



NTNU – Trondheim
Norwegian University of
Science and Technology

Methods for determining PFD/SIL for workover control systems with short test-intervals and imperfect testing

Metoder for å bestemme PFD/SIL for
workover kontrollsystemer med korte
testintervall og ikke-perfekte tester

**Wilmer Alberto Aguilar
Martinez**

Reliability, Availability, Maintainability and Safety (RAMS)

Submission date: June 2014

Supervisor: Mary Ann Lundteigen, IPK

Co-supervisor: Stein Hauge, SINTEF

Norwegian University of Science and Technology
Department of Production and Quality Engineering

RAMS

Reliability, Availability,
Maintainability, and Safety

Methods for determining PFD/SIL for workover control systems with short test-intervals and imperfect testing

Wilmer Alberto Aguilar Martínez

June 2014

MASTER THESIS

Norwegian University of Science and Technology
Department of Production and Quality Engineering

Supervisor : Mary Ann Lundteigen, PhD

Co-Supervisor : Stein Hauge, Senior Scientist

MASTER THESIS**Spring 2014****for stud. techn. Wilmer Alberto Aguilar Martinez*****Methods for determining PFD/SIL for workover control systems with short test-intervals and imperfect testing******(Metoder for å bestemme PFD/SIL for workover kontrollsystemer med korte testintervall og ikke-perfekte tester)***

Systems like workover (WO) control systems are used to shut down the operation safely while doing well intervention and well maintenance. Due to the role as safety barriers, it is necessary to demonstrate the SIL performance according to standards like IEC 61508 and IEC 61511. WO control systems may be out of service for longer periods, then in operation for a shorter or longer period depending on the well maintenance program. The systems are frequently tested while in operation and they are always functionally tested just prior to each operation (and must be retrieved and re-tested if operation lasts too long). Standard calculation techniques for determining SIL performance result in very low average probability of failure on demand (PFD) estimates, and it has been questioned if these results are reasonable. The PFD is reduced even further if aspects such as imperfect test are not incorporated in the calculations. Imperfect testing is related e.g. to the fact that the complete functionality of the WO blow out preventer (BOP) is not tested. It has been debated among researchers and in the industry how PFD / SIL calculations should be done for such systems in a realistic manner, but no conclusions have been made on the subject.

The main objective of this master thesis is to suggest a new or alternative approach for how to determine and evaluate the PFD/SIL for safety-critical systems with short test intervals and non-perfect testing, using the WO control system as a case study.

Questions that may be of relevance to address as part of developing the new approach are:

- What are the factors leading to high reliability, when considering design properties as well as the way of operating/maintaining the system?
- What are the principal relationships between testing intervals and system reliability? Is the relationship between test interval and average PFD valid under all circumstances?
- What has been done in the literature on the topic of reliability assessment and short test intervals / non-perfect testing?

-
- Is the average PFD a suitable reliability measure for systems with short test intervals and imperfect tests? May other reliability measures be more suitable?
 - Is the test coverage alone a sufficient parameter to compensate the effects of imperfect testing (also in the case of short test intervals)? Could new factors/parameters be introduced? How may the value of the test coverage be determined?
 - Control and safety functions in a WO control system are performed using many of the same physical components. To what extent may/should this design impact the estimation of PFD/SIL?

The candidate will suggest which questions to give priority, in agreement with the supervisors, as part of the pre-study report. The priorities will also be discussed in the thesis report.

The case study should include a description and illustration of a WO control system and its applications. The definition of equipment under control, safety and control functions, type of demands, ways of testing, and governing requirements and available data for reliability performance for a WO control system should also be included.

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

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

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

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

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

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

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

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

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

Deadline: 10 June 2014.

Two bound copies of the final report and one electronic (pdf-format) version are required according to the routines given in DAIM. Please see <http://www.ntnu.edu/ivt/master-s-thesis-regulations> regarding master thesis regulations and practical information, inclusive how to use DAIM.

Responsible supervisor:

Professor Mary Ann Lundteigen
E-mail: mary.a.lundteigen@ntnu.no
Telephone: +47 930 59 365

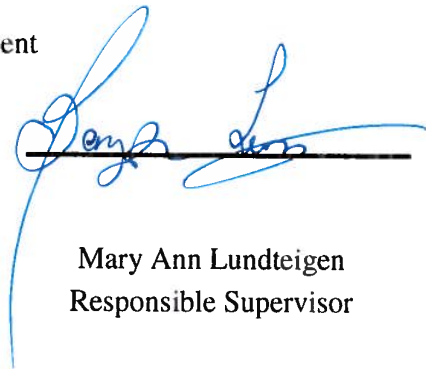
Supervisor(s) at the SINTEF:

Stein Hauge
E-mails: stein.hauge@sintef.no
Telephone: +47 930 18 395

**DEPARTMENT OF PRODUCTION
AND QUALITY ENGINEERING**


Per Schjøllberg

Associate Professor/Head of Department


Mary Ann Lundteigen
Responsible Supervisor

Preface

This is the report for the master's thesis *Methods for determining PFD/SIL for workover control systems with short test-intervals and imperfect testing*. The master's thesis has been written at the Department of Production and Quality Engineering(IPK) at the Norwegian University of Science and Technology(NTNU). The thesis is part of the two-year international master's degree programme, MSc in Reliability, Availability, Maintainability and Safety.

The master's thesis has been carried out under the supervision of Professor Mary Ann Lundteigen at the IPK Department at NTNU, and supervision of Stein Hauge, senior scientist at the Department of Safety Research at SINTEF.

The reader ought to have some knowledge on probability theory, methods for reliability assessment of safety systems, logic and algorithms. Moreover, it is highly recommended that the reader has familiarity with the standards IEC 61508, IEC 61511 and ISO 13628-7, and the PDS method.

Trondheim, 2014-06-05

Wilmer Alberto Aguilar Martínez

Acknowledgment

I would like to express my deepest thanks to Professor Mary Ann Lundteigen and Stein Hauge. The guidance I have got from them is reflected in this report.

I would also like to thank Professor Sigbjørn Sangesland at the Department of Petroleum Engineering and Applied Geophysics at NTNU, and to Pål Christensen, Principal Engineer at Statoil, for their feedback on the description, operation and maintenance of WorkOver Control Systems.

I would like to thank Yiliu Liu, Associate Professor at the Department IPK at NTNU for his feedback on Petri Net modelling and for his guidance on using the package GRIF.

Last, but not least, I would like to thank my wife Claudia for her patience and motivation.

W.A.

Executive Summary

Safety related-systems are subject to periodic proof testing, and it is often assumed that the proof test is perfect. In recent years, partial proof testing has been introduced in order to improve the system's reliability, and partial proof testing is often referred as imperfect proof testing. In this master's thesis we show that partial proof testing is different from imperfect proof testing, and, a mathematical model for modelling the effect of both partial and imperfect proof testing is proposed.

In addition to imperfect and partial proof tests, the system can also be subject to proof testing with short test intervals (intervals in the order of two or three weeks). In theory, a system that is subject to short test intervals is highly reliable, however, there are some factors like (i) human errors that are introduced during proof testing, and (ii) wear, that impact the system's reliability. We present and discuss the major contributors to the *unreliability* of a system, which is often known as the system's unavailability.

In this master's thesis we study four reliability assessment methods for estimating the probability of failure on Demand, PFD_{avg} of safety-related systems that are subject to partial and imperfect proof testing. In addition, the effects of short test intervals are also studied.

Additional factors that contribute to high reliability of a system during the system's life cycle are discussed and highlighted.

A Workover Control System functions as a safety barrier during workover and intervention operations for subsea production wells. In addition to partial and imperfect proof testing, this type of system is also subject to proof testing with short test intervals. This system is used as a case study to illustrate the use of the proposed model and to discuss the effects partial and imperfect proof testing.

Contents

Acknowledgment	v
1 Introduction	2
1.1 Limitations	5
1.2 Research Approach	5
1.3 Structure of the Report	7
2 System Description	9
2.1 Introduction	9
2.2 Completion/Workover System	9
2.2.1 Equipment Under Control	10
2.3 Workover Control System	12
2.4 WOCS Architecture	12
2.4.1 High-Pressure Unit	12
2.4.2 Master Control Panel	12
2.4.3 Remote Control Panel	13
2.4.4 Process Shutdown Panel	13
2.4.5 Emergency Shutdown Panel	13
2.4.6 Workover Control Module	13
2.4.7 Control Umbilicals	13
2.4.8 Other Equipment	14
2.5 WOCS Safety Functions	14
2.5.1 Process Shutdown Function	14
2.5.2 Emergency Shutdown Function	16

2.5.3	Emergency Quick-Disconnect Function	17
2.6	Design and Safety Requirements	18
2.6.1	General Safety Requirements	19
2.7	Operational and Testing Philosophy	19
3	Literature Review	21
3.1	Introduction	21
3.2	Proof Testing	22
3.3	Modelling of imperfect proof testing	23
3.4	The Effect of Short Test Intervals	24
4	Test Coverage Factor	26
4.1	Introduction	26
4.2	Definition and Use of the Test Coverage Factors	26
4.3	Failure Modes and Effects Analysis	28
4.4	Method for Estimating the Test Coverage Factors	28
4.4.1	Procedure(Summary)	30
4.4.2	Impact of the Test Coverage Factor to System's Reliability	32
5	Methods for the Reliability Assessment	33
5.1	Introduction	33
5.2	Reliability Block Diagrams	33
5.3	Average Unavailability of the WOCS	35
5.3.1	Background	35
5.3.2	Solution	37
5.4	Fault Tree Analysis	38
5.4.1	PDF _{avg} Calculations	38
5.4.2	Analytical Formulae Approach	39
5.4.3	Boolean Models	40
5.5	Petri Nets	42
5.5.1	Petri Nets driven by Virtual RBDs	43
5.5.2	Proof Testing Policies with Petri Nets	44

5.5.3	Perfect Full Proof Test without Partial Proof Tests	44
5.6	Method Comparison	49
5.6.1	Models Relationship	50
5.6.2	Analysis	50
6	Failure Modes and Reliability Data Analysis	52
6.1	Introduction	52
6.2	Failure Modes	52
6.2.1	Fail to Operate - Valves	52
6.2.2	Fail to Operate - Shear Seal RAM	53
6.2.3	Leakage	54
6.2.4	Electronic and Electrical Failures	54
6.3	Effects of Proof Testing	54
6.3.1	Reveal-Ability	55
6.4	Reliability Data Analysis	55
7	Reliability Calculation of the WOCS	57
7.1	Introduction	57
7.2	Method	57
7.2.1	Step 1. To Understand the System's Functionality	57
7.2.2	Step 2. To Develop a FTA > Draw a RBD	58
7.2.3	Step 3. To Develop a FMEA	58
7.2.4	Step 4. To Estimate the TCFs	58
7.2.5	To Compute the PFD_{avg}	58
7.3	Comments and Discussion	61
8	The Total Unavailability Function and the Optimization Problem	63
8.1	Introduction	63
8.2	Background	63
8.3	The Analytical Function and the Optimization Problem	64
8.3.1	Average unavailability between test intervals	65
8.3.2	Average Unavailability due to testing time	65

<i>CONTENTS</i>	xi
8.3.3 Average unavailability due to human errors	66
8.3.4 Unavailability due to on-demand failures at the beginning of the test	66
8.3.5 Unavailability due to failures during testing	66
8.4 The Analytical Function for the Total Unavailability	67
9 Summary, Conclusions and Further Work	70
9.1 Summary and Conclusions	70
9.2 Further Work	73
Bibliography	74
A Equipment Controlled by the WOCS	79
B Example of an FMEA Worksheet	82
C MATLAB Code	84
D Reduced Petri Net	88
E Calculation of TCF and TCF_{max}	92
F Commands in MATLAB for Computing the PFD_{avg}	94
G Calculation of PFD_{avg} by using the Formulae Approach	97
H Pre-Study Report	99

List of Figures

2.1	Boundary of the Equipment Under Control	11
2.2	Layout of a WOCS and controlled modules by the WOCS	15
2.3	Reliability Block Diagram for the PSD safety function of the WOCS	16
2.4	Reliability Block Diagram for the ESD safety function of the WOCS	17
3.1	Classification of a Proof Test. Adapted from (Rausand,2014)	23
4.1	(a)Reliability block diagram of failure rate that are revealed and non-revealed by proof tests. (b) Illustration of the Test Coverage Factor	27
5.1	Unavailability function $U_k(t)$ a single component that is subject to partial and full proof tests. (a) $U_k(t)$ when $TCF_{max} = 1$ (b) $U_k(t)$ when $TCF_{max} < 1$	35
5.2	Operational and Testing Philosophy. (a) Operational scheme for the WOCS. (b) WOCS unavailability function including partial proof tests and imperfect full proof tests.	36
5.3	Flow diagram for computing the average unavailability of a single component subject to partial and full proof test	37
5.4	Example of a Fault Tree	38
5.5	RBD of a structure of two components connected in parallel where each component is modelled by a series of two "subcomponents" with failure rate revealed at τ_p and τ respectively	40
5.6	Average unavailability calculation (Example)	41
5.7	Example of a simple Petri Net showing the main graphical elements	42
5.8	Example of a simple Petri Net Driven by a Virtual RBD	43

5.9	Petri Net for modelling Periodic perfect full proof test	44
5.10	Petri Net for modelling Periodic perfect full proof test and $m - 1$ partial proof tests in the test interval of full proof tests	46
5.11	Petri Net for modelling hidden failures that are never revealed	48
5.12	Petri Nets to be used in Petri Nets driven by RBD	49
7.1	Saw curve (unavailability function) for the ESD function of the WOCS	60
8.1	The unavailability function when considering all major contributors	68
8.2	Optimal test frequency of proof test by minimizing the unavailability function and the cost function	69
D.1	Petri Net for modelling Periodic perfect full proof tests and $m - 1$ partial proof tests in the test interval of full proof tests. (Reduced Model)	90
D.2	Example of Petri Net driven by RBD	91

List of Tables

2.1	Typical modes of operation of C/WO riser systems. Adapted from (ISO13628, 2005b)	10
4.1	Summary of the required information for estimating the TCF_{FM_i}	29
4.2	Matrix for determining the TCF_{FM_i} per failure mode	30
4.3	Failure modes and failure rates for the SS-RAM	31
4.4	Failure modes and failure rates of the Shear Seal RAM	32
7.1	Summary of the Test Coverage Factors TCF and TCF_{max} , and failure rates for the components used for fulfilment of the WOCS's safety functions	59
7.2	Results to the PFD_{avg}	60
A.1	Typical modules controlled by the WOCS. Adapted from (ISO13628, 2005b)	79
B.1	FMEA Worksheet)	83

Chapter 1

Introduction

Safety related systems are systems that carry out safety functions in order to prevent hazardous events. These type of systems normally operate in one of the following modes: (i)low demand mode, (ii)high demand mode, and (iii)continuous mode. Each mode is characterized for the frequency of demand (see for example, part 4 IEC61508, 2010).

Given that a safety-related system carries out safety functions that are only required during a hazardous event, the system has to be tested periodically in order to reveal hidden failures that may be introduced while the safety functions are passive. A system operating in low demand mode is often tested with an average frequency of one year. However, there are some safety systems that are tested with very short intervals (for example, less than one month).

In most cases, it is assumed that a proof test is perfect, meaning that all hidden failures are revealed. This assumption is seldom realistic, since a proof test differs from a real demand and some functions may be impossible to test due to potential damage or wear out of the final elements. In this case, the proof test is imperfect. In addition, the proof tests may be performed partially, meaning that just a fraction of the testable capabilities of the system are tested. The limitations of the partial proof tests may prevent us from revealing all possible hidden failures.

Imperfect proof testing differs from partial proof testing in the sense that a partial proof test is intentionally partial, whereas the degree of imperfection of a proof test is an inherent characteristic of the test itself. Therefore, we refer to imperfect proof tests as full proof tests that by nature are imperfect; on the other hand, we refer to partial proof tests as tests with the intention to reveal only a predefined fraction of hidden failures.

In addition to short test intervals, we can see that a system may be subject to partial and imperfect proof tests.

A WorkOver Control System(WOCS) is a safety-related system operating in low demand mode that is used to control equipment during intervention of subsea wells, and to function as a safety barrier to prevent hazardous events(e.g., release of hydrocarbons) during WorkOver(WO) operations. Due to the requirements for the WOCS to function as a safety barrier, it is necessary to demonstrate that this system meets the specified safety requirements in order to obtain the required risk reduction. On the Norwegian continental shelf it has been determined to carry out proof tests to this system every 14 days (a short test interval). In addition, the WOCS has components that are subject to imperfect proof test (e.g., a Shear Seal RAM).

From the literature review we conclude that few mathematical models have been developed to consider the effect of short tests intervals to the system's reliability. The reader may (mainly) find brief discussions of the effects of too frequent proof tests (see e.g., Voronov and Alzbutas, 2009; NEA/CSNI/R, 2002; Chowhury and Varde, 2011).

Limited literature is available on the topic of how to model the effects of partial and imperfect proof tests. The effects of non-perfect (imperfect) proof tests are briefly discussed by the standard IEC61508-6¹ and the concept of proof test coverage is introduced for modelling this issue. The practice of *partial stroke testing* of shutdown valves(as cite in Lundteigen and Rausand, 2008) has led to the concept of partial proof testing, and it is often referred as an imperfect proof testing (see e.g., Hauge et al., 2013).

Two main approaches are available for modelling the effects of partial *or* imperfect proof tests: (i) using the proof test coverage factor to split the failure rate into failure rate tested only by perfect proof tests and failure rate tested by partial proof test and also by perfect proof tests. (see e.g., Jin and Rausand, 2014; Brissaud et al., 2012; Oliveira, 2009; Hauge et al., 2013), and (ii) adding a constant contribution in order to compensate failures that are not revealed by a proof test (Hauge et al., 2013). In both cases, a perfect proof test takes place at some point in time.

In this master's thesis we propose a mathematical model for modelling the effect of partial and imperfect proof tests to system's reliability. The proof test coverage factor is essential for modelling the effects of partial and imperfect proof testing. The reader may find a detailed ap-

¹The reader is referenced to section B.3.2.5, IEC61508-6

proach developed by (Lundteigen and Rausand, 2008) for estimating the test coverage factor for partial proof tests of shutdown valves. We extend and simplify this approach for estimating the coverage factor for modelling partial proof tests of any component. The procedure for estimating the coverage factor is based on the use of the Failure, Modes, and Effects Analysis(FMEA).

We introduce the concept of maximum test coverage factor for modelling the effect of imperfect proof tests. With two coverage factors, we propose a model for calculating the time-dependent availability of components that are subject to partial and imperfect proof tests. This model is used for computing the PFD_{avg} of a system by applying standard methods for reliability analysis: (i)The structure function of reliability block diagrams, (ii)Formulae derived from Fault Tree Analysis, (iii) A Boolean approach by using Fault Trees. In addition, Petri Net models for modelling the effect of partial and imperfect proof tests are presented.

When considering the effect of short test intervals to system's reliability, the mathematical models should be different from those ones that are derived under the assumption that the failure rate is constant, mainly because too frequent proof testing leads to wear and therefore increased probability of failure. Mathematical expressions derived under the assumption that the failure rate is Weibull-distributed (e.g., λ increases over time, $\alpha > 1$) seems to be a more proper approach. Nonetheless, we assume that the failure rate remains constant over the lifetime of the system, but the proof test interval needs to have the proper length (optimum test interval) in such way that risk reducing criteria is still met. This optimum test interval can be found by optimizing the analytical unavailability function that depends on the test interval τ . It is possible only if the major contributors to the safety unavailability are quantified.

Along with the development of the new approaches, we also discuss (i)the factors that leads to high reliability, when considering design properties as well as the way of operating and maintaining a safety related system, (ii)the main relationship between test intervals and system reliability, and (iii) how safety functions and control functions affects the safety integrity level of safety-related systems

1.1 Limitations

The study under consideration is limited to the regulations and recommendations for safety-related systems used on the Norwegian continental shelf. For example, NORSOK-D010 (2013) recommends rigorous requirements with respect to test frequency of subsea equipment.

The optimum test interval found by optimizing the analytical unavailability function can be used for estimating the minimum related cost due to maintenance activities. However, cost analysis is beyond the scope of this master's thesis. We briefly discuss this issue by presenting the cost function and the use of the optimum test interval.

Modelling the effect of Common Cause Failures (CCFs) to the PFD_{avg} is not covered. However, CCFs are easily included by using the standard beta factor model, or the modified beta factor approach proposed in the PDS method (see e.g., Hauge et al., 2013).

Reliability data and exhaustive analysis of the failure modes of the components involved for the development of the system functions of the WOCS are essential for calculations of the PFD_{avg} . We assume that the reliability data is exponentially distributed, that the failure rates of the different failure modes of a component are independent, and when we do not find reliability data due to limited information available in the databases (OREDA, 2009b,a; Hauge and Onshus, 2013), we assume some values for failure rates.

1.2 Research Approach

In order to succeed in the development of this master's thesis, the following factors were considered:

Planning

During the first three weeks of this project, we worked on the understanding of the stated problem and how it was going to be treated. This was outlined in the pre-study report attached in Appendix H. That document served as a management tool towards controlling the development of this project.

Supervision

The supervision scheme was established early at the beginning of this project. In agreement with the supervisors, a meeting every week was planned. Every meeting was arranged to take place in a studio room, and for controlling the progress of the development of the master's thesis, meeting minutes were documented.

Overall Approach

Understanding the functionality and configuration of a WOCS represented one of the first steps in this project. For this purpose the part 7 of the standard ISO13628 (2005b) was carefully reviewed. In addition, the knowledge about this system was complemented with information available at SINTEF.

Feedback from people with experience in the configuration, operation and maintenance of WOCS was crucial for the understanding of the problem. We discussed this topic with the professor responsible for the course *Subsea Production Systems* at Petroleum Department at NTNU. In addition, this topic was also discussed with an engineer responsible for the operation of subsea wells who works for Statoil. It allowed us to become more confident to work in the solution of the problem.

For the analysis of the proper methods for the reliability analysis of the WOCS, the technical report ISO/TR-12489 (2013) was thoroughly reviewed. The standards IEC61508 (2010); IEC61511 (2003) were also examined.

In order to know the state of art on modelling the effect of partial and imperfect proof testing, and the effects of short test intervals to system's reliability, relevant scientific articles were reviewed. Some articles have been published by the Journal of Risk and Reliability, the International Journal of Reliability, the Journal Quality and Safety Engineering, the Journal of Reliability and Safety System and the Journal of Loss Prevention in the Process Industries. The PDS method was also of importance for understanding the proper use of the parameters for modelling imperfect proof testing.

Software

The use of software like MATLAB, GRIF and Microsoft Excel were used for calculations. MATLAB was used for coding the algorithm that computes and draws the time dependent availability of the safety functions carried out by the WOCS; GRIF was used for simulating the Petri Net models proposed in this project, and some calculations and plots were developed by using Microsoft Excel.

This report was written by using Latex.

1.3 Structure of the Report

In the following paragraphs a short description of the chapters of this report is provided.

In chapter 1, we described the context for the problem and the importance of it. We highlighted the main aspects to the stated problem that have been studied by other people and the main activities, and the purpose of this study were introduced. By providing a clear picture of the problem, the readers find this problem of interest.

In chapter 2, the WOCS is described; it includes the major components, the safety functions, and operational modes. In addition, the design and safety requirements are presented. The description of the system is essential for the application of the methods for its reliability assessment.

In chapter 3, findings from the literature review of the work done for modelling the effect of partial and imperfect proof testing, and the effect of short test intervals are documented. These three factors are very relevant this master's thesis, therefore, by knowing the state of the art of modelling these factors, we make sure that the gaps regarding to the stated problem are clearly defined and rework is prevented.

In chapter 4, the test coverage factor is explained and a method for estimating the TCF and TCF_{\max} is proposed. The coverage factors are the main parameters for modelling the effect of partial and imperfect proof tests.

In chapter 5, four methods for computing the PFD_{avg} are detailed and compared. Different alternatives are chosen in order to make sure that different approaches can be applied, and to demonstrate that the results are similar.

In chapter 6, the main failure modes that may affect a WOCS are discussed. In addition, we briefly comment on the reliability data available. The FMEA is the cornerstone for estimating an accurate test coverage factor, therefore, we explain the main failure modes of the WCOS in order to exemplify its importance and understanding.

In chapter 7, we present the results for the reliability assessment of the WOCS. A method for reliability assessment is proposed. The method is provided as a guide of the application of the proposed approaches.

In chapter 8, the major contributors to the unavailability of a safety system are presented in order to derive a total unavailability function. This function is used for finding the optimum test interval τ by satisfying the risk reducing criteria.

Finally, in chapter 9, the results of this project are summarized and briefly discussed. The main conclusions are stated and key points for further work are highlighted.

Chapter 2

System Description

2.1 Introduction

Well intervention in subsea production wells is carried out for several reasons varying from production recovery of hydrocarbons to well integrity. Well intervention activities are critical and therefore requires equipment that ensures safe, reliable and efficient operations. In this chapter, we present a short description of the equipment for workover operations¹. A short description of Completion/Workover (C/WO) riser systems is presented. A more detailed description of Workover Control System (WOCS) is included. The description of WOCS includes: main functions, design and safety requirements, major components, and operational and testing philosophy. This chapter is mainly based on the part 7 of the standard ISO13628 (2005b).

2.2 Completion/Workover System

A Completion/Workover (C/WO) riser is the main system used to re-enter the well through the subsea tree and run subsea equipment (e.g., a new down hole safety valve) into a wellbore. The C/WO riser system has typically two operations modes: Tubing hanger mode(through marine riser) and tree mode(through open sea). The typical operation modes of the C/WO riser systems that can be carried out with the two types of intervention equipment used, are summarized in table 2.1. Well completion is to finalise the construction of the well, well intervention-open

¹"workover operations" is a term used to describe operations on a completed production well.

Table 2.1: Typical modes of operation of C/WO riser systems. Adapted from (ISO13628, 2005b)

Typical Operation	Tubing Hanger Mode	Tree Mode
Well Completion	V & H. X-mas tree	V. X-mas tree
Well intervention - open Sea	NA	V & H. X-mas tree
Well intervention - inside drilling riser	V & H. X-mas tree	NA
Full workover	V & H. X-mas tree	V. X-mas tree

Note: V stands for Vertical and H stands for Horizontal

sea is the running of the open water workover system, and well intervention -inside drilling riser is the landing string which is used to run the tubing hanger inside the marine riser. The Full Workover is to retrieve the tubing hanger and the upper tubing part (cut or sheared out). The main modules controlled by the WOCS and the typical general arrangement of the main components of the C/WO riser for the two operational modes are presented in appendix A.

2.2.1 Equipment Under Control

IEC61508-4 defines the Equipment Under Control (EUC) as any apparatus used for process where risk may arise from this equipment (EUC risk). The Norwegian guidelines NOG-070 (2004) complements the definition of EUC by adding that the EUC is used for diverse operations and it is a source of hazards. C/WO riser systems are source of hazards during all operations on a subsea production well; release of hydrocarbons to the environment and blowouts are examples of undesired events during workover operations. The EUC are all the equipment that contains flow lines (e.g., the production line) *and* responds to output signals from the WOCS for preventing the release of hazardous events (e.g., release of hydrocarbons to the environment). The major equipment that are under control of the WOCS are the X-mas tree, the Lower Riser Package(LRP), and the Surface Flow Tree(SFT) on the rig. The red dashed line in figure (2.1) shows the boundary of the EUC. An important point about the EUC boundary is:

The important point will be that the EUC boundaries are clearly defined and in a manner such that all the relevant hazards to be considered in later lifecycle stages can be identified and described.

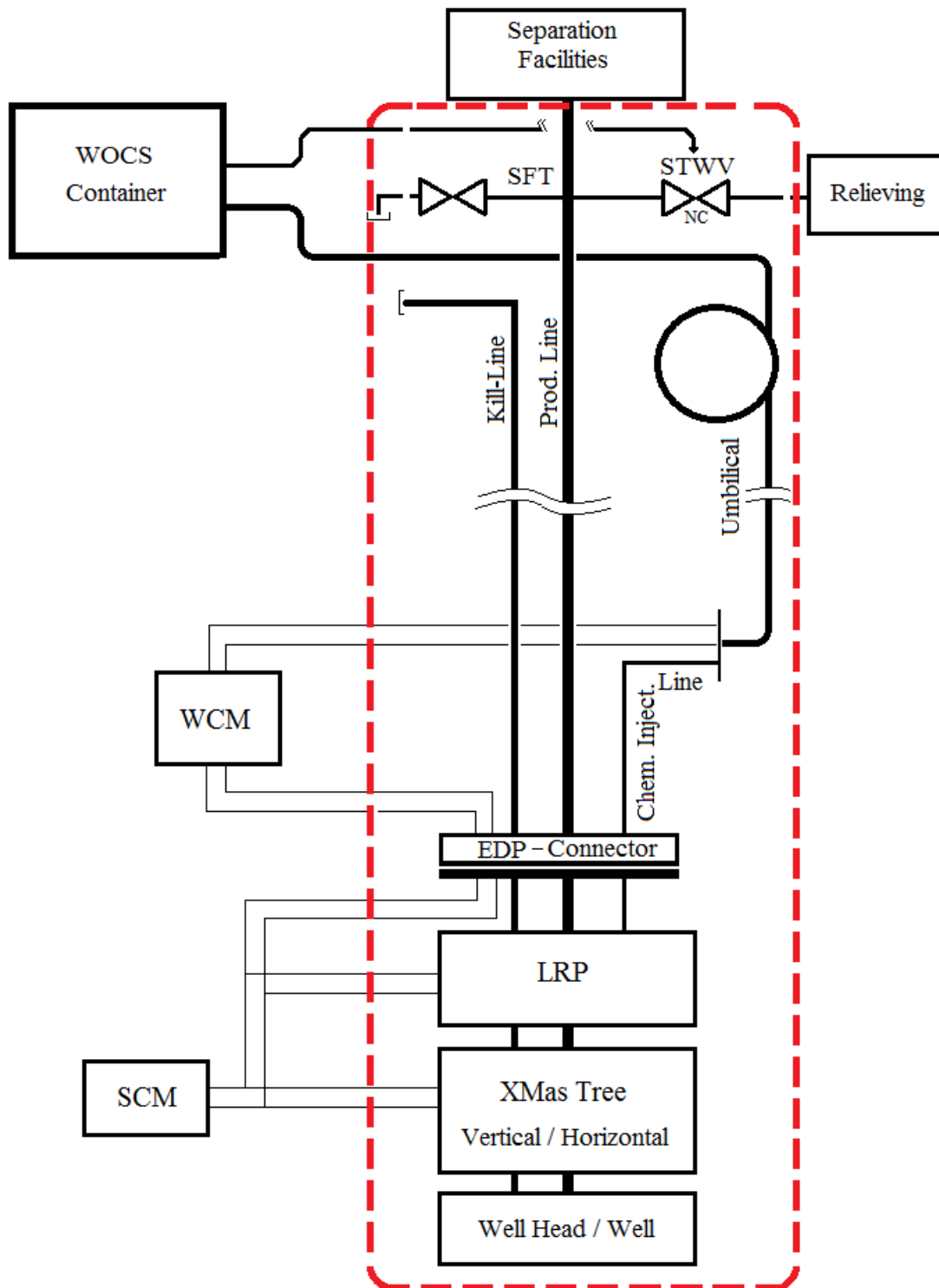


Figure 2.1: Boundary of the Equipment Under Control

2.3 Workover Control System

A workover control system (WOCS) is a system designed to provide the means to remotely control and monitor *all* functions on the (C/WO) riser system. The functions are split into WO operation functions and safety functions. These functions are mainly hydraulic, electric, control functions, and data acquisition functions. Most actuating elements of a WOCS are hydraulically operated and parameters like pressure and temperature need to be monitored.

WO operations functions include remote control and monitoring of installation, retrieval, testing of subsea equipment (e.g., subsea trees, tubing hangers, etc.) and initial well completion operations and subsequent well workover during the life of the well.

In order to provide a clearer picture of the safety functions that are carried out by a WOCS, we first present the major components of a WOCS. Safety functions of WOCS are described in section *WOCS Safety Functions*.

2.4 WOCS Architecture

The WOCS consists of seven main assemblies plus several miscellaneous and supplemental assemblies. These main assemblies comprises a high-pressure unit(HPU), a master control panel(MCP), a remote control panel(RCP), a process shutdown(PSD) panel, an emergency shutdown(ESD) panel, a workover control module(WCM) and control umbilicals.

2.4.1 High-Pressure Unit

The HPU includes pumps, pressure accumulators, supply and return pipes, flushing, filtering facilities, supply and control/alarm panel, amongst other elements. The HPU shall be capable to supply hydraulic power to operate all hydraulically actuated elements in the C/WO riser system, X-mas tree and the DHSV within the required response times and capacities.

2.4.2 Master Control Panel

The MCP is designed to distribute and supply pressurized hydraulic oil from the HPU. The MCP shall include a mimic type display featuring the layout of the system and equipment to be oper-

ated.

2.4.3 Remote Control Panel

The RCP is a control panel based on workstations that are designed to operate PSD, ESD and emergency quick disconnect (EQD) functions together with other process functions. The RCP shall be electrically connected to the MCP. The RCP shall operate as a slave to the MCP.

2.4.4 Process Shutdown Panel

The PSD panel is designed to initiate a process shutdown (e.g., the PSD safety function). The PSD panel shall be electrically connected either to the MCP or to the RCP or to both control panels.

2.4.5 Emergency Shutdown Panel

The ESD panel is designed to operate PSD, ESD and EQD functions. The ESD panel shall be electrically connected either to the MCP or to the RCP or to both control panels.

2.4.6 Workover Control Module

The WCM is designed to operate the Lower Riser Package (LRP) in tree mode operation. The WCM shall have capabilities for controlling the X-mas tree and downhole functions. The WCM shall be capable of providing feedback to topside system (WOCS on the rig) in order to verify correct operation. The WCM contains the solenoid valves that allow the flow of hydraulic oil for closing or opening the valves in the LRP. It also contains the high pressurized accumulators of hydraulic oil to ensure that the valves close within the required time (e.g., 30 sec).

2.4.7 Control Umbilicals

Umbilical hoses are used to transmit the necessary control and monitoring functions from the surface controls to the subsea functions. Signal to be transmitted may be both hydraulic and electrical.

2.4.8 Other Equipment

Lower Riser Package

The LRP contains the valves for isolating the well (e.g., the Production Isolation Valve, PIV; the Shear Seal RAM, SS-RAM), the valves for chemical injection (e.g., Inner and Outer chemical injection valves, ICIV/OCIV), the valves for isolation of the annulus line (e.g., UAIV), and the crossover valves, IXOV/OXOV, that connect the production line and the annulus for recirculating hydrocarbons. The LRP acts as a small Blow Out Preventer.

Emergency Disconnect Package-Connector

The EDP-Connector (see figure (2.2)) contains the valves that should close to prevent release of hydrocarbon to the sea in case that the EQD function is carried out. For example, the Riser Retainer Valve (RRV) isolates the production line and the Riser Annulus Isolation Valve isolates the annulus line.

Figure 2.2 shows a layout of the WOCS and the modules controlled by the WOCS.

2.5 WOCS Safety Functions

There are three types of safety functions that are carried out for a WOCS. These functions include ESD, PSD and (EQD) of the marine riser. The EQD function has the highest priority, followed by the ESD function, and PSD function with the lowest priority.

2.5.1 Process Shutdown Function

The PSD function operates the normally closed Surface Tree Wing Valve (STWV) on the SFT. The PSD function is activated manually in case of an uncontrolled event on the rig. By opening this valve, over-pressure in the production line is released safely. See figure 2.2.

Upon activation of 1oon ($n \geq 1$) PSD push-buttons, the WOCS's PLC (installed in the MCP) reads the change of state of the push-button and sends a signal to the *pulse operated hydraulic* valve that operates the STWV. When the *pulse operated valve* switches, the hydraulic pressure in the actuator of the STWV is bled off leading the SPWV to the opened position. The PSD function

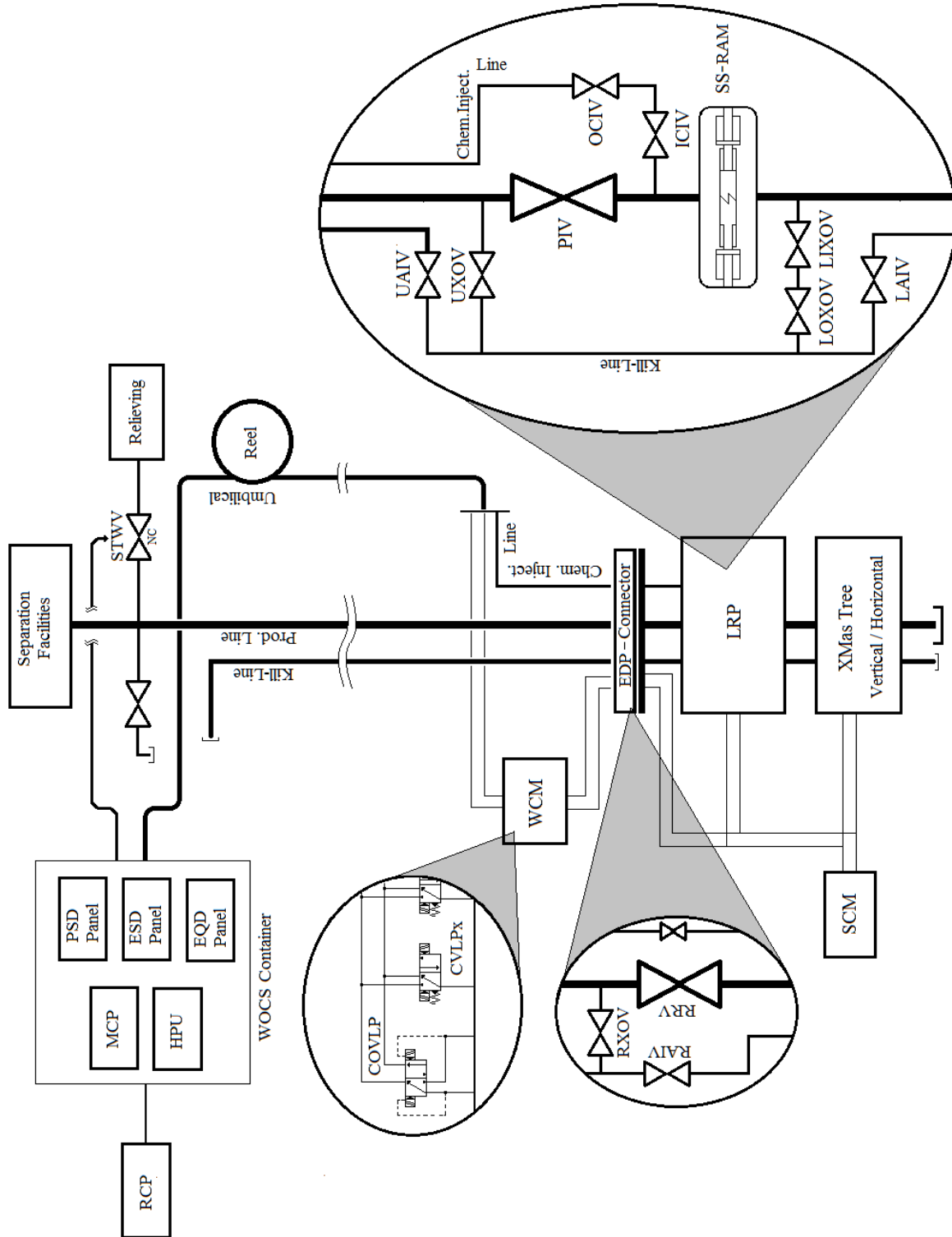


Figure 2.2: Layout of a WOCs and controlled modules by the WOCs

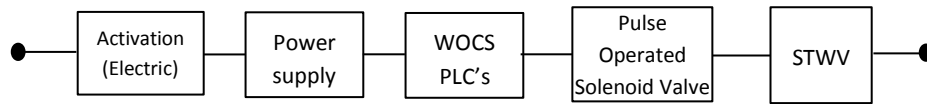


Figure 2.3: Reliability Block Diagram for the PSD safety function of the WOCS

is automatically activated when a platform (production) ESD is initiated. Figure 2.3 shows a simplified reliability block diagram for the PSD safety function.

2.5.2 Emergency Shutdown Function

An ESD consist of a sequential activation of all relevant components (e.g., LRP's valves) in order to isolate the well. The barrier element closing sequence considers the presence of coiled tubing and wireline and whether cutting results in falling or raising of the coiled tubing and wireline. Successful ESD is obtained by preventing flow either through the production line, the annulus line or the chemical injection line in the LRP (see figure 2.2) or by closing the DHSV. Two modes for the ESD function are described: (i) Normal mode which means that the production line is not obstructed with running tools. (ii) Coiled tubing mode which means that equipment is being run into the wellbore.

ESD in Normal Mode

The flow through the production line, the annulus line and the chemical injection line is sufficiently prevented if:

- 1 The valves PIV, 1oo2 CIV, 1oo2 AIV, and the UXOV or 1oo2 LXOV closes sufficiently, or
- 2 The valves SS-RAM, 1oo2 AIV, and the UXOV or 1oo2 LXOV closes sufficiently, or
- 3 The DHSV closes sufficiently.

ESD in Coiled Tubing Mode

The flow through the production line, the annulus line and the chemical injection line is sufficiently prevented if:

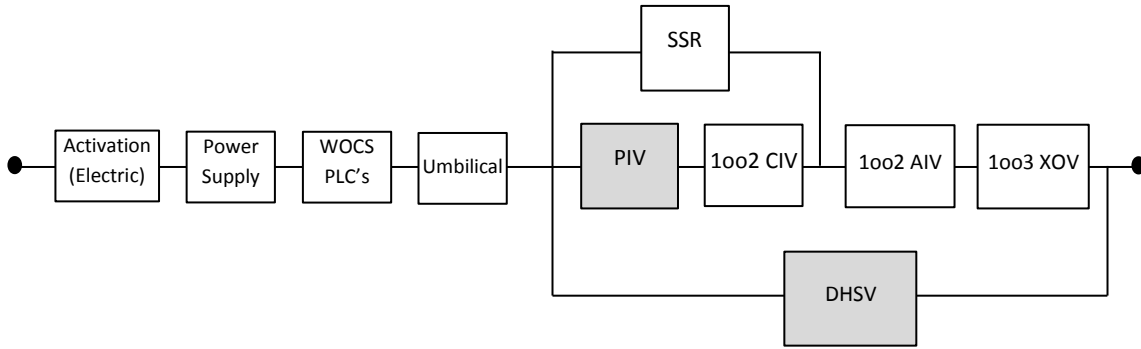


Figure 2.4: Reliability Block Diagram for the ESD safety function of the WOCS

- 1 The valves SS-RAM, 1002 AIV, and the UXOV or 1002 LXOV closes sufficiently.

The PIV and the DHSV are not part of the ESD function in coiled tubing mode given that these valves do not have cutting capabilities.

NOTE. A valve closes sufficiently if it closes and prevents unintended flow through the line within a required time.

Figure 2.4 shows a simplified reliability block diagram of the ESD function for both normal mode and coiled tubing mode. The shadowed area highlights the components that are not part of the ESD function on coiled tubing mode.

Similarly to the PSD function and EQD function, the ESD function is activated upon activation of 100n pushbuttons on the SFT.

2.5.3 Emergency Quick-Disconnect Function

The EDP-Connector shall include the necessary functionality to allow disconnection of the WO/C riser from the LRP, leaving the well in a safe state with the LRP's valves closed, in the event of an emergency situation. The EQD function shall also close the DHSV at defined delay enabling time for possible removing of intervention equipment that can prevent or damage the DHSV. The EQD function is normally initiated by pressing one of n available electrical pushbuttons (e.g., 100n) on the rig. Initiating an EQD automatically activates the ESD function, closes the RRV and RAIV valves and disconnects the marine riser from the LRP.

The RBD comprises the same elements of the ESD function, with exception of the activation part, because the EQD function has its own activation(electric) subsystem. In addition to those

elements, the EQD functions is satisfactorily executed if the valves RRV and RAIV in the EDP-Connector are sufficiently closed. It means that the RBD for the EQD has two additional blocks in series in the RBD of the ESD.

2.6 Design and Safety Requirements

The standard ISO13628 provides general requirements, recommendations and overall guidance for development of subsea production systems. ISO13628-7 gives requirements and recommendations for the design, analysis, materials, fabrication, testing and operation of C/WO riser systems, including WOCSs. A WOCS shall be designed, manufactured and tested in accordance with²

- Functional requirements: Clause 5 of ISO13528-7.
- Design requirements: Clause 5 of the part 6 of ISO13628. The part 6 of the standard provides the design requirements for subsea production control systems.
- System integration test: Clause 8 of ISO13238-7.

As a safety-related system, the WOCS shall follow the recommendations provided in the standard IEC61508 in order to meet *a specified* reliability and safety performance³. This performance is often measured as the probability that system satisfactorily perform the specified safety functions under all the stated conditions within a stated period of time. This probability is known as the safety integrity of a system. (see section 3.5.4, part 4 IEC61508, 2010).

On the Norwegian continental shelf there are no regulatory requirements for the safety integrity for WOCSs. However, some companies have adapted the recommendations for Blow Out prevents (BOP) given in the guideline NOG-070, application of the standards IEC61508 and IEC61511 in the Norwegian petroleum industry. For example, the Statoil governing document TR0034: Subsea X-mas Tree and Completion/Workover Riser Systems states that a WOCS shall meet the safety integrity level SIL 2 as given for BOPs in the guideline NOG-070.

²Those items are extracted of table 2, ISO13628-7.

³The specified performance is defined by the user

The Norsok standard D-010, Well integrity in drilling and well operations does not specify any requirements concerning to safety integrity of WO systems, however, it recommends proof testing every 14 days for well control equipment (e.g., LRP for well intervention) (See e.g., Table 42 Norsok-D010, 2013).

This requirement of short test intervals impacts the reliability measure of the WOCS. This issue is discussed later in this document. In addition, general considerations concerning to reliability during the life cycle of the system are also highlighted.

2.6.1 General Safety Requirements

The WOCS is designed to ensure that no single failure will cause an unacceptable risk to personnel safety, the environment and to loss of financial assets. A single point failure (e.g., There is no redundancy) in the *control system* shall not cause a total system shutdown or prevent the ability to secure the well, or prevent the execution of the ESD/EQD functions.

The WOCS is designed to perform the emergency shutdown within an acceptable response time based on a total assessment of the possible emergency situations and the consequences of such situations. The workover control system is designed so that emergency disconnection can be carried out within a time interval determined in relation to the development of unforeseen situations on the workover vessel after the barriers against blowout have been established. TR0034 provides response time requirements for the ESD and EQD functions (e.g., 30 seconds in average).

In the case of an unplanned disconnection, all fail-safe functions shall automatically go to a safe position (e.g., all valves in the LRP and EDP-Connector shall go to the closed position). Following disconnections, the system shall be designed to minimize ingress of ambient fluids (i.e. seawater) into the hydraulic control circuits of the disconnected modules (i.e. EDP-connector, LRP, subsea test tree, etc.).

2.7 Operational and Testing Philosophy

A WO operation is an activity for well intervention that usually does not last more than two or three weeks and it depends on the demand of this type of activities in the offshore industry. A

WOCS can be onshore for a couple of months before the WO Operation starts. Before the WO operation, the WOCS is tested onshore, on the rig and when it is connected to the X-mas tree. The test include functional testing and pressure integrity testing of all valves(see e.g., clause 11, part 6 ISO13628, 2005a) .

During a WO operation, most of the valves in the LRP are operated due to operational requirements (e.g., recirculation, chemical injection). Some operators carry out a functional test of valves (e.g., close and open) without pressure integrity testing every seven days. This is not a requirement on the standards or governing documents for WO operations and it may be part of internal policies of some operators. Nonetheless, there exist a requirement to perform pressure integrity testing of all valves in subsea equipment (e.g., LRP, EDP-Connector, X-mas tree, DHSV) every 14 days (see e.g., Annex A. NORSOK-D010, 2013). It includes the testing of the functionality of all components in the chain for fulfilling the safety functions (e.g., pushbuttons, PLC's, HPU, and so on).

After a WO operation, the WOCS is taken to onshore and a maintenance is carried out. It includes, amongst other activities, exhaustive inspections of all components, change of packing or sealing devices, functional testing and pressure integrity.

The cutting capabilities of the SS-RAM in the LRP is never tested. This destructive testing is carried out only for the prototype prior to the production of this component, and it is assumed that all produced components are an exact "copy" of the SS-RAM that complies with the design and manufacturing requirements.

The reader may notice that a WOCS has strict maintenance and testing requirements. The effects of this issues to the reliability of the WOCS are discussed in further paragraphs.

Chapter 3

Literature Review

3.1 Introduction

Proof testing has a crucial bearing on the achievement of the hardware safety integrity of safety-related systems. Therefore, the proof testing policy adapted to the WOCS is an important aspect that requires attention in order to understand the effects on the reliability of this system. For instance, it is commonly accepted that frequent proof tests increase the reliability of any systems, however, there are some factors like wear-out and human errors that have a significant impact in the reliability measure. For example, the reliability assessment of a WOCS should consider the effect of short test intervals (requirement of NORSOK-D010 (2013)) to the reliability measure.

In this chapter we present the state of art of modelling the effects of proof tests to the unavailability of safety systems. The effects of (i) different types of proof tests (e.g., perfect proof tests, imperfect and partial proof tests), and (ii) short test intervals, to system's reliability are covered in further detail in this chapter.

In order to gain a comprehensive range of knowledge about the main topics to be covered in this chapter, some keywords were selected to find the relevant literature on this matter: Logic combinations of words like *proof tests*, *testing*, *unavailability*, *failure on demand*, *over-testing*, *short testing*, *less testing*, *reliability*, *hidden*, and *revealed* were used.

3.2 Proof Testing

A proof test is a periodic test performed to reveal hidden failures, and to restore or to retain the safety-related system to *as-good-as-new* condition. Rausand (2014) introduces a classification and definition of proof tests of different types.(see also (Aguilar M., 2013)). A proof test may be full or partial. Both full and partial may be perfect or imperfect. See figure 3.1.

In practice, a proof test is imperfect (Jin et al., 2011) and few approaches are used to model the effects of the degree of imperfection of proof tests. A proof test is imperfect mainly because the test conditions deviate from demand conditions and because the proof test is not able to detect all hidden failures.

A partial proof test is a planned test to reveal a fraction¹ the hidden failures. Partial proof test is becoming a widely accepted technique for reducing the PFD_{avg} of safety-related systems (Lundteigen and Rausand, 2007, 2008).

Rausand (2014) and Aguilar M. (2013) present and discuss (respectively) some mathematical models for PFD_{avg} calculations considering the effect of imperfect/partial proof tests of safety instrumented systems.

Partial proof test may be claimed to be the same as imperfect proof test given that a fraction of hidden failures are not revealed after a proof test. Concerning partial proof tests, it is decided to reveal a fraction of hidden failures(hence, it is called *partial*); on the other hand, for imperfect proof tests, the fraction of failures that are not revealed is due to the nature of the test itself. It is clear that the fraction of hidden failures that may be revealed during an imperfect (full) proof test is closed to 100%, whereas, the fraction of hidden failures that may be revealed during a partial proof tests is scarcely bigger than 90%.(ACM, 2001; Oliveira, 2009). Under the assumption that there exist a perfect (full) proof test at some point in time, the mathematical model for PFD_{avg} calculations is the same when modelling the effects of imperfect (full) proof tests or partial proof tests.

¹This fraction is often estimated based on the knowledge of the system, procedures, etc.

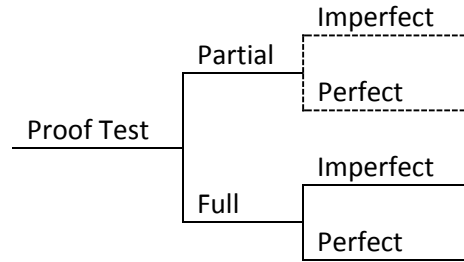


Figure 3.1: Classification of a Proof Test. Adapted from (Rausand,2014)

3.3 Modelling of imperfect proof testing

As mentioned, limited literature can be found concerning modelling the effects of imperfect proof test. The effects of imperfect proof tests are modelled by IEC61508² (e.g., see Section B.3.2.5, part 6 IEC61508, 2010) by introducing the Proof Test Coverage (PTC) as the fraction of hidden failures that may be revealed by a proof test. The PDS method (Hauge et al., 2013) presents a more detailed discussion about the effect of imperfect proof tests by examining the PTC. In addition to the PTC, Hauge et al. (2013) introduces the Probability of test independent failures, P_{TIF} for modelling the effect of imperfect proof tests. The PDS method also (Hauge et al., 2013) discusses the suitability of the use of the PTC or the P_{TIF} .

When the coverage factor is used to model partial proof tests and there are hidden failures that are never tested, and this type of failures are random hardware failures, we shall use two coverage factors: a Test Coverage Factor, TCF, used to model the effect of partial proof test and a maximum test coverage factor TCF_{max} used to model the effect of imperfect full proof tests. TCF and TCF_{max} are described in detail in chapter 4. In addition, a step-wise procedure is presented. The procedure is based on the approach for determining the partial stroke testing coverage factor for shutdown valves proposed by Lundteigen and Rausand (2008).

Other approaches to model the effect of imperfect are available. Bukowski and Van Beurden (2009) propose a measure of proof test effectiveness, PTE, that is an indicator of completeness and correctness of a proof test. This measure is derived from simplified Markov models. Kumar et al. (2008) extends the use of Markov models to incorporate imperfect proof tests. Zhang et al. (2008) also uses the Markov approach to model imperfect inspections (e.g. proof tests).

²IEC61508-6 refers to imperfect proof test as non-perfect proof test

However, the complexity of the Markov models increases exponentially with the number of systems nodes and states (see e.g., Kumar et al., 2008; Zhang et al., 2008). Moreover, standard Markov models should not be used to model such systems that are subject to periodic proof test (IEC61508-6; ISO/TR-12489, 2013) because of the deterministic test interval. In this case, the transitions from a failed state to a working state are not exponentially distributed.

3.4 The Effect of Short Test Intervals

The frequency of proof test intervals is of paramount importance for achieving high hardware safety integrity, however, very short test intervals are unacceptable for practical reasons with regard to operation. For example, loss of production due to downtime; Moreover, too frequent testing have negative impact on reliability due to system degradation (unnecessary wear) and possible errors of personnel (items that may not have been correctly restored to its operational mode); In addition, there are also cost related impacts due to the increase of man hours (Vaurio, 1995).

The frequency of testing is mainly chosen by engineering judgment: (i) based on general practices (Voronov and Alzbutas, 2009) or (ii) common traditions (Lehtinen et al., 1984). Nonetheless, when reliability data is available (e.g., failure rates), the selection of the reasonable level of testing should be treated as an optimization problem. In order to determine the optimal test strategy, a complete set of information should be gathered (for example, functional analysis, cost related issues, failure rates, etc.). The analyst (e.g., a reliability engineer) should consider the Failure Mode and Effects Analysis (FMEA) as the starting point to gather the required information for the reliability analysis. A brief description of the FMEA is presented in chapter 4 and the main failure modes that we can affect the reliability of WOCSs are discussed in chapter 6.

As mentioned in chapter 2, most of the acting elements (e.g., Valves) of a WOCS are functionally tested (e.g., open and close) with a *daily* basis because of the operating requirements. It allows the operator to identify which valves are *stuck*, for example, in the closed position, which it is a critical failure mode for shutdown valves. However, too frequent strokes leads to wear and increase the likelihood of damage of seal and/or seat of the valve. We can easily deduce that

assuming an exponential distribution for the failure rate of those valves leads to unrealistic reliability measures. Weibull distribution is a proper probability distribution to model increasing failure rates.

Mathematically speaking, short test intervals lead to high reliability. See for example the approximation formulas for PFD_{avg} calculation of safety instrumented systems presented by Rausand and Høyland (2004). Very low PFD_{avg} corresponds to high safety integrity. However, that not necessarily means that the systems is highly reliable. This issue is discussed in more detail in chapter 7.

Very large consequences due to system's failure may be a good reason for carrying out too frequent proof testing. However, results from accurate reliability predictions should be the criterion for defining the test interval. Therefore, all factors that influence the system's reliability should be considered. The major contributors to safety unavailability are discussed in chapter 8 and the optimization problem is presented.

Chapter 4

Test Coverage Factor

4.1 Introduction

As mentioned in Chapter 3, the proof test coverage (PTC) introduced by IEC61508-6 is used to model the effect of imperfect and partial proof testing, and partial proof testing is implemented to reduce the unavailability (e.g., PFD_{avg}) of safety systems (Lundteigen and Rausand, 2008). In the literature we find some methods for reliability assessment of safety instrumented systems subject to partial proof test. See for example, (Jin and Rausand, 2014; Brissaud et al., 2010; Oliveira, 2009). Those articles cover the application of the coverage factor, but they do not present details in how to determine it. A procedure for how to determine the partial stroke testing coverage factor is elaborated by (Lundteigen and Rausand, 2008). This approach is limited to shutdown valves and we extend this method for estimating the test coverage factors (TCF and TCF_{max}) of any component that can be partially tested or it is subject to imperfect proof testing.

4.2 Definition and Use of the Test Coverage Factors

The concepts of TCF and TCF_{max} were briefly introduced in chapter 3. The definition and description of these two parameters follows

☞ **TCF**: Fraction of hidden failures that can be detected by partial proof tests.

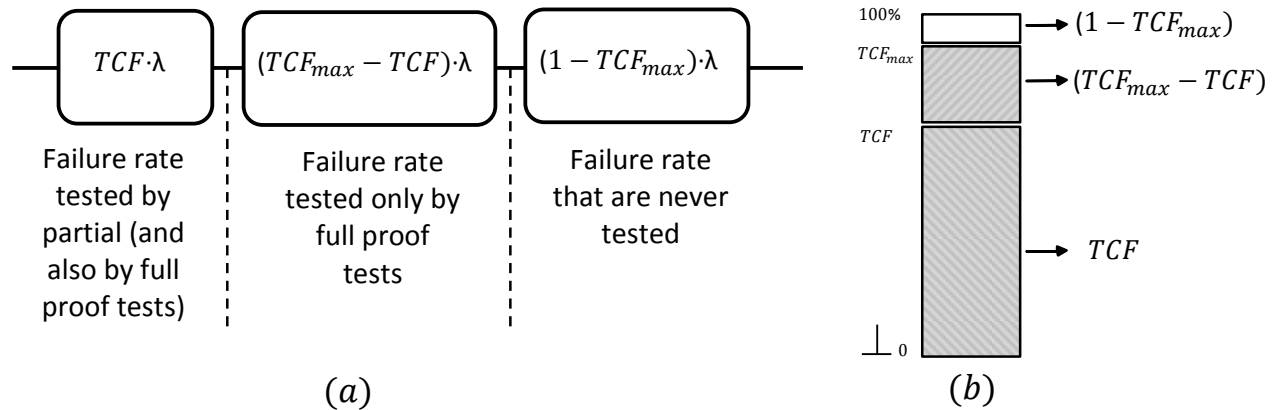


Figure 4.1: (a) Reliability block diagram of failure rate that are revealed and non-revealed by proof tests. (b) Illustration of the Test Coverage Factor

☞ **TCF_{max}** : Fraction of hidden failures that can be detected by imperfect proof tests.

The method that we present for estimating TCF and TCF_{max} is based on the FMEA approach. The FMEA approach is discussed in the next section.

If the coverage factor is equal to 100%, the proof test is obviously perfect and full; whereas if the test is imperfect because not all hidden failures can be revealed by a full proof test, the coverage factor has a maximum value (TCF_{max}) and there are therefore hidden failures that are never tested. If partial proof test is implemented, we should have an estimate of the TCF of hidden failures that may be revealed by the test.

From the previous definition, the failure rate can be split into hidden failures detected only by full proof test (e.g., $(TCF_{max} - TCF) \cdot \lambda$); hidden failures that are detected by partial and also by full proof tests (e.g., $TCF \cdot \lambda$); and hidden failures that are never detected by a proof test (e.g., $(1 - TCF_{max}) \cdot \lambda$). Figure (4.1a) shows the reliability block diagram of failure rate that are revealed and not revealed by proof tests. The split of failure rate is similar to the approach presented by (Jin and Rausand, 2014; Brissaud et al., 2010; Rausand, 2014), but they do not consider failures rates that are never tested. Figure (4.1b) illustrates the concept of the TCF and its relationship with proof tests.

4.3 Failure Modes and Effects Analysis

IEC60812 (2006) defines FMEA as a systematic procedure for the analysis of a system to identify the failure modes, their causes and effects on system performance. A simple example of a FMEA worksheet is presented in appendix B. There are two variations of the FMEA approach: the FMECA and the FMEDA.

FMECA (Failure Modes, Effects and Criticality Analysis) is an extension to the FMEA to include a means of ranking the severity of the failure modes to allow prioritization of countermeasures (IEC60812, 2006).

FMEDA (Failure Modes Effects and Diagnostic Analysis) has additional columns to cover failure classification, diagnostic related for each failure mode, detectability of failure modes, systems specific failure rates and diagnostic coverage (Rausand, 2014).

An FMEA is a simple and powerful tool for qualitative reliability analysis. It helps us to understand how and why a system can fail. A thorough understanding of the functionality of a system may be obtained by the correct application of this technique. As mentioned, here, we use an FMEA as the basis for determining the TCF both for partial and full proof test. Some examples of FMEDA, with suggested coverage factors for specific products are available on the web from some projects developed by *Exida*¹. The procedure for determining the coverage factor is not described in the reports developed by Exida.

4.4 Method for Estimating the Test Coverage Factors

The procedure for determining the TCF is based on the method described by (Lundteigen and Rausand, 2008). We recall that TCF corresponds to the coverage factor of partial proof tests and TCF_{\max} to coverage factor for modelling imperfect (full) proof tests. Lundteigen and Rausand (2008) propose that the coverage factor can be expressed as

$$TCF = \sum_{i=1}^n TCF_{FM_i} \cdot w_i \quad (4.1)$$

¹Exida is an international consulting company that provides product certification with IEC61508

Failure modes	Failure rate	Weight	Partial proof tests	Full proof tests
FM_i	λ_{DU_i}	w_i	$TCF_{FM_i}^P$	$TCF_{FM_i}^F$

Table 4.1: Summary of the required information for estimating the TCF_{FM_i}

where FM_i denotes the i th failure mode that may be found by an FMEA amongst n failures modes; w_i is the weight(importance) of the FM_i amongst all failures modes of the component, and it can be found from

$$w_i = \frac{\lambda_{DU_i}}{\sum_{i=1}^n \lambda_{DU_i}} \quad (4.2)$$

and TCF_{FM_i} denotes the percentage that a FM_i is covered by a proof test. FM_i is basically estimated by expert judgment.

The information required to estimate the TCF for both partial and full proof tests can be gathered for each failure mode as shown in table (4.1)

As mentioned, the estimation of TCF_{FM_i} is based on expert judgment; but also it can be estimated based on analysis of the component under study. The analysis should consider for example, functionality, interfacing, dynamics, ageing, deterioration of the internal parts of the item. By doing this analysis, we can find the relationship between the different failures modes FM_i and their effects on each single part j of the item. For example, consider a hydraulically operated fail-safe valve (a shutdown valve) during partial stroke testing: (i) the spring of the actuator is decompressed a few centimetres, (ii) the seat and the seals of valve are not tested, (iii) the hydraulic oil contained in the actuator is not fully bled off, and so on.

The failure modes identified through the FMEA are examined against each part of the component (e.g., the spring, the seat, the seal, the gate, etc. of a shutdown valve). From this examination we can quantify how much each part is tested while revealing a FM_i . This is quantified as the percentage δ . Table (4.2) shows a template for documenting the information required for the quantification of δ . For example, for the failure mode *fail to open* of a valve, the seat of the valve is not tested while revealing this failure mode, therefore, δ is equal to zero. On the other hand, for example, the spring is decompressed a few centimetres. This fraction of decompression of the spring is a measure of δ for the spring while considering the failure mode *fail to open*.

F. Modes	Parts	Part 1	Part 2	...	Part j	...	Part n
	FM_i	δ_1	δ_2	...	δ_j	...	δ_n

Table 4.2: Matrix for determining the TCF_{FM_i} per failure mode

When δ is equal to zero, this value should not be taken into account in computation of TCF or TCF_{\max} (see 4.3).

The TCF_i for both full and partial proof test can be found as the geometric mean amongst all δ_j as follow

$$TCF_{FM_i} = \sqrt[n]{\prod_{j=1}^n \delta_j} \quad (4.3)$$

Notice that for a full perfect proof test, δ is always equal to 1, therefore, TCF (e.g., in 4.1) is equal to 1.

4.4.1 Procedure(Summary)

In this part, we exemplify the procedure for estimating the TCF and the TCF_{\max} . These parameters are computed for the SS-RAM used in the WOCS safety functions ESD and EQD.

Step 1. Perform an FMEA. The first step consist in performing an exhaustive FMEA. The main objective is to find all the failure modes and the corresponding failure rate λ . The main failure modes of the SS-RAM are listed in table (4.3).

Step 2. Computation of importance of each failure mode. The weight w_i is an indicator of the importance of the failures modes identified through the FMEA.

The weight of each failure mode is presented in the last column of the table (4.3). The values were calculated by using (4.2) and the values of λ from table (4.3).

Table (4.3) summarizes the failure modes, their corresponding failure rates and weight, for the SS-RAM. The information of the failure rates was extracted from OREDA (2009a).

Step 3. Computation of the TCF per failure mode. TCF_{FM_i} may be found by expert judgment or by using (4.3).

The objective is to quantify how much each part is tested while revealing a FM_i during a proof test. Since the computation of TCF_{FM_i} by using (4.3) requires a deep understanding and

Failure modes	Failure rate ($\cdot 10^{-6}$)	Weight w_i
Fail to Close	38	0.357
Fail to Shear	6.2	0.058
Fail to Open	38	0.357
Internal Leakage	18	0.169
External Leakage	6.2	0.058

Table 4.3: Failure modes and failure rates for the SS-RAM

knowledge of the SS-RAM, we omit to use that approach. As a result, the following assumptions are made:

- The failure mode *fail to close* is fully tested by both partial and full proof tests. During this proof tests the SS-RAM travels from the opened position to the closed position, therefore, for this failure mode, TCF_{FM}^P and TCF_{FM}^F are equal to one for both proof tests.
- The failure mode *fail to shear* is only revealed during a real demand, hence, TCF_{FM}^P and TCF_{FM}^F are equal to zero for both proof tests.
- The failure mode *fail to open* is fully tested by both partial and full proof tests. The SS-RAM should be returned to the opened position, therefore, for this failure mode, TCF_{FM}^P and TCF_{FM}^F are equal to one for both proof tests.
- The failure mode *internal leakage* is partially tested in a partial proof test. We assume that 60% of the seals are tested during this test. During a full proof test, this failure mode is fully tested.
- The failure mode *external leakage* is partially tested during a partial proof test. We assume that this failure mode is detected when the SS-RAM remains in closed position. Given that the SS-RAM remains closed a short fraction of time during a partial proof test, 20% may be reasonable value for TCF_{FM}^P . This failure mode is fully tested by full proof tests.

Table (4.4) summarizes the values estimated for TCF_{FM}^P and TCF_{FM}^F for each failure mode.

Step 4. Computation of the TCFs. The estimated TCF and TCF_{max} can be found by using (4.1).

Failure modes	TCF _{FM_i} Partial Proof Tests	TCF _{FM_i} Full Proof Tests
Fail to Close	1	1
Fail to Shear	0	0
Fail to Open	1	1
Internal Leakage	0.7	1
External Leakage	0.2	1

Table 4.4: Failure modes and failure rates of the Shear Seal RAM

The TCF and TCF_{max} for the SS-RAM become

$$\text{TCF} = 1 * 0.357 + 0 * 0.058 + 1 * 0.357 + 0.7 * 0.169 + 0.2 * 0.058 = 84.39\% \quad (4.4)$$

$$\text{TCF}_{\max} = 1 * 0.357 + 0 * 0.058 + 1 * 0.357 + 1 * 0.169 + 1 * 0.058 = 94.1\% \quad (4.5)$$

4.4.2 Impact of the Test Coverage Factor to System's Reliability

It can be noticed that the test coverage factors are estimated for components, and the main assumption is that the failure rate λ of each failure mode is independent from other failure modes. It allows to split the failure rate into the three components as explained in section 4.2. The main effect of a test coverage factor is that, it illustrates how much the time dependent probability failure on demand, PFD(t), is reduced when a proof test is carried out. High coverage factors lead to low PFD_{avg}.

Let us consider a coverage factor for a safety function. This *new* coverage factor obviously depends on the TCF and the TCF_{max} and it is reasonable to state that there is a direct correlation between the *new* coverage factor and TCF, or TCF_{max}. For example, an increase of TCF or TCF_{max} leads to an increase of the coverage factor of the safety function. This issue is no longer discussed in this master's thesis.

The use of the TCF and TCF_{max} is exemplified in the next chapter and these parameters are the cornerstone for the model of the time dependent availability that we propose in this master's thesis.

Chapter 5

Methods for the Reliability Assessment

5.1 Introduction

In previous chapters we presented some of the factors influencing reliability assessment of WOCS. Amongst them, we discussed the effect of partial and imperfect proof testing, short test intervals and test coverage factors. In addition, the description, operational and testing philosophy of the WOCS system were provided.

The reliability of safety systems is often assessed by calculating the average unavailability. In this chapter we discuss some methods for reliability assessment of safety systems (e.g., a WOCS). The main advantages and disadvantages of each method are discussed.

In chapter 8 we focus on the total unavailability of a simple component considering the major contributors to this reliability measure (e.g., PDF_{avg} , unavailability due duration of the test, repair times, etc). In this chapter we focus on some methods for determining the PDF_{avg} of complex systems. We recall that the PFD_{avg} is often used as the reliability measure for safety systems.

5.2 Reliability Block Diagrams

A Reliability block diagrams (RBD) is a successful-oriented network¹ describing a function of a system (e.g., a safety system). It represents the logical connections of components of the system

¹The networks are built by thinking in terms of functions

under study. The resulting logical diagram of the components connected in parallel or in series, or a combination of both, indicates how the specified system function is fulfilled.

By using the formulas for the structure function of single logical diagrams in series or parallel, we can find the reliability function of the system under study. These formulas are presented in (5.1) and (5.2)²

$$R_S(t) = \prod_{k=1}^n R_k(t) \quad \text{For series systems} \quad (5.1)$$

$$R_P(t) = 1 - \prod_{k=1}^n (1 - R_k(t)) \quad \text{For parallel systems} \quad (5.2)$$

Where $R_k(t)$ is the reliability function of one single component.

If the system is subject to proof testing and consequent repair actions, the reliability function is referred as the availability function (e.g., $A(t)$).

Consider a component that is subject to partial and full proof tests at τ_p and τ respectively; and also consider that the component has hidden failures that are revealed and never revealed by proof tests as discussed chapter 4. If we assume that the failure rates of the component are exponentially distributed, the availability function $A_k(t)$ of this component may be found from (5.3).

$$A_k(t) = e^{-TCF \cdot \lambda \cdot (t - \tau_{p,j,i})} e^{-(TCF_m - TCF) \cdot \lambda \cdot (t - \tau_i)} e^{-(1 - TCF_m) \cdot \lambda \cdot t} \quad (5.3)$$

$A_k(t)$ in (5.3) is valid for $t \geq 0$, $i \geq 1$, $1 \leq j \leq n$, and $\tau_{p,j,i}$ denotes the j th of n partial proof tests in test interval $(\tau_i, \tau_{i+1}]$ of full proof tests. In (5.3), τ is not a fixed value and it increases over the time. The length of the interval (τ_i, τ_{i+1}) may be (but not necessarily) constant (e.g., periodic proof testing). The same concept applies for τ_{p_j} . We clarify that at the time instant of a full proof test, $\tau_p = \tau$.

As mentioned, we are interested in the unavailability function for the reliability assessment of safety systems. Figure (5.1) shows the curve of the unavailability function $U_k(t) = 1 - A_k(t)$. The figure (5.1) presents the two cases when $TCF_{\max} = 1$ and when the $TCF_{\max} < 1$.

If the full proof tests are periodic and perfect, TCF_{\max} is equal to one, leading the average unavailability \bar{U}_k to be equal in each full proof test interval (see figure (5.1a)). In contrast, if the

²The formulas presented is the result of the use of probability theory by assuming independent components

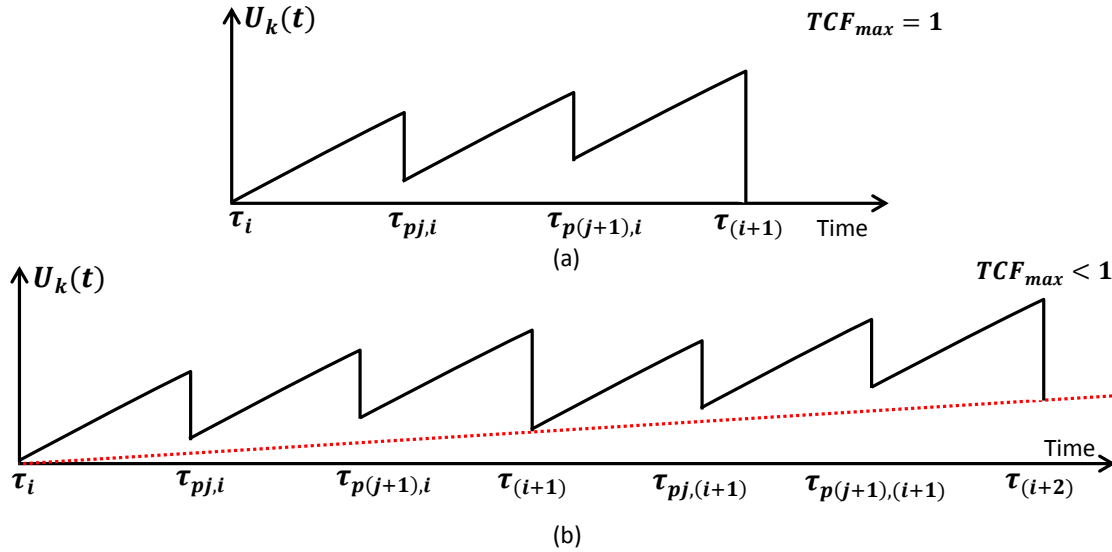


Figure 5.1: Unavailability function $U_k(t)$ a single component that is subject to partial and full proof tests. (a) $U_k(t)$ when $TCF_{max} = 1$ (b) $U_k(t)$ when $TCF_{max} < 1$

full proof tests are imperfect, the likelihood of failure on demand increases over time (see figure (5.1b)).

5.3 Average Unavailability of the WOCS

5.3.1 Background

The operational philosophy of the WOCS described in chapter 2 may be summarized and illustrated as in figure (5.2a). The WOCS is *in-service* or is not, with an unknown duration period. The testing requirement of carrying out a full proof test, just before the WOCS is put into a workover operation, is shown in figures (5.2a) and (5.2b) (e.g., τ_0, τ_1, τ_2). The figure (5.2b) shows the effect of imperfect full proof test to the unavailability function at the time instant τ . It also can be seen that the WOCS is subject to partial proof test every 7 days (e.g., τ_{pi}). The red dashed line in figure (5.2), indicates the assumption that after a WO operation, there are hidden failures that keep dormant until the maintenance that is carried out between WO operations. (e.g., between intervals $(t_1, t_2), (t_3, t_4)$). The instantaneous unavailability between these periods is of importance, because the WOCS is subject to imperfect proof tests. We assume that the maintenance carried out after a WO operation eliminates all hidden failures, except the failure "fail to shear" of the

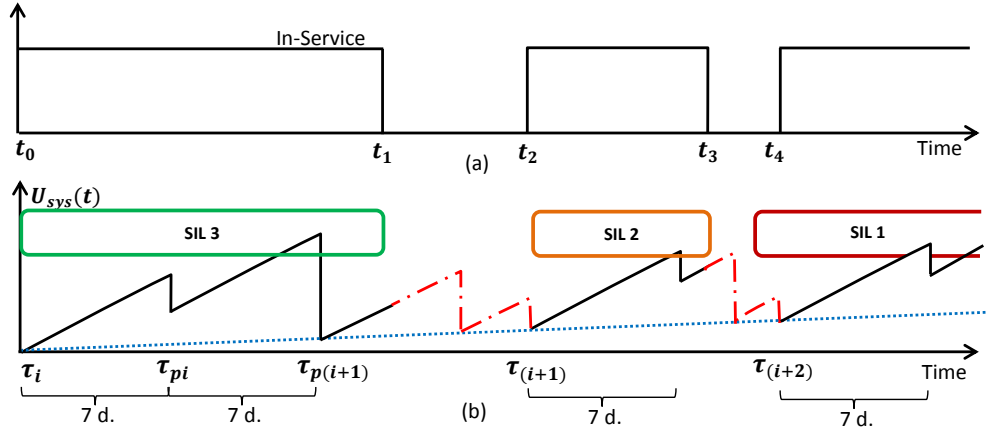


Figure 5.2: Operational and Testing Philosophy. (a) Operational scheme for the WOCS. (b) WOCS unavailability function including partial proof tests and imperfect full proof tests.

SS-RAM. We assume that the proof test every 14 days reveals all hidden failures, excepting the failure "fail to shear" of the SS-RAM.

The average unavailability of the WOCS, \bar{U} , better known as the PFD_{avg} , is found for each safety function by using (5.4).

$$PFD_{avg} = 1 - \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} A(t)_{SYS} dt \quad (5.4)$$

$A(t)_{SYS}$ may be found from the RBD of the safety functions described chapter 2 by using (5.1), (5.2) and (5.3). If the full proof test are perfect and periodic, (5.4) can be calculated in the interval $(0, \tau)$; by determining the proper test interval, the safety integrity level(SIL) is kept equal during the life cycle of the system. This is valid only under the assumption that after a full proof test, the system is brought to a state "as-good-as-new". On the other hand, if the full proof test is imperfect, the average unavailability in the interval $(\tau_i, \tau_{i+1}]$ is not a proper indicator of the reliability of the system. In such case, it is better to consider the average unavailability in each interval, or use other reliability measure, like the frequency of failure. Nonetheless, any chosen reliability measure increases overtime. Figure (5.2b) shows that the safety integrity level reduces over the time because of imperfect proof tests.

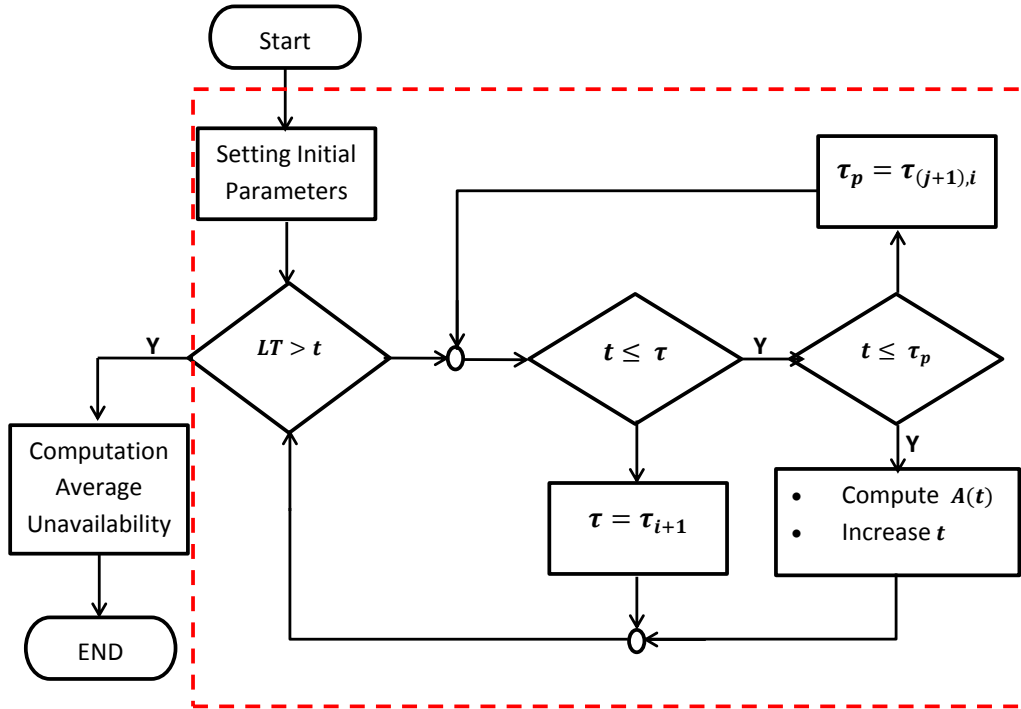


Figure 5.3: Flow diagram for computing the average unavailability of a single component subject to partial and full proof test

5.3.2 Solution

The analytical solution of (5.4) can be rather complex and it requires the use of a software algorithm. We implemented an algorithm in MATLAB that computes the average unavailability of a system taking into account the issues illustrated in figure (5.2). The algorithm implemented in MATLAB for computation of the average unavailability of a single component is summarized in the flow diagram shown in figure (5.3). *Setting of the initial parameters* includes the definition of (for example) the failure rates, test coverage factors, instant times for partial and full proof tests and period of interest, (e.g., life time, $[0, LT]$).

In order to compute the PDF_{avg} , the process into the red dashed box in figure (5.3) must be run for each component for obtaining the time dependent availability as in (5.3). Afterwards, the time dependent availability of the system is computed by using (5.1) and (5.2) depending on the RBD that represents the system's function of interest.

Finally, the PDF_{avg} is computed by using (5.4). The average unavailability \bar{U} depends on the value of TCF_{max} . For $TCF_{max} = 1$, the PDF_{avg} is computed in the interval $(0, \tau)$. For $TCF_{max} < 1$,

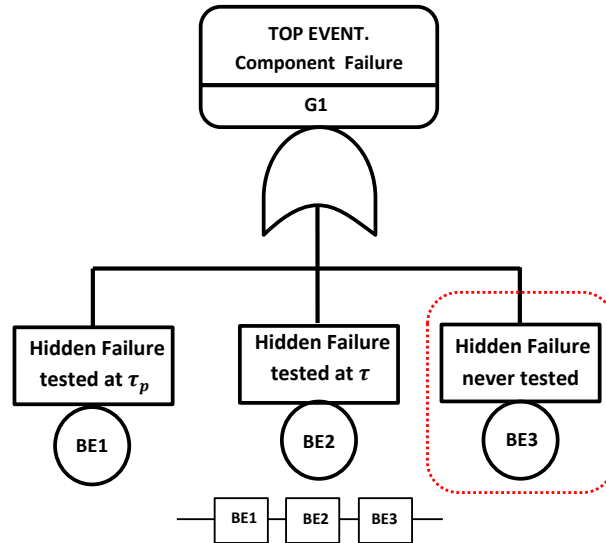


Figure 5.4: Example of a Fault Tree

the average is computed for the interval of interest. (e.g., Lifetime, $[0, LT]$).

The script of the algorithm implemented in MATLAB can be found in appendix C.

5.4 Fault Tree Analysis

A Fault Tree Analysis (FTA) is a top-down analysis performed from the top event (e.g., unwanted event) by building step by step, logical links between individual failures (e.g., basic events). Logic gates (e.g., AND-gates, OR-Gates) are used for the construction of the Fault Tree as shown in figure (5.4). Figure (5.4) is the Fault Tree that represents the component failure of a component modelled by the reliability block diagram in figure (4.1a). The three basic events corresponds to a hidden failures revealed by partial and full proof tests, hidden failure revealed only by full proof tests and hidden failures that are never tested, as discussed in chapter 4.

5.4.1 PDF_{avg} Calculations

The quantification of the PDF_{avg} of a system represented in a Fault Tree may be performed using the following approaches:

- 1 Conversion of the Fault Tree into a RBD and then computation the PDF_{avg} as explained in the previous section.

- 2 Computation of the PDF_{avg} by the use of analytical formulae approach.
- 3 Computation of the PDF_{avg} from the instantaneous unavailability curve of the TOP EVENT by using Boolean algebra.

5.4.2 Analytical Formulae Approach

The minimal cut set theory is the foundation for the analytical models. From a RBD or a FTA, we can determine the minimal cut sets (e.g., r). From the series structure³ of these r minimal cut sets, we compute the average unavailability of the system. By assuming that, (i) the minimal cut sets are independent, and (ii) the product of the average unavailability (e.g., \check{Q}_i) of the minimal cut sets are negligible compared with its sum, the average unavailability of the system (e.g., Q_o in (5.5)) can be found from the summation of the of these quantities. The result from (5.5) gives a conservative value, because (i) the products from the formula used in order to find the probability $\Pr(E_1 \cup E_2 \cup \dots \cup E_n)$ are disregarded and (ii) the minimal cut sets are positively dependent since some components may be in several minimal cut parallel structures (Rausand and Høyland, 2004).

$$Q_o \approx \sum_{i=1}^r \check{Q}_i \quad (5.5)$$

A minimal cut parallel structure fails if all components in the structure fail. However, since the average probability of periodically tested components cannot be used directly to calculate the average probability of a minimal cut set, because the average probability of a product is not the product of the average of these quantities ((ISO/TR-12489, 2013), the product of the failure probabilities may be corrected by a factor depending on the number of channels (e.g., n) in the minimal parallel structure ((Lundteigen and Rausand, 2008)). Therefore, \check{Q}_i in (5.5) can be found from

$$\check{Q}_i \approx \frac{2^n}{n+1} \cdot \prod_{j=1}^n \bar{q}_j \quad (5.6)$$

³A system with r minimal cut sets may be represented by a series structure of the r minimal cut parallel structures

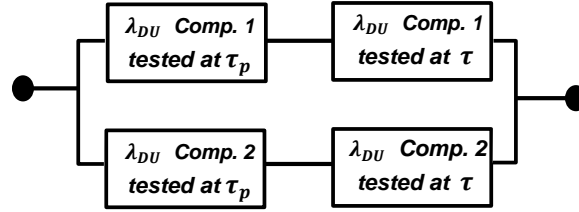


Figure 5.5: RBD of a structure of two components connected in parallel where each component is modelled by a series of two "subcomponents" with failure rate revealed at τ_p and τ respectively

where \bar{q}_j in (5.6) is the average probability of failure of a single component and it can found from⁴

$$\bar{q}_j \approx \frac{\lambda_j \cdot TCF_j \cdot \tau_p}{2} + \frac{\lambda_j \cdot (1 - TCF_j) \cdot \tau}{2} \quad (5.7)$$

where λ_j is the failure rate of the j th component in the minimal cut set and TCF_j is its proof test coverage factor. We reader should notice that \bar{q}_j does not include the basic event 3 from figure (5.4). This is because of the underlying assumption for the analytical formulae, that the components are periodically tested and the full proof test are perfect.

Consider a system of two independent components connected in parallel. Also consider that the system is subject to partial proof tests and the average unavailability of each component can be found by using (5.7), therefore, the system can be modelled by the RBD in figure (5.5). The simple system in figure (5.5) has four minimal cut sets; if the failure rate of the 2 main components are in the same order of magnitude, the products of the four terms from (5.6) are also in the same magnitude (none term can be neglected).

An important characteristic of this approach is that it gives proper results when the components have the same instant time for the full proof tests. Otherwise, the quantity in (5.6) gives non-conservative values. This is because of the static feature of the fault trees. The components, however, may be subject to different number partial proof tests.

5.4.3 Boolean Models

Probabilistic calculations based on Boolean equations are basically time independent. Nevertheless, if the components in a system are independent, time-dependent formulas can be still

⁴Once again, we assume that the product of the average probabilities is negligible compared with its sum.

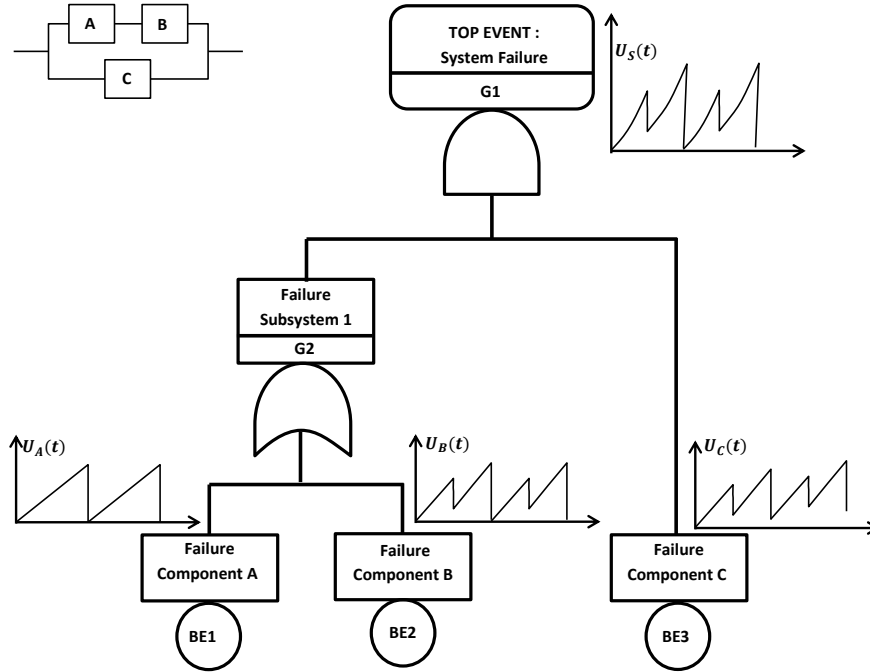


Figure 5.6: Average unavailability calculation (Example)

used(ISO/TR-12489, 2013).

The formulas in (5.8) and (5.9) can be used for the computation of the time dependent unavailability of events in a Fault Tree. Notice that formulas are similar to (5.1) and (5.2), but in this case the formulas are derived thinking in terms of failures. Figure (5.6) exemplifies the use of (5.8) and (5.9). The output of the gate $G2$ is found by using (5.9), and the output of the gate $G1$ is found by using (5.8).

The algorithm implemented in MATLAB can be used for computation of the instantaneous unavailability $U_k(t)$ (e.g., $U_k(t) = 1 - A_k(t)$).

$$U_{\cap}(t) = \prod_{j=1}^n U_k(t) \quad \text{For AND-gates} \quad (5.8)$$

$$U_{\cup}(t) = 1 - \prod_{j=1}^n (1 - U_k(t)) \quad \text{For OR-gates} \quad (5.9)$$

As it has been shown, the time dependent unavailability $U_k(t)$ is input to the logic gates (e.g., see figure (5.3)). This unavailability function may correspond to events at upper levels or basic events in a Fault Tree (e.g., a single component as represented in the RBD in figure(5.4)).

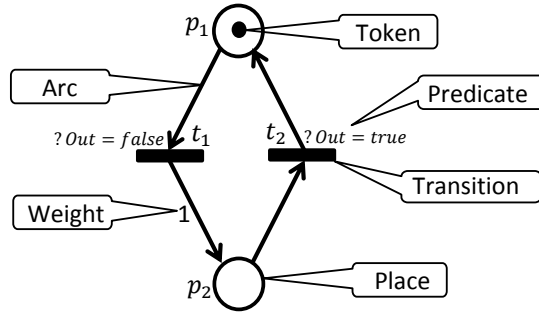


Figure 5.7: Example of a simple Petri Net showing the main graphical elements

The instantaneous unavailability $U_S(t)$ is found by using (5.8) and (5.9) and the average unavailability \bar{U} (e.g., PDF_{avg}) can be found by using

$$\bar{U} = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} U_S(t) \quad (5.10)$$

5.5 Petri Nets

A Petri Net is a technique for describing the behaviour of a system by modelling the relationship between states and events. The states are represented by places and the events are represented by transitions; places and transitions can be connected by arcs. A place may contain tokens for simulating, for example, a working state, a failed state, etc. A place represents an active state if it contains a token. Sometimes, the place may require more than one token to represent an active state. Transitions may be constrained by (i) deterministic values (e.g., a delay) (ii) stochastic variables (e.g., a random value that follows a specified probability distribution), (iii) conditional statements (predicates), and (iv) arc constrains (e.g., weights or inhibitors).

Calculations from Petri Nets are based on Monte Carlo Simulation. Figure (5.7) summarizes the graphical elements used in a Petri Net.

In this chapter we present the use of Petri Nets for modelling the unavailability of a system with failure rate revealed and non-revealed by proof tests. Virtual RBDs are used to drive the building of the Petri Nets. It basically helps to build the Petri Net and understand the behaviour of the system.

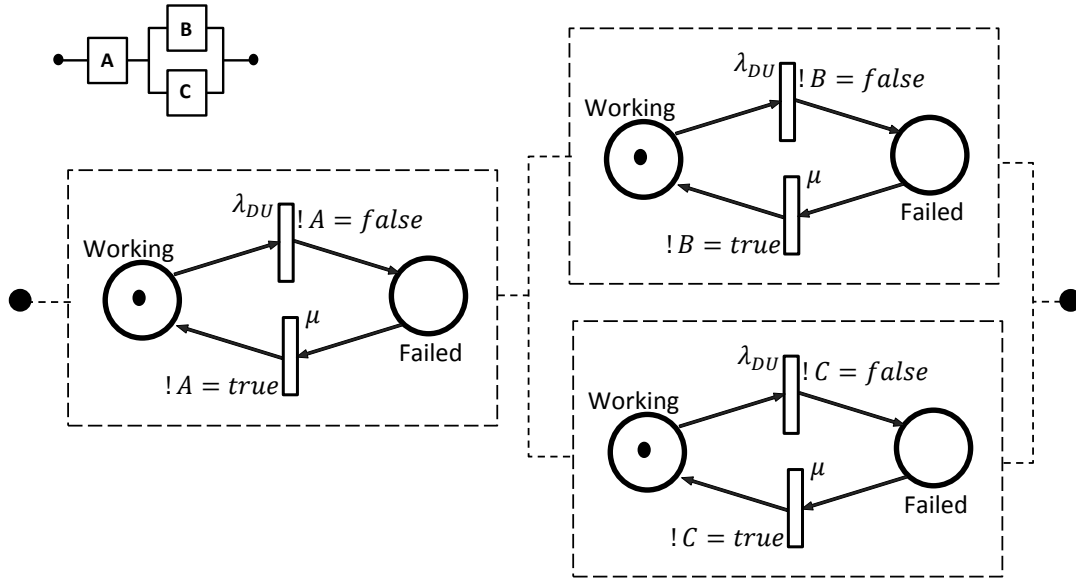


Figure 5.8: Example of a simple Petri Net Driven by a Virtual RBD

5.5.1 Petri Nets driven by Virtual RBDs

Given a system's RBD, we can draw a Petri Net for each block (of the RBD) for representing a single component. The Petri Net for modelling the behaviour of the whole system, is therefore the group of all single Petri Nets. This concept is exemplified for a system composed by three components as shown in figure (5.8).

Consider the simple system as shown in figure (5.8). A component *A* in series with two components in parallel (*B*,*C*). The Boolean equation that indicates if the system is functioning is given by (5.11)(e.g. $Out = 1$).

$$Out = A \cap (B \cup C) = A \cdot (B + C) \tag{5.11}$$

A,*B*,*C* represents the binary states of functioning or failed state of the components. Notice that a variable (*A*,*B*,*C*) is created for each component in order to indicate if it is functioning or failed. For example, the variable is set to *false* during the transition from working state to failed state, and it is set to *true* during the transition from failed state to working state. These assertions are represented in a Petri Net by the character *!*. (e.g. $!A=true$ as shown in figure (5.8)).

In order to know the average unavailability of the system, an auxiliary Petri Net as shown

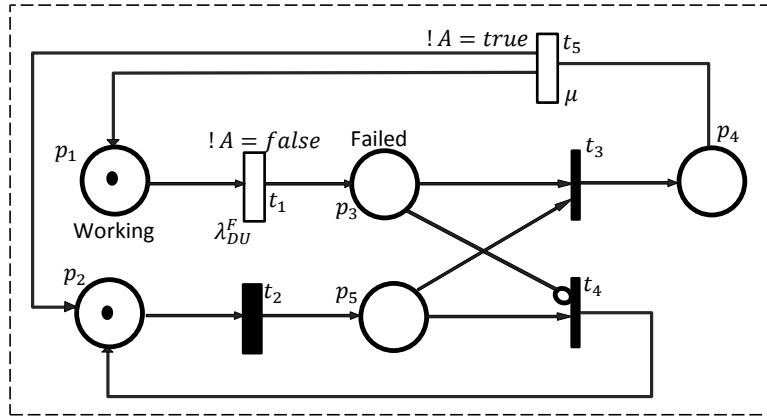


Figure 5.9: Petri Net for modelling Periodic perfect full proof test

in figure (5.7) is required. The transitions t_1 and t_2 in figure (5.7) are constrained by the predicates $?Out=false$ and $?Out=true$ respectively. Therefore, the average unavailability of the system is given by the mean marking of the place p_2 . (average proportion of time that the place p_2 contains a token). In this case, the average unavailability can also be found by adding the mean markings of the places that are used to represent failed states.

5.5.2 Proof Testing Policies with Petri Nets

The behaviour of safety system comprises two main aspects: (i) the way the system fails, which it can be modelled by the use of random events following a specified probability distribution, and (ii) the way that the system is maintained, which for safety systems it follows a predefined maintenance policy (e.g., periodic proof test). By considering the model presented to the failure rate revealed by partial and full proof tests and failure never revealed, as presented in chapter 4, we have Petri Nets to represent the combinations of proof tests when considering the effect of imperfect full proof tests and partial proof tests. In the following sections we present and propose some Petri Nets for modelling the behaviour of a safety system.

5.5.3 Perfect Full Proof Test without Partial Proof Tests

The Petri Net that may be used to model the test regime of periodic perfect proof test (without partial proof tests) is presented in figure (5.9).

A token in place p_1 indicates that the component is functioning. When the component has a hidden failure (failure event due to λ_{DU}^F), the transition t_1 is fired and the token in place p_1 is removed and transferred to the place p_3 . The token in place p_3 is removed when there is token in place p_5 (meaning that a proof test is ongoing). If the transition t_3 is fired, it means that the hidden failure is revealed and repair actions take place (a token is released to place p_4). The token in place p_4 is removed after the mean down time due to repair actions (e.g., $1/\mu$). When the transition t_5 is fired, a token is released to place p_1 (the component is restore to a working state), and a token is released also to place p_2 (a new test period is started).

The transition t_2 is fired every τ (delay of t_2). the transition t_4 is fired when the proof test is ongoing and the component does not have hidden failures. The duration of the proof test may be simulated by specifying a delay in transitions t_3 and t_4 respectively⁵. Notice that the variable A is set to *false* when there is failure and it is set to *true* when the component is restore to a working state. This variable can be used in the Boolean equation of the RBD of the system, as explained at the beginning of this section. In this simple Petri Net, the average unavailability of the component is equal to the sum of the mean marking of the places p_3 and p_4 . As mentioned, the Petri Net from figure (5.7) can also be used to find the average unavailability. Therefore, the sum of the mean markings of the places p_3 and p_4 is the same as the mean marking of the place p_2 in figure (5.7). In this case $Out = A$. This Net is also described by (Rausand, 2014).

Perfect Full Proof Test and Partial Proof Tests

a Petri Net for modelling the test policy that a component is partially tested $m - 1$ times in a test interval of perfect full proof tests is presented in figure (5.10). This Petri Net is consistent with the idea that a component has (i) hidden failures revealed by partial proof tests and also by full proof tests, and (ii) hidden failures revealed only by full proof tests.

The Petri net in figure (5.10) has two places (p_4 and p_{10}) to denote that a failure event with failure rate equal to $\lambda_{DU}^P = TCF \cdot \lambda_{DU}$ or $\lambda_{DU}^F = (1 - TCF) \cdot \lambda_{DU}$ may occur. The total failure rate of the component is equal to $\lambda_{DU} = \lambda_{DU}^P + \lambda_{DU}^F$. Notice that we assume that the failure events are independent.

After a failure event due to λ_{DU}^P , the transition t_1 is fired and a token is released to place p_4 .

⁵In general, the transitions with the shape as t_3 are instant transitions

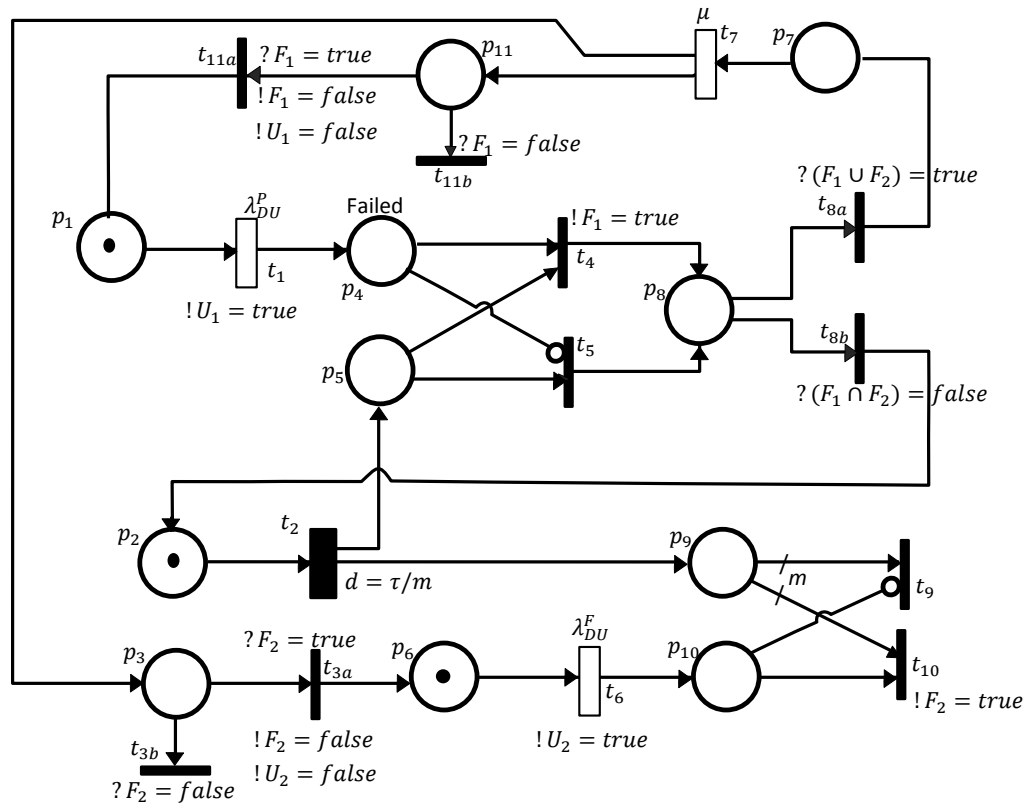


Figure 5.10: Petri Net for modelling Periodic perfect full proof test and $m - 1$ partial proof tests in the test interval of full proof tests

Similarly, after a failure event due to λ_{DU}^F (hidden failures only revealed by full proof tests), the transition t_6 is fired and a token is released to place p_{10} .

When a partial proof test takes place (the transition t_2 has been fired) a token is present in place p_5 , therefore, if there is a hidden failure due to λ_{DU}^P , transition t_4 is fired; or, if there is no hidden failures due to λ_{DU}^P , the transition t_5 is fired. Nonetheless, a token is released to place p_8 . Transitions t_{8a} and t_{8b} are constrained by the predicates $F_1 \cup F_2 = true$ and $F_1 \cap F_2 = false$, respectively. At this point, a decision is made whereas repair actions take place or a new testing interval starts. The variables F_1 and F_2 are used to indicate if a failure has occurred and repair actions should take place. For example, F_1 and F_2 are set to *true* when hidden failures has been revealed. See transitions t_4 and t_{10} in figure (5.10).

When the transition t_2 is fired a token is also released to place p_9 . However, transition t_9 or t_{10} is not fired until the number of tokens in place p_9 are equal to m , meaning that a full proof

test is taking place; If hidden failure occurs due to λ_{DU}^F (represented by a token in place p_{10}), the variable F_2 is set to *true* and repair actions take place, because the predicate in transition t_{3a} is met.

After repair actions, transitions t_{11a} and/or t_{3a} are fired *if and only if* failures due to λ_{DU}^P and λ_{DU}^F had occurred, respectively; otherwise, the tokens in places p_4 and p_3 are removed through transitions t_{11b} or t_{3b} avoiding the increase of the number of tokens in places p_1 or p_6 . The decision taken in transitions t_{11b} and t_{3b} are constrained if failures have occurred. For example, the variable F_1 is set to *true* when a hidden failure due to λ_{DU}^P is revealed and set to *false* after a repair.

We have used several assertions (e.g., $!F_2 = false$) and predicates (e.g., $?F_1 = true$). They help to reduce the number of places and the complexity the Petri Net.

It is straightforward to show that the places p_1 and p_6 can be reduced to one place by establishing additional constrains (predicates) to the transitions t_1 and t_6 . The resulting Petri Net is described in appendix D.

The average unavailability of a component modelled by the Petri Net in figure (5.10) can be found by using the Petri Net in figure (5.7). Figure (5.7) requires the two variables (e.g., U_1 and U_2) to enable the transitions t_1 or t_2 . For example, the variable U_1 is toggled to true when failure due to λ_{DU}^P occurs, and it is toggled to false when this type of failure is repaired. Now we can use $Out = (U_1 \cup U_2)$ in the Petri Net in figure (5.7). If the component is unavailable, $Out = 1$. We recall that the average unavailability is given by the mean marking of the place p_2 in figure (5.7).

Modelling hidden failures that are never revealed

For modelling hidden failures that are never revealed by using Petri Nets, we only requires two places and one transition. Figure (5.11) shows the simple Petri Net that can be used for this purpose. The transition t_1 is fired only once, meaning that a failure event with failure rate $\lambda_{DU}^N = (1 - TCF_{max}) \cdot \lambda_{DU}$ has occurred.

In summary, for modelling a component that is subject to imperfect full proof test, the Petri Nets in figures (5.9) and (5.11) are used together. In this case the failure rate of hidden failures revealed during a full proof test becomes equal to $\lambda_{DU}^F = TCF_{max} \cdot \lambda_{DU}$.

For modelling a component that is subject to imperfect full proof test and partial proof test,

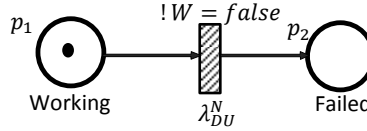


Figure 5.11: Petri Net for modelling hidden failures that are never revealed

the Petri Nets in figure (5.10) and (5.11) are used together. In this case the failure rate of hidden failures revealed only during a full proof test becomes equal to $\lambda_{DU}^F = (\text{TCF}_{\max} - \text{TCF}) \cdot \lambda_{DU}$.

By using the combination of these Petri Nets (e.g., Figures (5.9), (5.10), (5.11)), we can build a Petri Net driven by virtual RBD as in figure (5.8). The resulting Petri Net considers independent repair teams, which it is usually not the real case. In order to find a realistic average unavailability of the safety system that models a single repair team, we need to modify the Petri Net in figure (5.10). The *new* Petri Net is shown in figure (5.12). The Petri Net in figure (5.12) was built by considering the following:

- Only one transition like t_2 with a delay equal to τ/m that models the periodic proof test is required. Therefore, arcs should connect transition t_2 to each place that is used to indicate that a test is ongoing (e.g., p_5 and p_9)
- Only one place like p_8 is required (For example in the first component).
- Only one transition like t_{8a} is required, and its predicate must contain all variables that indicates that a hidden failure has occurred. (e.g., $?F_1 \cup F_2 \cup F_3 \cup \dots \cup F_n = true$). If only one of n failures occur, repair action takes place.
- Only one transition like t_{8b} is required, and its predicate must contain all variables that indicates that a hidden failure has occurred. (e.g., $?F_1 \cap F_2 \cap F_3 \cap \dots \cap F_n = false$). If none of n failures has occurred, a new test interval starts.
- Only one transition like t_7 is required. Therefore, arcs should connect transition t_7 to places like p_{11} and p_3 .

As we can notice, the place p_8 is not required in $n-1$ components of the system to be modelled. Figure (5.12) shows the resulting Petri Nets. The Petri Net in figure (5.12a) is repeated for

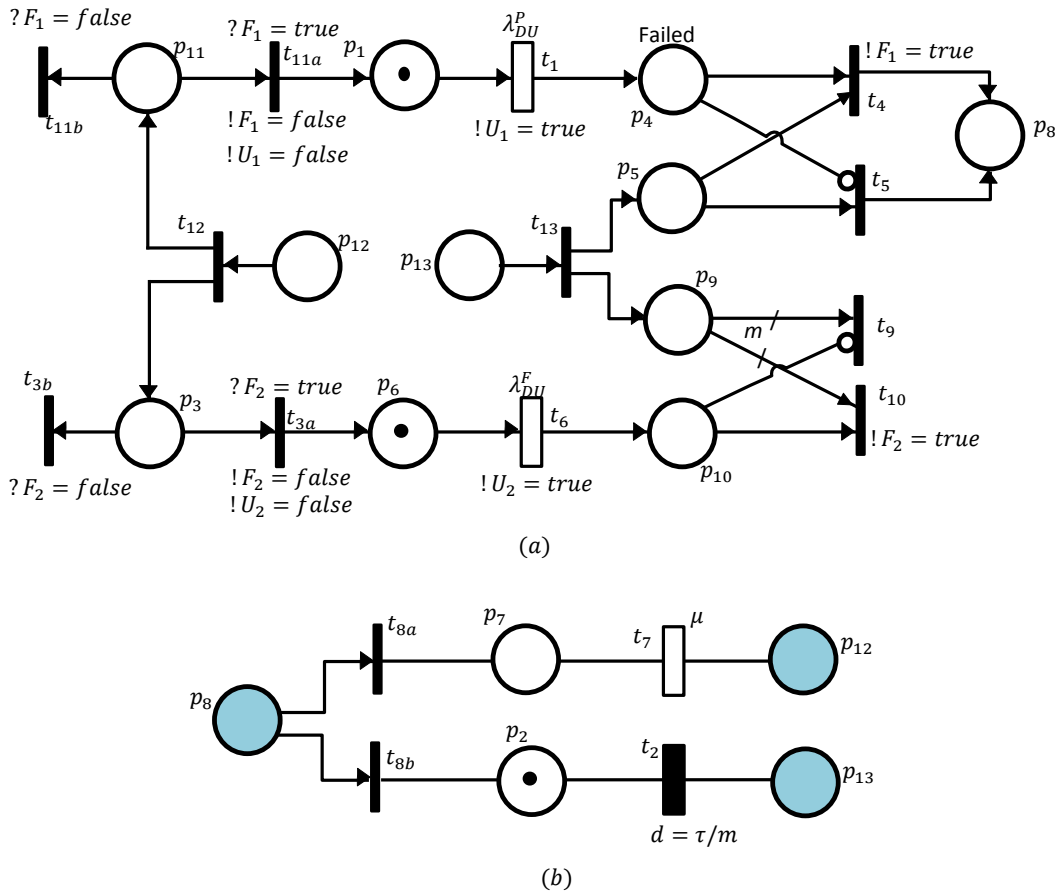


Figure 5.12: Petri Nets to be used in Petri Nets driven by RBD

each component of the system that is subject for partial proof test (without p_8 ; check the second item in previous paragraphs). The Petri Nets in figure (5.12b) models the delay of partial tests and the repair. Notice the circles in blue colour, these are *shortcuts* used to connect to places with the same label (e.g., p_{12}). For each component added in the Petri driven by RBD, a shortcut should be added for the repair and the test actions. In appendix D we present a simple example Petri Net driven by RBD.

5.6 Method Comparison

We have presented four approaches for assessing the unavailability due to time related failures. These approaches are the use of (i) the structure functions of RBD, (ii) Analytical Formulae de-

rived from Fault Tree analysis, (iii) time dependent unavailability based on Fault Tree analysis (which it is another way of presenting RBD), and (iv) Petri Nets which uses Montecarlo Simulation to perform the analysis.

Amongst the known techniques available for reliability analysis (see e.g., ISO/TR-12489, 2013) we have not discussed Markov analysis. This is because we are interested in modelling the effect to proof testing (e.g., of safety systems), and because proof tests are carried out a deterministic time instants (Brissaud and Oliveira, 2012), transition from failed states (under the assumption that the failure is repaired) are not exponentially distributed, which is the foundation for Markov chains (Rausand and Høyland, 2004). In this case, multi-phase Markov models are more proper to include the effect of periodic proof testing (ISO/TR-12489, 2013).

The methods discussed in this chapter may be compared taking into account two main factors (see e.g., Brissaud and Oliveira, 2012). Features of the model and of the analysis.

5.6.1 Models Relationship

RBD are built in term of functions and it may lead to unknown effects of failure of components in the system. This disadvantage can be overcome by the use of Fault Tree Analysis. However, both *RBD* and *FTA* are *static models* and therefore the dynamics of the system cannot be described. On the other hand, *Petri Nets* are suitable for modelling the dynamics of the system and they can be easily built by using virtual *RBD*, *Virtual RBD* that can be drawn from *FTA*. The size of the *virtual RBDs* is almost equal to number of components of the system. This make the graphical representation of the model easy to read and understand it, even whit the inclusion of *Petri Nets*. The use of *Petri Nets* driven by virtual *RBD* makes the model less prone to modelling errors because the component's *Petri Net* have the same structure.

5.6.2 Analysis

In the previous paragraph we discussed the main relationship amongst the techniques used in this report and how we can end using *Petri Nets*. However, each technique (the technique itself) has its own way for doing the analysis. As we are interested on the average unavailability of safety systems subject to periodic full proof test, partial proof test, imperfect proof test, we proposed a

model (e.g., see Eq (5.3)) and we incorporated the proposed model in the use of each technique.

As mentioned, the analytical solution for finding the total availability of the system from the RBD⁶ and using the proposed model requires the use of software. It can be a limitation since foundation in programming is essential for understanding the model and avoid the use of the algorithm that we presented as a "black box". However, the correct use of the proposed algorithm provides an exact solution and a very good illustration of the instant unavailability by including the effect of proof tests (perfect, partial or imperfect). Other advantage of the proposed approach is the flexibility to include other probability distributions. For example, we can use the availability function by assuming the Weibull distribution in the same way that we used the exponential distribution.

We also discussed the use of analytical formulae derived from the minimal cut set theory. As mentioned, with this approach we cannot model the effect of imperfect proof testing and several approximations are needed to compute the average unavailability. The "difficult" part is to find the minimal cut sets; but software tools are available for this matter (e.g., CARA). From the package CARA we can also compute the average unavailability based on the upper bound approximation (Rausand and Høyland, 2004) which is less conservative than the result that can be obtained from Eq. (5.5). The main disadvantage of this approach is that it is limited to failure rates exponentially distributed.

Petri Nets driven by virtual RBD are easy to build and the technique is very flexible. Different factors like demands and test duration may be included. The limitation of this technique lies on the package capabilities and the ability of the analyst, mainly due to systematic errors. Brisaud and Oliveira (2012) claim that the only drawback of this technique is the time required to perform the analysis.

⁶RBD that can be derived from a FTA

Chapter 6

Failure Modes and Reliability Data Analysis

6.1 Introduction

The identification of the modes in which a system may fail is as important as the technique used in the reliability analysis. In this chapter we discuss the main failure modes that may affect the major components of a WOCS. For each failure mode we present a short description and the effects due to proof testing.

6.2 Failure Modes

6.2.1 Fail to Operate - Valves

Fail to operate (open or close) is one the most common failure modes for process valves. Shutdown valves are the main type of valves used in safety systems, and in principle a shutdown valve should close in order to prevent hazardous events, making *fail to close* one of the most critical failure modes. Valves used in subsea production systems are usually fail safe and hydraulically operated valves. A subsea shutdown valve may not close because (i) it gets jammed, (ii) the supply of pressurized hydraulic oil¹ is not high enough to overcome the column of hydraulic oil from the (e.g.,) LRP to the sea level and (iii) or the return line that allows to bleed off the hydraulic oil is obstructed. The valve may get jammed because mechanical failure of the stem, the spring or

¹Even though the valves are designed to fail safely, the movement of the gate to the closed position may require extra force

the piston. (e.g., a broken part). A return line may be obstructed because pilot valves (usually pulse operated solenoid valves) does not switch or because other valves(e.g., manual valves) in the return flow line are closed. When the depth of installation of the LRP is deep enough that it avoids the spring to overcome the column of hydraulic oil, supply of pressurized hydraulic oil is required to help the spring for the displacement of the valve's gate to the closed position. If the pressure in the hydro-pneumatic accumulators² is not high enough, or the supply line is obstructed, the valve may fail to close on demand, or at least it closes slowly, which it is other failure mode that may have negative effects for the fulfilment of safety functions.

Fail to open for shutdown valves may not be critical regarding to safety issues. However, fail to open for the surface tree wing valve used for the PSD function is a critical failure mode. This type of failure for shutdown valves may have negative economic impacts due to delays, for example during a proof testing. In this case, in order to open the valve, pressurized hydraulic oil is supplied from the surface, therefore, fail to open may be strongly related to failure of the HPU.

6.2.2 Fail to Operate - Shear Seal RAM

The actuator of a SS-RAM, functions similarly as the actuator of gate valves(metal blocks are slid due to release of high hydraulic pressure); In this case, the actuators of the SS-RAM are fitted with RAMS that are designed to shear (cut) a coiled tubing, to stop the flow of hydrocarbons and to provided seal. Fail to close and fail to cut are referred as the same type of failure for SS-RAMs. However, fail to close is properly used to refer to the fact that a SS-RAM does not close when there are not running tools into the wellbore, on the other hand, fail to cut, to refer the fact that the SS-RAM is not able to close by shearing the coiled tubing or wireline running down the wellbore. In both cases, the SS-RAM may fail to close because of mechanical failures in the internal parts of one or both cylinder assembly that comprises the actuator of a SS-RAM. A SS-RAM may also fail to close if the supply of hydraulic oil is insufficient, or mechanical failure of the hydraulic assembly of the actuator. Fail to cut of the SS-RAM may occur due to collapse or crush the ends of the blades while shearing. (Van Winkle, 2013)

²Hydro-Pneumatic accumulators are used to store hydraulic energy by pressurizing an inert gas

6.2.3 Leakage

Leakage (internal or external) is a failure mode that may be present in all components that are designed to isolate two fluid or to connect two (e.g., metal) bodies. Leakage is mainly a failure due to degradation of the sealing devices (e.g., an O-ring, a gasket) placed between the two surfaces. The sealing devices are classified into dynamic and static. Degradation is affected by pressure, temperature, surfaces to be joined, surface roughness, vibration, chemical attack, compression set, plastic deformation, fluid properties (Piff, 2011). Degradation is also caused by stress or fatigue, erosion or corrosion (Haarberg, 2011). Other factors that may lead to leakage are (i) improper maintenance (replacement) of this components, (ii) material defects of the sealing devices, (iii) sand deposits, (iv) hydrates formation, and (v) formation of paraffin wax.

Leakage may be present in all major components of a WOCS (e.g., valves, pilot valves, umbilical, SS-RAM, housings, housing connectors). Leakage may lead to hazardous events or higher consumption of fluids (e.g., hydraulic oil).

A subsea production systems will experience leaking problem during its lifetime (NORSOK-D010, 2013), therefore, overcoming the leakage problems is one of the challenges for designer and operator of subsea production system.

6.2.4 Electronic and Electrical Failures

The failure mechanism of electronic and electrical (EE) failures of circuit boards for controlling the solenoid valves in the WOCM and EE failures of the other electronic components (pressure transmitters, flow transmitters) are related to excess of temperature, excess of current and/or voltage, corrosion and stress. EE failures may lead to erratic reading of operating parameters, or erratic outputs (commands) signals. Erratic signals may lead to unintended development of the safety functions and loss of communication from the subsea equipment and the top side.

6.3 Effects of Proof Testing

The main objective of the proof testing is to reveal (and repair if it is necessary) failure modes as described in the previous sections. A component usually has more than one failure mode and

a proof test in carried out to reveal all of them or at least a fraction. On one hand, proof testing has positive effects (revealing the failure mode is obviously the main one): movement and lubrication of a mechanical part, stressing of electronic components between normal ranges of operations, in general physical stimulation is necessary for good performance of the system. On the other hand, physical stimulation has a significant correlation with wear, stress and fatigue. Therefore, How much "stimulation" is needed?. The answer of this question depends on factors like operating time, frequency of maintenance (inspections and replacement of wear items), operating parameters, component's material, safety requirements.

6.3.1 Reveal-Ability

Some failure modes are easily revealed and they do not require sophisticated means for the revealing process. For example, fail to operate is found simply by sending commands to the actuating component. On the hand, testing for leakage requires closed chambers and maybe a different fluid. Other failure modes, like fail to sharing never is revealed because it is a destructive test. In order to measure how much a failure mode is revealed, a proof coverage factor is used. (e.g., TCF) and it is equal to one if the failure mode is revealed. The coverage factor of fail to operate depends on how much the valve or SS-RAM travels from one position to the other.

We recall that the coverage factor used in the reliability analysis concerns to proof tests of specific components rather than component's failure modes. However, the coverage factor of failure modes is used to estimate the coverage factor of proof tests as explained in chapter 4.

6.4 Reliability Data Analysis

An FMEA is used to gather and summarize all information of failure modes of the different components of a system. This information is of high quality if different types of data are analysed. For example, we need maintenance data in the form of records; technical data in the form of datasheets, drawings (e.g., electrical, hydraulic), functional block diagram for the understanding of the functionality of the system; operational data with operational procedures, operational parameters under control (e.g., pressure) for assuring high performance of the equipment.

In addition, and equally important, we need reliability data for correct estimation of ability

of the system to function over the time (reliability prediction) without failures and consequent avoidance of undesired events, especially for safety-critical systems.

Reliability data is mainly classified as generic, plant specific and based on expert judgment (Rausand, 2014). Several databases are available for generic reliability data. See for example Rausand (2014) for a list of the most used databases. Plant specific reliability data is the most proper data, but often it is not available in usable form (e.g., without statistical analysis) or very small that it does not allow us to estimate with enough level of confidence.

A common characteristic of most reliability sources is that the failure rate is assumed to be constant (e.g., based on exponential distribution or Poisson process). This assumption is valid for electronic components ((Fuqua, 1987)). For mechanical components, modelling an increasing failure rate is more accurate. In addition, time independent factors that influence the failure rate should also be included. Brissaud et al. (2011) proposes a model based on the Weibull distribution and the Cox proportional hazard model for modelling the time-dependent failure rate and influencing factors. Factor like design factors, factors related to manufacturing, factors induced in the installation and maintenance. Factors or stressors like flow rate, sand content are included in the Cox regression model. The introduction or exclusion of factor in the Cox-model lead to different failure rates.

Chapter 7

Reliability Calculation of the WOCS

7.1 Introduction

In chapter 5 we described four approaches for estimating the PFD_{avg} . The proposed model to the time dependent availability (e.g., $A(t)$) takes into account that components may be subject to partial proof tests and imperfect proof test (see e.g., Eq. 5.3). In chapter 4, we presented the approach for estimating the test coverage factor to be used for modelling partial and imperfect proof testing. In chapter 8 we discuss the major contributors to the unavailability of a safety system and we presented the model for calculating the total average unavailability \bar{U} .

In this chapter we present the results to the PFD_{avg} for the WOCS by using the approaches discussed in chapter 5. A step-by-step method for computing the reliability measure of a WOCS is included. Finally, some comments on the results are provided.

7.2 Method

7.2.1 Step 1. To Understand the System's Functionality

The first step is to understand the functionality of the system. It is very important to know each component of the system, inputs, outputs, operating parameters, operational ranges, boundaries, etc. It allows us to understand how the system functions, but most important how the system may fail. We presented a description of the WOCS in chapter 2.

7.2.2 Step 2. To Develop a FTA > Draw a RBD

Given that a Fault Tree is built thinking in terms of failures, the ultimate RBD(s) shall be drawn based on the FTA(s). Notice that a system may be designed to develop more than one function. It means that a RBD is required for each function. For example, for the WOCS we have three RBDs, one for each safety function: PSD, ESD, EQD. These functions were described in chapter 2.

7.2.3 Step 3. To Develop a FMEA

The basic events identified on the FTA are usually components' failures. Those components are the critical components to be included in a FMEA study. An exhaustive analysis of the failure modes for each component should be carried out; it will allow us to estimate a realistic test coverage factor(s) to be used in the reliability prediction.

We have not provided an FMEA for the WOCS described in chapter 2, however, we have discussed the main failures modes for the major components of the WOCS (see chapter 6). A discussion like we presented in chapter 6 shall be carried out and the information shall be summarized in an FMEA worksheet like in appendix B.

7.2.4 Step 4. To Estimate the TCFs

The information collected in the FMEA developed in the previous step is used to estimate the TCFs. In chapter 4, we exemplified how to estimate the coverage factors for both the TCF and the TCF_{max} for the SS-RAM. In the same way, we estimate TCF and TCF_{max} for the other components used for fulfilment of the WOCS's safety functions. In table (7.1) we present the estimated values for TCF and TCF_{max} . In appendix D we present detailed calculations for the test coverage factors.

7.2.5 To Compute the PFD_{avg}

The only parameter that is missing for the calculation for the PFD_{avg} is the total failure rate of the components. Assuming that the failure modes are disjoint, the total failure rate λ_{DU} of the components is equal to the sum of the failure rates of its failure modes. In appendix E we present detailed information of the failure modes and failure rate for the components. When

Component	Total λ_{DU} ($\cdot 10^{-6}$)	TCF (Partial Test)	TCF _{max} (Full Test)	Safety Functions
Pushbuttons	0.3	100%	100%	PSD,ESD,EQD
Power Supply	39.93	100%	100%	PSD,ESD,EQD
WOCS's PLCs	4.94	100%	100%	PSD,ESD,EQD
Pulse Operated Solenoid Valve	7.01	100%	100%	PSD
STWV	2	100%	100%	PSD
Umbilical	3.6	100%	100%	ESD,EQD
SS-RAM	46.44	64.3%	86.6%	ESD,EQD
PIV	17.42	94.3%	100%	ESD,EQD
CIV	0.22	86.0%	100%	ESD,EQD
AIV	0.22	86.0%	100%	ESD,EQD
XOV	0.22	86.0%	100%	ESD,EQD
DHSV	3.2	80.5%	100%	ESD,EQD
RRV	0.22	86.0%	100%	EQD
RAIV	0.22	86.0%	100%	EQD

Table 7.1: Summary of the Test Coverage Factors TCF and TCF_{max}, and failure rates for the components used for fulfilment of the WOCS's safety functions

some reliability data was not available (e.g., specific failure rate per failure modes), we assume some values. The failure rates λ_{DU} are presented in table (7.1).

Figure (7.1) shows the saw curve - PFD(t), of the ESD function operating in normal mode (without wireline or coiled tubing). The curve was computed for 700 hours, However the PFD_{avg} corresponds to 14 days (336 hours). Given that the SS-RAM is connected in parallel with other components subject to perfect proof test every τ , the effect of imperfect proof test disappear (the time dependent probability failure on demand is reduced to 0). In appendix E the reader can find the code in MATLAB that was used to compute the PFD_{avg} for the WOCS's safety functions.

In table (7.2), we summarizes the results obtained to the PFD_{avg} from the methods explained in this report. For the WOCS there are components that are not perfectly tested, therefore, the results from formulae derived from FTA should not be considered because the requirements of this approach is that the proof tests are periodic and perfect. Nonetheless, *if* we assume that the SS-RAM is no subject to imperfect proof test, we can use the formulae approach.

The results from the structure functions of the RBDs and from the continuous PFD(t) derived

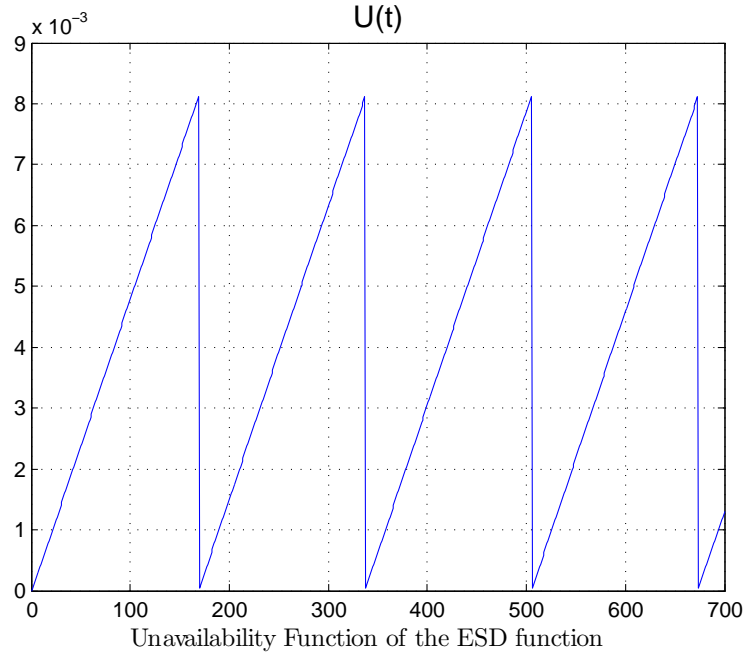


Figure 7.1: Saw curve (unavailability function) for the ESD function of the WOCS

Safety Function	RBD / FTA
PSD	0.0045
ESD	0.0041
EDQ	0.0047

Table 7.2: Results to the PFD_{avg}

from FTA are identical since the same formulas are used. In appendix G, we present the calculations of PFD_{avg} for ESD WOCS’s safety function by using the formulae approach. We can notice that the result is similar to the value computed by using the script developed in MATLAB. An important aspect of the computation of the PFD_{avg} by using the formulae approach (based on the minimal cut set theory) is that the component that are not redundant are the main contributors to total PFD_{avg} .

In chapter 8 we describe the major contributors to the total unavailability \bar{U} . The only contributor considered for the WOCS is the PFD_{avg} . The WOCS is available to function as a safety system during the proof test, and if repairs take place during a proof test, there are other means

to secure the well (e.g., the DHSV, Valves in the X-mas tree).

7.3 Comments and Discussion

The values computed for the PFD_{avg} are not as small as we expected. The values indicate that the SIL2 requirements are met. However, it is very important to take into account the assumptions that were made: amongst others, we have assumed, (i) normal mode of operation for the ESD and EQD functions, meaning that most valves are redundant, (ii) the effect of imperfect proof testing of the SS-RAM is null, and (iii) The RBDs are simplified. For example, there are some subsystems like the workover control module and the high-pressure unit that should be considered.

On the other hand, by adapting the policy of proof testing with short test intervals does not necessarily mean that the system becomes highly reliable. The length of the test interval should be selected by considering the major contributors to safety unavailability (see chapter 8), the demand rate of hazardous events, redundancy, and, the reliability data.

Regarding to the demand rate, we recall the specified classification of demand modes of operation (see e.g., section 3.5.16 IEC61508, 2010). Some authors argue that the specified distinction between low and high demand modes is arbitrary (Hokstad, 2014). We disagree with that statement. The frequency of demand is a relevant parameter when defining the proper reliability measure. It is not reasonable to carry out too frequent testing to safety systems that are seldom demanded, as well as, it is very risky to perform proof testing with long test intervals to systems subject to high demand rate.

The WOCS is a system operating in low demand mode and it is subject to short test interval. For the WOCS's architecture that we have studied, some components are not redundant and they have the highest failure rate compared with system's components. from the table in appendix G, we can see that those components have the highest probability of failure.

The PFD_{avg} is the proper reliability measure when the effects of imperfect proof testing are null or negligible. In addition, the PFD_{avg} is properly used when the frequency of demand is low (as specified by the IEC61508-4). When the demand rate is difficult to be established, other reliability measure may be considered.

In chapter 6 we discussed the effects of proof testing. It is reasonable to claim that the developing of control functions by safety systems should be considered as partial proof tests. This argument is valid when that the physical stimulation as a result of the developing of the control functions are between normal operating ranges.

Chapter 8

The Total Unavailability Function and the Optimization Problem

8.1 Introduction

The reliability of a safety system is measured by the average unavailability between test intervals (under the assumption that at the time instant of a full proof testing, the test is perfect). In addition to the PFD_{avg} , there are other contributors to the total unavailability of a system, that also depend on the test interval τ . In this chapter, we present the major contributors to the unavailability of a safety system.

We also show in this chapter that the total average unavailability which is function of τ (e.g., $\bar{U}(\tau)$) has a minimum value. It means that we can select the proper length of the test interval τ that leads to an average value of the unavailability that still meets the safety integrity requirements.

The starting point for selecting τ is the optimization of the unavailability function $\bar{U}(\tau)$.

8.2 Background

Probabilistic Safety Assessment (PSA) models based on fault tree analysis are widely used in the industry, especially in the nuclear sector (NEA/CSNI/R, 2002). However, fault tree models cannot incorporate some maintenance strategies, like staggered and sequential testing. Analytical

formulae derived from fault tree analysis *are* suitable when the system is subject to periodic and perfect proof testing. This *is* due to the static characteristic of the fault trees. Nonetheless, The effect of partial proof test can also be incorporated in models derived from fault tree analysis, as we have described in chapter 5.

The unavailability models derived from fault tree analysis only cover the PFD_{avg} of the system. A proper approach to include factors like testing time, repair time, human errors, unavailability due to "on-demand" failures, is the use of analytical unavailability models because, analytical formulae derived from fault tree analysis only consider the unavailability due to time related failures. (see e.g., WS-Atkins, 1998)¹.

The PDS method consider three major contributors to the unavailability: (i)the PFD_{avg} (ii)the unavailability due to testing and repair actions, and (iii) the probability of test independent failures P_{TIF} . In addition to this unavailability contributors, Chowhury and Varde (2011) consider also the effect of human errors during testing and the effect of degradation/ageing of the system component occurred during testing.

Similar approaches for determining the unavailability model can be found in the literature, and the main objective of those articles is to optimize the analytical function in order to find the optimal test interval. (see e.g., Lehtinen et al., 1984; Srinivas et al., 2012; WS-Atkins, 1998).

WS-Atkins (1998) develops a detailed analysis of major contributors to the unavailability of stand-by systems (e.g. a safety system) in order to present a procedure to determine the optimal test interval. Amongst the articles revised, WS-Atkins (1998) is the only author who consider the implications of variation of the test intervals.

8.3 The Analytical Function and the Optimization Problem

Why should we optimize the analytical function for the test interval, when the reliability measure is constrained by recommendations on safety standards?. The optimization problem should be addressed because (i)It allows us to be in the *safe side* from the analytical point of view; (ii)as we show in further paragraphs, the unavailability is insensitive up to twice the optimum test interval that leads to the minimum value of \bar{U} ; (iii)it helps to reduce too frequent proof

¹This report can be accessed by direct request to the Health and Safety Executive organization

testing by satisfying the risk criteria (e.g., average unavailability); and (iv) it allows to determine an estimate of the minimum related cost.

Let us consider a single component. By combining the major contributors to the total unavailability of a system, proposed by Chowhury and Varde (see e.g., 2011); WS-Atkins (see e.g., 1998); Hauge et al. (see e.g., 2013), the unavailability function is equal to the sum of the following terms:

8.3.1 Average unavailability between test intervals

For one single component, the unavailability due to time related failures is given by the well-known and often approximated quantity

$$\text{PFD}_{\text{avg}} \approx \frac{\lambda_{DU} \cdot \tau}{2} \quad (8.1)$$

where λ_{DU} is the failure rate of hidden failures, and τ is test interval. We recall that this term does not consider contributors to the unavailability like duration of the test, repair times, also that tests or repairs will not leave the system in a failed state, and the failure rate is exponentially distributed. Some methods for determining this unavailability for complex systems are discussed in detail in chapter 5.

8.3.2 Average Unavailability due to testing time

This unavailability due to testing time, \bar{U}_{tt} is given by the fraction between the testing time (T) and the total time between tests

$$\bar{U}_{tt} = \frac{T}{\tau} \quad (8.2)$$

The reader can notice that this term corresponds to the downtime due to functional testing/preventive maintenance presented in the PDS method (Hauge et al., 2013), when the operation of the system continues without protection during the proof test.

8.3.3 Average unavailability due to human errors

The unavailability due to human errors, \bar{U}_{he} , is proposed by (Chowhury and Varde, 2011) as

$$\bar{U}_{he} = F_h \cdot \frac{T}{\tau} \cdot N \quad (8.3)$$

where F_h is the fraction of human errors (e.g., No. of failures due to humans / total No. of system failures); the term $\frac{T}{\tau}$ was presented in the previous subheading, and N denotes the number of testing per year² (e.g., total hours in a year(8760) / τ)

8.3.4 Unavailability due to on-demand failures at the beginning of the test

On-demand failures are failures that are independent of time and occur as a result of a demand (WS-Atkins, 1998). For example, these failures are due to start-up loads. Consider for example an open electric circuit. When the circuit closes for some reason, the demand of current may cause that the power supply fails. In other words, during a start-up the component has a transition from a "cold" state to a "active" state. It is assumed that these kind of failures are found at the beginning of a test, therefore, they are repaired immediately. The unavailability due to on-demand failures is given by

$$\bar{U}_d = \frac{P_d \cdot MRT}{\tau} \quad (8.4)$$

where MRT denotes the mean repair time, and P_d is the probability of occurrence of this type of failure. Since they are independent of time, a natural estimate of P_d is equal $\frac{N_f}{N_d}$, where N_f is the number of failures recorded, and N_d is the number of system demands.

8.3.5 Unavailability due to failures during testing

If there are failure modes that are introduced during the testing time with (active) failure rate λ_a , the unavailability due to this kind of failures is given by

$$\bar{U}_a = \frac{P_a \cdot MRT}{\tau} \quad (8.5)$$

²For the WOCS, N should be computed for the operating time.

where P_a is the probability of occurrence of λ_a . The probability P_a is given by $\lambda_a \cdot T$

8.4 The Analytical Function for the Total Unavailability

By assuming that the contributors to the total unavailability are independent, the combination of the major contributors described from (Eq. (8.1) to Eq. (8.5)) lead to the following function

$$\bar{U}_{TOT} \approx \text{PFD}_{\text{avg}} + \bar{U}_{tt} + \bar{U}_d + \bar{U}_a \quad (8.6)$$

$$\bar{U}_{TOT} \approx \frac{\lambda_{DU} \cdot \tau}{2} + \frac{1}{\tau} \cdot (T + P_d \cdot \text{MRT} + P_a \cdot \text{MRT}) \quad (8.7)$$

The reader can notice that the contributor due to human errors cannot be added since it is not independent from the unavailability due to testing time. We omit to include this term by assuming that its contribution is negligible.

We may also add the unavailability due to P_{TIF} to the total unavailability in (8.7).

By optimizing 8.7 with respect to τ (e.g., $\frac{d(\bar{U}(\tau))}{d\tau} = 0$), τ becomes

$$\tau_{opt} = \sqrt{\frac{4 \cdot \rho}{\lambda_{DU}}} \quad (8.8)$$

where

$$\rho = T + P_d \cdot \text{MRT} + P_a \cdot \text{MRT} \quad (8.9)$$

τ_{opt} in 8.8 is similar to the result obtained by (Vaurio, 1995). According to (Vaurio, 1995), τ_{opt} derived from the unavailability function (e.g., (8.7)) should not be used as the only criterion for selecting the frequency of testing.

As mentioned, the average unavailability is insensitive to the test interval from approximately $\tau_{opt}/2$ to $2 \cdot \tau_{opt}$, therefore, it is acceptable to select the maximum $t_{opt}^* = 2 \cdot t_{opt}$ as the optimum test interval. This is easily understood by analysing the resulting curve from (8.7).

Figure (8.1) was constructed by assuming a failure rate $\lambda = 4 \times 10^{-6} [\text{hour}]^{-1}$, $\rho = 12 \text{hours}$. Hence, $\tau_{opt} \approx 3460 \text{hours}$. The data in the figure (8.1) shows the value of \bar{U} is very similar in the interval $\tau_{opt}/2$ to $2 \cdot \tau_{opt}$. As mentioned, by finding the optimum test from the average unavailability function, it allow us to estimate the minimum related cost. The total cost per time unit

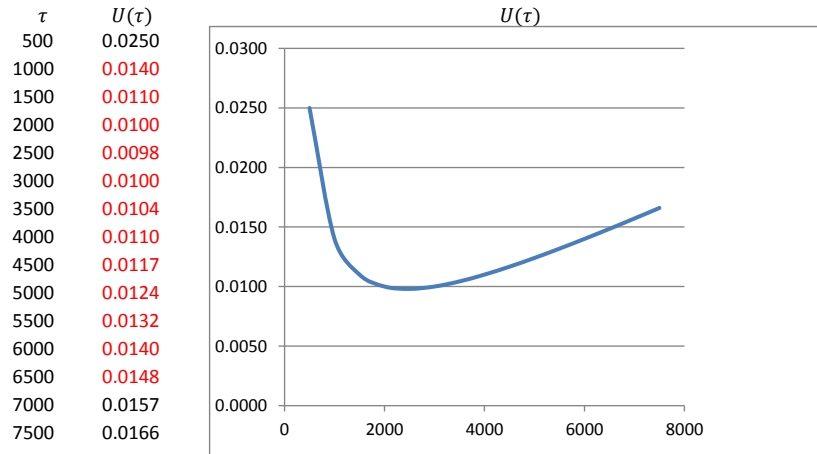


Figure 8.1: The unavailability function when considering all major contributors

for system with constant failure rate and safety functions is given by (Vatn, 2013)

$$C(\tau) = \frac{C_P}{\tau} + C_R \cdot \left(\lambda_{DU} - \frac{\lambda_{DU}^2 \tau}{2} \right) + C_H \frac{\lambda_{DU} \tau}{2} f_D \quad (8.10)$$

where C_P is the preventive maintenance cost due to the proof test and C_R concerns to repair related cost (corrective maintenance costs) and C_H indicates the hazard related costs, and f_D corresponds to the rate of undetected demands (Vatn, 2007).

The minimum estimated cost can be found by inserting (8.8) into 8.10. Figure (8.2) illustrates the relationship between the average unavailability function, the cost function and the optimum test interval.

The estimation of the hazard relates cost is a challenge. The impact of hazardous events may be catastrophic and the magnitude of the consequences are not possible to estimate accurately.

The optimization problem may also be solved by the use of advanced computer algorithms like genetic algorithm (GA)³ or Monte Carlo Simulation. According to Chowhury and Varde (2011), if the problem encircles multiple objectives (e.g., unavailability, cost, production), the implementation of a GA is a good technique because its flexibility and robustness.

³Genetic algorithms are computational tools founded on a direct analogy with the physical evolution of species (Goldberg, 1989)

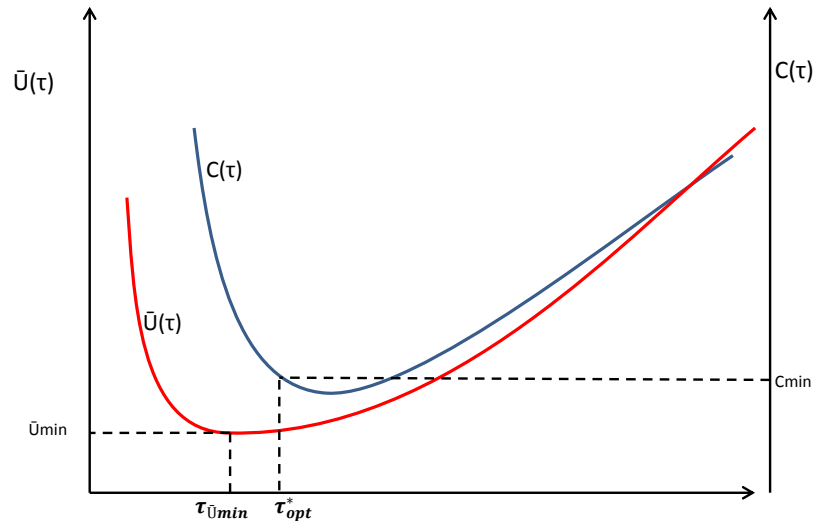


Figure 8.2: Optimal test frequency of proof test by minimizing the unavailability function and the cost function

When reliability data is not available, the expert's judgment seems to be the best approach. For example, Abrahamsen and Røed (2012) present a framework for selection of the test method and test interval for safety critical valves with limited reliability data.

Chapter 9

Summary, Conclusions and Further Work

9.1 Summary and Conclusions

We found that little work has been done on mathematical models for modelling the effects of short test intervals. This topic is barely discussed in the information available. When the length of the test interval is short and it has negative impacts to the system's reliability, the problem is addressed by optimizing the unavailability function that depends on the test interval τ .

The optimization problem requires the analysis of the major contributors to safety unavailability. Amongst these contributors, the PFD_{avg} , unavailability due to testing time, unavailability due to human errors, unavailability due to failures introduced during proof tests, are taken into account.

When considering the effect of imperfect and partial proof testing, two main approaches are available: (i) the use the test coverage factor and (ii) and the addition of a constant contribution to the safety unavailability in order to compensate failures that are not revealed by a proof test. In both cases, a perfect proof test takes place at the time instant of the full proof test.

It is recognized that the reliability of a system is a function of the test interval τ and the failure rate λ . In theory, short test intervals and low failure rate lead to high reliability (e.g., low PFD_{avg}). This is *true* if the proof test does not contribute to unnecessary wear, degradation or deterioration of the components and introduction of failures due to human interaction.

High reliability also depends on the reliability considerations during the all design phases of the system. In order to build high reliability into the system, a well-defined reliability engineer-

ing programme should consider amongst other factors, understanding of the failure modes of the system, the required satisfactory performance (e.g., the target reliability measure), redundancy, the operating environment and conditions, the life time of the system and the maintenance policy.

The FMEA becomes a design tool that allows to system designers, operators and maintenance personnel to identify potential system weaknesses in order to do modifications during early design phases, establish good operating and maintenance practices and policies.

We discussed four methods for the reliability assessment of the WOCS. As a support to the reliability assessment, the main components of a WOCS were described; its operational and maintenance philosophy were discussed with personnel with experience in this matter, and the outcome was include as part of the description of the system. This description allowed us to describe the safety functions of the WOCS. The RBDs derived from the description of the safety functions were used for reliability calculations.

The models available when modelling the effect of imperfect proof test do not consider random hardware failures that are never revealed by a proof test. This kind of failures lead to an increasing unavailability over the time. We introduced the concept of a maximum coverage factor (TFC_{max}) that in conjunction with the generally accepted *proof test coverage* factor (that we have called TCF), we proposed a mathematical expression that models the effect of both partial proof tests and imperfect proof tests due to random hardware failures. The model is derived under the assumption that the failure rate is exponentially distributed.

Taking into account the proposed model, the methods discussed for the reliability assessment (e.g., computation of the PFD_{avg}) were: (i) the structure function of a RBD, (ii) simplified formulae derived from fault tree analysis, (iii) time dependent unavailability by using Fault Trees and (iv) Petri Net models. With exception of (ii), the methods consider the use of the both the TCF and TCF_{max} .

An algorithm in MATLAB was developed for the use of the methods (i) and (iii), the package GRIF was used for simulating the Petri Net models proposed in this master's thesis and Microsoft Excel[®] spreadsheets were used to compute the simplified formulae.

The simplified formulae approach is not a proper technique when the system is subject to imperfect proof testing. In this case, we recommend to use the proposed model (the mathe-

mathematical expression for the time dependent availability) which gives an exact solution for PDF_{avg} calculations. The proposed Petri Nets models give very similar results when we simulate a single component subject to perfect, partial or imperfect proof tests. It was not possible to simulate the Petri Net models driven by RBDs, because the package GRIF did not follow the logic for computing the average unavailability.

A simplified procedure for the estimation of the coverage factors was proposed. It is based on the outcomes of an FMEA, therefore, realistic results for both TCF and TCF_{max} depend on a targeted and exhaustive FMEA. We estimated these coverage factors for all components required for fulfilment of the safety functions of the WOCS. However, limited information about the failure rate per failure modes can be found in the databases. This information is especially limited for equipment used for drilling and WO than for topside side equipment. Therefore, the coverage factor presented for the components involved in the development of the safety functions, possibly might not be as accurate as preferred.

When a component is a single point of system's failure, and this component is subject to imperfect proof tests, the PFD_{avg} should carefully be considered as the reliability measure of safety related system because it increases over time. In fact, in this situation, any reliability measure changes towards a low reliability (e.g., the frequency of failure increases, the mean time between failures reduces, and so on). When the system has redundant components, (especially when the redundant channels are ≥ 3), the contribution to the unavailability is considerable small if only one channel (e.g., $1oo3$) is required to fulfil the safety function.

The computations of the PFD_{avg} for the safety functions of the WOCS fulfil the SIL 2 requirements as described in the standard IEC61508. The *main* aspects that leads to a constant PFD_{avg} over the time are: (i) It is assumed that perfect proof tests take place, (ii) despite the fact that the SS-RAM is subject to imperfect proof test, it has redundant final elements that are assumed to be perfectly tested, (iii) for the EQD function, it is assumed that decoupling action of the marine riser from the lower riser package functions perfectly, (iv) the PFD_{avg} calculations for the ESD and EQD functions correspond to the normal mode, when the production line is not obstructed with running tools and most valves are redundant, and (v) we used simplified RBDs.

We conclude that the PFD_{avg} is the proper reliability measure when the effects of imperfect proof testing are null or negligible. In addition, the PFD_{avg} is properly used when the frequency

of demand is low. When the demand rate is difficult to be establish, other reliability measure may be considered.

We also conclude that it is reasonable to claim that the developing of control functions by safety systems should be considered as partial proof tests. This argument is valid when that the physical stimulation as a result of the developing of the control functions are between normal operating ranges.

Finally, the average unavailability of a safety system should not only consider the PFD_{avg} . We discussed most of the contributors to the total unavailability, and a mathematical expression for the total average unavailability was derived. This function was used to exemplify how to find the optimal test interval and to estimate the minimal related cost. This approach is relevant, when the safety system is unavailable during the testing time.

9.2 Further Work

Reliability data is the cornerstone for the estimation of the coverage factors. Proper reliability data gathering methods or process should be enhanced.

Exhaustive description of the failure modes of the components involved in the development of the WOCS's safety functions need to be examined. It is strongly related with the process of gathering reliability data.

Generalization of a model for computation of the PFD_{avg} of *koon* architecture by using the proposed model for computing the time dependent availability is recommended.

A research for defining a new reliability measure when is not possible to distinguish between low and high demand modes of operation is required.

Bibliography

Abrahamsen, E. and Røed, W. (2012). A framework for selection of test method and test interval for safety critical valves in situations with limited data. *Reliability: Theory & Applications*, 7(1).

ACM (2001). Acm automation. how partial stroke testing helps keep a high sil rating? *Practical Solutions for Today's HSE Challengers*.

Aguilar M., W. (2013). Reliability assessment of safety instrumented systems with imperfect proof testing. *Project Thesis, MSc in Reliability, Availability, Maintainability and Safety at the Norwegian University of Science and Technology*. Available online at www.ntnu.edu/web/ross/books/sis/chapt11.

Brissaud, F, Barros, A., and Bérenguer, C. (2010). Probability of failure of safety-critical systems subject to partial tests.

Brissaud, F, Barros, A., and Bérenguer, 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(4):426–436.

Brissaud, F, Lanternier, B., and Charpentier, D. (2011). Modelling failure rates according to time and influencing factors. *International Journal of Reliability and Safety*, 5(2):95–109. cited By (since 1996)2.

Brissaud, F and Oliveira, L. (2012). Average probability of a dangerous failure on demand: Different modelling methods, similar results. volume 8, pages 6073–6082. cited By (since 1996)0.

- Bukowski, J. and Van Beurden, I. (2009). Impact of proof test effectiveness on safety instrumented system performance. pages 157–163.
- Chowhury, S. and Varde, P. (2011). Surveillance test interval optimization for nuclear plants using multi objective real parameter genetic algorithms. *International Journal of Reliability, Quality and Safety Engineering*, 18(2):159–177. cited By (since 1996)0.
- Fuqua, N. (1987). *Reliability Engineering for Electronic Design*. CRC Press, Hoboken, NJ, 1st edition.
- Haarberg, S. (2011). Condition monitoring on subsea installations. *MARINTEK Report*, 93:37. Available online at <http://www.navsea.navy.mil/nswc/carderock/src/mechrel/products/handbook/CHAPTER3RevG.pdf>.
- Hauge, S., Hokstad, P., Langseth, H., and Oien, K. (2013). Reliability prediction method for safety instrumented systems. *SINTEF*.
- Hauge, S. and Onshus, T. (2013). Reliability data for safety instrumented systems - pds data handbook. *SINTEF*.
- Hokstad, P. (2014). Demand rate and risk reduction for safety instrumented systems. *Reliability Engineering and System Safety*, 127:12–20. cited By (since 1996)0.
- IEC60812 (2006). Analysis techniques for system reliability. procedure for failure mode and effects analysis (fmea). *Geneva: International Electrotechnical Commission*.
- IEC61508 (2010). Functional safety of electrical/electronic/programmable electronic safety-related systems, part 0-7. *Geneva: International Electrotechnical Commission*.
- IEC61511 (2003). Functional safety: Safety instrumented systems for the process industry sector, part 1-3. *Geneva: International Electrotechnical Commission*.
- ISO13628 (2005a). Petroleum and natural gas industries - design and operation of subsea production systems - part 6: Subsea production control systems. *Switzerland: International Organization for Standardization*.

- ISO13628 (2005b). Petroleum and natural gas industries - design and operation of subsea production systems - part 7: Completion/workover riser systems. *Switzerland: International Organization for Standardization.*
- ISO/TR-12489 (2013). Petroleum, petrochemical and natural gas industries – reliability modelling and calculation of safety systems. *Switzerland: International Organization for Standardization.*
- Jin, H. and Rausand, M. (2014). Reliability of safety-instrumented systems subject to partial testing and common-cause failures. *Reliability Engineering and System Safety*, 121:146–151.
- Jin, J., Zhao, S., and Hu, B. (2011). Test coverage of the safety instrumented system. pages 4228–4231.
- Kumar, M., Verma, A., and Srividya, A. (2008). Modeling demand rate and imperfect proof-test and analysis of their effect on system safety. *Reliability Engineering and System Safety*, 93(11):1720–1729.
- Lehtinen, E., Mankamo, T., and Pulkkinen, U. (1984). Optimum test interval of closing valves. *NUCL. ENGG. DES.*, 81(1 , 1984):99–104. cited By (since 1996)0.
- Lundteigen, M. and Rausand, M. (2007). The effect of partial stroke testing on the reliability of safety valves. volume 3, pages 2479–2486.
- Lundteigen, M. and Rausand, M. (2008). Partial stroke testing of process shutdown valves: How to determine the test coverage. *Journal of Loss Prevention in the Process Industries*, 21(6):579–588.
- NEA/CSNI/R (2002). The use and development of probabilistic safety assessment in nea member countries. *NUCLEAR ENERGY AGENCY COMMITTEE ON THE SAFETY OF NUCLEAR INSTALLATIONS.*
- NOG-070 (2004). Application of iec 61508 and iec61511 in the norwegian petroleum industry. *Stavanger, Norway.*

- NORSOK-D010 (2013). Norsok standard: Well integrity in drilling and well operations, rev. 4. *Lysaker:Standards Norway*.
- Oliveira, L. (2009). Pfd of higher-order configurations of sis with partial stroke testing capability. volume 3, pages 1919–1928.
- OREDA (2009a). Offshore reliability data handbook. volume 1 - subsea equipment. *SINTEF*.
- OREDA (2009b). Offshore reliability data handbook. volume 1 - topside equipment. *SINTEF*.
- Piff, H. (2011). *Handbook of Reliability Prediction Procedures for Mechanical Equipment*. Naval Surface Warfare Center, Carderock Division, West Bethesda, MA, rev. g edition. Available online at <http://www.navsea.navy.mil/nswc/carderock/src/mechrel/products/handbook/CHAPTER3RevG.pdf>.
- Rausand, M. (2014). *Reliability of Safety-Critical Systems: Theory and Applications*. Wiley, Hoboken, NJ, 1st edition.
- Rausand, M. and Høyland, A. (2004). *System Reliability Theory: Models, Statistical Methods, and Applications*. Wiley, Hoboken, NJ, 2nd edition.
- Srinivas, G., Verma, A., Srividya, A., and Khattri, S. (2012). Reliability based optimization of technical specification of frontline systems of nuclear power plants using multi-objective approach. *International Journal of Reliability, Quality and Safety Engineering*, 19(1). cited By (since 1996)0.
- Van Winkle, D. (2013). Shear seal blowout preventer. US Patent 8,567,490.
- Vatn, J. (2007). *TPK5170: Maintenance Optimization*. Compendium, Trondheim, 1st edition.
- Vatn, J. (2013). *TPK5170: Maintenance Optimization*. Lecture Notes, Trondheim, 1st edition.
- Vaurio, J. (1995). Optimization of test and maintenance intervals based on risk and cost. *Reliability Engineering and System Safety*, 49(1):23–36. cited By (since 1996)97.
- Voronov, R. and Alzbutas, R. (2009). Optimization of test interval of ignalina nuclear power plant auxiliary feedwater pumps. volume 4, pages 601–605. cited By (since 1996)0.

WS-Atkins (1998). Testing interval optimization. *HSE, Health and Safety Executive, Internal Report.*

Zhang, T., Wang, Y., and Xie, M. (2008). Analysis of the performance of safety-critical systems with diagnosis and periodic inspection.

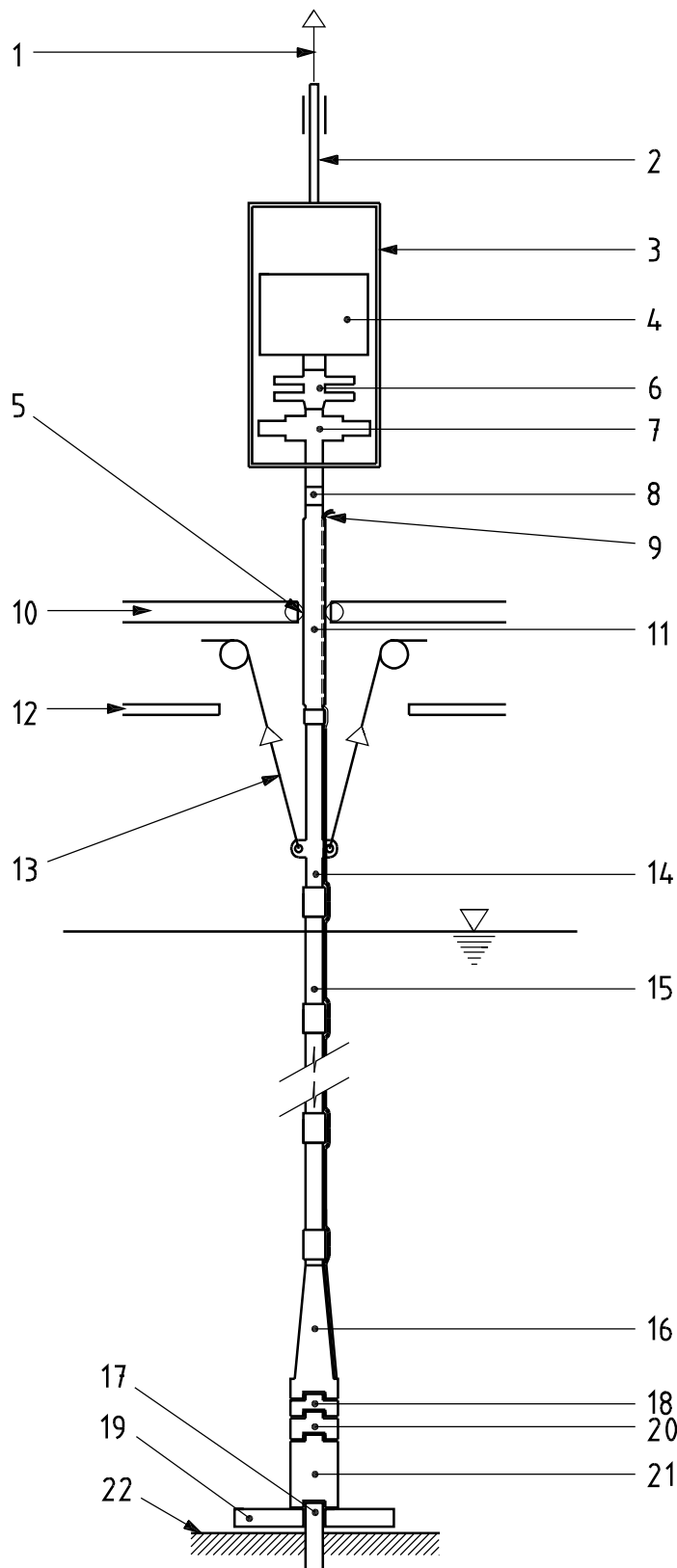
Appendix A

Equipment Controlled by the WOCS

In the following table, the typical modules controlled by the WOCS are listed. In the next two pages, the typical general arrangement of the main components of C/WO riser systems for the operational modes (tubing hanger mode and tree mode) are presented.

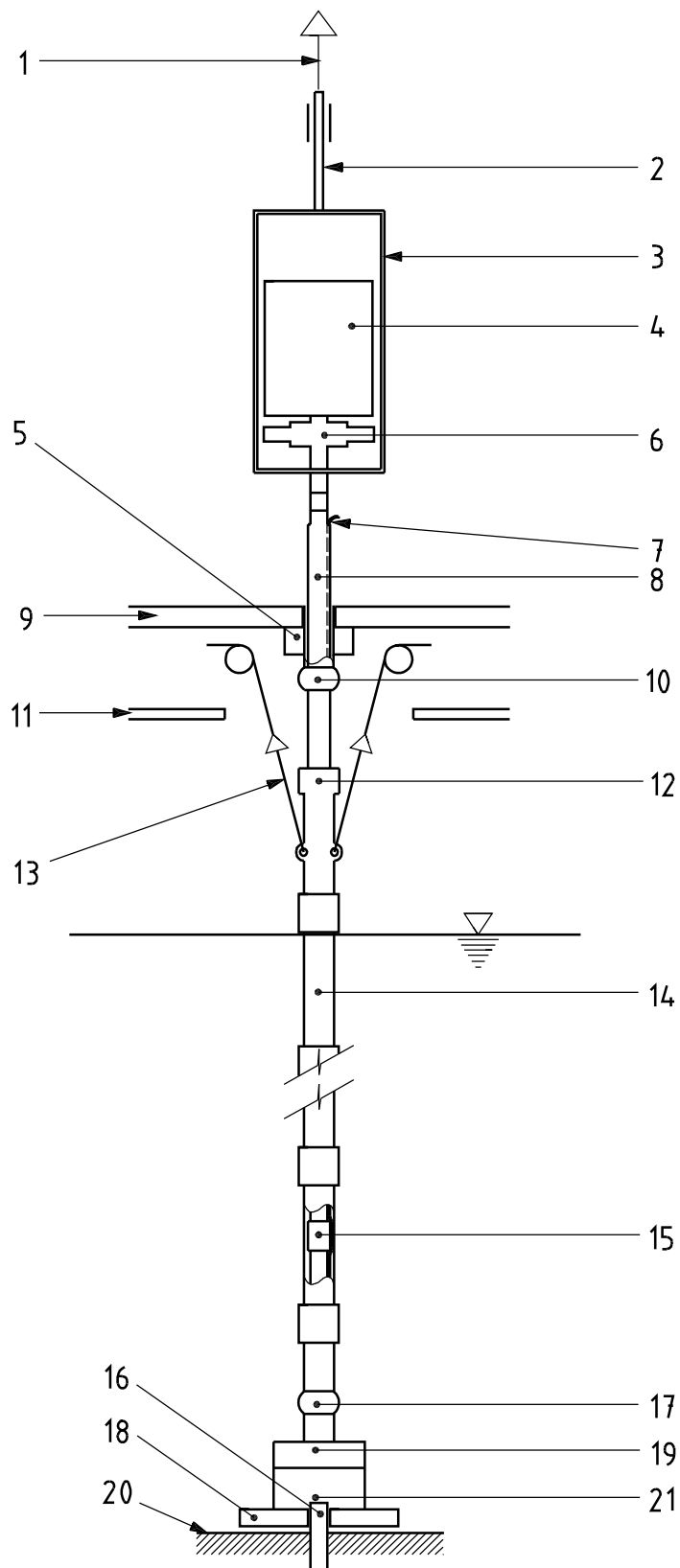
Table A.1: Typical modules controlled by the WOCS. Adapted from (ISO13628, 2005b)

Tubing hanger mode	Tree mode
Surface flow tree	Surface flow tree
Lubricator valve	Lubricator valve
Retainer valve	Retainer Valve
Subsea test tree	Emergency disconnect package
Tubing hanger running tool	WCT-BOP
Tubing hanger	Tree running tool
Tree cap running tool	Subsea tree
Internal tree cap	Internal tree cap
Subsea tree	Downhole monitoring and flow control functions
Downhole monitoring and flow control functions	SCSSV
SCSSV	-



- Key**
- 1 top drive
 - 2 drill sub
 - 3 surface-tree tension frame
 - 4 coiled tubing injector
 - 5 roller bushing
 - 6 surface BOP
 - 7 surface tree
 - 8 surface-tree adapter joint
 - 9 umbilical (to hose reel)
 - 10 drill floor
 - 11 slick (cased wear) joint
 - 12 moon pool area
 - 13 riser tension wires
 - 14 tension joint
 - 15 standard riser joints
 - 16 stress joint
 - 17 wellhead
 - 18 emergency disconnect package
 - 19 guide base
 - 20 lower riser package
 - 21 subsea tree
 - 22 seabed

Typical C/WO riser general arrangement — Tree mode



Key

- 1 top drive
- 2 drill sub
- 3 surface-tree tension frame
- 4 surface equipment
- 5 diverter
- 6 surface tree
- 7 umbilical (to hose reel)
- 8 slick joint
- 9 drill floor
- 10 ball joint
- 11 moon pool area
- 12 telescopic joint
- 13 riser tension wires
- 14 drilling riser joints
- 15 standard C/WO riser joints
- 16 wellhead
- 17 flex-joint
- 18 guide base
- 19 LMRP
- 20 seabed
- 21 BOP

Typical C/WO riser general arrangement — Tubing hanger mode

Appendix B

Example of an FMEA Worksheet

End Item: Operating Period:		Item: Revision:					Prepared by: Date:				
Item Ref.	Item Description and Functions	Failure Mode	Failure Mode Code	Possible Failure Causes	Local Effect	Final Effect	Detection Method	Compensating Provision Against Failure	Severity Class	Frequency or Probability of Occurrence	Remarks

Table B.1: FMEA Worksheet

Appendix C

MATLAB Code

The code developed in MATLAB consists of four subroutines. The subroutine Availability.c computes the time dependent availability. In other words it computes

$$A_k(t) = e^{-TCF \cdot \lambda \cdot (t - \tau_{p_{j,i}})} e^{-(TCF_m - TCF) \cdot \lambda \cdot (t - \tau_i)} e^{-(1 - TCF_m) \cdot \lambda \cdot t} \quad (C.1)$$

The code follows

```
function [Aoft]=Availability(LT,m,Tau,Lambda,TCFm,TCFp)

t=0:1:LT;    % Definition of the period of interest (lifetime)
[TauVector TparVector]=Tests(LT,m,Tau); %Computation of instant time of
                                         %full and partial proof tests
                                         %for periodic proof tests.

%Determination of failure rates
l1=TCFp*Lambda;
l2=(TCFm-TCFp)*Lambda;
l3=(1-TCFm)*Lambda;
tp=TparVector;
tf=TauVector;
j=1;
i=1;
```



```

r=zeros(size(t));
k=1;
%Computation of time dependent unavailability for a single component
while t(k) < LT
if t(k) <= TauVector(i+1)
    if t(k) <= TparVector(j+1)
        r(k)=exp(-l1*(t(k)-tp(j))).*exp(-l2*(t(k)-tf(i))).*exp(-l3*t(k));
        k=k+1;
    else
        j=j+1;
    end
else
    i=i+1;
end
end
Aoft=r(1:LT); %time dependent availability for a single component
end

```

Notice that the code Availability.c calls the function Test.c. The code for Test.c follows

```

function [TauVector TparVector]=Tests(LT,m,Tau);
nfpt=ceil(LT/Tau);
TparVecTemp=zeros(1,2);
    TauVector=zeros(1,2);
    lppt=round(Tau/m);
    nppt=ceil(LT/lppt);

%Determine instant time of periodic partial proof tests
for y=2:nppt+2
if TparVecTemp(end) < LT
    TparVecTemp(y)= TparVecTemp(y-1)+ lppt;
else

```

```

    end
end
TparVector=TparVecTemp(1,1:end);

%Determine the instant time of periodic full proof tests (Tau vector)
for y=2:nfpt+2
    TauVector(y)= TauVector(y-1)+ Tau;
end
TauVector;
end

```

The code for computation of

$$R_S(t) = \prod_{k=1}^n R_k(t) \quad \text{For series systems} \quad (\text{C.2})$$

can be found by using the subroutine Series.c. The code for Series.c follows

```

function [PFDseries]=Series(varargin)
PFDseries=varargin{1};

if nargin > 1
    for n = 2:nargin
        PFDseries=PFDseries.*varargin{n};
    end
end
end

```

The code for computation of

$$R_P(t) = 1 - \prod_{k=1}^n (1 - R_k(t)) \quad \text{For parallel systems} \quad (\text{C.3})$$

can be found by using the subroutine Parallel.c. The code Follows

```

function [PFDparallel]=Parallel(varargin)

```

```
if nargin > 1
    y=(1-varargin{1}).*(1-varargin{2});
    for n = 2:nargin-1
        y=y.*(1-varargin{n+1});
    end
end
PFDparallel=1-y;
end
```

Appendix D

Reduced Petri Net

Perfect Full Proof Test and Partial Proof Tests

In this Petri Net, the place p_1 from figure (5.10) has two tokens to indicate that there are two types of hidden failures. One type revealed by partial proof tests and another type revealed by full proof tests. The Petri net in figure (D.1) has two places (p_4 and p_{10}) to denote that a failure event with failure rate equal to $\lambda_{DU}^P = TCF \cdot \lambda_{DU}$ or $\lambda_{DU}^F = (1 - TCF) \cdot \lambda_{DU}$ may occur. The total failure rate of the component is equal to $\lambda_{DU} = \lambda_{DU}^P + \lambda_{DU}^F$. Notice that we assume that the failure events are independent.

After a failure event due to λ_{DU}^P , the transition t_1 is fired and a token is released to place p_4 . Similarly, after a failure event due to λ_{DU}^F (hidden failures only revealed by full proof tests), the transition t_6 is fired and a token is released to place p_{10} .

When a partial proof test takes place (the transition t_2 has been fired) a token is present in place p_5 , therefore, if there is a hidden failure due to λ_{DU}^P , transition t_4 is fired; or, if there is no hidden failures due to λ_{DU}^P , the transition t_5 is fired. Nonetheless, a token is released to place p_8 . Transitions t_{8a} and t_{8b} are constrained by the predicates $F_1 \cup F_2 = true$ and $F_1 \cap F_2 = false$, respectively. At this point, a decision is made whereas repair actions take place or a new testing interval starts. The variables F_1 and F_2 are used to indicate if a failure has occurred and repair actions should take place. For example, F_1 and F_2 are set to *true* when hidden failures has been revealed. See transitions t_4 and t_{10} in figure (D.1).

When the transition t_2 is fired a token is also released to place p_9 . However, transition t_9 or

t_{10} is not fired until the number of tokens in place p_9 are equal to m , meaning that a full proof test is taking place; If hidden failure occurs due to λ_{DU}^F (represented by a token in place p_{10}), the variable F_2 is set to *true* and repair actions take place, because the predicate in transition t_{8a} is met.

After repair actions, transitions t_{11a} and/or t_{3a} are fired *if and only if* failures due to λ_{DU}^P and λ_{DU}^F had occurred, respectively; otherwise, the tokens in places p_4 and p_3 are removed through transitions t_{11b} or t_{3b} avoiding the increase of the number of tokens in places p_1 . The decision taken in transitions t_{11b} and t_{3b} are constrained if failures have occurred. For example, the variable F_1 is set to *true* when a hidden failure due to λ_{DU}^P is revealed and set to *false* after a repair.

The variable $OF_1 = true$ is used to indicate that a failure due to λ_{DU}^P has occurred and transition t_1 cannot be fired until the variable is set to *false* after a repair. In the same way, the variable $OF_2 = true$ is used to indicate that a failure due to λ_{DU}^F has occurred and transition t_6 cannot be fired until the variable is set to *false* after a repair.

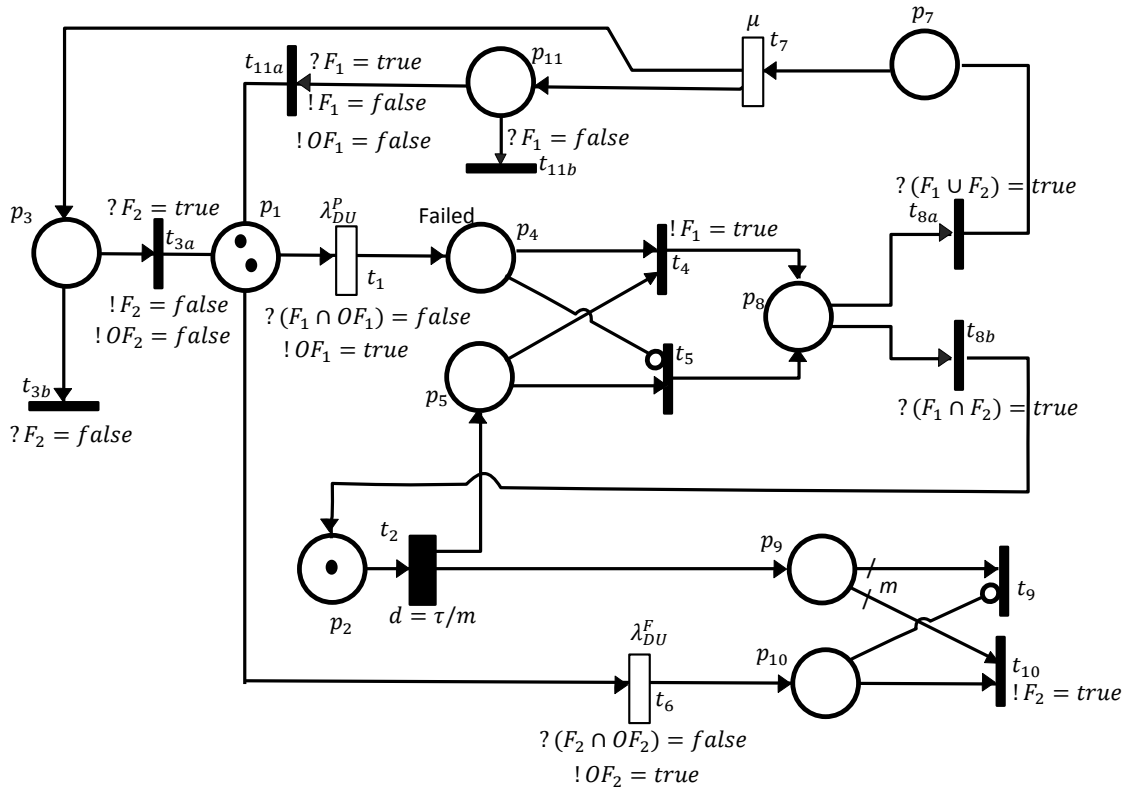


Figure D.1: Petri Net for modelling Periodic perfect full proof tests and $m - 1$ partial proof tests in the test interval of full proof tests. (Reduced Model)

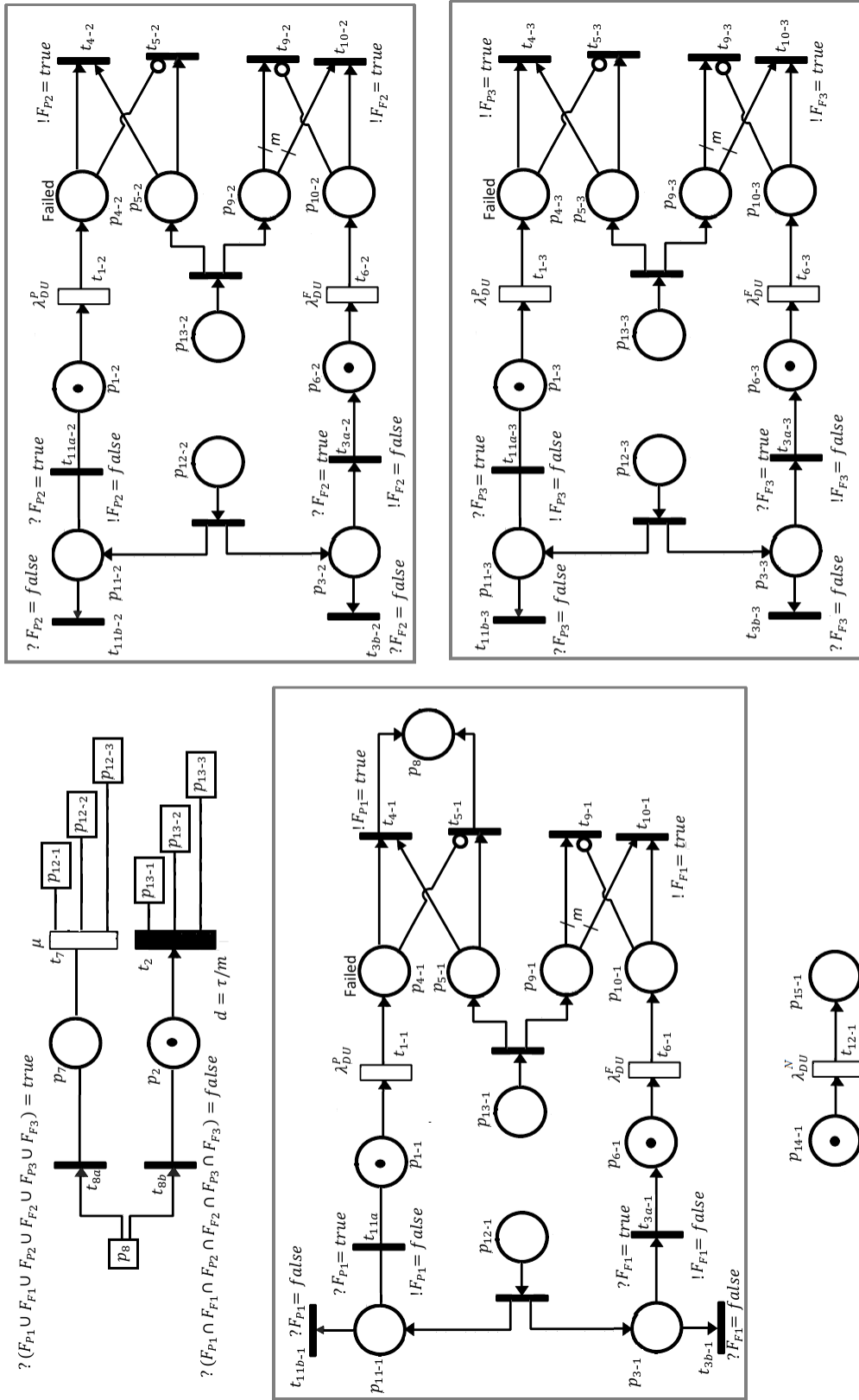


Figure D.2: Example of Petri Net driven by RBD

Appendix E

Calculation of TCF and TCF_{\max}

In the next table we present the calculation of the TCF and TCF_{\max} by using the method proposed in chapter 4. The failure rate is in the order of 10^{-6} .

SS-RAM	F. Rate	Weight	TCF p / F.R	TCF p	TCF f / F.R	TCF F	Data source
Fail to Close	8.02	0.173	1	0.643	1	0.866	Oreda Subsea Equipment (2009). p125
Fail to Shear	6.2	0.134	0		0		
Fail to Open	8.02	0.173	1		1		
Internal Leakage	18	0.388	0.7		1		
External Leakage	6.2	0.134	0.2		1		

PIV	F. Rate	Weight	TCF p / F.R	TCF p	TCF f /F.R	TCF F	Data Source
Fail to Close	8.02	0.460	1	0.943	1	1	Oreda Subsea Equipment (2009). p111
Fail to Open	8.02	0.460	1		1		
Internal Leakage	0.99	0.057	0		1		
External Leakage	0.39	0.022	1		1		

CIV, XOV, AIV,RAIV, RRV	F. Rate	Weight	TCF p / F.R	TCF p	TCF f /F.R	TCF F	Data Source
Fail to Close	0.077	0.350	1	0.860	1	1	PDS Method Data Handbook (2013). p118
Fail to Open	0.077	0.350	1		1		
Internal Leakage	0.044	0.200	0.7		1		
External Leakage	0.022	0.100	0.2		1		

DHSV	F. Rate	Weight	TCF p / F.R	TCF p	TCF f /F.R	TCF F	Data Source
Fail to Close	0.96	0.300	1	0.805	1	1	PDS Method Data Handbook (2013). p113
Fail to Open	0.96	0.300	1		1		
Internal Leakage	0.8	0.250	0.7		1		
External Leakage	0.48	0.150	0.2		1		

Component	F. Rate	Data Source
Power Unit	39.93	Oreda. Topside Equipment(2009), p83
Pushbutton	0.3	PDS Method - Data Handook(2013), p73
PLC	4.94	PDS Method - Data Handook(2013), p79,80,81
Umbillical	3.6	Oreda. Subsea Equipment(2009), p83
STWV	7.01	PDS Method - Data Handook (2006), Table 5

Appendix F

Commands in MATLAB for Computing the PFD_{avg}

```
clear
clc
Tau=336;           %It is equivalent to 14 days
m=2;              %Number of proof tests in a test interval Tau
LT=700;           %Life time in hours

% Subsystem RS1: Pushbuttons in an architecture 1oo2
Lambda=0.3/1000000; %Failure Rate
TCFm=1;           % Maximum test coverage factor
TCFp=1;           % Patial test coverage factor
s1=Availability(LT,m,Tau,Lambda,TCFm,TCFp); % Solution of Eq. 5.3
RS1=Parallel(s1,s1); % Solution of Eq. 5.2

% Subsystem RS2: Power Supply, WOCS's PLC and Umbillical in series.
Lambda=48.47/1000000; %Failure Rate = 39.93+4.94+3.6
TCFm=1;           % Maximum test coverage factor
TCFp=1;           % Patial test coverage factor
s2=Availability(LT,m,Tau,Lambda,TCFm,TCFp); % Solution of Eq. 5.3
```

```

RS2=Series(1,s2); % Solution of Eq. 5.1

% Subsystem RS3: SS-RAM.
Lambda=46.44/1000000; %Failure Rate
TCFm=0.866; % Maximum test coverage factor
TCFp=0.643; % Patial test coverage factor
s3=Availability(LT,m,Tau,Lambda,TCFm,TCFp); % Solution of Eq. 5.3
RS3=Series(1,s3); % Solution of Eq. 5.1

%Subsystems RS4: Valves CIV, or AIV in an architecture 1oo2 .
Lambda=0.22/1000000; %Failure Rate
TCFm=1; % Maximum test coverage factor
TCFp=0.86; % Patial test coverage factor
s4=Availability(LT,m,Tau,Lambda,TCFm,TCFp); % Solution of Eq. 5.3
RS4=Parallel(s4,s4); % Solution of Eq. 5.2

%Subsystem RS5: PIV.
Lambda=17.42/1000000; %Failure Rate
TCFm=1; % Maximum test coverage factor
TCFp=0.943; % Patial test coverage factor
s5=Availability(LT,m,Tau,Lambda,TCFm,TCFp); % Solution of Eq. 5.3
RS5=Series(1,s5); % Solution of Eq. 5.1

%Subsystem RS6: DHSV.
Lambda=3.2/1000000; %Failure Rate
TCFm=1; % Maximum test coverage factor
TCFp=0.805; % Patial test coverage factor
s6=Availability(LT,m,Tau,Lambda,TCFm,TCFp); % Solution of Eq. 5.3
RS6=Series(1,s6); % Solution of Eq. 5.2

```

```

% Subsystem RS7 corresponds to RS5 (PIV) in series with RS4 (1oo2 CIV)
RS7=Series(RS5,RS4);          % Solution of Eq. 5.1

% Subsystem RS8 corresponds to RS3 (SS-RAM) in Parallel with RS7
RS8=Parallel(RS3,RS7);       % Solution of Eq. 5.2

%Subsystems RS9: Valves XOV in an architecture 1oo3 .
Lambda=0.22/1000000; %Failure Rate
TCFm=1;          % Maximum test coverage factor
TCFp=0.86;       % Patial test coverage factor
s9=Availability(LT,m,Tau,Lambda,TCFm,TCFp); % Solution of Eq. 5.3
RS9=Parallel(s9,s9,s9); % Solution of Eq. 5.2

% Subsystem RS10 corresponds to RS8 in series with RS4 (1oo2 AIV)
%in series with RS9 (1oo3 XOV)
RS10=Series(RS8,RS4,RS9); % Solution of Eq. 5.1

%Subsystem RS11 corresponds to RS10 in parallel with RS6 (DHSV)
RS11=Parallel(RS10,RS6); % Solution of Eq. 5.2

%The total system corresponds to RS1 (pushbutton) in series with RS2 (Power
%Supply, WOCS's PLC and Umbillical) in series with RS11
RST=Series(RS1,RS2,RS11); % Solution of Eq. 5.1

%The time dependent Unavailability for the safety function ESD
AESD=1-RST;
S=AESD(1:Tau);
PFDavg=mean(S)

```

Appendix G

Calculation of PFD_{avg} by using the Formulae Approach

In the figure, we present the computation of the PFD_{avg} by using

$$Q_o \approx \sum_{i=1}^r \check{Q}_i \approx \frac{2^n}{n+1} \cdot \prod_{j=1}^n \bar{q}_j \quad (\text{G.1})$$

where

$$\bar{q}_j \approx \frac{\lambda_j \cdot TCF_j \cdot \tau_p}{2} + \frac{\lambda_j \cdot (1 - TCF_j) \cdot \tau}{2} \quad (\text{G.2})$$

Minimal Cut Sets	\check{Q}_i	Components	Failure Rate	TCFp	TCFmax	qp	qf	Tau-partial t	Tau-full test.
Pushbuttons	8.4672E-10	Pushbuttons	3E-07	1	1	2.52E-05	0	168	336
Power supply	0.00335412	Power supply	3.99E-05	1	1	0.003354	0	168	336
WOCS's PLCs	0.00041496	WOCS's PLCs	4.94E-06	1	1	0.000415	0	168	336
Umbilical	0.0003024	Umbilical	3.6E-06	1	1	0.000302	0	168	336
SS-RAM, PIV,DHSV	5.25751E-09	SS-RAM	4.64E-05	0.643411	1	0.00251	0.002782	168	336
SS-RAM, CIVs(1oo2), DHSV	2.41424E-15	PIV	1.74E-05	0.943169	1	0.00138	0.000166	168	336
AIVs(1oo2),DHSV	2.85129E-13	AIV	2.2E-07	0.86	1	1.59E-05	5.17E-06	168	336
XOVs(1oo3), DHSV	9.61098E-18	XOV	2.2E-07	0.86	1	1.59E-05	5.17E-06	168	336
		CIV	2.2E-07	0.86	1	1.59E-05	5.17E-06	168	336
		DHSV	3.2E-06	0.805	1	0.000216	0.000105	168	336

$Q_o = 0.0040714 = PFD_{avg}$

Appendix H

Pre-Study Report

Preface

This report is intended to produce an overview and acting as a management tool towards controlling the progress of the master thesis "Methods for determining PFD/SIL for workover control systems with short test-intervals and imperfect testing".

I thank you in advance to Professor Mary Ann Lundteige and, to Stein Hauge, senior scientist at SINTEF, for their academic and technical guidance during this master thesis.

The pre-Study report has been carried out by stud. Techn. Wilmer Alberto Aguilar Martinez, International Master Student in Reliability, Availability, Maintainability and Safety (RAMS), at the Norwegian University of Science and Technology (NTNU).

Trondheim, 2014-01-27

Wilmer Alberto Aguilar Martínez

Problem Description

Systems like workover control systems (WOCS) are used to shut down the operation safely while doing well intervention and well maintenance. Due to the role as safety barriers, it is necessary to demonstrate the SIL performance according to standards like IEC61508 and IEC61511. WOCS may be out of service for longer periods, then in operation for a shorter or longer period depending on the well maintenance program. The systems are frequently tested while in operation and they are always functionally tested just prior to each operation (and must be retrieved and re-tested if operation lasts too long).

Standard calculation techniques for determining SIL performance result in very low average probability of failure on demand (PFD_{avg}) estimates, and it has been questioned if these results are reasonable. The PFD_{avg} is reduced even further if aspects such as imperfect test are not incorporated in the calculations.

Objectives

The main objective of the master thesis is to suggest a new or alternative approaches for how to determine and evaluate the PFD_{avg}/SIL for safety critical systems with short test intervals and non—perfect testing, using the WOCS as a case study. More specific objectives are:

1. Present a description of WOCS including architecture design, applications, functional requirements, analysis of the operational and maintenance philosophy, overview of guidelines and standards.
2. Perform and document a literature study of approaches for reliability assessment of WOCS.
3. Establish the methods available for reliability analysis of WOCS highlighting the underlying assumptions and influencing factors leading to high/low reliability measures and taking into account the effect of non-perfect proof tests and short test intervals.
4. Present a stepwise procedure for estimating the test coverage factor for modelling the effect of imperfect/partial proof tests.

5. Present a discussion of the impact in the reliability measures of the fact that WOCS perform safety and control functions.

Methodology

This section describes the methodology to be applied during the development of this project. It is composed of the phases described in the following paragraphs.

Phase 1. Literature Review

The first phase of this master thesis is to study relevant information in the standards that govern safety-critical systems. The standards (IEC61508, 2010) and (IEC61511, 2003) are the primary source of information to functional safety. The guidelines OLF-070, application of the two standards IEC in the Norwegian petroleum industry is also a primary reference.

An overview of workover control systems can be found in the standard (ISO13628, 2005b), design and operation of subsea production systems: Completion/workover riser systems.

The guidelines (ISO/TR-12489, 2013), reliability modelling and calculation of safety systems, is the main document to study the techniques that are applicable for reliability analysis of WOCS.

Information available at the Department of Safety Research, SINTEF, is also of paramount importance for the developing of this master thesis.

The process for collecting scientific information regarding to this master thesis is mainly based on the database Scopus, Elsevier, Google scholar, Onepetro and IEEE Xplore.

Phase 2. Design

Based on the literature review and analysis of previous work on reliability assessment of WOCS, alternative methods for determining the PFD_{avg}/SIL of WOCS are to be proposed. The techniques considered in the first instance are listed below. The techniques are not limited or bound to the analysis.

- Reliability Block Diagrams / Fault tree analysis

- Multi-phase Markov Models
- Mathematical expressions
- Petri Nets

Phase 3. Implementation and Test

The technique(s) chose in phase 2 is(are) implemented and tested for reliability assessment of WOCS. The results shall be compared, advantages and disadvantages shall be highlighted. Remarkable conclusions should be drawn.

Phase 4. Writing the Report

This is the final phase of this project. The results will be presented in a structured and scientific manner. The initial content of the final report includes.

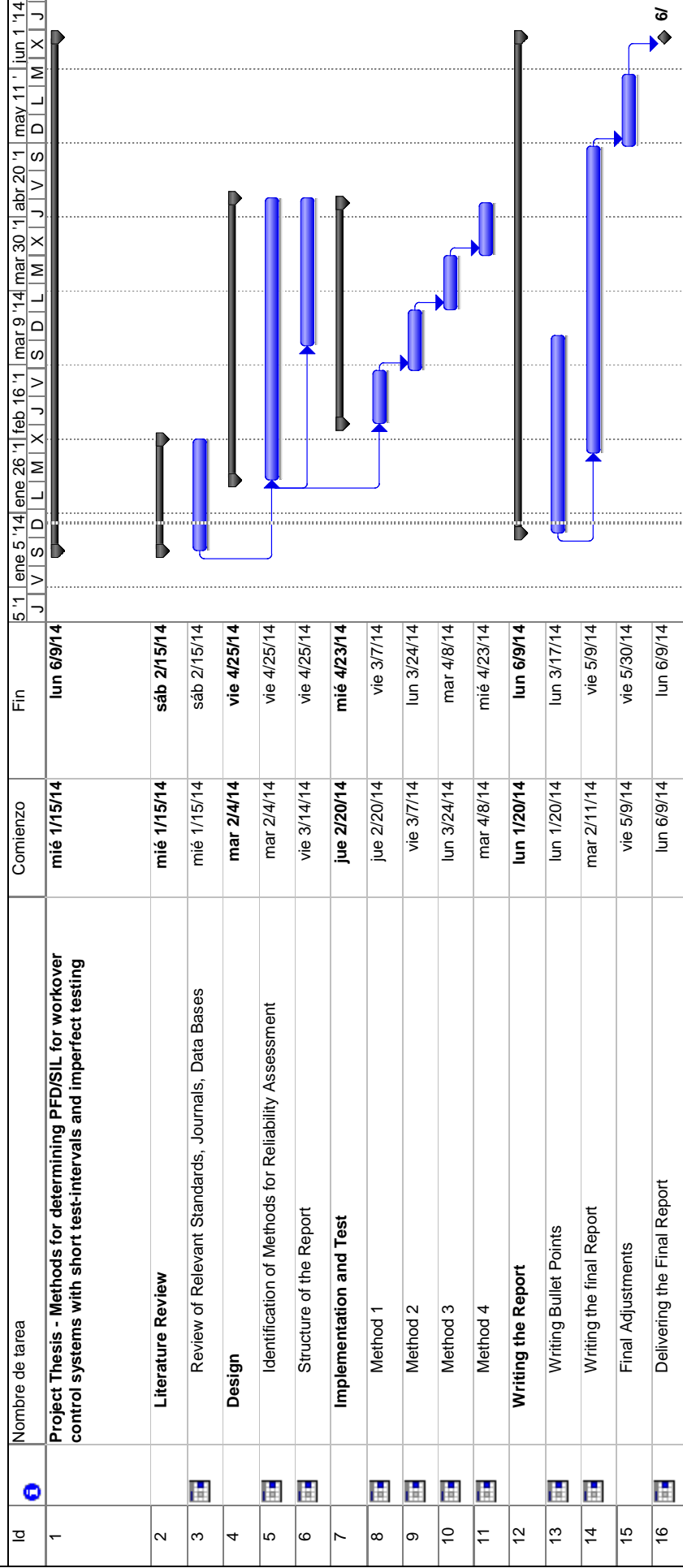
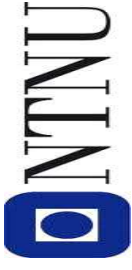
- Introduction
- Modelling imperfect proof tests
- WOCS description
- Models for reliability assessment of WOCS
- Summary and conclusions
- Further work

Project Plan



Project Plan

Methods for determining PFD/SIL for workover control systems with short test-intervals and imperfect testing



Projecto: Proyect1.mpp
Fecha: jue 1/23/14

Tarea		Tarea resumida		Tareas externas	
Progreso		Hito resumido		Resumen del proyecto	
Hito		Progreso resumido		Agrupar por síntesis	
Resumen		División		Fecha límite	

Wilmer Alberto Aguilar Martinez



Block 22, Room 51, Moholt Alle, Trondheim, 7050, Norway

+47 45174797, +57 316 454 21 55

✉ wilmeraa@stud.ntnu.no, ing_wil@hotmail.com

☎ Skype: wilmer.aguilar3

EDUCATION AND TRAINING

From August 2012 to June 2014

Master of Science in Reliability, Availability, Maintainability and Safety (RAMS)

Norwegian University of Science and Technology, Trondheim, Norway

- Master Thesis
Methods for determining PFD/SIL for workover control systems with short test intervals and imperfect testing
- Project Thesis
Reliability Assessment of Safety-Instrumented Systems with Imperfect Proof-Testing
The report is available as an additional reading to chapter 11 of the latest book written by professor Marvin Rausand, at <http://www.ntnu.edu/web/ross/books/sis/chapt11>
- Principal subjects
Reliability and Safety Analysis, Maintenance Management, Risk Analysis, Risks in Project Management, Lifetime Analysis, Applied Statistics, RAMS Engineering and Management, RAMS Optimization.
- Additional Courses
Subsea Production Systems, Robotics, Industrial Systems Engineering

From August 1996 to April 2004

Bachelor in Electronics Engineering

Universidad Francisco de Paula Santander, Cúcuta, Colombia

- Project Thesis
Design and implementation of a system for monitoring and data acquisition of operating parameters of the pump stations of pipeline Caño Limon Coveñas, Colombia
- Professional Profile
Able to design, analyse, implement, adapt, configure, test, operate and perform maintenance of electronic systems in areas of instrumentation and control systems. Able to identify, formulate and solve engineering problems efficiently.

WORK EXPERIENCE

From July 2011 to July 2012

Maintenance Inspector Engineer at SERINGTEC S.A.S, Cúcuta, Colombia
www.seringtec.com

- Sector
- Oil and Gas
Seringtec SAS provides consultancy and EPC services in Colombia for the oil and gas industry.
- Main Responsibilities
- To establish technical specifications of field instrumentation in the Optimization Project of the pipeline Caño Limón Coveñas, Colombia.
 - To assist in writing pump station operation & maintenance manuals for the pipeline Caño Limón Coveñas, Colombia.

From April 2010 to December 2010

Engineer II at TECNICONTROL S.A. Bogotá, Colombia
www.tecnicontrol.com.co

- Sector
- Oil and Gas
Tecnicontrol SA provides consultancy and EPC services in Latin America. Tecnicontrol SA covers mainly the market segment of the oil and gas, mining and construction industry.
- Main Responsibilities
- To establish technical specifications of field instrumentation and control systems for the onshore facilities of Ecopetrol Coveñas ODC-ACN, Colombia.

From April 2005 to April 2010

Technical Engineer at CONSORCIO ICAMEX-TERMOTECNICA. Cúcuta, Colombia

- Sector
- Oil and Gas
Consortium ICAMEX-Termotecnica provided outsourcing services for maintenance of pump stations and pipelines in Colombia
- Main Responsibilities
- To supervise maintenance development of field instrumentation and control systems of the onshore facilities - Coveñas ODC-ACN, Colombia

PERSONAL SKILLS

Languages skills	Mother tongue: Spanish Other language: English Norwegian Self-Assessment: Proficient User Self-Assessment: Beginner
Communication skills	<ul style="list-style-type: none">I express myself clearly and positively, both verbally and in writing; Communications skills gained through dynamic participation in different events in my previous jobs.
Organisational / Managerial skills	<ul style="list-style-type: none">Leadership: Responsible for maintenance team of control system and instrumentation in Coveñas ODC-ACN. Skill reinforced during the course Experts in Team at NTNU.Cooperation and Commitment: Member of interdisciplinary teams responsible for maintenance development and projects execution.Planning and scheduling: Management of Work Orders in Coveñas ODC-CAN.Setting and maintaining performance of standards: Responsible for documentation management required by the certification ISO 9001:2008 of plant Coveñas ODC-CAN in the area of control and instrumentation.Good time ManagementKnow how to prioritize: As a member of the maintenance crew, I was responsible for making decision on prioritizing maintenance tasks.
Job-related and Technical skills	<ul style="list-style-type: none">To assist in Layer Protection Analysis (LOPA), Hazardous and Operability Studies (HAZOP), SIL assessment, Safety and Requirements Specifications (SRS). Skills learned during the FS workshops led by Risknowlogy in Coveñas and Bogota, Colombia.To develop control strategies for Basic Process Control Systems such as DCS ABB, and implement new product technologies as well. Skill acquired during my job at Consortium Icamex-Termotécnica.To follow standards and procedures. Core skill learned in previous jobs
Computer skills	<ul style="list-style-type: none">Good command of Microsoft OS™ and Microsoft Office™ toolsGood command of Minitab, CARA, MATLAB, LaTeXBasic command of Visual Basic 2010

ADDITIONAL INFORMATION

Additional Training	<ul style="list-style-type: none">Introduction to Systems Engineering, www.coursera.org, April 2014 to June 2014 MOOC developed by the University of New South Wales, Australia
Seminars	<ul style="list-style-type: none">Functional Safety, Gas ATEX Risk Management, SIS for Gas ATEX Protection, led by Risknowlogy, November 28-30, 2011 Bogota, Colombia,Best Measurement Practices by FMCTechnologies, April 2008, Bogota Colombia,
Honours	<ul style="list-style-type: none">Best ECAES 2003 – Electronics Engineering – Universidad Francisco de Paula Santander, Cúcuta, Colombia.Leader HSE, Consorcio ICAMEX-TERMOTECNICA, 2008, Coveñas ODC-ACN, Colombia
Reference(s)	<ul style="list-style-type: none">It will be provided on request
Work Experience Certificate(s)	<ul style="list-style-type: none">It will be provided on request