical entities of safety-critical systems, which means that the focus is the hardware part. Other parts such as: software, human reliability and organizational procedures are not covered. The time to accomplish this masters thesis is 20 weeks which limits the scope the study. Reliability assessment, incomplete testing and degradation are quite complex subjects and a variety of approaches could be done to evaluate these topics together.

1.5 Report Structure

This masters thesis is structure in 5 chapters. A brief description of each chapter is provided below:
Chapter 1 presents the masters thesis motivation regarding the Safety Integrity Systems degradation due to proof test and the main researches related to it. The thesis objectives are also described.

Chapter 2 gives an introduction to SIS and the basic concepts and terminology within the reliability of safety-critical systems. An important subject in this chapter is the discussion about the proof testing concepts.

Chapter 3 describes the interaction between the lifetime and multi states models and the degradation due to proof test. Moreover, the proof test completeness is also introduced in the models and its impact is assessed.

Chapter 4 presents 2 case studies. Both applies the theory described in the Chapter 3, the first one is related to Blowout Preventer (BOP) blind shear rams and the second one is regarding the High Integrity Protection Pressure System (HIPPS) in subsea production environment. The PFD as a function of time is calculated and discussed in both cases.

Finally, in **Chapter 5** summarizes the thesis idea and compare the results from the results analyzed in Chapter 4. A conclusion is presented and recommendations for further work are suggested.

Chapter 2

Reliability Assessment of Safety-Critical Systems

This chapter presents basic concepts and definitions of safety-critical systems which are fundamental for the thesis understanding. The sub-sections describe the relevant standard available nowadays, the relevant parameters for the reliability assessment and the different classifications and its impact in the safety-critical systems unavailability.

2.1 General Concepts

Unfortunately, all kinds of operations are associated with a certain level of risk. Therefore, to mitigate or control these risk, the safety-critical system implementation is required. In this master thesis, the following definition is used: *safety-critical system is a system whose failure may lead to harm to people, economic loss, and/or environmental damage (Rausand, 2014a).*

As it was said before, the safety-critical systems are installed to protect any system against an undesired event. The system which is protected are called Equipment Under Control (EUC). It is important to highlight the difference between a safety barrier and a safety-critical system. A safety barrier is a term used in the risk analysis and it can be a technical system or an operation procedure. In this case, the procedure is a safety barrier, but it is not a safety-critical system. In other words, an EUC can be protected by several safety barriers, but not all of them are safety-critical systems. Most of all safety-critical systems are based on electrical, electronic, or programmable electronic (E/E/PE) technology. The aim of a safety-critical system is to provide functional safety. Functional safety represents the absence of unreasonable risk due to hazards caused by malfunctioning behavior of E/E/PE systems.

All the framework related to E/E/PE safety-critical systems is presented in the standard

called IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems. The objective of this standard is to overcome the challenge of E/E/PE design and operation by providing requirements related to the design, operation and decommission based on life-cycle approach.

2.2 Safety Instrumented Systems

Safety-critical systems (SIS) are responsible to ensure the operational safety when a hazard event occurs. SIS is the general term for safety-critical system adapted by process sector in IEC 61511 (IEC 61511, 2016). In order to reduce the magnitude of an accident consequence, and bring the EUC to a safe state, the Safety Instrumented System (SIS) was implemented in the industry. A SIS consists of a least three subsystems: input elements, logic solver and final elements. Figure 2.1 provides an illustration of the SIS elements.

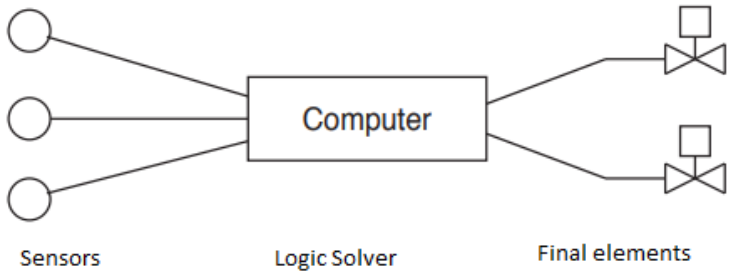


Figure 2.1: SIS elements

2.2.1 Input Elements

Input elements like sensors, are used to monitor a certain process variable condition (e.g. temperature, pressure, level). Sensors in a SIS are responsible to measure any possible deviation which can lead to a potential hazard. The most important consideration when selecting sensors for safety applications is that they accurately and reliably measure the process variable (Goble William and Cheddie, 2005). Figure 2.2 illustrates an example of a pressure sensor.

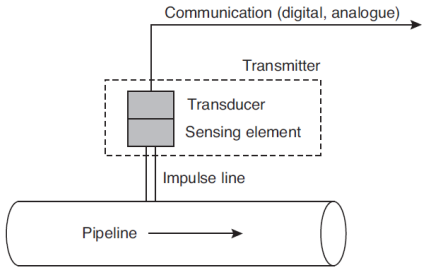


Figure 2.2: Pressure Transmitter in a pipeline

2.2.2 Logic Solver

After the sensor measured the process condition, a signal is sent to the logic solver. The logic solver is the brain of the Safety Instrumented Systems. It will perform the logic based on the signal from the sensors as well as other potential functions such as filtering, averaging or comparison. A typical example of a logic solver is the Safety Programmable Logic Controller (PLC). Normally, the PLC can replace the relays and include graphical displays with the logic which can help the operators. Moreover, it can check utilities errors and has quick documentation capability. Special techniques are applied to protect the PLC against systematic faults and, therefore, ensure software reliability. Figure 2.3 presents an illustration of a safety PLC.

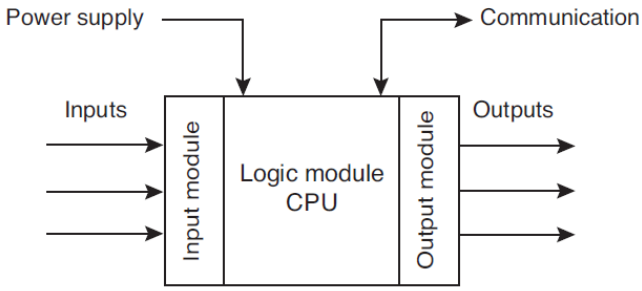


Figure 2.3: Logic Solver main elements

2.2.3 Final Elements

A variety of devices can be used as a final element in a safety instrumented function. In the oil and gas industry, the most common final element is a remote actuated valve (Goble William and Cheddie, 2005). This device normally consists of 3 main parts: pneumatic/hydraulic control assembly, an actuator and a valve. This final element will be the focus of the reliability assessment of this master thesis. Figure 2.4 presents the assem-

bly of a remote actuated valve which mainly consists of solenoid valve, actuator and the mechanical valve.

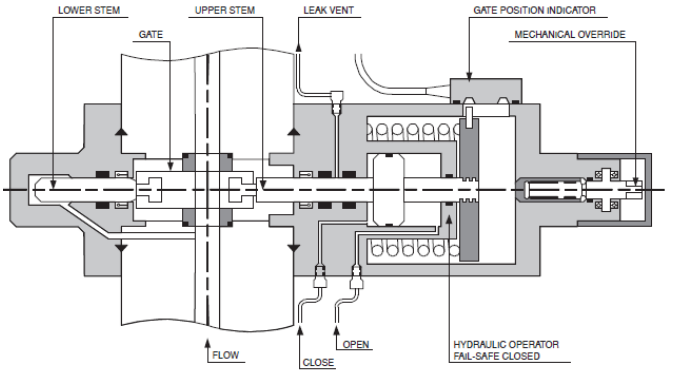


Figure 2.4: Fail-safe gate valve used in subsea oil/gas production

All these elements described above (input element, logic solver and final element) are governed by the general requirements from IEC 61508 and the specific requirements for the process industry is in IEC 61511. The SIS is designed to provide one or more Safety Instrumented Functions (SIF) and they shall meet the Safety Integrity Level (SIL) requirements. To ensure the availability of the SIS over the production lifetime, proof tests must be performed according to a specific test interval.

2.3 Safety Instrumented Functions

As per IEC 61508, a Safety Instrumented Function (SIF) shall be implemented by an E/E/PE safety-related system or other risk reduction measures, that is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event (IEC 61508, 2016b). It is important to emphasize this definition because the function is related to a specific hazard. Therefore, the equipment function shall be clearly identified to avoid auxiliary equipment included in the SIF, which it could not be providing protection against the hazard. A SIS will normally perform more than one SIF. A SIF will have dedicated input and final elements, but the logic solver can be shared since it is complex systems with several channels and software. The pathway connecting the input and final elements of a SIF with the logic solver is referred as a safety loop.

2.4 Design Aspects SIS

There are different measures related to a SIS which can enhance its reliability. (Rausand, 2014a) describes important measures such as redundancy, voting and hardware fault tolerance. (Rausand, 2014a) presents the redundancy concept as when the system has two or more items which if one of them fails, the system can continue to function. The term

redundancy can also be referred as fault tolerance. It can be implemented in different ways.

The main approaches used in the industry are:

- **Active redundancy**: when redundant items are actively performing the same function and in the case of one item fails, the system can still perform the required function just with one item.
- **Standby redundancy**: when one or more items are performing the function, while the rest of the components are in standby mode, waiting to be put in operation in case of maintenance of the active items or in case of a failure.

Introducing redundancy to a system does not necessarily imply that will be an improvement of the reliability. The enhance of reliability is determined by the voting selection for the redundant architecture. The voting concept can be defined as the number of failures tolerated until the system overall function is lost. In general, a system function structure can be expressed as k of its n components are functioning. It can be said that the system voted structure is k-out-of-n (KooN). A good example of the voting is a 2oo3 pressure transmitters of a subsea pressure system as illustrated in Figure 2.5. In this case, the system has three pressure transmitters functioning but at least two of them need to send the signal to the logic solver in order to an action can be performed. As described above, the

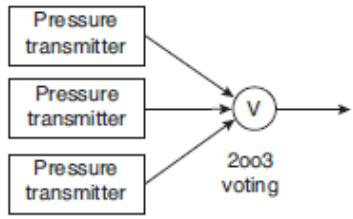


Figure 2.5: Pressure transmitters 2oo3 voting

KooN voted group is performing the required function if at least k of its n components is functioning. This system can tolerate up to (n – k) failures without losing the ability to perform the required function. This is the definition of the Hardware Fault Tolerance (HFT) concept. Therefore, the HFT of a KooN voted group can be expressed as (n – k).

2.5 Operational Aspects - SIS

After presenting the design aspects of a SIS, it is also important to take into account the operational conditions that the SIS are going to be exposed. The two main relevant operational aspects of a SIS are its safe state and the SIF demand. The safe state of a SIS is an important aspect to be defined during the design phase of a SIS. (IEC 61508, 2016b) defines safe state as the state of the EUC when safety is achieved. The safe state may differ depends on the actual reason why the SIS is demanded. In a case of response to a demand

the safe state could be one and in case of loss of power supply the safe state could be the opposite.
Usually, the SIS has the same safe state no matter the reason of the demand. If the SIS has different safe states, it could lead to a high design complexity of the SIS. The operation mode of the SIS also plays an important role in the operational aspects. The mode of operation of a certain SIS is related to how often the SIF is demanded. IEC 61508 presents three main modes of operation and they are described as per (IEC 61508, 2016b):

- **Low-demand mode**: where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is no greater than one per year.
- **High-demand mode**: where the safety function is only performed on demand, in order to transfer the EUC into a specified safe state, and where the frequency of demands is greater than one per year.
- Continuous mode: where the safety function retains the EUC in a safe state as part of normal operation;

The two last modes are combined in IEC 61508 and it is referred as the high-demand/continuous mode. However, there is a significant different between these two demand modes. (Rausand, 2014a) states that a SIF in demand mode is passive in the sense that it does not perform any active function during normal operation but is an add-on to the EUC and is only called upon when something goes wrong. While, a SIF which operates in continuous mode, plays an active role in the control of the EUC and a hazardous event will occur almost immediately when a dangerous failure of the SIF occurs.

2.6 Failure modes and classification

Failure and failure mode are the two main important concepts in any reliability analysis of a technical system. According to (IEC 61511, 2016) failure is the loss of ability to perform as required. This standard categorizes the types of failure mode into two categories (random hardware failure and systematic failure) and they are defined as:

- **Random hardware failure**: it occurs at a random time, which results from one or more of the possible degradation mechanisms in the hardware (IEC 61511, 2016). This degradation natural phenomenon could be due to stress of the component or either from a normal ageing.
- **Systematic failure**: it is related to a pre-existing fault, which consistently occurs under particular conditions, and which can only be eliminated by removing the fault by a modification of the design, manufacturing process, operating procedures, documentation or other relevant factors (IEC 61511, 2016).

In the (PDS Handbook, 2013), the systematic failure is split into five categories of causes. Figure 2.6 illustrates that categories.

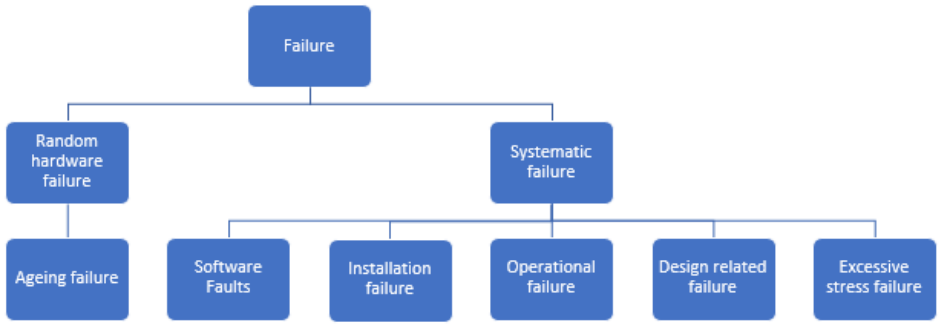


Figure 2.6: Failure classification by cause based on (PDS Handbook, 2013)

(Rausand, 2014a) states that the borderline between random hardware failures and systematic failures is not fully clear and analysts often differ in their views regarding the failure classification. This difference of point of views is clear when IEC 61508 and PDS handbook are compared. IEC 61508 requires only random hardware failure to be considered when unavailability (PFDavg or PFH) is quantified, while PDS Handbook considered both types of failure in the calculation. Thus, when the quantification is performed, it is important to know which standard the calculation is following and what are the assumptions. In this master thesis, the IEC 61508 approach is followed. Therefore, IEC 61508 classify the random hardware failure in:

- **Dangerous (D) failure**: A dangerous failure is a failure that impedes or disables a given safety action upon demand. The dangerous failure further divided into two categories: dangerous undetected (DU) which are only revealed only by proof testing or when a demand occurs. DU failures are the main contributors to the calculation of SIF unavailability. The other category is the dangerous detected (DD) which identify the failure in a short time by automatic diagnostic testing.
- **Safe (S) failure**: a safe failure is the one that do not put the item in a state which it cannot perform its safety function. Therefore, the safe failure brings the EUC to a safe state. As the same way as dangerous failure, the safe failure is split into two categories: detected and undetected.

Figure 2.7 illustrates the different classification of failure modes.

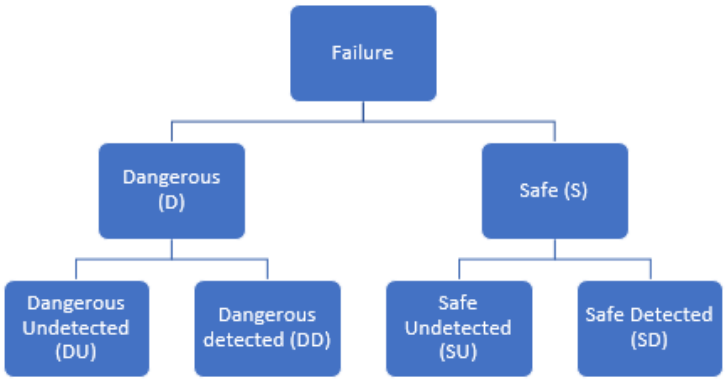


Figure 2.7: Classification of failure modes

2.7 Safety Integrity Level

The principal of using Safety Integrity Levels (SIL) as part of the overall risk reduction process has been established for many years based on IEC 61508 and IEC 61511 standards. The SIL quantify the reduction of risk to be achieved by the implementation of preventive barriers by the Safety Instrumented System (SIS).

IEC 61508 distinguishes between four different safety integrity levels, SIL 1, SIL 2, SIL 3 and SIL 4, with SIL 4 being the most reliable and SIL 1 to the lowest one. IEC 61508 also differentiates the SIL quantification according to the operation mode. For a safety function operating in low demand mode, the standard uses the Average Probability of Dangerous Failure on Demand (PFDavg) as a target failure measurement. A high demand / continuous mode of operation utilizes the Average Frequency of a Dangerous Failure of the Safety Function (PFH) as the name to indicate the SIL. One example for each measurement could be the process shutdown system for an oil platform which is expected to be demanded less than once a year (low demand) and the railway signaling system which is a safety-critical system and it is used to control rail traffic and it is expected to be continuously demanded (high/continuous demand) since the railway industry face more strict requirements.
Figure 2.8 and Figure 2.9 presents the target failure values according to each SIL depending on the demand mode of operation.

Safety integrity level (SIL)	Average probability of a dangerous failure on demand of the safety function (PFD_{avg})
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

Figure 2.8: Safety integrity levels target failure measures for a safety function operating in low demand mode of operation (IEC 61508, 2016b)

Safety integrity level (SIL)	Average frequency of a dangerous failure of the safety function [h^{-1}] (PFH)
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

Figure 2.9: Safety integrity levels target failure measures for a safety function operating in high demand mode or continuous mode of operation (IEC 61508, 2016b)

Based on IEC 61508 life cycle, the SIL plays an important role to assess the systems safety. In the first part of the life cycle, a SIL requirement shall be established based on a risk analysis. After that, a predict SIL shall be defined based on the design model. Later on, during the operation, an actual SIL shall be quantified in order to reflect the operational experience and the project as-built design.

2.8 SIL Requirement

Besides the quantitative requirements presented above (PFDavg and PFH) which include random hardware failure, common cause failure and relevant failures, there is also another type of requirement. The qualitative requirement, expressed by architectural constraints includes the hardware fault tolerance (HFT), Safe Failure Fraction (SFF) and the type of system (A or B). These requirements are better explained below.

- Hardware Fault Tolerance (HFT) is part of the qualitative requirement to achieve the required SIL. It consists of the ability of the system to continue to perform the required function in the cause of faults. For instance, if the system has a 1oo2 voting configuration, the HFT = 1.

- As per (IEC 61508, 2016b), the Safe Failure Fraction (SFF) is defined as a property of a safety related element that is defined by the ration of the average failure rates of

safe plus dangerous detected failures and safe plus dangerous failures. The equation which describes this description is:

$$SFF = \frac{(\sum \lambda_{S\ avg} + \sum \lambda_{Dd\ avg})}{(\sum \lambda_{S\ avg} + \sum \lambda_{Dd\ avg} + \sum \lambda_{Du\ avg})}$$

- IEC 61508 states that there are two main types of equipment: Type A and Type B. Type A equipment is the one which the failure modes are well defined, the behavior of the equipment under fault conditions can be completely determined and there is sufficient dependable failure data to show that the claimed rated of failure for DD and DU are met. Type B equipment is the one that the criteria described before are not met.

Figure 2.10 summarizes the relation between the requirement of HFT, SFF and Type of equipment according to the SIL range.

	minimum HFT with type A			minimum HFT with type B		
SFF	0	1	2	0	1	2
<60%	SIL1	SIL2	SIL3	-	SIL1	SIL2
≥60%, <90%	SIL2	SIL3	SIL4	SIL1	SIL2	SIL3
≥90%, <99%	SIL3	SIL4	SIL4	SIL2	SIL3	SIL4
≥99%	SIL3	SIL4	SIL4	SIL3	SIL4	SIL4

Figure 2.10: Summary of HFT, SFF and Type of equipment per SIL range

2.9 SIL Allocation

After the development of the required SIL of the safety functions, the next step is to allocate these safety functions. Several allocation methods are available in the literature for determining the required SIL for a SIF. (IEC 61508, 2016a) does not provide any specific method for allocation of overall safety functions, but recommended theses:

- Risk graph
- ALARP Method
- Fault Three Analysis (FTA)
- Event Three Analysis (ETA)
- Layer of Protection Analysis (LOPA)

After allocating the safety function, the next step is to determine the required SIL. The main methods used by the industry are Risk Graph and LOPA. The Risk Graph method

allows both quantitative and qualitative assessment of the analyzed EUC. This method uses several parameters which describes the hazard event, such as: consequence level (C), frequency of and exposure in the hazardous zone (F), possibility of failure in avoiding the hazardous event (P) and the how often the hazardous event will occur (W). After combining these parameters, a SIL is defined. LOPA method is a semi-quantitative method introduced by the Center for Chemical Process Safety in 1993 (Crowl and American Institute of Chemical, 2010). The main objective of the LOPA is to determine whether there are enough layers of protection against the hazardous scenario. Normally, LOPA is applied after a HAZOP study, since the input for a LOPA is the initiating events. The application of the LOPA methodology is performed according to the following steps:

- Plan and prepare
- Develop the accident scenarios
- Identify initiating events and address its frequency
- Identify the IPLS and the corresponded PFD
- Estimate the risk related to each scenario
- Evaluate the risk
- Recommendations to reduce the risk
- Report the Analysis

(OLF 070, 2016) does not recommend any SIL allocation methods. Besides, the OLF 070 standard presents a method that is not risk based. The minimum SIL requirement is used to enhance standardization across the industry. This method calculation is developed by applying the formulas in (PDS Handbook, 2013). The reliability data used is from OREDA and SINTEF Database handbook.

2.10 SIS Testing

The testing is a key activity to confirm that the SIS is achieving the required reliability and performance. The SIS testing is able to detect a potential failure which has impact in the system reliability. (IEC 61508, 2016b) and (IEC 61511, 2016) provide clear requirement for regular testing of the SIS. In this master thesis the focus will be the analysis of low-demand mode SIS, which means that they are kept passive during the normal operation time. It will be activated only during an emergency situation. Therefore, the SIS shall be tested in order to guarantee that in a demand scenario, it will be performing the required function. There are 3 main types of test:

- **Proof Test**: It is a planned periodic test, which is designed to detect all the dangerous undetected failures for all components in a SIF. After a proof test, the user can decide if there is the necessity of maintenance or not. If yes, the associated repair can bring the component to as called as-good-as-new (AGAN) or to the as-bad-as-old (ABAO) one.

- **Functional Test**: The aim of the functional test is to ensure that the SIF is performing the required function. In the case of redundant configuration systems, the functional test is not sufficient. Therefore, a functional test is not always a proof test.
- **Diagnostic Test**: It is performed automatically in order to detect a specific failure. The diagnostic test is often performed within a shorter time interval than proof test. It can be expressed as the ratio of dangerous detected (DD) failures during diagnostic tests among all dangerous failures (DU + DD). Normally, the typical failures that ca be detected by diagnostic testing are signal loss, impulse line pluggage, drifted analogue signal, signal out of range, and final element in the wrong position (Rausand, 2014a).

$$DC_D = \frac{\lambda_{DD}}{\lambda_{DD} + \lambda_{DU}}$$

There are important aspects to take into account in a quantitative analysis. One of them is the proof test interval, which is the time between the initiation of two consecutive proof tests and is denoted by . The proof test interval is defined to be a magnitude order lower than the mean downtime due to a DU failure. The proof test procedure shall be described in the components Safety Manual and it should reflects the real operation conditions. As it was mentioned before, it can be problematic sometimes to perform a fully realistic test because it can generate a hazard situation or degrade the equipment. Figure 11 illustrates the proof test procedures.

The proof test improves the safety system reliability. However, there some consequences such as: shutdown of the EUC, which leads to stop the production. The shutdown and restart are hazardous operations (Rausand, 2014a). The second important aspect is how perfect or complete is the proof test, which means that in case of an imperfect or incomplete testing, just part of the DU failures are revealed. There are several reasons to perform an imperfect or incomplete testing like the test is not adequate or not able to reveal all types of DU failures or the test is performed under different conditions than the operational ones. (IEC 61508, 2016b) uses the term imperfect proof test to classify this type of test. The third aspect is the Proof Test Coverage (PTC). (Rausand, 2014a) presents a good definition to PTC, as part of the testing strategy between what is needed to be revealed and what is safe to do at the plant or with the system in question. The PTC is the conditional probability that a DU fault will be detected by the proof test, given the fault is present when initiating the proof test. The previous sentence is expressed in a mathematic equation below.

When the proof test is planned, and it is designed to reveal just part of failure modes without disturbing the EUC, the test is called Partial Proof-Testing. The ratio PTC, described above, is used to demonstrate the percentage of failures covered by the test. Normally, the partial proof testing is carried out between full proof tests in order to improve the reliability of the SIF and also extend the test interval (). It can be explained since the partial test does not affect the production while the full proof test needs to shutdown the process. The term Partial Stroke Test (PST) is presented in (Rausand, 2014a). This term is a common application of the partial proof testing in valves. It is performed by partially closing the valve, and then return to the initial position. Even though the valves movement is really

soft, it can reveal relevant dangerous failure modes of the valve such as failure to close (FTC) and broken signal paths.

2.11 Test Scheduling

There are several ways to plan a proof test. The three main strategies categories:

- **Simultaneous Testing**:This type of test tests all the components of the SIFs subsystem at the same time. Since it tests everything during the same time, the EUC is unprotected by the respective SIF. Due to that, this strategy is not accepted at some production facilities.
- **Sequential Testing**:During a sequential test, the subsystem components are tested one after the other. It means that after the next component is tested, the previous one is restored to perform its required function. The good point of this strategy is to keep the SIS able to act in case of an emergency situation, even if part of the SIS is under testing.
- **Staggered Testing**:The key aspect of the staggered test is to test redundant components at different times but keeping a constant test interval. The benefits of that is to improve SIF availability and reduced the probability of Common Cause Failures (CCF).

2.12 Reliability assessment

Analytical methods are used to evaluate the SIF reliability. (IEC 61508, 2016b) suggests several methods to quantify the reliability of a SIF and they are:

- Reliability Block Diagram (RBD)
- Simplified approximation formulas
- IEC 61508 approach
- PDS method
- Fault Tree Analysis (FTA)
- Markov Analysis
- Petri Nets

The functional safety standards require that a quantification is performed in order to achieve a safety level. The methods presented above are examples of techniques which are recommended by the standards. However, there is no prescription on how to calculate this safety level. The problem with this approach is that many techniques will be used based on different assumptions and they will be compared in a wrong way since they are based in different premises. (Rouvroye and van Den Bliek, 2002) presents in his paper

an approach to compare these safety analysis methods. In the paper, it is highlighted that this difference among the safety methods can lead to different quantitative results. Some analysis techniques are often used during the design phase since they require less details, like FTA and RBD. When more information is available (repair procedures and testing intervals), methods like Markov and Petri nets are recommended. (Rouvroye and van Den Bliek, 2002) states that a major problem is that the analysis complexity and effort to perform an analysis increase as the modelling power increases as presented in Figure 2.11. After the comparison is made, it shows that Markov analysis covers most aspects for quantitative safety evaluation. (Rouvroye and Brombacher, 1999) performed quantitative calculations in order to demonstrate this difference and the conclusion was the same as the previous paper. (Rouvroye and Brombacher, 1999) affirms that the lower value for PFDavg for the Markov models is caused by the fact that in general in a Markov model all system states (including so-called safety states) are taken into account and it results in a lower contribution to the PFD and this aspect cannot be covered by the other safety methods.

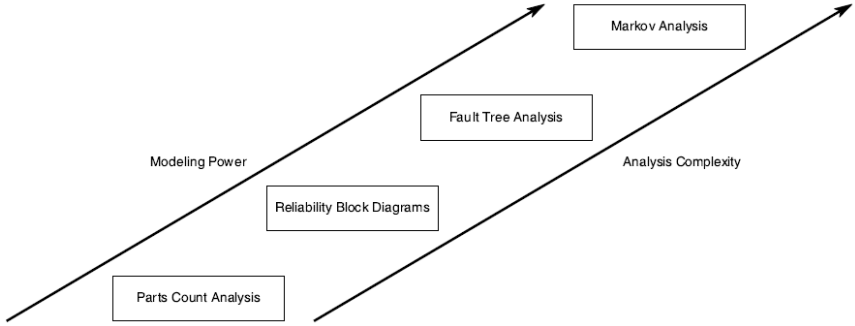


Figure 2.11: Relation of modelling power and analysis complexity for quantitative analysis techniques (Rouvroye and van Den Bliek, 2002)

2.13 PFDavg Quantification

According to IEC 61508 part 4 (IEC 61508, 2016a), PFDavg is the mean unavailability of an E/E/PE safety-related system to perform the specified function when a demand occurs from the EUC or EUC control system. It is the most common reliability measure for a SIF which operates in low demand mode. An important aspect to be considered in a quantitative analysis of a SIS is the repair time duration after a failure is detected. The first term used is the Mean Repair Time (MRT). MRT is the mean time between a DU failure is revealed by a proof test and the time that takes to the component to be repaired. The second term is the Mean Time to Restoration (MTTR). MTTR is the mean time between a DD failure occurs and the time the component is restored to perform the required function. These terms are better explained in Figure 2.12, Figure 2.13 and Figure 2.14. If we

consider a time period of t and the E[D(t)] as the average downtime. Then, we can have:

$$PFD_{avg} = \frac{E\left[D\left(t\right)\right]}{t}$$

During the component lifecycle, the SIS can have different behaviours between proof tests. The first case could be no dangerous failure between proof tests. This performance is illustrated Figure 2.12. In the next case, a DD failure occurs and a MTTR is required

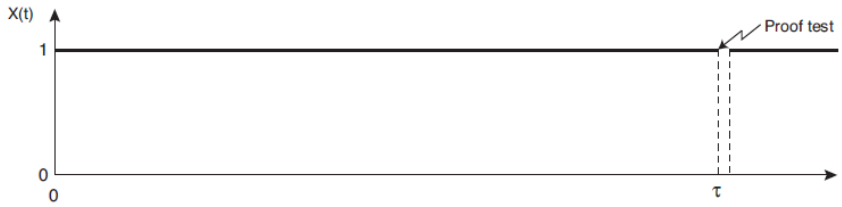


Figure 2.12: SIS Performance. No dangerous failure occurs. (Rausand, 2014b)

to repair the SIS. The SIS performance is presented in Figure 2.13. The last case, a DU

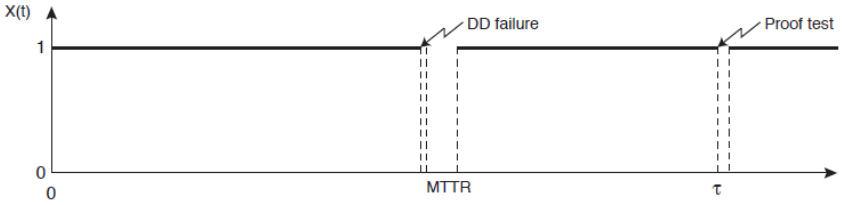


Figure 2.13: SIS performance. DD failure occurs within the proof test interval (Rausand, 2014b)

failure occurs between proof tests and a MRT is required to bring the SIS to as good as new condition. Figure 2.14 shows the SIS behaviour after a DU failure. As mentioned

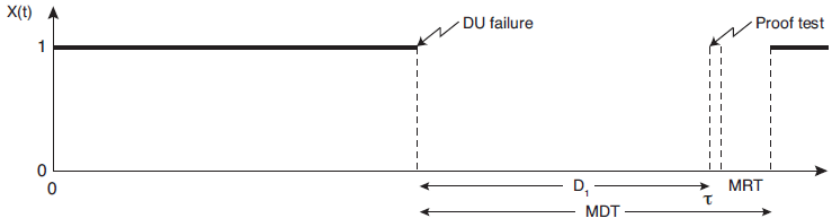


Figure 2.14: SIS performance. DU failure occurs within proof test interval (Rausand, 2014b)

before, the SIS consists of three subsystems: sensors, logic solver and final elements. The average probability that the SIF fails on demand (Ei) is described by this equation:

In many applications, the end user is interested in the PFDavg and not the PFD(t). Figure 16 illustrates the PFDavg for a periodically proof tested component.

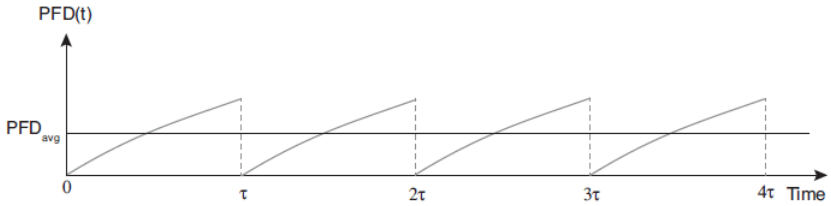


Figure 2.15: SIS performance and PFDavg (Rausand, 2014a)

2.14 Relevant Standards

All the terms discussed before are referred in the following standards and each one has yours definition and a different way to consider in the reliability quantification of safety instrumented systems.

2.14.1 IEC61508

The standard IEC 61508 was developed by the International Electrotechnical Committee (IEC) to overseas the design of safety-critical systems. The international standard IEC 61508 is related to the functional safety of electrical/electronic/programmable electronic safety. It provides a generic overview specification, design and operation for different types of SISs throughout life cycle phases. The main idea of the standard is to present all the requirements to develop the basis of the SISs. A notable feature of IEC 61508 is that it is risk-based, which means that reliability requirements for the E/E/PE safety-related systems (i.e., SISs) must be allocated based on the results from a risk analysis. Figure 2.16 illustrates the 16 SISs life cycle phases.

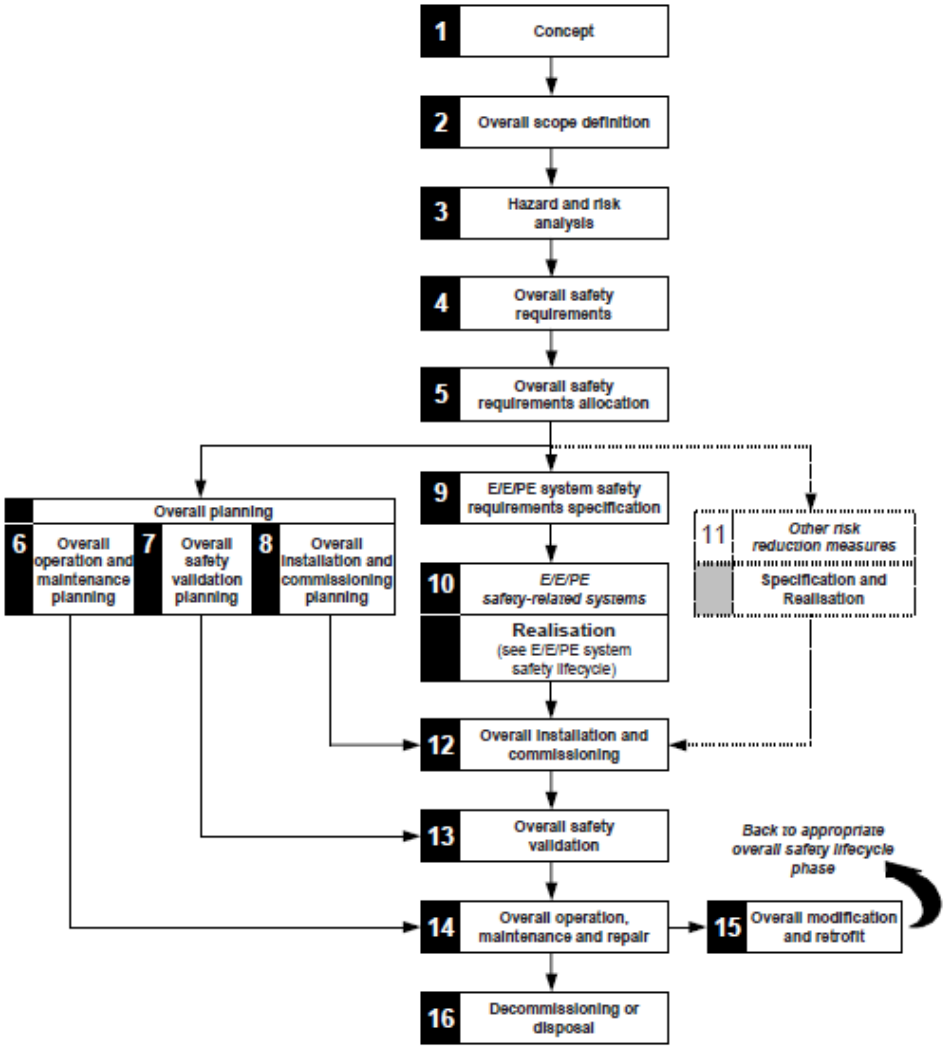


Figure 2.16: IEC 61508 Life Cycle

IEC 61508 is split into eight parts.

- **Part 0 Functional Safety and IEC 61508**:It provides an overview of the IEC 61508 and its applications.
- **Part 1 - General Requirements**: Based on life cycle approach, it presents the key phases of design and operation for safety functions.
- **Part 2 Requirements for electrical/electronic/programmable electronic safety-related systems**:It focuses on hardware and the integration of hardware and soft-

ware.

- **Part 3 Software requirements**:It covers the software requirements part related to the application program, operation logic for the SIS elements (sensors, logic solver and final elements)
- **Part 4 Definitions and abbreviations**:It presents all the definitions used in the standard.
- **Part 5 Examples of methods for the determination of safety integrity levels**:Through examples, it covers the application of IEC 61508-1 to determining the SIL.
- **Part 6 Guidelines on the application of IEC 61508-2 and IEC 61508-3**:It shows how to apply IEC 61508 part 2 and 3.
- **Part 7 Overview of techniques and measures**:It illustrates some reliability quantification techniques.

The first 5 parts are called the normative publications which means that they are mandatory, so in order to be comply with the standard, the user shall follow these requirements. Parts 5 to 7 are just informative, which means that methods are recommended and can be used. For instance, different users can apply different reliability methods (e.g. Markov or Reliability Block Diagram (RBD)). The focus of IEC 61508 is to provide SIS general requirements to the products manufactures. It facilitates the development of products and to be able to fully take into account and meet the specific requirements of product users and its applications.

IEC 61508-part 6 (IEC 61508, 2016a) presents formulas to calculate PFDavg. The approach calculated in IEC 61508 consider both types of dangerous failures, DD and DU. This is the first different between simplified formulas. The objective of the IEC formulas is to calculate the PFDavg based on the average dangerous group failure frequency, D,G, the mean downtime for a single channgel, tCE, and the group-equivalent mean downtime, tGE. Figure 2.17 illustrates the separation considered in the standard. The tCE for the

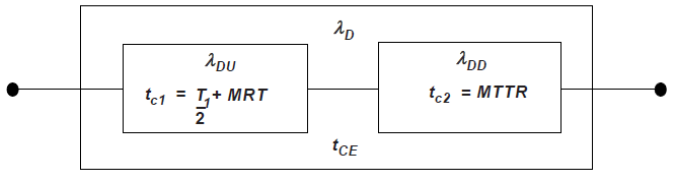


Figure 2.17: Separation of DU and DD failures with respect repair time (IEC 61508, 2016a)

channel is: And the tGE for a KooN system is defined by: Then, the PFDavg can be calculated as: The CCF failures can be also be included in the IEC 61508 formulas. In this particular case, there are two beta factors. One for the DD failures (D) and another one for the DU failures (). The series structure representing all kind of failures is presented in

Figure 2.18: Series structure representing CCFs for DU and DD failures (IEC 61508, 2016a)

Figure 2.18. The PFDavg analytical formulas for these two types of CCFs are: The overall PFDavg formula for the IEC 61508 is:

2.14.2 IEC61511

IEC 61511 is a standard for the applications within the process industry covering diverse kinds of industries such as refineries, oil and gas production units and chemicals. The overall scope of this standard is the application of Safety Instrumented System (SIS) as a process safety device. IEC 61511 is based on IEC 61508 which is a generic standard that covers a general framework for E/E/PE systems requirements as described before. The main idea of IEC 61511 is to standardize the criteria for equipment selection for the SIS using a risk-based approach. Moreover, it defines requirements for the SISs design and operation. IEC 61511 has its primarily concern, the aspects related to safety availability and do not cover aspects of overall reliability. Throughout a safety life cycle, the standard presents the SISs design and management requirements. The idea of this approach is to cover different parts of the SIS life, such as: initial concept, design, implementation, operation and maintenance. The standard is divided in 3 main parts:

- **Part 1: Framework, definitions, systems, hardware and software requirements**
- **Part 2: Guidelines for the application of IEC 61511-1.**
- **Part 3: Guidance for the determination of the required safety integrity levels.**

The focus of IEC 61511 is the integrators and systems users. It is important to highlight that the standard shall be applied together with other relevant standards such as: local regulations, legal requirements and corporate practices. Figure 2.19 presents the relationship between the standard public focus. As it was mentioned before, manufactures and suppliers shall follow IEC 61508, whereas safety instrumented systems designers, integrators and user shall follow IEC 61511. There is a gray area regarding these terms. The standard does not give any concrete interpretation of who is who. A company cannot be considered a manufacture in a project and an integrator in other one. One possible way to manage this impasse is to consider the operator as the only integrator and the others shall follow IEC 61508. Figure 2.20 describes the differences in scope and application of IEC 61508 and IEC 61511.

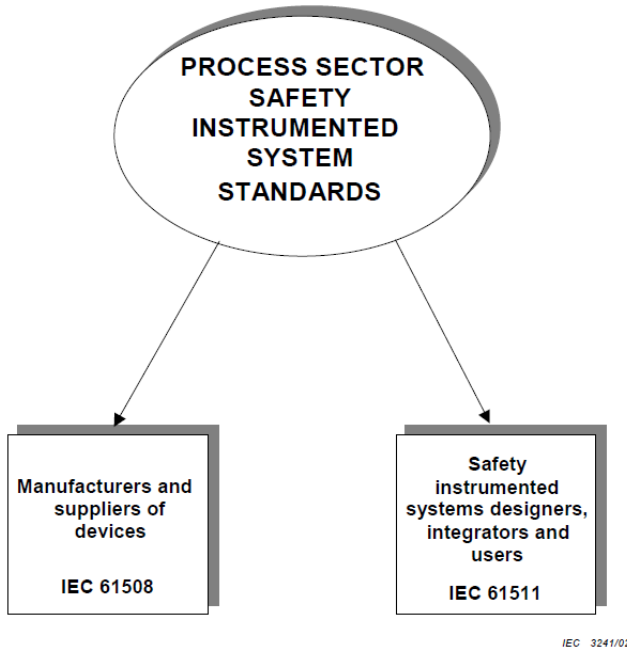


Figure 2 – Relationship between IEC 61511 and IEC 61508

Figure 2.19: Relationship between IEC 61508 and IEC 61511

2.14.3 PDS Method

PDS is a method used to quantify the safety unavailability and loss of production for safety instrumented systems (SISs) (PDS Handbook, 2013). The PDS method is presented in the SINTEF report. It is a work carried out by the collaboration between different OG companies, consultancies and governmental bodies. It is aligned with IEC 61508 and IEC 61511 standard principles and the focus of the PDS method is in the quantitative part. According to the handbook, the PDS method only take into account the contribution from unknown downtime unavailability, which means it only considers dangerous undetected failures (DU). There is a new variable called Downtime Unavailability (DTU) that represents the downtime part for safety unavailability. There are two elements: DTUR and DTUT (PDS Handbook, 2013):

- DTUR compromises the downtime unavailability due to repair of dangerous failures, resulting in a period when it is known that the function is unavailable. The average duration is the MTTR.
- DTUT consists of the planned downtime resulting from activities such as testing and planned maintenance.

IEC 61508 and IEC 61511 use the beta factor to include the contribution of Common Cause Failures (CCFs) and it is the most common model used. The PDS method brings

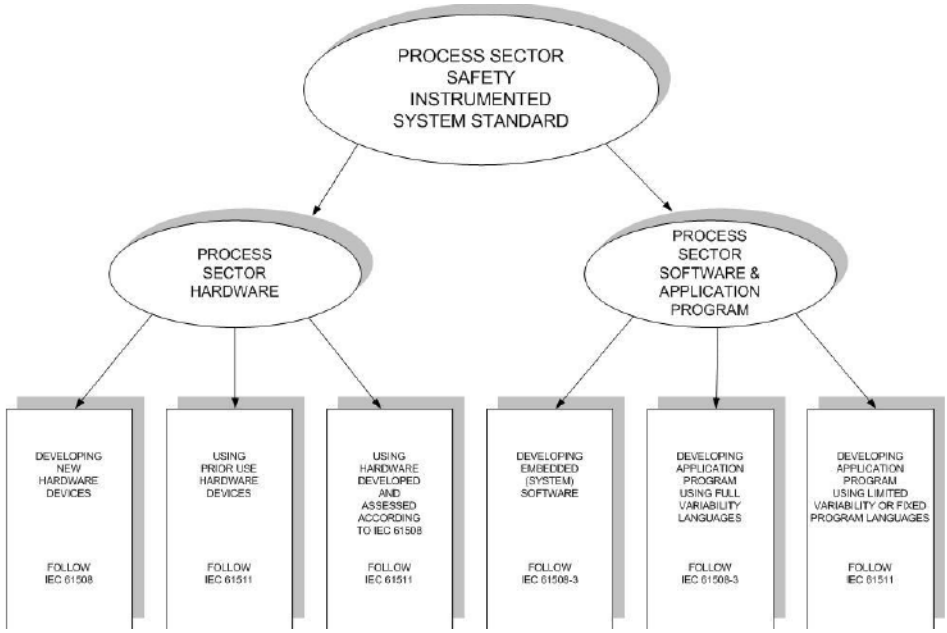


Figure 2.20: Relationship between IEC 61511 or IEC 61508 (IEC 61511, 2016)

an interesting discussion about the veracity of this model since no distinction is made regarding the voting configurations. Based on this discussion, the PDS method proposed a new method. The multiples beta-factor model takes in consideration the different voting logics. A modification factor is introduced based on expert judgement. The PDS method is composed by 8 chapters:

- Chapter 1: Introduction
- Chapter 2: reliability calculations
- Chapter 3: Failure classification and reliability parameters
- Chapter 4: Modelling of CCFs
- Chapter 5: Low demand mode system calculations
- Chapter 6: High demand versus Low demand
- Chapter 7: Multiple layer safety systems reliability calculations
- Chapter 8: Study Case

The PDS Handbook is written to reliability and safety engineers, site managers, project designers and technical operators within the safety instrumented systems domain.

2.14.4 ISA-TR84.00.02

It is called Safety Instrumented Functions (SIF) and has several parts which covers different areas of SIS framework. The aim of the standard is to provide a variety of reliability methodologies within the process industry that can be used to evaluate the Safety Integrity Level (SIL) of a Safety Instrumented Function (SIF). ISA-TR84.00.02 consists in 5 main parts. The overall idea of these 5 parts is to present definitions, symbols, explanations of SIS element failures and compare different techniques.

2.14.5 OLF 070

The guideline was developed by a joint project between industry operators, engineering companies and consultancies with the financial support of the Norwegian Oil and Gas Association. The intention of the Norwegian Association was to elaborate a standard with the overall purpose to guide on the application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry. The OLF 070 applies to offshore facilities operating under the regulations of the Petroleum Safety Authority (PSA) in the Norwegian Continental Shelf (NCS) (OLF 070, 2016). The relevant point of OLF 070 which differs it from the IEC 61508 and IEC 61511, is that it is not risk-based. A minimum SIL requirement concept is used. This approach is a set of predefined SIL requirements that are proposed for typical SIFs in relation to process safety, fire and explosion protection, well drilling and well intervention (Rausand, 2014a). These minimum requirements are based on industry best practices and principles, and a continuous improvement process uses the past experience to improve safety performance. Whereas IEC 61508 describes a fully risk based approach for determining the SIL requirements, the OLF 070 standard provides minimum SIL requirements for the most common instrumented safety functions on a petroleum production installation (OLF 070, 2016).

Chapter 3

Integrating degradation effects, proof testing and lifetime models

After presenting the basic concepts of safety-critical system and all the requirements associated to it, now in this chapter, the idea is to go deeper in the SIS proof testing effects and its quantification. Normally, the PFDavg calculations consider the test to be complete and it is known that it is not always true. This chapter will evaluate the impact of proof test in the components and assess several approaches to quantify this effect.

3.1 Proof Testing effects

In the process industry, it is normally assumed that the proof testing is complete such that all failure modes are detected, and the safety loop is repaired to As-Good-As-New (AGAN) condition after each test. This assumption is often not realistic, and both the proof test and the repair actions may be incomplete or partial. (Rausand, 2014a) presents a typical example of an incomplete repair in the case when the proof test reveals that a shutdown valve has slightly too long closing time, but the end user postpone the repair since the valve is still closing within the acceptable limits.

An important discussion is necessary regarding the proof test classification in order to standardize the approach of this master thesis. (IEC 61508, 2016b) uses the term perfect testing to refer to proof test which covers all the failure modes and in the opposite way, it uses imperfect testing for the proof tests which do not cover all the failure modes, just a fraction of the component failures. (Aguilar Martinez et al., 2014) brings a different nomenclature for this type of test, the term incomplete testing is used. The term imperfect testing is reserved for the tests that are not reliable. (Bukowski and van Beurden, 2009) presents another concept regarding proof test correctness. Besides the completeness of the proof test, (Bukowski and van Beurden, 2009) introduces the term correct and incorrect which indicates the probability that the actual test, as specified, is correctly executed

by the tester, that existing failures are revealed, repaired entirely, and that no systematic failure is introduced and it is a function of the maintenance capabilities and culture at a specific plant site. A reliability model is presented in the paper that accounts for both proof test correctness and completeness and its effect in the average probability of failure on demand and as a function of time as well. (Hafver et al., 2017) presents an interesting discussion regarding the proof test classification and its implications for safety. In this paper, Hafver compares the distinction between incomplete test and imperfect tests since the two assumptions can lead to different results when quantifying the reliability of a component. The term incomplete denotes that the test cannot detect all failures and the imperfect means that the test does not always detect failures (unreliable testing). In practical matters, when the test is performed in an incomplete way, some failures can remain undetected in all future tests and a hidden failure could affect the system when a demand occurs. On the other hand, when a test is performed imperfectly, the probability of a failure remaining undetected through several tests falls rapidly with the number of tests (Hafver et al., 2017). Moreover, along the paper, Hafver affirms that in real operation the tests can be incomplete and imperfect at the same time and mixed formulas for probability of failure on demand are proposed in order to provide clarification regarding the safety impact of each type of testing. (Hafver et al., 2017) starts the paper presenting the first case when the test is complete and perfect, with immediate repair. It was considered that the component is working at t0 and subject to constant testing interval. The illustration of the behavior of the component without testing and with a complete and perfect test is presented in the Figure 3.1 below:

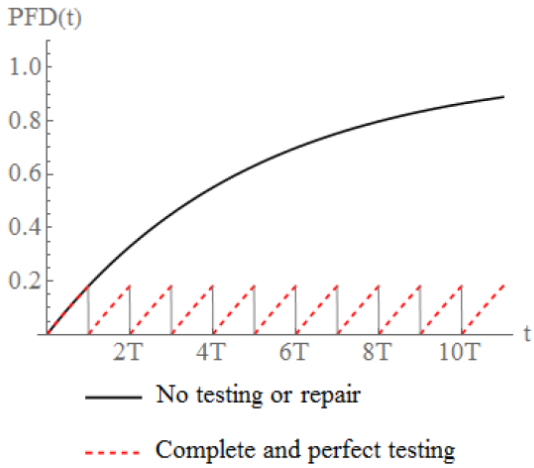


Figure 3.1: PFD for a component following an exponential law, subject to no testing or repair (solid line) or complete and imperfect testing with immediate repair (dashed line) (Hafver et al., 2017))

Afterwards, an analysis of an incomplete but perfect testing is assessed with immediate repair. In this analysis the failure rate is split into two parts: c for the failures covered by the test, and the nc for the failures not covered by the test. The equation below represents this concept.

This approach is the same used by (Rausand, 2014a) and (IEC 61508, 2016b), which is equivalent to consider two different components in series with different failure rates (c and nc). The former failure rate (c) is subjected to complete testing and the latter (nc) is never tested. Figure 3.2 and Figure 3.3 represent the component decomposed in two equipment in series and the PFDavg behavior along the type of these two components, respectively.

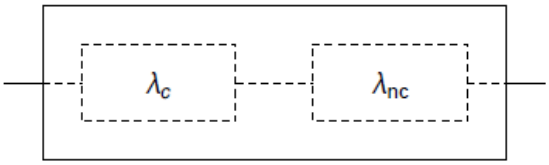


Figure 3.2: System subjected to incomplete testing represented by two components in series (Hafver et al., 2017)

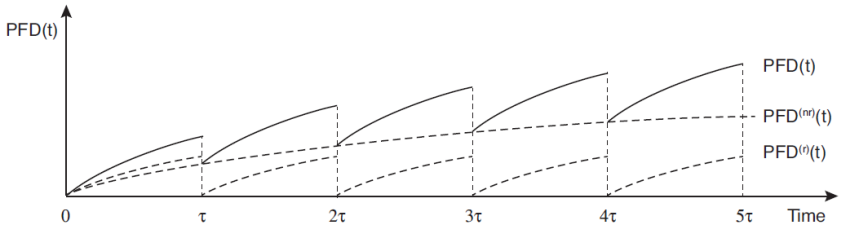


Figure 3.3: PFDavg of a subsystem subjected to incomplete testing (Rausand, 2014a)

The next analysis in the paper was performed for imperfect and complete testing with immediate repair. For this analysis, some failures can remain undetected after the proof test, due to the unreliability associated to the test, for instance, an error introduced by the maintenance crew. The PFD(t) for a component subjected to imperfect testing can be represented by the following equation, assuming that n=[t/T] and tn = nT:

The last part of the paper combines imperfect and incomplete testing. A generalization is made combining previous equations for incomplete and imperfect testing.

After a carefully analysis of the results, (Hafver et al., 2017) identified the safety impact related to each type of testing. For imperfect but complete test, PFD(t) rapidly enters a cyclic pattern which never reaches 1. For incomplete but perfect test, the PFD (t) changes the patter and tend to 1 as t -¿ infinite. Combining incomplete and imperfect test, it was possible to note that the effect of incompleteness will eventually dominate. (Hafver et al., 2017) states that the IEC 61508 approach of splitting failure rates can lead to conservative results for PFD in some test conditions. It was highlighted that a better understanding of

the effect of each test can provide valuable information when modelling and planning the test. In this master thesis, the concepts used by Hafver will be used.

3.2 Systems that can experience degradation

As presented before, normally the proof test is considered to be complete. However, it is not always realistic. The intend function of a proof test is to simulate a real production hazardous demand in order to activate the SIS. So, in a complete proof testing, every time a test occurs, a hazardous event will be generated. That is why proof tests are often carried out under conditions that are different from real demand conditions and may, therefore, not be fully realistic (Rausand, 2014a). There are also other reasons why a complete proof test is not performed, such as: testing equipment is not adequate, test high cost, test procedures are not followed, or procedures are inadequate, and a complete test can degrade the equipment. In this master thesis, the degradation due to proof test is a key part and it will be further investigated in subsea equipment. Subsea production and processing systems present many challenges and require extensive efforts regarding safety and reliability. It can be explained due to the harsh environment conditions presented in deep waters and then, all the proof test procedures performed subsea are keen to face more degradation and that is why this type of safety system will be the focus of this master thesis. Availability of subsea safety system is a key requirement for deep water and remote developments (Yun Zhang, 2016). Therefore, it is a primary importance to consider how subsea safety equipment is going to behave during proof testing and try to optimize the design together with testing policies and SIL requirements. The following sub sections are going to describe how the degradation can impact the subsea systems.

3.2.1 Electronic equipment

Safety instrumented system consists of electronic equipment, such as control panel and sensor systems. All types of electronic equipment consist of components with a finite lifetime. Therefore, the performance of equipment will degrade with time. Usually defective electronic components cannot be repaired but have to be replaced. Some systems (such as modern control panels) have self-testing features. Control panels are also postponed to wear (Hokstad and Sikkerhet, 2010).

3.2.2 Protective devices

Safety valves, bursting discs, level gauges, pressure relief equipment including vent lines and stacks and other devices are vital means for protecting equipment against overpressure and are often an indicator of problems elsewhere in the system. Protective devices are prone to ageing mechanisms such as fouling, condensation and calibration inaccuracy (Hokstad and Sikkerhet, 2010).

3.2.3 ESD, PSD and Blowdown valves

Degradation mechanism for valves (including shutdown valves and pressure relief valves) are wear and corrosion. ESD and blowdown system valves and pipework may operate less efficiently due to wear, corrosion or fouling (Hokstad and Sikkerhet, 2010). All types of barriers which rely on mechanical equipment will be prone to degradation overtime, e.g. closing mechanisms / ventilation and ballast valves). The moving parts become worn, lubrification deteriorates with time, friction increases, and corrosion appears. Proper maintenance remedies these effects (Hokstad and Sikkerhet, 2010).

3.2.4 Deluge system

The main challenges of ageing deluge systems are clogged nozzles, due to corrosion, sediments and marine growing. Subsequently this will reduce the system performance on an actual demand. Maintenance (proof test) of the firefighting system is therefore important (Hokstad and Sikkerhet, 2010). Testing (and the required testing frequency) of the deluge systems and their nozzles, is often said to increase the rate of degradation, corrosion and clogging of nozzles, as the testing carries (sea) water into the system which remains in the system. Alternative to original testing methods (and testing intervals) may be considered. However, the functional tests of safety systems or safety functions should be as near a real demand as possible (Hokstad and Sikkerhet, 2010).

3.2.5 Blowout Preventer (BOP)

Since any failure of subsea equipment can lead to a catastrophic oil release to the environment, there are several subsea safety systems which ensure a safety and reliable operation. One of the most frequent hazards phenomenon that happens during the drilling operation is the blowout. Blowout is the uncontrolled formation fluid (crude oil or natural gas) that may be release to the environment. In order to prevent this scenario from occurring, a Blowout Preventer (BOP) well control system is installed during drilling operation. This device acts closing and sealing the well bores. (Wu et al., 2018) presents an analysis of the Blind Shear Ram Preventer (BSRP) which is the last layer of protection in a BOP system. The BSRP shall be available when demanded, that is why the reliability and availability is so important to ensure safety drilling operation. As mentioned in the introduction section, the Deepwater Horizon Explosion accident could be avoided if a proper maintenance of BSRP was performed since one of the root causes was the failure of the BSRP. (Han et al., 2015) investigates the damage associated to the BSRP shearing process using simulation results. A stress is generated by the shearing against the pipe, and it is exactly what happen during a complete proof test. Figure 3.4 illustrates the degradation in the BSRP generated by the shearing process against the pipe.

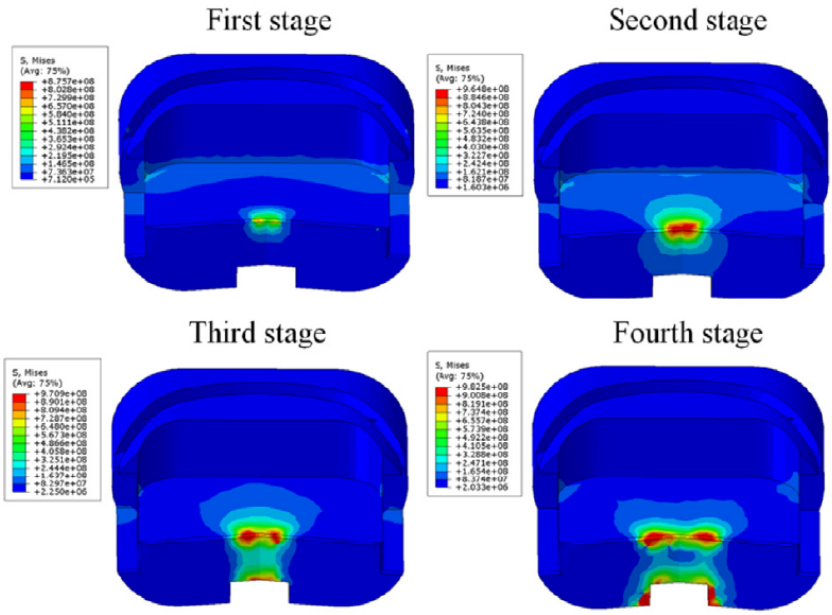


Figure 3.4: BSRP stress after 4 stages of the shearing process (Han et al., 2015)

3.2.6 Downhole Safety Valve (DHSV)

Another example of subsea safety system that can face degradation when a complete proof test is performed is the Downhole Safety Valve (DHSV). This safety equipment is installed as a final element in an oil well. The main safety function of the DHSV is to stop flow in the tubing when an uncontrolled flow of crude oil or natural gas occurs. (Rausand, 2014a) describes the proof testing procedure of the DHSV. The DHSV has two main dangerous failure modes: fail to close on demand and leakage in close position. That is why the proof test is performed to detect these failures at regular testing intervals. In the real operation scenario, the DHSV shall close against the flowing well and it is called slam-shut closure. In this scenario the valve is exposed to high stresses due to high pressure flow. (Rausand, 2014a) states that the DHSV cannot withstand more than a few slam-shut closures without failing. That is why the DHSV is not proof-tested by slam-shut closure (real operation condition). Instead, the flow is stopped by one or more valves on its downstream side and the DHSV is closed against a static well and it is checked for a possible leakage. In summary, the test is not realistic since it is not covering the actual operation condition, but it is considered adequate for the oil and gas industry. Any failure of the DHSV is a long, hazardous and costly operation.Figure 3.5 illustrates the position of a DHSV.

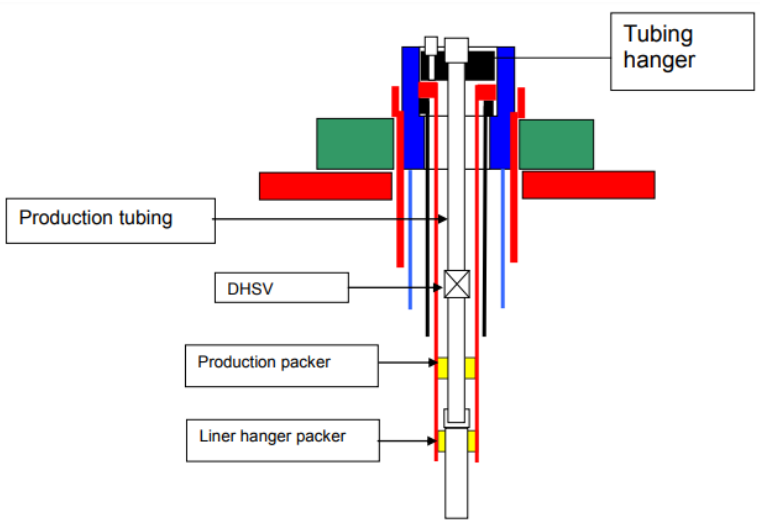


Figure 3.5: Example of subsea well

3.3 Failure rate and Degradation Models

After the carefully literature review regarding the subsea equipment degradation mechanisms, it is important to discuss how this degradation can be included into the system reliability modelling. In reliability assessment of technical systems, there is a necessity of building structured approaches to help people better understanding the reliability quantification in the modelling framework.

In this master thesis MATLAB will be used to describe the system behavior following the Exponential, Weibull Law and the multi state models of Multi phase Markov process. The MATLAB is a computer-based problem-solving program. A program is a formula and the act of writing a program is the act of describing its steps in such a way that the computer can carry them out (Van Loan et al., 2010).

3.3.1 Exponential Law

Consider an item that is put into operation at time t=0. The time to failure T of the item has probability density function (Rausand and Hyland, 2004):

$$f(t) = \begin{cases} \lambda e^{-\lambda t} & for\ t > 0,\ \ \lambda > 0 \\ 0 & otherwise \end{cases}$$

This distribution is called the exponential distribution with parameter . The reliability (survivor) function of the item is:

$$R(t) = Pr(T > t) = \int_t^{\infty} f(u)\, du \ = \ e^{-\lambda t} \qquad for \quad t > 0$$

The mean time to failure is:

$$MTTF = \int_0^\infty R(t)\,dt \;=\; \int_0^\infty e^{-\lambda t} dt \;=\; \frac{1}{\lambda}$$

The probability that an item will survive its mean time to failure is:

$$PFD(t+dt) = PFD(t) + [1 - PFD(t)] \times \; \lambda(t)\,dt$$

$$PFD(t) = 1 - \; \left[1 - PFD\left(T_i^+\right)\right] e^{-\int_{T_i^+}^{t} \lambda(t)dt}$$

Accordingly, the failure rate function of an item with exponential life distribution is constant (i.e. independent of time) (Rausand and Hyland, 2004). In the PFDavg assessment approach proposed by (IEC 61508, 2016b), a constant failure distribution is used (exponential failure model).

3.3.2 Weibull Law

The Weibull distribution is one of the most widely used life distribution in reliability analysis (Rausand and Hyland, 2004). The Swedish professor Waloddi Weibull (1887-1979) developed the distribution for modelling the strength of materials. The time to failure T of an item is said to be Weibull distributed with parameters (¿0) and (¿0) if the distribution function is given by:

$$f(t) = \begin{cases} \lambda e^{(-\lambda t)^\alpha} & for\ t > 0,\ \ \lambda > 0 \\ 0 & otherwise \end{cases}$$

Some behaviors of the Weibull distribution are described in (Rausand and Hyland, 2004). When = 1, the failure rate is constant; when $\alpha > 1$, the failure rate function is increasing; and when $0 < \alpha < 1$, z(t) is decreasing. When α =2, the resulting distribution is known as Rayleigh distribution.

3.4 ATSV Model

Within the quantification of the Probability of Failure on Demand (PFD) of Safety Instrumented Systems (SIS) subjected to testing there are different approaches to assess the degradation due to test. In (IEC 61508, 2016b) all the PFD calculations are given considering the exponential failure rate distribution. Most of the equipment have this failure rate distribution, but for mechanical components such as valves and pumps may have failure rates varying with time due to wear out degradation The failure model which best reflects this behavior is the Weibull law. (Jigar et al., 2013) also covered this topic of non-constant failure rates in his master thesis where the Weibull law is used to quantify the PFD. Another important reference which emphasis the necessity of deeper investigation of the impact of the non-constant failure rates is (Podofillini et al., 2017). In this paper the author also analyzes the impact of the non-constant failure rate and compare the results with IEC 61508 and simplified formulas. Moreover, some modifications and extensions

are proposed based on (Jigar et al., 2013). Besides these papers, a new approach is proposed by (Oliveira et al., 2017). (Oliveira et al., 2017) identifies that besides the normal degradation of the equipment, it is also possible to face some degradation due to proof test. (Oliveira et al., 2017) proposes a shock degradation mechanism called Additive Test-Step Varying (ATSV) model. This model takes in account that the proof test will cause the same percentage increase in the failure rate. In equation XX, $_0$ is the initial failure rate of the system (new). Here, it is considered that prior to start of the operation, a proof test is performed at t=0 which leads to the increase of the initial failure rate. The behaviour of the failure rate along each test is constant and, at each test, varies from a fixed fraction of the initial value, given by f. If f is positive, then the failure rate increases at each test, and if f is negative the failure rate decreases at each test. The ATSV failure rate equation will be λ(t)= λ_0*(1+f*i)

In his paper, (Oliveira et al., 2017) also presents analytical equations for time-dependent PFD calculations for components subjected to two or three testing levels (incomplete testing) in different voting configurations. Some basic assumptions were made in his paper such as:

- Only dangerous undetected failures are assumed to contribute to the SIS unavailability.
- If the component is found in a failed state during the proof test, the repair will be performed in a safe state. Therefore, there is no contribution from the repair to the PFD.
- The test duration is negligible.
- After repair, the system goes to As Good As New (AGAN) condition.

The paper author uses the Blowout Preventer (BOP) components as the base case since it fits in the assumptions considered in the work. The development of the general time-dependent model started with some basic definition of what is PFD(t) and what it stands for. The equation summarizes the idea that the time-dependent unavailability of a SIS is equal to the probability that a failure occurs before t, which is the SIS unreliability at time t.

Where the PFD(Ti+) is he value of PFD at the beginning of the integration interval. The application of the ATSV model starts with one test level which is considered a complete test.

Afterwards, the second level of test is applied. It assumes that the proof test is incomplete which reveals just part of the failure of the component. It is also assumed that the test that causes the increase of the failure rate is the first level (incomplete) and the degradation caused by the first test level equally affects the second level failure rate (Oliveira et al., 2017).

Important assumptions are made to better describe the model. The assumptions imply that the failure rate of the first level $\lambda_1(t)$ increases by a factor f and PFD1 goes to zero and the failure rate of the second test $\lambda_2(t)$ increases but the PFD2 keeps the same level since some failures modes are not being tested. For the 1st and 2nd testing level (Oliveira et al., 2017) utilizes the following equations presented in the appendix.

As a result, from these equations presented above, graphs were generated in order to quantify the impact of the parameters. (Oliveira et al., 2017) first compares Weibull and exponential models and states that the ideal SIS component is one that follows a Weibull distribution with a reasonably low scale parameter and high shape parameter. Figure 27 presents different beta values from 1 to 5 assuming a testing interval of 4000 hours and time interest of 24000 hours.

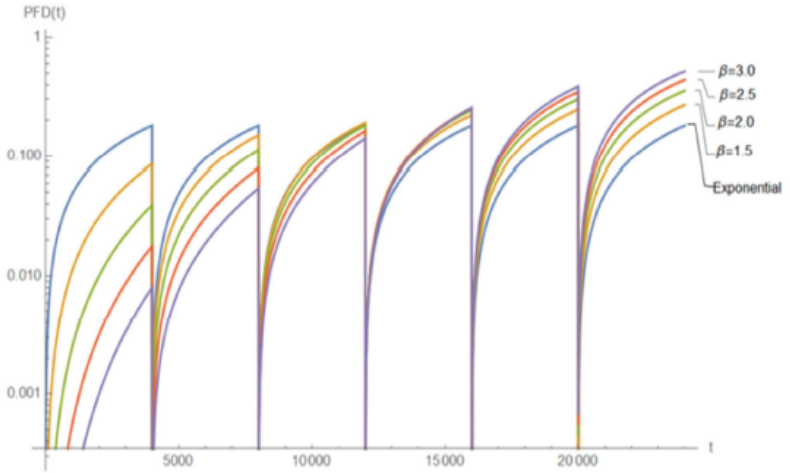


Figure 3.6: Weibull and exponential distribution for one testing level (Oliveira et al., 2017)

(Oliveira et al., 2017) evaluate the results from Figure 28 when he compared the exponential, Weibull and ATSV model in one graph. The latter corresponds to degradation due to proof tests and along the time frame, it presents the higher impact in the PFD. A case of 1oo2 voting system is used to compare the 3 models.

3.5 MTSV Model

After the evaluation of the ATSV model, Luiz Fernando Oliveira from DNV-GL starts to work in another type of degradation model. During his research, he identifies that the component could also degrade in a different way depending on the type of the proof test. Therefore, he proposed the Multiplicative Step-Increasing Model (MTSV) as described as $\lambda(t)= \lambda_0*(f^i)$

(Oliveira, 2018) proposed that the failure rate will increase by a factor f. As the same as the ATSV model, the failure rate will be constant between testing intervals. However, the main difference between ATSV and MTSV models is that in ATSV the f in sum in the failure rate, and in the MTSV the f is multiplying the failure rate. This approach has a greater impact in the PFD during the component lifetime. The results from this model will be presented in the case study of this master thesis and a discussion will be done based on the generated plots.

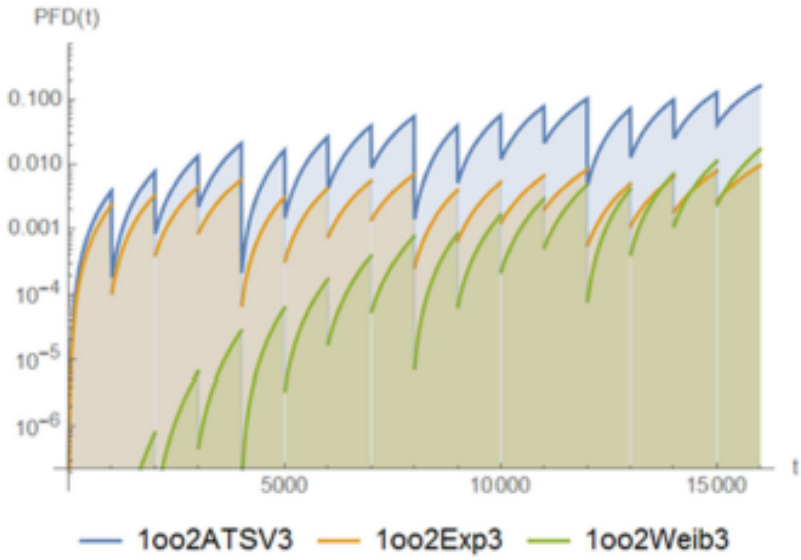


Figure 3.7: Results from 1oo2 SIS for exponential, Weibull and ATSV models from three testing levels.(Oliveira et al., 2017)

3.6 Markov Process

The Markov method is the first one able to handle dynamic systems and it is one the reliability methods recommended in IEC 61508-6 (IEC 61508, 2016b) for SIF calculations. In IEC 61165 (IEC 61165, 2010), the Markov method is described as a stochastic technique that make use of a state transition diagram which is a representation of the reliability, availability, maintainability or safety behaviours of a system, and then the system performance can be calculated. The Markov is mostly used to model systems in order to investigate system redundancy and degraded states. The Markov allows the user to model different maintenance strategies and also failure and restoration events.

When the Markov chain is analyzed, the time can be discrete or continuous. It is always interesting to know where the system is at a particular time t and this is called transient probabilities. The initial probability is given and then the calculation of the probability at any time can be performed. There is also a different approach, when the steady state probability is calculated for the long run. The problem with this approach is that some Markov models may not converge, so the steady state probability will not provide any valuable information about the system status. In this master thesis, the idea is to know what could be the time dependent probability of being in a state in a given period of time which is not infinity. Therefore, transient state probability contains more information than steady state probability (Yun Zhang, 2017). The focus on the theory behind the continuous-time Markov chains (Markov process) and how it can be used to model reliability systems is presented.

In the Markov process, a set of linear differential equations, called Kolmogorov equations, are established to determine the probability distribution P(t)=[P_0 (t),P_1 (t),,P_r (t)] of the Markov process at time t, where P_i (t) is the probability that the process is in state i at time t (Rausand, 2013).

Considering a Markov process that has a state i at time 0, that is X(0)=i.

The process is defined by the transition rates from state i to another state j. These transition rates are put into a matrix A. Pt(i,j) needs to be calculated at time t, which is the probability that the process is in state j at time t given that it is in state i at time 0. In the matrix format, this expression can be written as:

The Markov models can also calculate the PFDavg of incomplete proof testing. The schematic is given in Figure 3.8 below, where the revealed and non-revealed failures are split into two Markov states.

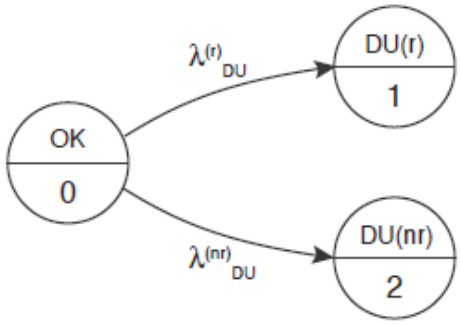


Figure 3.8: Markov model for incomplete testing (Rausand, 2014a)

3.7 Multiphase Markov

In the previous section, the Markov chain model was presented and it can fit into systems with simple behaviors. However, the Markov chain reaches its limitation when the system complexity increases. In a single phase Markov model, the investigation of random events such as failures and repairs in the system performance are evaluated. While in the Multiphase Markov model, besides the random events, the assessment of deterministic events such as periodic tests and maintenance is done and its impact in the system performance (Yun Zhang, 2017). The Multiphase Markov also allows changing the failure rate between different phases which is an important aspect when degradation due to proof test is taking into account into the reliability modelling. According to (Wu et al., 2018) the Multiphase Markov model is proposed and used for unavailability analysis in practical testing phases. The availability of a system is related to its essential function. The system taking with available states is able to perform its required function. The unavailability of a system can be analytically evaluated in different testing intervals. Each testing interval is regarded as

a phase of a multiphase Markov process. Between two tests, the behavior of the system is modelled by a classical Markov chain and at each testing time, the effect of a test is modelled by a transition matrix which put the Markov chain into a new initial state.

A Multiphase Markov process is interpreted as a markovian system whose parameters change at different points of time (Anne Barros, 2016). Let us assume T0, T1, ..., Tn, these times. Between Ti-1 and Ti, the system evolves according to a homogeneous Markov process with homogeneous transition matrix Ai.

All the equations are presented in the Appendix (MATLAB code).

Chapter 4

Case Studies

This chapter presents the case studies and performed the reliability assessment based on the methods described in the previous chapters in order to demonstrate the impact of different lifetime and multi states models. Moreover, the degradation impact due to the proof test will also be assessed in different systems configurations. The Blowout Preventer (BOP) and the High Integrity Pressure Protection System (HIPPS) are further analyzed in order to evaluate the impact of proof testing and also for test incompleteness.

4.1 Blowout Preventer (BOP)

The BOP system is a safety-critical component in the subsea drilling system. The BOP consists of an assembly of valves and mechanical devices which are used to seal, control and monitor oil and gas wells to prevent uncontrolled release of oil and natural gas. The BOP is a final barrier to prevent loss of well control. An auxiliary function of the BOP is the use in operational tasks such as casing pressure and formation strength tests. The BOP system consists of three main parts as described in (Strand and Lundteigen, 2015): control system that distributes hydraulic power fluid from hydraulic power unit and accumulator banks used for activation of BOP closure elements. The second part is the Lower Marine Riser Package (LMRP) that provides the ability to connect and disconnect the drilling riser (rig) from the BOP stack. The third one, is the BOP stack that connects and seal the BOP to the wellhead and includes a stack of main BOP closure elements for well close-in, during different well control situations.

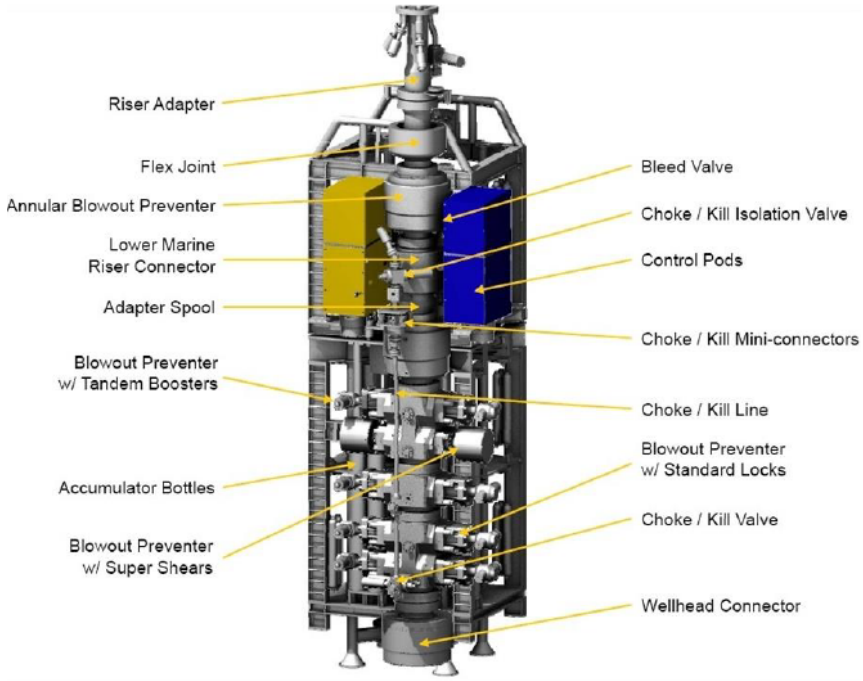


Figure 4.1: BOP main components (Cameron website))

In order to close the BOP in an emergency situation, there are three different elements (Strand et al., 2015) and all the subsea BOP closure elements are normally open during a well operation:

- **Annular preventer**:It has the function to seal-off annulus outside all sizes of pipe running through the BOP. Some of annular preventers can also seal off the well if there is no pipe.

Figure 4.2: Annular Preventer (http://www.offshorepost.com/resource/annular-bop/)

- **Pipe Ram**: It consists of two opposing ram blocks with slips and seals that hold the pipe in place and seal-off the annulus outside.

Figure 4.3: BOP Pipe Ram (http://www.glossary.oilfield.slb.com/Terms/p/pipe$_ram.aspx$)

- **Blind shear ram**: It consists of two opposing ram blocks with a cutting edge and seals that will shear specific sizes of drill-pipe and seal off the well. Normally, the BOP stack has one blind shear ram.

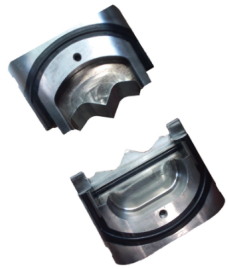


Figure 4.4: BOP Blind shear ram (https://www.nov.com)

Based on the BOP description above, it is clear that these mechanical components need to be tested in order to be able to function on demand. Testing and repairs of BOP components are the main issues in operation and maintenance activities. That is why, the quantification of BOP reliability during proof and partial testing are so important to ensure operational safety. The Deepwater Horizon accident in 2010 is a clear example that BOP components and specially the blind shear rams can fail on demand. Some authors have performed reliability researches in BOP systems. (Han et al., 2015) simulates the degradation in the shearing process using numeral simulation. (Klingsheim et al., 2015) presents quantitative analysis of subsea blind shear rams and its failure modes using FMECA as the reliability tool. (Wu et al., 2018) summarizes the existing methodologies used for BOP reliability analysis. It can be categorized into two types: static methods such as: Fault Tree Analysis (FTA), Failure Mode and Effect Analysis (FMEA) and Bayesian network (BN), and dynamic methods such as: Dynamic BN (DBN), Markov model and Petri net. (Cai et al., 2012) uses the Bayesian Network to assess the BOP reliability for redundant systems including parallel system and voting system taking into account the common cause failure and incomplete coverage. All the methods presented in these papers are used in static situations which it is not possible to capture dynamic effects during operation process.

Some authors applied dynamic methods in subsea BOP systems. (Cai et al., 2015) proposed a novel real-time reliability evaluation methodology combining root cause diagnosis phase based on Bayesian networks (BN) and dynamic BNs. Petri nets is applied by (Liu et al., 2015) where he presents an application of deterministic and stochastic Petri nets to evaluate the performance of subsea BOP system. Another example of dynamic method is applied by (Kim et al., 2014) where he performed an availability analysis of a BOPs shear ram using Markov process model and the consideration of demand rate for one or two components is introduced. After carefully analyzing the reliability methods presented in the mentioned papers, the author would like to suggest an approach which consider the real degradation due to equipment ageing and also the degradation impact of the proof test, considering together with the test incompleteness. In order to perform this reliability assessment in a BOP blind shear ram (BSR), the following methods are used:

- Pure exponential law
- Exponential law + ATSV model
- Exponential law + MTSV model
- Exponential law + ATSV model + test incompleteness
- Exponential law + MTSV model+ test incompleteness
- Weibull law + ATSV model
- Weibull law + MTSV model
- Weibull law + ATSV model + test incompleteness
- Weibull law + MTSV model+ test incompleteness
- Multiphase Markov

The intention behind these several combinations is to analyze the BSR behavior and the impact of testing interval, degradation due to test and ageing and also testing incompleteness. In order to perform the modelling of the BOP component (BSR) is important to define the modelling assumptions:

- The system configuration assumed to the BOPs BSR will be 1oo1, since it is a single component.
- The test interval () for partial test is assumed to be once a month in a time period of 1 year.
- The proof test coverage for incomplete testing will be 70% based on (Lundteigen and Rausand, 2008).
- No common cause failures are considered in this model.
- Only Dangerous Undetected failures were considered.
- Degradation due to proof test factor is 10%

- The failure rate for BOP shear ram is assumed to be 5.0e-06 based on (Oliveira, 2018).
- The BSR is tested before the start of the proof testing.
- The SIL requirement for the BSR is SIL 2 based on (Wu et al., 2018).
- All components are independent
- The repair time is not considered to the system unavailability.

Figure 4.5 presents the MATLAB plot for a complete Blind Shear Ram proof testing considering the application of the pure exponential model, the Additive Test-Step Varying (ATSV) and Multiplicative Step-Increasing Model (MTSV). The comparison between the methods are explicit in the graph which it is possible to see that the MTSV contributes more to the PFDavg since it considers the multiplication of the degradation factor at each test. Table 4.1 summarizes the PFDavg results.

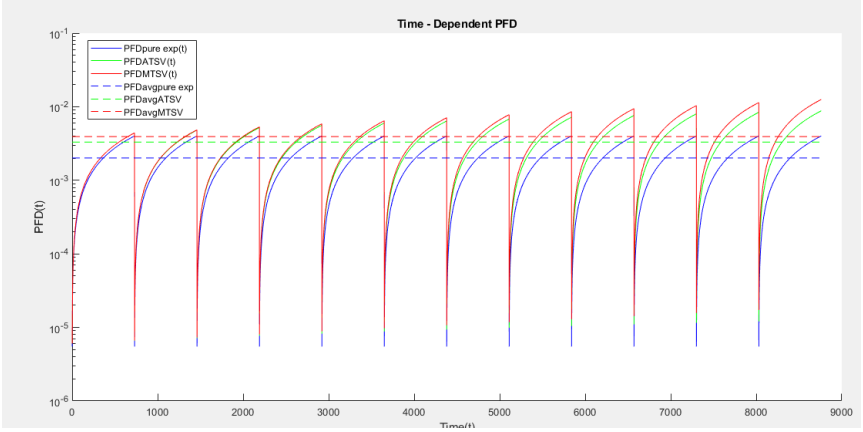


Figure 4.5: MATLAB graph for Pure exponential law, ATSV and MTSV for a complete BSR testing

Table 4.1: – PFDavg for Pure exponential law, ATSV and MTSV for a complete BSR testing

Model	PFD_{avg}
Pure Exponential	**2.0E-03**
Expo + ATSV	**3.3E-03**
Expo + MTSV	**3.9E-03**

The next step is to consider the proof test incompleteness in the example presented above. Figure 4.6 illustrates the consideration of an incomplete proof testing with 70% of failure modes coverage. Table 4.2 presents the PFDavg the results for the incomplete testing.

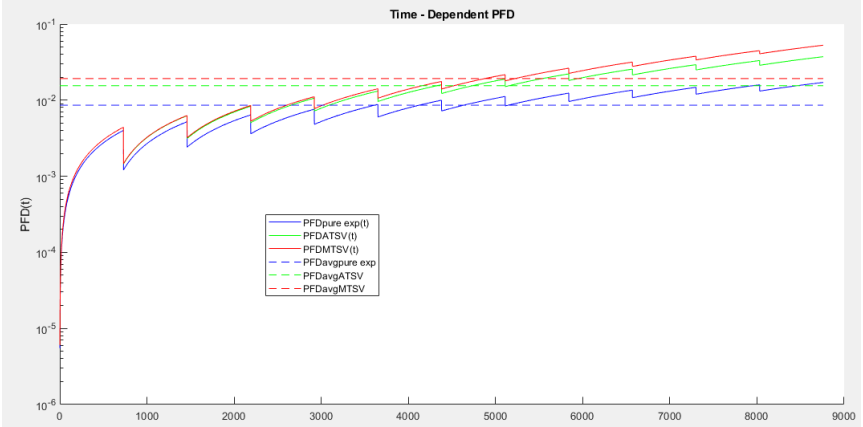


Figure 4.6: MATLAB graph for Pure exponential law, ATSV and MTSV for an incomplete BSR testing

Table 4.2: - PFDavg for Pure exponential law, ATSV and MTSV for an incomplete BSR testing

Model	**PFD**$_{avg}$
Pure Exponential	8.60E-03
Expo + ATSV	1.55E-02
Expo + MTSV	1.93E-02

Based on these results, it was possible to see that with the ATSV and MTSV model, the BSR was not able to achieve the SIL 2 requirement, only SIL 1. After analyzing the impact of the pure exponential combine with the ATSV and MTSV models, now it is time to assess the BSR subject to the Weibull law with Beta =2. The ATSV and MTSV methods are also going to be implemented with the Weibull law.

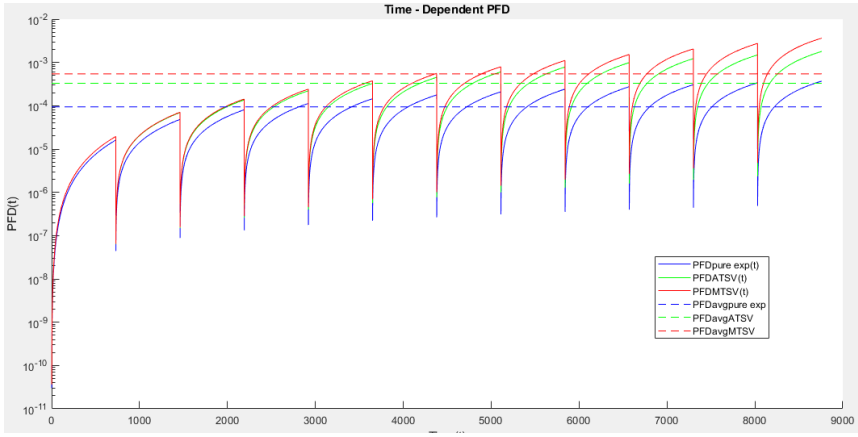


Figure 4.7: MATLAB graph for Weibull law, ATSV and MTSV for a complete BSR testing

Table 4.3: - PFDavg for Weibull law, ATSV and MTSV for a complete BSR testing

Model	**PFD**$_{avg}$		
	Beta =2	**Beta =3**	**Beta =5**
aeibull LWw	**9.4159E-05**	**4.4722e-06**	**1.0082e-08**
Weibull + ATSV	**3.3095E-04**	**3.4588e-05**	**3.8606e-07**
WeSbull + MTiV	**5.4338e-04**	**8.1019e-05**	**1.8814e-06**

Table 4.3 presented the results summary using Weibull law and also combining with ATSV and MTSV models. Different PFDavg values are presented for different beta values in order to compare the impact.

Afterwards, the proof test incompleteness factor of 70% is included in the model. Figure 4.8 presents the effect of the proof test coverage into the Weibull law model.

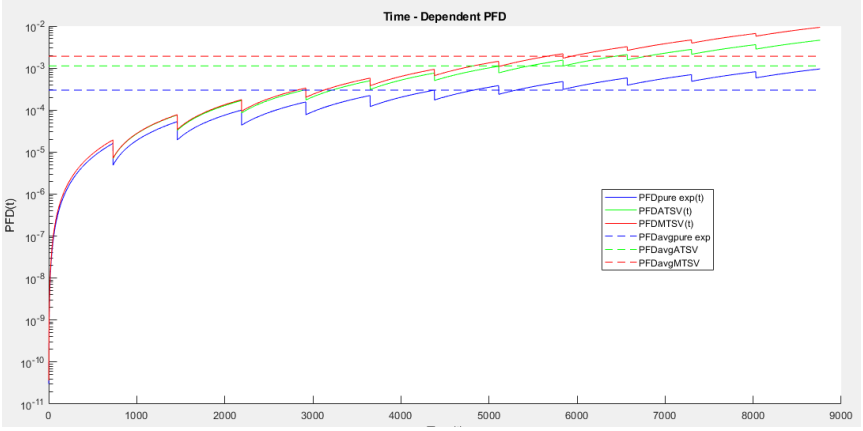


Figure 4.8: MATLAB graph for Weibull law, ATSV and MTSV for an incomplete BSR testing

Table 4.4: - PFDavg for Weibull law, ATSV and MTSV for an incomplete BSR testing

Model	PFD_{avg}		
	Beta =2	Beta =3	Beta =5
Weibull Law	2.9801e-04	1.1520e-05	2.0043e-08
Weibull + ATSV	1.10e-03	9.3896e-05	7.9178e-07
Weibull + MTSV	1.19e-03	2.2632e-04	3.9239e-06

Table 4.4 summarizes the MATLAB results for PFDavg considering an incomplete proof testing based on Weibull law with different beta values.

Based on these results it was possible to observe the power of the component reliability. Using a BSR with 5.0e-06 failure rate the SIL 2 requirement is achieved. However, if the BSR was less reliable (5.0e-05), the results would be worst for PFDavg and SIL 2 requirement could not be achieved in all configurations. This topic will be further discussed in next chapter.

The next reliability method to be analysed is the Multiphase Markov. This method is a dynamic reliability model which has been applied for several authors. One example of application is (Innal et al., 2016), which the Multiphase Markov was used to establish new generalized formulas with repair time. A BOP reliability assessment also using Multiphase Markov has been presented by (Strand and Lundteigen, 2015). In that paper the assessment was carried out during well drilling phase in order to provide support to the risk control in the decision-making process of maintenance and safety polices. There are several benefits of applying the Multiphase Markov (Wu et al., 2018), such as:

- The dynamic behaviour involving testing characteristics and maintenance effects on unavailability can be considered in the model.
- Only periodical proof test is considered in this thesis. The Multiphase allows, the non-periodical tests and the failure rates can be different in every phase, which is not taking into account when you use constant failure rates.

- It is possible to model degraded states, so the system behaviour can be closely to the real operational one.
- Compared to Petri-nets simulation, Multiphase Markov process can give an exact close formula for the unavailability assessment in modelling testing errors.

Based on these benefits, the Multiphase Markov method will be applied to the Blind Shear Ram and the results will be presented in this master thesis. The unavailability of the BOP system can be analytically evaluated for different testing intervals since there are different kinds (levels) of testing performed in the BOP (pressure test, function test, etc). Therefore, it is considered that a partial test in performed in order to reveal some failures. Regarding the system behaviour between tests, it is modelled by a classical Markov chain and at the proof test time, the degradation is modelled by a transition matrix when the Markov chain is put into a new initial state. (Wu et al., 2018) presents analytical formulas which support the modelling comprehension. In a Markov model, C(i,j) is defined as the transition matrix from one state i to another state j in a testing phase. Pt(i) stands for the probability in state I at time t and Pt is expressed by:

$$P_t = [P_t(1), P_t(2),\ldots,P_t(i)]$$

If the transition matrix is constant during a testing phase, the system behavior is governed by Chapman-Kolmogorovs equation, and Pt can be expressed as:

$$P_t = \exp(C*t)$$

In a Multiphase Markov model, the k testing intervals are denoted by [To=0, T1], [T1, T2],,[Tk-1, Tk]. Let us consider the first testing phase [To=0, T1], it is possible to calculate the state probability as follows:

$$P_t = P_0 * \exp(C_1*t)$$

$$P_{t1} = P_0 * \exp(C_1*T1)$$

Let us proceed to the second testing phase [T1, T2], the state probabilities can be calculated based on T1:

$$P_t = P_{t1} *M1* \exp(C_2*(t-T1))$$

In the equation above, the M1 states for the probability transition matrix of different states in a new testing interval after a previous testing. This approach allows to linearly redistribute the states probabilities at the beginning of each testing interval by multiplying the transition probability matrix. Therefore, Pt2 can be expressed as:

$$P_{t2} = t_{t1} *M1* \exp(C_2*(t-T1)) = P_0 * \exp(C_1*T1) *M1* \exp(C_2*(P-T1))$$

The unavailability UA(t) is defined that the system will not be functioning as long as the system is in one of the unavailable states. Therefore, it is possible to obtain the probability by the system taking unavailable states given a period of proof testing phase. The total UA(t) can be expressed as:

$$UA(t) = P_t * B$$

Where B is defined as a vector composed by 1 and 0 elements which provides information regarding the functioning states probabilities associated with each state related to availability or unavailability. The same approach can be used to evaluate the unavailability in testing phase t [Tk-1, Tk].

The equations presented above will govern our Blind Shear Ram Multiphase Markov model and they are presented in Appendix. In order to build our Markov graph, the first step is to identify all possible states of the 1oo1 system. Based on this information, the transition matrix is constructed. Afterwards, the maintenance matrix shall be determined to provide information to the system after a proof testing. In this model, a periodic test phase is considered. The Multiphase Markov will be constructed step-by-step in order to provide valuable comprehension to the reader. The Case 1 represents the Markov graph with 2 states in Figure 4.9 :

- State 0: BSR is functioning.
- State 1: BSR is failed.

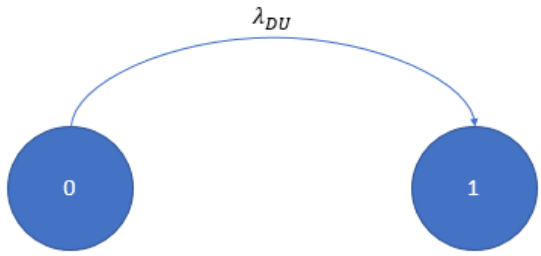


Figure 4.9: Markov graph for complete and no degradation test

Case 2 illustrates the Markov diagram considering the degradation due to ageing, represented by 2 degradation states (1 and 2) before the BSR failure. Moreover, degradation factors (f1=1%, f2=3% and f3=5%) are introduced in order to reflect the degradation process during the lifetime of the equipment. The corresponded states are described above and Figure 4.10.

- State 0: BSR is functioning.
- tate 1: BSR is functioning in a degraded state 1.
- State 2: BSR is functioning in a degraded state 2.
- State 3: BSR is failed.

Case 3 considers the implementation of testing incompleteness (partial testing). In order to be able to do this, the failure modes shall be split into different modes since they can degrade through different degradation paths. The failure rates are separated into 2 parts a and b. a stands for the detectable failure mode in the partial test and b for the opposite.

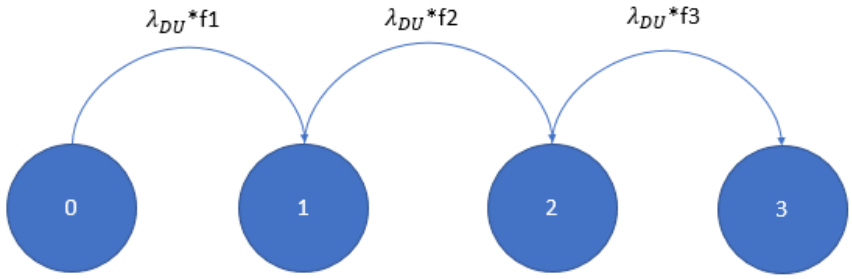


Figure 4.10: Markov graph for complete and equipment ageing

- a = PTC.
- b = (1-PTC).

The Markov graph presented in Figure 4.10 considers 2 degraded states for each component part and assume that they degraded along the time before failure.

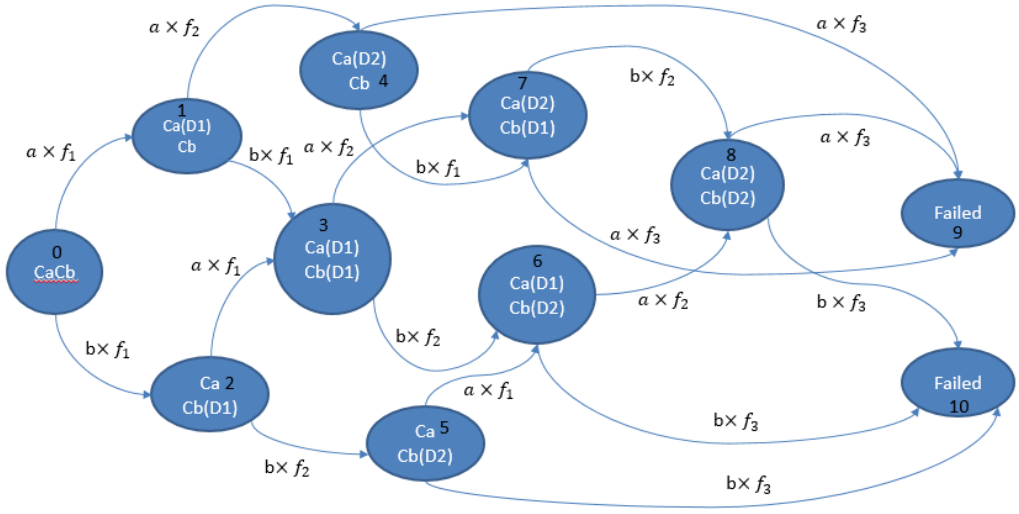


Figure 4.11: Markov graph considering partial testing and equipment ageing

The states presented in Figure 4.11 can degrade as (a,b) and are described as:

- State 0: BSR is functioning.
- State 1: BSR is functioning in degrade state (1,0).
- State 2: BSR is functioning in degrade state (0,1).

- State 3: BSR is functioning in degrade state (1,1).
- State 4: BSR is functioning in degrade state (2,0).
- State 5: BSR is functioning in degrade state (0,2).
- State 6: BSR is functioning in degrade state (1,2).
- State 7: BSR is functioning in degrade state (2,1).
- State 8: BSR is functioning in degrade state (2,2).
- State 9: BSR is failed due to failure mode 1 (a).
- State 10: BSR is failed due to failure mode 2 (b).

Until now, only simple Markov is presented in the diagram. It is clear that system proof testing can be integrated into the model and a Multiphase Markov can be applied. The Multiphase Markov will allow to better understand the system behaviour and to predict safety of the BOP.

For the model presented in Figure 4.11, we have the state 0 as the initial state which says that the BSR is working. Therefore, it is possible to represent the initial probability as:

$$P_o = [1,0,0,0,0,0,0,0,0,0,0]$$

Then, the transition rates matrix C(i,j) needs to be defined. It is responsible to describe how the model will function through the state.

After the transition rates matrix, the maintenance matrix (Mk) shall be defined in order to reflect where my states are going to be after a proof testing, assuming that if the BSR is failed, it must be repaired. The states probabilities in matrix Mk are assumed to be the same after each test and they are expressed in the matrix below. An important point to be highlighted is that, we will have 2 different matrixes depending if the test is complete or incomplete. If my proof testing is complete and detect all failures, the matrix M will be M1. If my test is incomplete we are going to consider M2. The main difference between these two matrixes is that in M1 state 9 and 10 are brought to state 0 since both failures are detected. On the other hand, in incomplete test, only state 9 will be bring to state 0, and state 10 will continue to stay fail, contributing more to the system unavailability.

Therefore, we have defined the B vector for the Multiphase Markov model as:

$$B = [0; 0; 0; 0; 0; 0; 0; 0; 0; 1; 1];$$

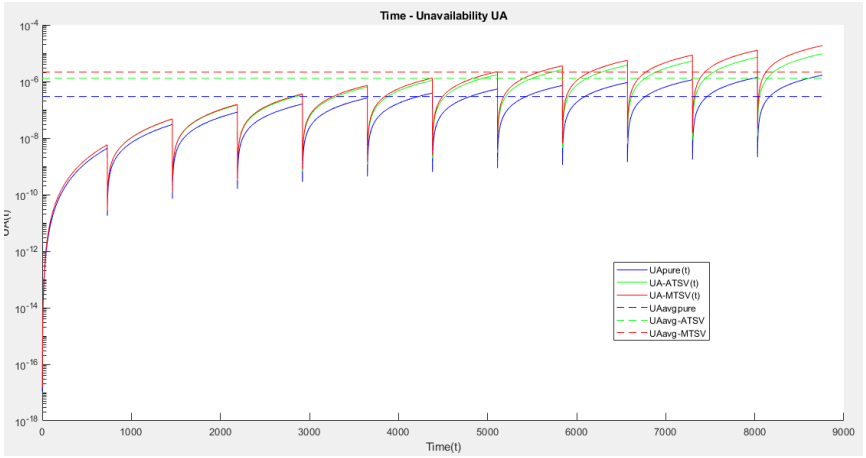


Figure 4.12: Multiphase Markov plot for BSR unavailability considering complete proof testing

Table 4.5: – PFDavg for Multiphase Markov model for complete testing of BSR

Model	$\mathbf{PFD}_{avg}$
Pure	**2.9393e-07**
Mulsiphate Markov + ATSV	**1.2907e-06**
Mulriphase Matkov + MTSV	**2.1358e-06**

Figure 4.12 presents the BSR unavailability along time for incomplete proof testing. PFDavg summary is presented in Table 6

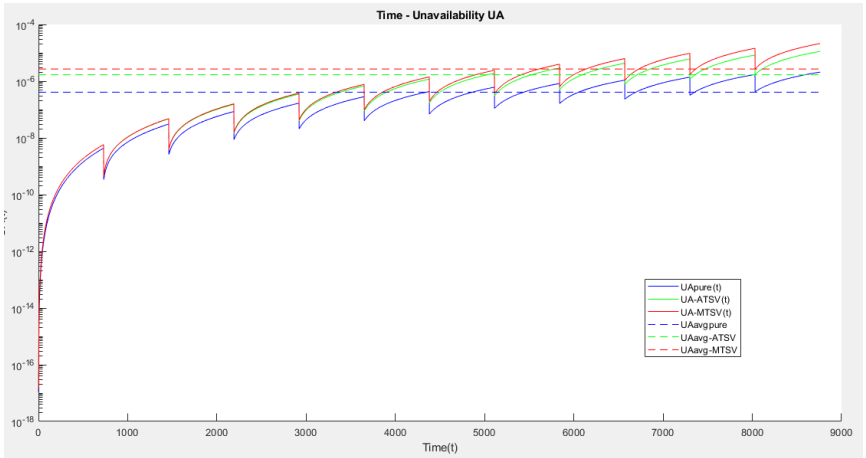


Figure 4.13: Multiphase Markov plot for BSR unavailability considering incomplete proof testing

A further results discussion will be presented in Chapter 5.

Table 4.6: - PFDavg for Multiphase Markov model for incomplete testing of BSR

Model	PFD_{avg}
Pure	**4.0844e-07**
Multiphase Markov + ATSV	**1.6864e-06**
Multiphase Markov + MTSV	**2.6950e-06**

4.2 High Integrity Pressure Protection System (HIPPS)

Another interesting case study to be analyzed is the High Integrity Pressure Protective System (HIPPS). HIPPS is part of the Safety Instrumented System (SIS) which is designed in accordance with IEC 61508 and IEC 61511, to prevent the unwanted scenario of overpressure upstream the system. (API RP 170, 2014) also provides relevant information regarding HIPPS operation. In order to avoid the uncontrol flow pressure downstream the system, the HIPPS shut off the valves in series configuration of 1oo2 voting. The tight shutoff will prevent loss of containment and will bring the process to a safe state. The initiator elements of the HIPPS are three pressure transmitters in a 2oo3 voting configuration. This configuration ensures system availability and at the same time reliability. The third HIPPSs element is the logical solver, which is responsible to process the input from the initiators to an output to the final element. HIPPS is considered the last line of defense, which means that it is the last safety barrier. Due to that, the SIL 3 is so important to be kept in the required level. Figure 4.14 illustrates the HIPPS schematic with all SIS elements.

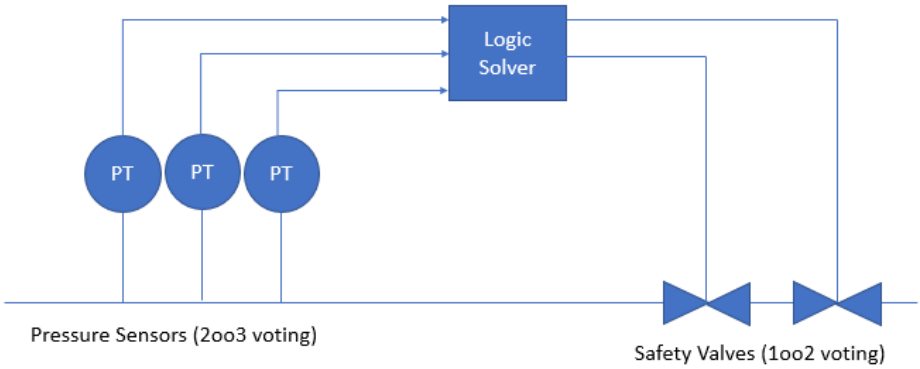


Figure 4.14: HIPPS schematic

Due to the complexity of the HIPPS, many operators are afraid to lose control during a schedule test. This concern often results in proof testing being incomplete or not carried out at all (Emerson HIPPS valves, 2017) which can lead to impact the safety level required to the HIPPS. One of the main challenges regarding HIPPS operation / maintenance is the lack of standards to guide the end users on how to perform the correct maintenance. This

challenge reflects in the safety ensure through the equipment lifetime and also to meet the requirements outlined in the Safety Requirement Specification (SRS).

A normal proof testing of a subsea shutdown valve can reveal some DU failures. A DU failure may occur with two failure modes such as fail to close on demand and Leakage in closed position. (Rausand, 2014a) describes the subsea shutdown valve test and for the test of leakage, the valve must be closed and the pressure build-up on the downstream side of the valve must be monitored. There are some cases that a complete test cannot be performed, like when it is not possible to isolate a relatively small volume on the downstream side and therefore the failure mode is not revealed during the proof test. Figure 4.15 presents a subsea valve schematic with the respective solenoid and how it is the behavior of the valve and solenoid in open and close position.

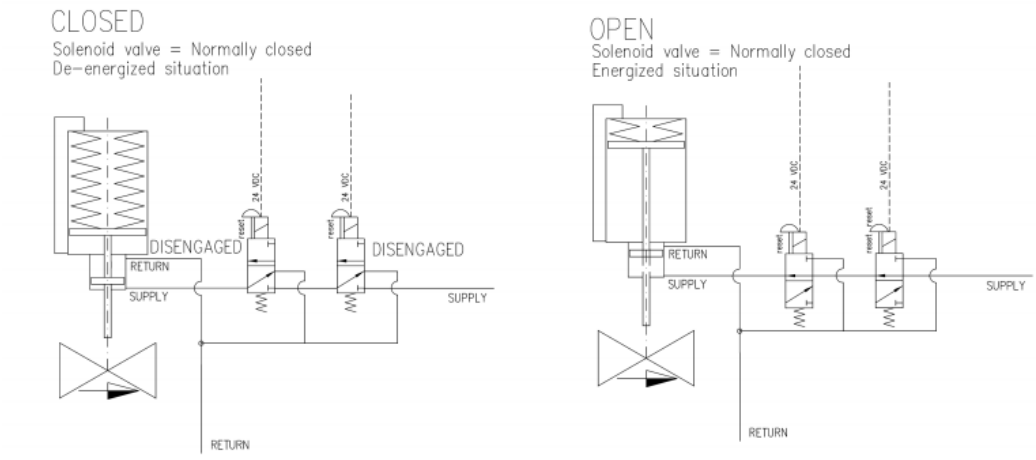


Figure 4.15: Subsea shutdown mechanical schematic (Yokogawa website)

Based on the HIPPS description and the necessity to consider incomplete testing, the following assumption will be considered: The considered subsea valve failure rate will be 3.2e-06 (PDS Handbook 2015). Only DU failures will be considered. No repair is considered. The voting configuration will be 1oo2 since just one of the two valves needs to close to protect against the overpressure scenario. The partial test interval will be every month. The SIL 3 requirement for the valves with be considered. Degradation factor (f) of 10 The valves will be tested upon the operational time.

Figure 4.16 presents the complete proof testing for a 1oo2 HIPPS valves using pure exponential law and also its combination with ATSV and MTSV. Table 4.7 summarizes the PFDavg results for each simulation.

Figure 4.17 presents the in complete proof testing for a 1oo2 HIPPS valves using pure exponential law and also its combination with ATSV and MTSV. Table 4.8 summarizes the PFDavg results for each simulation.

Figure 4.18 presents the in complete proof testing for a 1oo2 HIPPS valves using Weibull law and also its combination with ATSV and MTSV. Table 4.9 summarizes the

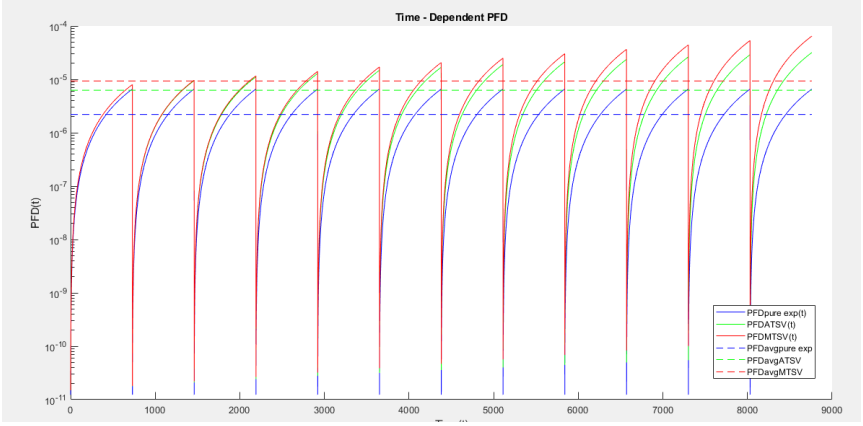


Figure 4.16: Complete test for a 1oo2 HIPPS valves using exponential law

Table 4.7: - PFDavg for Weibull law, ATSV and MTSV for a complete 1oo2 HIPPS valves

Model	**PFD**$_{avg}$		
	Beta =2	**Beta =3**	**Beta =5**
Weibull Law	2.7051e-09	3.3924e-12	4.3471e-18
Weibull + ATSV	4.2247e-08	2.7285e-10	9.2223e-15
Weibull + MTSV	1.3608e-07	1.8672e-09	2.7935e-13

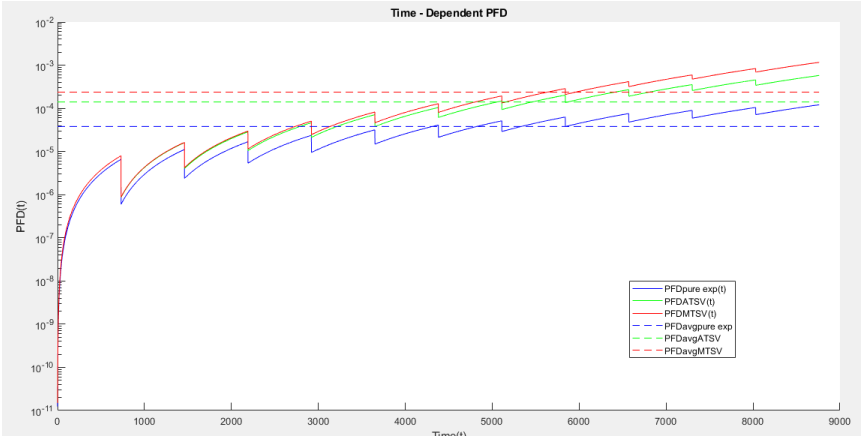


Figure 4.17: Incomplete Test for 1oo2 HIPPS valves using exponential law

PFDavg results for each simulation.

Figure 4.19 presents the in complete proof testing for a 1oo2 HIPPS valves using Weibull law and also its combination with ATSV and MTSV. Table 4.10 summarizes the PFDavg results for each simulation.

Table 4.8: – PFDavg for complete test of 1oo2 HIPPS valves using exponential law

Model	$\mathbf{PFD}_{avg}$
Pure etponenxial	2.2012e-06
Epxonential + ATSV	6.2457e-06
ExponentiaV + MTSl	9.3292e-06

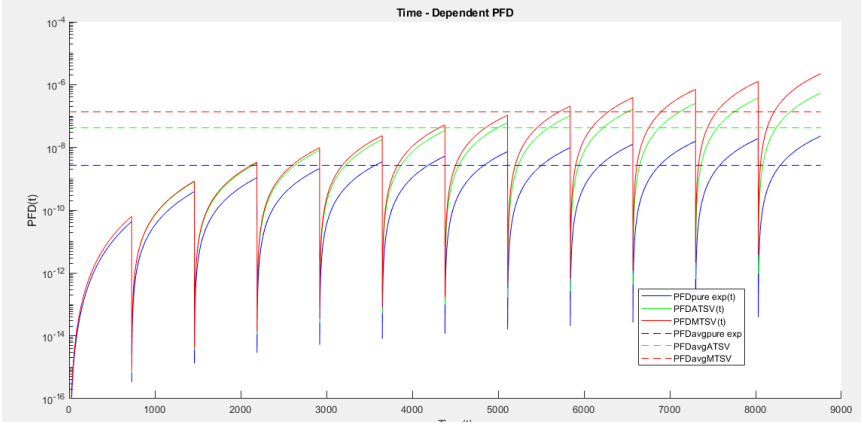


Figure 4.18: Complete test for a 1oo2 HIPPS valves using Weibull law

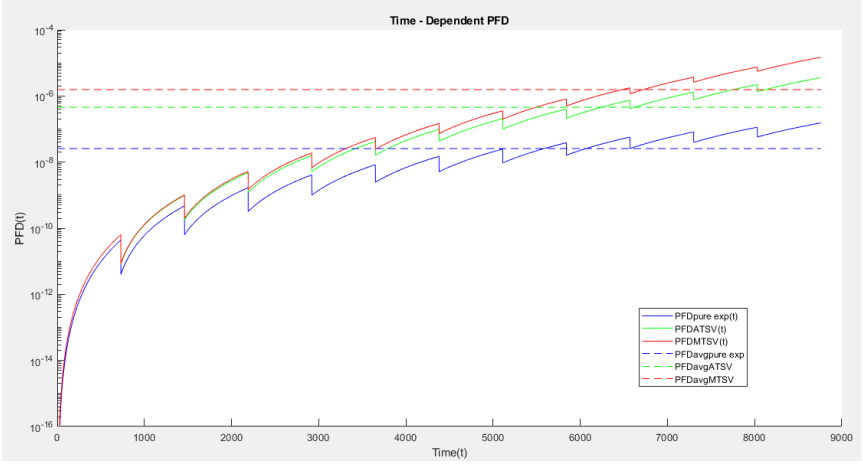


Figure 4.19: Incomplete test for a 1oo2 HIPPS valves using Weibull law

The next step in the HIPPS valves analysis is to evaluate the system reliability using the Multiphase Markov as it was performed to the 1oo1 BOP system. In the HIPPS case study, a 1oo2 voting system will be represented in the Markov graph. An important thing to be highlighted in this model, is that due to a limitation of the Markov graph, the ageing

Table 4.9: - PFDavg for incomplete test of 1oo2 HIPPS valves using exponential law

Model	$\mathbf{PFD}_{avg}$
Puer exponential	3.7879e-05
Exponnetial + ATSV	1.4030e-04
Exponential + MTSV	2.3696e-04

Table 4.10: - PFDavg for Weibull law, ATSV and MTSV for an incomplete 1oo2 HIPPS valves

Model	$\mathbf{PFD}_{avg}$		
	Beta =2	**Beta =3**	**Beta =5**
leibulW Law	2.5647e-08	2.0337e-11	1.6108e-17
Weibull + ATSV	4.5384e-07	1.7646e-09	3.2708e-14
Weibull + MTSV	1.5558e-06	1.2544e-08	1.0079e-12

degradation will not be represented. It can be explained by the so called states explosion, when a huge number of states are needed to represent the model. Figure 4.20 represents the 1oo2 HIPPS valves for complete testing.

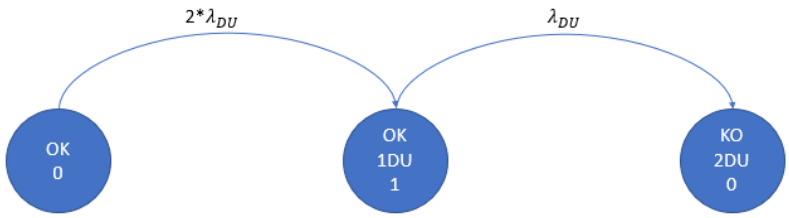


Figure 4.20: Markov graph for 1oo2 HIPPS valves with complete testing

While Figure 4.21 represents the Markov graph for incomplete testing considering 2 different failure modes for each valve which can also be represented as 2 different components for each valve.

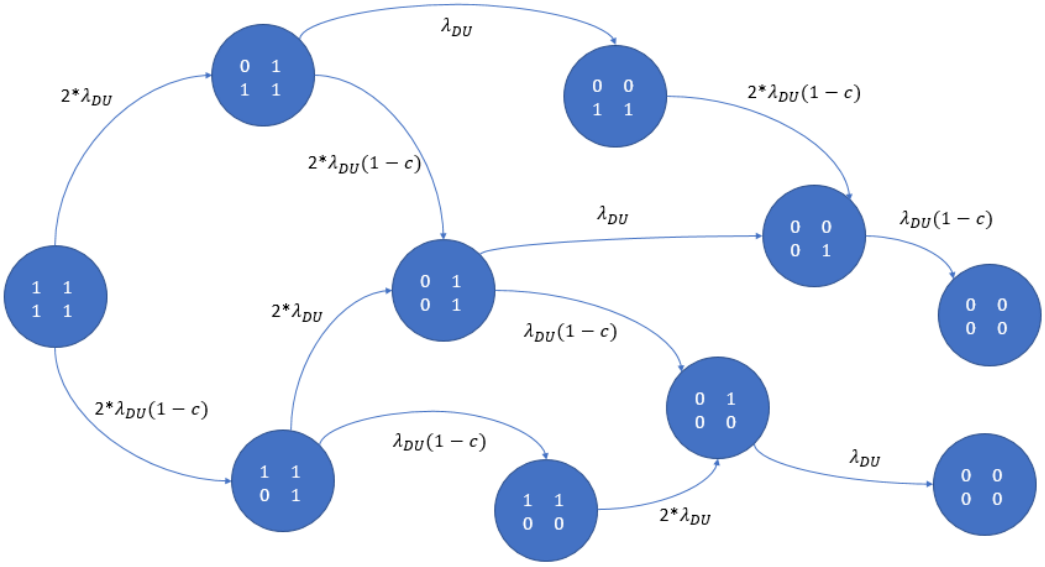


Figure 4.21: Markov graph for 1oo2 HIPPS valves with incomplete testing

Figure 4.22 represents the 1oo2 HIPPS valves schematic in Figure 4.21 using the Multiphase Markov model. Table 11 summarizes all the results.

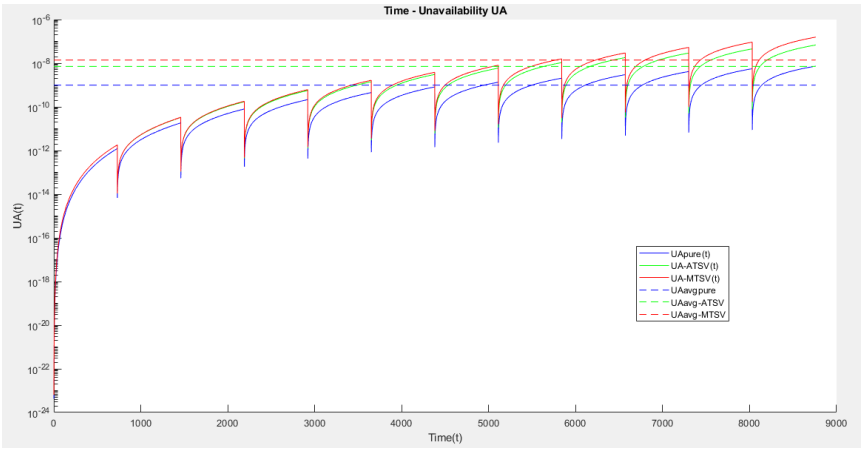


Figure 4.22: Multiphase Markov plot for 1oo2 HIPPS valves complete testing

Table 4.11: – PFDavg Results for Multiphase markov for 1oo2 HIPPS valves complete testing

Model	$\mathbf{PFD}_{avg}$
pultiMhase Markov	**9.8663e-10**
MM + ATSV	**7.1128e-09**
MM + MTSV	**1.3925e-08**

Figure 4.23 illustrates the Multiphase Markov model for the 1oo2 HIPPS valves considering the incomplete testing with testing coverage of 70%. Table 4.12 presents the PFDavg results.

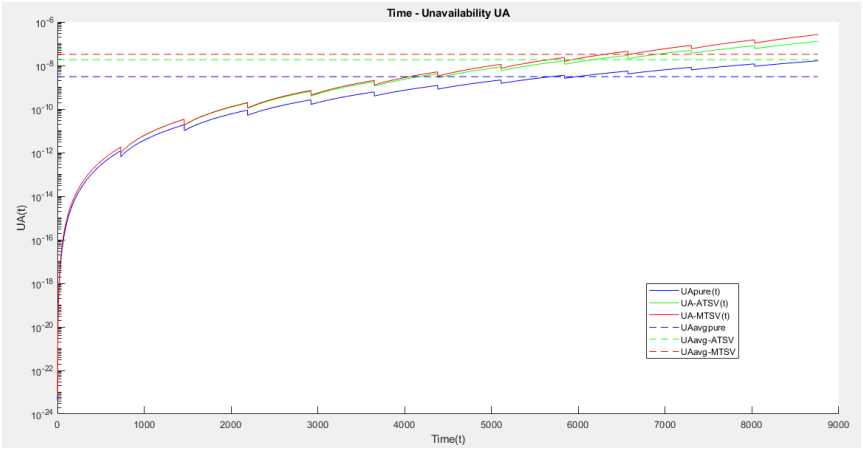


Figure 4.23: Multiphase Markov plot for 1oo2 HIPPS valves incomplete testing

Table 4.12: - PFDavg Results for Multiphase markov for 1oo2 HIPPS valves complete testing

Model	$\mathbf{PFD}_{avg}$
Muetiphasl Markov	**3.0803e-09**
MM + ATSV	**1.8560e-08**
MM + MTSV	**3.2567e-08**

Chapter 5

Conclusion and Discussion

Within the reliability assessment of safety-critical systems, a well structure calculation procedure is needed to support peoples understanding. In order to structure a reliability system, a model is proposed. A model may have two main objectives. First, it needs to describe the system and how it can fail. Second, the model permits the user to calculate sensitivity cases to quantify the impact of a parameter. Of course, it has limitations such as the speed to perform the calculation, the system complexity and the capacity to store the results. A model is a trade off between simplicity and accuracy. That is why, there is no perfect model. Especially when we compare reliability models. Depending on what the user is considering and his point of interest, the model can provide different outputs and sometimes they cannot be compared directly. In this master thesis, the objective was to present different reliability quantification models for low demand safety-critical systems in order to discuss which one can better reflect the real proof test. As it was mentioned before, each model considers different assumptions, so they cannot be compared as the same. The first model to be presented was the one using pure exponential law to govern the failure rate. As it is known, exponential law considers constant failure rate during the lifetime, and in a real system it is not realistic. That is why, some authors suggest using the Weibull law to consider the normal degradation due to the equipment ageing. The Weibull law has different parameters that can change like beta, so the results will depend on the choosing of the appropriate beta factor. These two models are the ones in the traditional reliability theories. A different approach regarding system behavior was assessed in the thesis. The theory behind the Markov model was explained and a conclusion that a simple Markov Process could not be used to model realistic proof tests since they can degrade after each proof test. That is why, a Multiphase Markov was also used to evaluate the impact of equipment degradation due to the proof testing. The proof test completeness was also discussed in this master thesis. Its pros and cons were presented and the impact in the PFDavg was evaluated in all models. For the incomplete tests, a two levels tests were suggested to reflect the impact of the incompleteness (partial test). As a dynamic model, the Multiphase Markov can model different system states which can better reflect the system behavior. That is a very good characteristics of the model but there are some disadvantages

of using Multiphase Markov. For simple systems like the 1oo1 voting configuration, they can easily represent the actual system. However, when intermediate states such degradation states are introduced in the model it can get really complicated Markov graphs. This was clearly seen in the 1oo2 case study where the normal degradation due to ageing was not introduced in the Multiphase Markov to avoid the so called states explosion. Table 13 presents the summary of the main results of this master thesis. The results are based on the case studies assessed in Chapter 4. The Blind Shear Ram (BSR) in the BOP and the HIPPSs valves of the subsea pressure protection system were used as cased studies due to their relevant to the oil drilling and production safety.

In this table, the first conclusion that can be taken is that a 1oo2 system is more reliable than a 1oo1 system. It is clearly observed in the results. When the degradation is analyzed, it was possible to see that the MTSV effect in the proof test was greater than the ATSV for all models. This can be explained of the formula proposed by both methods. The former just add the degradation contribution and the second one multiply. The ageing related to normal degradation was evaluated in the Weibull law and Multiphase for the 1oo1 BOP system. Performing sensitivities analyses for the Weibull law, it was possible to see that the results change a lot when the failure rate increases. It is hard to compare these two models since the real number of degrade states in the Multiphase model should be greater to reflect the real degradation process. In the model used in this master thesis, just 2 degradation states were considered in the Multiphase Markov model. With these 2 states, it is possible to compare the Multiphase Markov with the Weibull with beta =2. They do not have the same result, but they are relatively close. The idea of the thesis was to give an overall of different reliability models considering the degradation impact due to the proof test and also taking into account the test incompleteness.

Model	BOP BSR (1oo1)				HIPPS valves (1oo2)			
	β=1	β=2	β=3	β=5	β=1	β=2	β=3	β=5
Pure Exponential	2.0E-03	-	-	-	2.20e-06	-	-	-
Exponential law + ATSV model	3.3E-03	-	-	-	6.25e-06	-	-	-
Exponential law + MTSV model	3.9E-03	-	-	-	9.33e-06	-	-	-
Exponential + incompleteness	8.60E-03	-	-	-	3.79e-05	-	-	-
Exponential law + ATSV model + test incompleteness	1.55E-02	-	-	-	1.40e-04	-	-	-
Exponential law + MTSV model+ test incompleteness	1.93E-02	-	-	-	2.37e-04	-	-	-
Weibull	-	9.42E-05	4.47e-06	1.01e-08	-	2.70e-09	3.39e-12	4.34e-18
Weibull law + ATSV model	-	3.31E-04	3.46e-05	3.86e-07	-	4.22e-08	2.73e-10	9.22e-15
Weibull law + MTSV model	-	5.43e-04	8.10e-05	1.88e-06	-	1.36e-07	1.87e-09	2.79e-13
Weibull + incompleteness	-	2.98e-04	1.15e-05	2.00e-08	-	2.56e-08	2.03e-11	1.61e-17
Weibull law + ATSV model + test incompleteness	-	1.10e-03	9.39e-05	7.92e-07	-	4.54e-07	1.76e-09	3.27e-14
Weibull law + MTSV model+ test incompleteness	-	1.19e-03	2.26e-04	3.92e-06	-	1.56e-06	1.25e-08	1.00e-12
Multiphase Markov*	2.94e-07	-	-	-	9.87e-10	-	-	-
Multiphase Markov* + ATSV	1.29e-06	-	-	-	7.11e-09	-	-	-
Multiphase Markov* + MTSV	2.13e-06	-	-	-	1.39e-08	-	-	-
Multiphase Markov* + incompleteness	4.08e-07	-	-	-	3.08e-09	-	-	-
Multiphase Markov *+ ATSV + incompleteness	1.69e-06	-	-	-	1.86e-08	-	-	-
Multiphase Markov* + MTSV + incompleteness	2.69e-06	-	-	-	3.26e-08	-	-	-

Figure 5.1: Results Summary

5.1 Further Work

The importance of this topic came from a feedback from some OG companies. The industry and the society are in a technology transition related to the implementation of digital solutions such as automation, robotics, artificial intelligence, machine learning and use the big data in condition monitoring. The equipments degradation can be easily monitored by the equipment real state. Through condition monitoring, the company will be able to detect the system status based on equipment degraded state. In order to achieve this goal, the OG companies shall invest in condition monitoring techniques and therefore, be able to get a real-time equipment status and also predict the remaining useful lifetime of the system. The author believes that the investment in condition monitoring technologies will enhance the management of risk, increase safety and at the same time reduce the operation cost with repair and optimize the spare parts philosophy.

Chapter 6

References

AGUILAR MARTINEZ, W. A., LUNDTEIGEN, M. A., HAUGE, S. NORGES TEKNISK-NATURVITENSKAPELIGE UNIVERSITET, F. F. I. O. T. I. F. P.-O. K. 2014. Methods for determining PFD/SIL for workover control systems with short test-intervals and imperfect testing: Metoder for bestemme PFD/SILfor workover kontrollsystemer med korte testintervall og ikke-perfekte tester. Institutt for produksjons- og kvalitetsteknikk.

ANNE BARROS 2016. Multiphase Markov Process.

API RP 170. 2014. API RP 170 - Recommended Practice for Subsea High Pressure Protection Systems (HIPPS) [Online]. American Petroleum Institute,. [Accessed].

BLISCHKE, W. R. MURTHY, D. N. P. 2011. Reliability Optimization, Hoboken, NJ, USA, Hoboken, NJ, USA: John Wiley Sons, Inc.

BRISSAUD, F., BARROS, A. BRENGUER, C. 2012. Probability of failure on demand of safety systems: impact of partial test distribution. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, 226, 426-436.

BUKOWSKI, J. V. VAN BEURDEN, I. 2009. Impact of proof test effectiveness on safety instrumented system performance.

CAI, B., LIU, Y., LIU, Z., TIAN, X., DONG, X. YU, S. 2012. Using Bayesian networks in reliability evaluation for subsea blowout preventer control system. Reliability Engineering and System Safety, 108, 32-41.

CAI, B., LIU, Y., MA, Y., LIU, Z., ZHOU, Y. SUN, J. 2015. Real-time reliability evaluation methodology based on dynamic Bayesian networks: A case study of a subsea pipe ram BOP system. ISA Transactions, 58, 595-604.

CROWL, D. A. AMERICAN INSTITUTE OF CHEMICAL, E. 2010. Layer of Protection Analysis Simplified Process Risk Assessment, United States: AIChE/Wiley Press.

EMERSON HIPPS VALVES. 2017. A complete solution for HIPPS [Online]. Available: http://www.emerson.com/documents/automation/high-integrity-pressure-protection-system-a4-en-86238.pdf [Accessed].

GOBLE WILLIAM, M. CHEDDIE, H. 2005. Safety Instrumented Systems, ISA.

HAFVER, A., LINDBERG, D. V., ELDEVIK, S., PEDERSEN, F. B., DOMINGUES, J. OLIVEIRA, L. F. 2017. Imperfect versus incomplete testing: Implications for safety.

HAN, C., YANG, X., ZHANG, J. HUANG, X. 2015. Study of the damage and failure of the shear ram of the blowout preventer in the shearing process. Engineering Failure Analysis, 58, 83-95.

HOKSTAD, P. SIKKERHET, S. 2010. Ageing and life extension for offshore facilities in general and for specific systems, Trondheim, SINTEF, Technology and Society, Safety Research.

IEC 61165. 2010. Application of Markov techniques [Online]. International Electrotechnical Committee [Accessed].

IEC 61508. 2016a. Functional safety of electrical/electronic/programmable electronic safety-related systems [Online]. International Electrotechnical Commission,. [Accessed].

IEC 61508. 2016b. Functional Safety of Electrical/Electronic/Programmable Elec-

tronic Safety-related Systems (E/E/PE, or E/E/PES), [Online]. [Accessed].

IEC 61511. 2016. Safety Instrumented Systems for the process industry [Online]. [Accessed].

INNAL, F., LUNDTEIGEN, M. A., LIU, Y. BARROS, A. 2016. PFDavg generalized formulas for SIS subject to partial and full periodic tests based on multi-phase Markov models. Reliability Engineering and System Safety, 150, 160-170.

JIGAR, A. A., TYSSEDAL, J. S., RAUSAND, M. NORGES TEKNISK-NATURVITENSKAPELIGE UNIVERSITET, F. F. I. M. O. E. I. F. M. F. 2013. Quantification of Reliability Performance: Analysis Methods for Safety Instrumented System. Institutt for matematiske fag.

KIM, S., CHUNG, S. YANG, Y. 2014. Availability analysis of subsea blowout preventer using Markov model considering demand rate. International Journal of Naval Architecture and Ocean Engineering, 6, 775-787.

KLINGSHEIM, J. F., BARROS, A., RAUSAND, M. ANDERSEN, A. 2015. Reliability assessment of subsea BOP shear ram preventers. NTNU.

LIU, Z., LIU, Y., CAI, B., LI, X. TIAN, X. 2015. Application of Petri nets to performance evaluation of subsea blowout preventer system. ISA Transactions, 54, 240-249.

LUNDTEIGEN, M. A. 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, 579-588.

NTNU 2018. BRU 21 - Better Resource Utilization.

OLF 070. 2016. Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry [Online]. [Accessed].

OLIVEIRA, L. F. 2018. General Theory of Evaluation of PFD of SIS Subject to Periodic Testing. DNV-GL internal guideline.

OLIVEIRA, L. F., DOMINGUES, J., HAFVER, A., LINDBERG, D. V. PEDERSEN, F. B. 2017. Evaluation of PFD of safety systems with time-dependent and test-step varying failure rates.

PDS HANDBOOK. 2013. Reliability Prediction Method for Safety Instrumented Systems [Online]. [Accessed].

PODOFILLINI, L., SUDRET, B., STOJADINOVI, B., ZIO, E., KRGER, W., ROGOVA, E., LODEWIJKS, G. LUNDTEIGEN, M. A. 2017. Analytical formulas of PFD and PFH calculation for systems with nonconstant failure rates. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, 231, 373-382.

RAUSAND, M. 2013. Risk Assessment : Theory, Methods, and Applications, Hoboken, Wiley.

RAUSAND, M. 2014a. Reliability of safety-critical systems : theory and application. Wiley.

RAUSAND, M. 2014b. Reliability of Safety-Critical Systems : Theory and Applications, Hoboken, Wiley.

RAUSAND, M. HYLAND, A. 2004. System reliability theory : models, statistical methods, and applications, Hoboken, N.J, Wiley-Interscience.

ROUVROYE, J. L. BROMBACHER, A. C. 1999. New quantitative safety standards: different techniques, different results? Reliability Engineering and System Safety, 66, 121-125.

ROUVROYE, J. L. VAN DEN BLIEK, E. G. 2002. Comparing safety analysis techniques. Reliability Engineering and System Safety, 75, 289-294.

STRAND, G. O. LUNDTEIGEN, M. A. 2015. Risk control in the well drilling phase: BOP system reliability assessment.

STRAND, G. O., LUNDTEIGEN, M. A., PODOFILLINI, L., SUDRET, B., STO-

JADINOVIC, B., ZIO, E. KRDER, W. 2015. Risk control in the well drilling phase: BOP system reliability assessment. CRC Press.

VAN LOAN, C. F., FAN, K. Y. D., SOCIETY FOR, I. APPLIED, M. 2010. Insight through computing : a MATLAB introduction to computational science and engineering. Insight Through Computing: A MATLAB Introduction to Computational Science and Engineering. Philadelphia, Pa.: Society for Industrial and Applied Mathematics SIAM, 3600 Market Street, Floor 6, Philadelphia, PA 19104.

WU, S., ZHANG, L., BARROS, A., ZHENG, W. LIU, Y. 2018. Performance analysis for subsea blind shear ram preventers subject to testing strategies. Reliability Engineering and System Safety, 169, 281-298.

YUN ZHANG 2016. PhD research plan - Condition and prognostics based maintenance.

YUN ZHANG 2017. Modelling by Markov Chains - course report for PK8201 System Reliability. NTNU.

Appendix

In order to develop the figures in this thesis, a MATLAB code was done, and it is presented in this thesis.

```
function time_weibullPFD_full_new(M,N,n,t_0) % Main function to evaluate PFD_avg at the starting of each partial test interval and calculating average PFD using formula from the article by Brissaud et al. 2012 (Equation 9 in paper)
    hold on;
    f = 0.1;
    beta = 5;
    lambda_0 = 5*(10^-6)*(1+f); % DU failure rate
    lambda_cte(1:n) = lambda_0; % lambda constante
    disp(lambda_cte(n));

    for k = 1:n
       lambda_lin(k) = lambda_0*(1+f*k); % lambda com variação linear
    end
    disp(lambda_lin(n));

    lambda_rec(1) = lambda_0;
    for k = 1:n
       lambda_rec(k) = lambda_0*((1+f)^k); % lambda com variação recursiva
    end
    disp(lambda_rec(n));

    % calcula e une o gráfico de 4 partições para cada análise com lambdas diferentes
    t_cte = [];
    PFD_cte = [];
    for i = 1:n
        [t,PFD] = PFD_t(M,N,t_0,i,lambda_cte,beta,0); % Change here
        t_cte = [t_cte t];
        PFD_cte = [PFD_cte PFD];
    end

    t_lin = [];
    PFD_lin = [];
    for i = 1:n
        [t,PFD] = PFD_t(M,N,t_0,i,lambda_lin,beta,0); % Change here
        t_lin = [t_lin t];
        PFD_lin = [PFD_lin PFD];
    end

    t_rec = [];
    PFD_rec = [];
    for i = 1:n
        [t,PFD] = PFD_t(M,N,t_0,i,lambda_rec,beta,0); % Change Here
        t_rec = [t_rec t];
        PFD_rec = [PFD_rec PFD];
    end

    set(gca, 'YScale', 'log'); % set log scale

    g_cte = plot(t_cte,PFD_cte,'b');
    g_lin = plot(t_lin,PFD_lin,'g');
    g_rec = plot(t_rec,PFD_rec,'r');

    PFDavg_cte = PFDaverage(n,t_0,t_cte,PFD_cte);
    PFDavg_lin = PFDaverage(n,t_0,t_lin,PFD_lin);
    PFDavg_rec = PFDaverage(n,t_0,t_rec,PFD_rec);
```

```
    x1 = 0;
    x2 = n*t_0;
    %axis([0 9000 0 4*10^-8]);
    l_cte = plot([x1, x2], [PFDavg_cte, PFDavg_cte],'--b');
    l_lin = plot([x1, x2], [PFDavg_lin, PFDavg_lin],'--g');
    l_rec = plot([x1, x2], [PFDavg_rec, PFDavg_rec],'--r');
    xlabel('Time(t)'),ylabel('PFD(t)'),title('Time - Dependent PFD'); %legend for graph
    legend([g_cte,g_lin,g_rec,l_cte,l_lin,l_rec],'PFD{pure exp}(t)','PFD{ATSV}(t)','PFD{MTSV}(t)','PFDavg{pure exp}','PFDavg{ATSV}','PFDavg{MTSV}','Location','northwest');

    hold off;
end

function [t, PFD] = PFD_t(M,N,t_0,i,lambda,beta,f) % function that calculates and plots maximum as well as time dependent values of PFD_avg during and at the end of each partial test
    E = 0.7; % theta (PTC)
    AVL = zeros(1,t_0); % initiaiizing availability vector
    ONE = ones(1,t_0); % vector of ones
    t = (i-1)*t_0+1:1:(i)*t_0;
    for k = M:N
        Ae = exp(-E*lambda(i)^beta*(1+i*f)*(t.^beta-((i-1)*t_0).^beta)).*exp(-(1-E)*(1+i*f)*(lambda(i))^beta*t.^(beta)).*exp((1-E)*f*lambda(i)^beta*(i*(i-1)/2)*t_0);
        A = nchoosek(N,k)*Ae.^k.*(ONE-Ae).^(N-k);
        AVL = AVL + A;
        PFD = ONE - AVL;
    end
    %disp(PFD);
end

function [PFD_avg] = PFDaverage(n,t_0,t,PFD) % function used to implement PFD_avg formula in Brissaud et al. 2012 (can be used for any "koon" structure)
    tau = n*t_0;
    I = 0;
    for i = 1:length(t)
        I = I+PFD(i);
    end
    PFD_avg = I/tau; % average PFD in [0,tau]
    disp('Average');
    disp(PFD_avg);
    disp('Max');
    disp(max(PFD));
end
```

```
function multiphase_markov_new()
    hold on;
    n = 12;
    t_0 = 730;
    f = 0.1;
    lambda_0 = 5*(10^-6)*(1+f); % DU failure rate
    lambda_cte(1:n) = lambda_0; % lambda constante
    disp(lambda_cte);

    for k = 1:n
       lambda_lin(k) = lambda_0*(1+f*k); % lambda with linear increament
    end
    disp(lambda_lin);


    for k = 1:n
       lambda_rec(k) = lambda_0*(1+f)^k; % lambda with multiplicative increament
    end
    disp(lambda_rec);

    % calcula e une o gráfico de n partições para cada análise com lambdas diferentes
    t_cte = [];
    UA_cte = [];
    for k = 1:n
        [t,UA] = UAk_t(t_0,k,lambda_cte);
        t_cte = [t_cte t];
        UA_cte = [UA_cte UA];
    end

    t_lin = [];
    UA_lin = [];
    for k = 1:n
        [t,UA] = UAk_t(t_0,k,lambda_lin);
        t_lin = [t_lin t];
        UA_lin = [UA_lin UA];
    end

    t_rec = [];
    UA_rec = [];
    for k = 1:n
        [t,UA] = UAk_t(t_0,k,lambda_rec);
        t_rec = [t_rec t];
        UA_rec = [UA_rec UA];
    end

    set(gca, 'YScale', 'log'); % set log scale

    g_cte = plot(t_cte,UA_cte,'b');
    g_lin = plot(t_lin,UA_lin,'g');
    g_rec = plot(t_rec,UA_rec,'r');

    UAavg_cte = UAaverage(n,t_0,t_cte,UA_cte);
    UAavg_lin = UAaverage(n,t_0,t_lin,UA_lin);
    UAavg_rec = UAaverage(n,t_0,t_rec,UA_rec);
```

```
    x1 = 0;
    x2 = n*t_0;
    %axis([0 9000 0 4*10^-8]);
    l_cte = plot([x1, x2], [UAavg_cte, UAavg_cte],'--b');
    l_lin = plot([x1, x2], [UAavg_lin, UAavg_lin],'--g');
    l_rec = plot([x1, x2], [UAavg_rec, UAavg_rec],'--r');
    xlabel('Time(t)'),ylabel('UA(t)'),title('Time - Unavailability UA'); %legend for graph
    legend([g_cte,g_lin,g_rec,l_cte,l_lin,l_rec],'UA{pure}(t)','UA{-ATSV}(t)','UA{-MTSV}(t)','UAavg{pure}','UAavg{-ATSV}','UAavg{-MTSV}','Location','northwest');

    hold off;
end

function [t, UA] = UAk_t(t_0,k,lambda)
    PTC = 0.7; % proof test coverage
    P_0 = [1 0 0 0 0 0 0 0 0 0 0];
    B = [0; 0; 0; 0; 0; 0; 0; 0; 0; 1; 1];
    PROD = eye(11); % matrix identity
    t = (k-1)*t_0+1:1:k*t_0;
    for i = 1:(k-1)
        [Ci, Mi] = calculate_matrix(i,PTC,lambda);
        PROD = PROD*expm(t_0*Ci*Mi);
    end
    [Ci, ~] = calculate_matrix(k,PTC,lambda);
    UA = [];
    for tt = (k-1)*t_0+1:1:k*t_0
        UA = [UA P_0*PROD*expm((tt-(k-1)*t_0)*Ci)*B];
    end
    %disp(UA);
end

function [C, M] = calculate_matrix(k,PTC,lambda)
    a = lambda(k)*PTC;
    b = lambda(k)*(1-PTC);
    f1 = 1.01;
    f2 = 1.03;
    f3 = 1.05;
    C = [-(a*f1+b*f1) a*f1 b*f1 0 0 0 0 0 0 0 0;
         0 -(a*f2+b*f1) 0 b*f1 a*f2 0 0 0 0 0 0;
         0 0 -(a*f1+b*f2) a*f1 0 b*f2 0 0 0 0 0;
         0 0 0 -(a*f2+b*f2) 0 0 b*f2 a*f2 0 0 0;
         0 0 0 0 -(a*f3+b*f1) 0 0 b*f1 0 a*f3 0;
         0 0 0 0 0 -(a*f1+b*f3) a*f1 0 0 0 b*f3;
         0 0 0 0 0 0 -(a*f2+b*f3) 0 a*f2 0 b*f3;
         0 0 0 0 0 0 0 -(a*f3+b*f2) b*f2 a*f3 0;
         0 0 0 0 0 0 0 0 -(a*f3+b*f3) a*f3 b*f3;
         0 0 0 0 0 0 0 0 0 0 0;
         0 0 0 0 0 0 0 0 0 0 0];
   M = [1 0 0 0 0 0 0 0 0 0 0;
        0 1 0 0 0 0 0 0 0 0 0;
        0 0 1 0 0 0 0 0 0 0 0;
        0 0 0 1 0 0 0 0 0 0 0;
        0 0 0 0 1 0 0 0 0 0 0;
        0 0 0 0 0 1 0 0 0 0 0;
```

```
        0 0 0 0 0 0 1 0 0 0 0;
        0 0 0 0 0 0 0 1 0 0 0;
        0 0 0 0 0 0 0 0 1 0 0;
        1 0 0 0 0 0 0 0 0 0 0;
        0 0 0 0 0 0 0 0 0 0 1];


    %disp(C);
end

function [UA_avg] = UAaverage(n,t_0,t,UA) % function used to implement UA_avg
    tau = n*t_0;
    I = 0;
    for i = 1:length(t)
        I = I+UA(i);
    end
    UA_avg = I/tau; % average UA in [0,tau]
    disp('Average');
    disp(UA_avg);
    disp('Max');
    disp(max(UA));
end
```