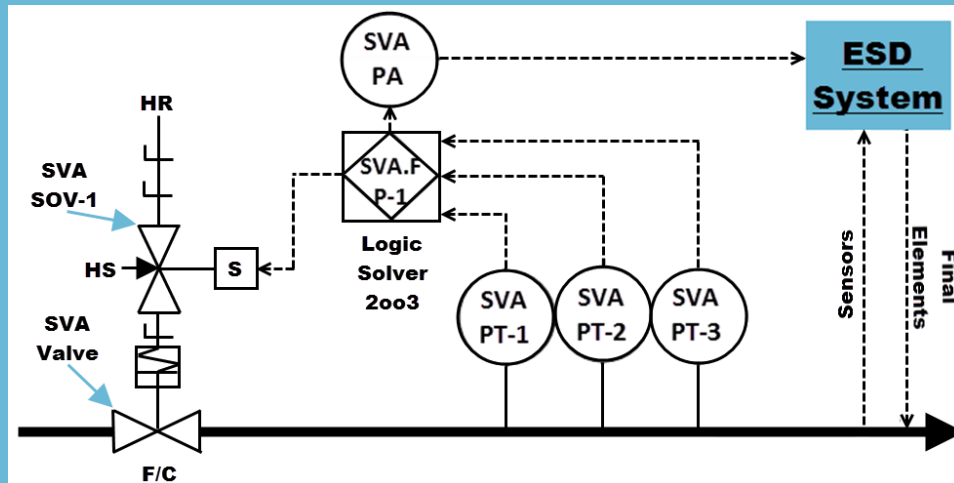
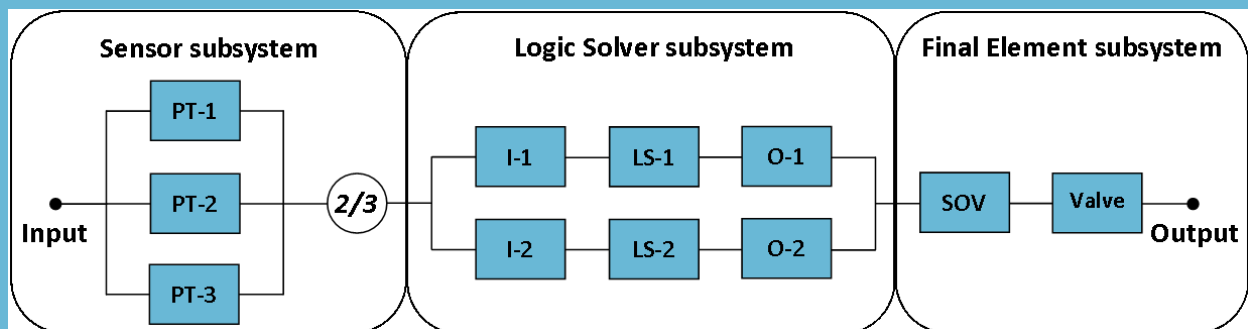




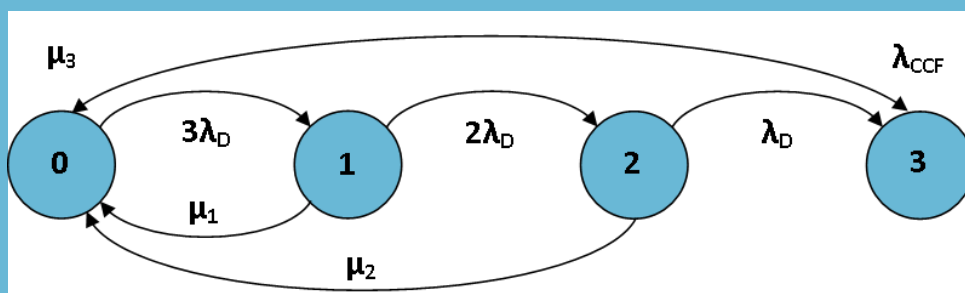
SVEND HIPPS



Reliability Block Diagram



Markov Model – 2oo3 Voting



Master Thesis: *Quantitative reliability modelling and functional safety calculations of Svend topside High Integrity Pressure Protection System*

Aalborg University Esbjerg

10th semester M.Sc. in Offshore Energy Systems – group OES10-2-F17

Jacob Glæsner

Printed June 8th 2017

(This page is intentionally left blank)

Title Page

Project title:	Master Thesis: <i>Quantitative reliability modelling and functional safety calculations of Svend topside High Integrity Pressure Protection System</i>
University:	Aalborg University Esbjerg
Study program:	Master of Science Programme in Sustainable Energy Engineering with specialization in Offshore Energy Systems
Semester, group:	10 th semester, OES10-2-F17
Semester theme:	Master Thesis in Offshore Energy Systems
Project period:	February 1 st 2017 to June 8 th 2017
ECTS:	30
Supervisor:	Mohsen Soltani
Number of pages:	109 numbered pages, including appendix
Front page picture:	Own creation

By signing this document or uploading it to the project data base each group member confirms to have participated equally in the project and share the responsibility of the content of the report. In addition, all group members confirm that plagiarism is not present in the report.

Jacob Glæsner

(This page is intentionally left blank)

Abstract

A conducted Layers Of Protection Analysis of Svend oil & gas platform predicted a hazardous incident to cause up to 10 fatalities and up to 1000 MMUSD so an upgrade of the High Integrity Pressure Protection System (HIPPS) was suggested. A HIPPS is a Safety Instrumented System that must have a certain level of reliability in order to fulfill the required Safety Integrity Level (SIL) 2. The Svend HIPPS architecture and different quantitative reliability methods i.e. Reliability Block Diagrams (RBD), Fault Tree Analysis (FTA) and Markov modelling are described. Functional safety calculations i.e. the Probability of Failure on Demand (PFD_{Avg}) are performed with each method and compared. RBD and FTA are much similar in approach but the complexity increases when using Markov modelling as the number of states may increase exponentially. However, the SIS can be described more detailed with Markov modelling. The results of the PFD_{Avg} show a deviation within 1 % regardless of chosen method and the required SIL 2 is obtained with the proposed components and architecture for Svend topside HIPPS. It is more important that the user of a particular method is competent in using the chosen method than the method, which is actually used.

(This page is intentionally left blank)

Preface

During a 9th semester internship at Maersk Oil I worked with Safety Instrumented Systems (SIS) and particularly installation of a High Integrity Pressure Protection System (HIPPS) at the unmanned Svend Platform – see Chapter 3 page 15 for a more detailed description of the Svend platform and HIPPS. Installation of a HIPPS is a long process with many considerations and calculations especially regarding safety. I was introduced to reliability and functional safety calculations during the internship and concluded that it would be a natural continuation of the internship to study this further in my master thesis.

This 10th semester master thesis is written by Jacob Glæsner as part of the M.Sc. in Offshore Energy Systems study program at Aalborg University Esbjerg (AAUE). The master thesis is a continuation of the work done in a 9th semester internship but with a dedicated focus on the reliability and functional safety of the HIPPS and different means to calculate the reliability. In this context the thesis contains sections, which would have been excluded in a commercial report.

The report is written in a language that requires prior knowledge to the Oil and Gas Industry. Even though the Oil and Gas Industry is the foundation for this master thesis, reliability engineering is used in several other industries. Relevant figures, tables and text from the 9th semester report will be included.

References to documentation and literature are placed in [brackets].

Used acronyms are explained in the text. A list of used acronyms can also be found at page xi.

Maersk Oil legends are used throughout the report. A list of used legends is provided at page xiii.

The PDF version of this report has bookmarks that ease navigation.

Special thanks are given to my supervisor Mohsen Soltani (assistant professor at AAUE) and colleagues at Maersk Oil for technical assistance throughout the project period.

Table of Contents

Title Page	i
Abstract	iii
Preface	v
Table of Contents	vi
Abbreviations, Acronyms and Symbols	xi
Legends	xiii
Introduction Section	1
1 Scope of Thesis	3
1.1 Motivation	3
1.2 Objective	3
1.3 Limitations	4
1.3.1 Quantitative approaches	5
1.3.2 Modes of operation	6
1.3.3 Conclusion of limitations	6
1.4 Method	6
1.5 Literature	6
1.5.1 IEC and ISO standards	7
1.5.2 Maersk Oil documents	8
1.5.3 Books	8
1.5.4 Articles	9
1.6 State of the art Analysis	9
1.6.1 'Reliability Engineering and Safety Systems' Journal	10
1.6.2 Other Articles	10
1.7 Structure of the Report	11
1.7.1 Introduction Section	11
1.7.2 Modelling Section	11
1.7.3 Concluding Section	11
2 Safety Instrumented Systems	12
2.1 Elements in SIS	12
2.1.1 Sensors	12

2.1.2	Logic Solver	12
2.1.3	Final Element	13
2.1.4	Design principle – fail safe	13
2.2	Safety Instrumented Function	13
2.3	Safety Integrity Level	13
3	Svend Platform & HIPPS Installation	15
3.1	Equipment Under Control	16
3.2	HIPPS	17
3.2.1	Current Svend HIPPS	17
3.2.2	Future HIPPS	17
3.2.3	SIL requirement of future HIPPS	18
	Modelling Section	21
4	Failure Modes	23
4.1	No Effect Failure	23
4.2	Safe Failure	23
4.3	Dangerous Failure	23
4.4	Failure Rate	24
4.5	Common Cause Failure (CCF)	25
4.5.1	β -factor standard	25
4.5.2	β -factor corrected	26
4.5.3	β -factor – non-identical components	27
4.6	Svend HIPPS Failure Modes	28
5	Probability of Failure on Demand	29
5.1	Definition of PFD	29
5.2	Requirements	30
5.3	PFD Formulas Relevant for Svend HIPPS	30
5.3.1	IEC 61508-6 Formulas	30
5.3.2	Simplified Formulas	31
5.3.3	CCF	32
5.4	Summary of Formulas	33
6	Reliability Block Diagrams	34
6.1	Assumptions and Definitions	34

6.1.1	State of system	34
6.1.2	State of components.....	34
6.2	Graphical & Mathematical Illustration of Boolean Logic [40].....	35
6.2.1	Series structures.....	35
6.2.2	Parallel structures and m out of n (moon) structures.....	35
6.2.3	Other structures.....	36
6.3	Probability Calculations	36
6.3.1	Constant probability of failure or success.....	37
6.3.2	MoonN (non-identical components) IEC 11.8.2.....	37
6.4	Svend HIPPS – RBD and PFD Calculations	38
6.4.1	Sensor subsystem.....	38
6.4.2	Logic Solver subsystem	39
6.4.3	Final Element subsystem	39
6.5	Table Determination	39
6.5.1	Table Analysis	40
6.5.2	Summary.....	42
6.6	Results of Svend HIPPS Calculations	42
6.6.1	Article Comparison	43
7	Fault Tree Analysis [4] [3] [41]	46
7.1	FTA Boolean Operators and Symbols	47
7.1.1	Events.....	48
7.2	FTA Mathematics	48
7.2.1	AND-gate	48
7.2.2	OR-gate.....	49
7.2.3	Minimal Cut Sets.....	49
7.2.4	Average Probability of Failure on Demand.....	49
7.3	FTA of Svend HIPPS	50
7.3.1	Sensor Subsystem	50
7.3.2	Logic Solver Subsystem.....	51
7.3.3	Final Element Subsystem	52
7.4	Results: Svend HIPPS Basic Events.....	52
8	Markov Modelling	54

8.1	Basic Markov Modelling	54
8.2	Markov Mathematics	55
8.2.1	Kolmogorov Differential Equation [3].....	56
8.2.2	Time-dependent Solution.....	57
8.2.3	Steady State Solution.....	58
8.3	Results: Svend HIPPS – Markov Modelling.....	59
8.3.1	Sensor Subsystem	59
8.3.2	Logic Solver Subsystem	61
8.3.3	Final Element Subsystem	64
8.4	Summary of Results.....	65
9	Proof Test Interval	67
9.1	Perfect Proof Testing	67
9.2	Imperfect Proof Testing	68
	Concluding Section	69
10	Conclusion.....	71
10.1	SIS of Svend HIPPS.....	71
10.2	Comparison of RBD, FTA, and Markov Modelling.....	72
10.3	Results of PFD_{Avg}	73
10.4	Conclusive Summary	73
11	Bibliography	74
12	Appendix	79
12.1	Hazard Scenarios [42]	80
12.2	TREL Values for existing installations [37]	81
12.3	Oil Group Classification [45] [46].....	82
12.4	Overall framework of IEC 61508 [47].....	84
12.5	Use of methods for general dependability analysis tasks [48]	85
12.6	Characteristic of selected dependability analysis method [48]	86
12.7	Inservice Inspection System Overall View.....	87
12.8	DUC in the North Sea.....	88
12.9	Process Flow Diagram current HIPPS.....	89
12.10	Process Flow Diagram future HIPPS [42].....	91
12.11	PFD and SIL determination.....	92

12.11.1	<i>Initiating Cause (IC)</i>	92
12.11.2	<i>Independent Protection Layers (IPL)</i>	92
12.11.3	<i>TMEL</i>	92
12.11.4	<i>Example of SIL determination of Safety Impact</i>	92
12.12	2oo3 Structure Function	93
12.12.1	<i>Minimal Path Set</i>	93
12.12.2	<i>Minimal Cut Set</i>	93
12.13	moon non-identical components	95
12.13.1	<i>Boolean Truth Table</i>	95
12.13.2	<i>Karnaugh Maps</i>	96
12.14	Taylor Series Expansion	98
12.15	MATLAB – PFD Table Determination	99
12.16	MATLAB – Solving Time-Dependent Diff. Equations	101
12.17	MATLAB – Solving Steady State Diff. Eqns. 2oo3 voting	103
12.18	MATLAB – Solving Steady State Diff. Eqns. 1oo1 voting	105
12.19	MATLAB – Solving Steady State Diff. Eqns. 1oo2 voting	107
12.20	State Definition of a 2oo3 voting system	109

Abbreviations, Acronyms and Symbols

$F_{E,total}$	Total Event frequency pr. year
F_E	Event frequency pr. year
F_{IC}	Probability Initiating Cause pr. year
F_{IPL}	Probability Independent Layers of Protection pr. year
λ	Failure rate
β	Beta factor
$R(T)$	Reliability survivor function
$\phi(X)$	Structure function
E	Basic Event
BOEPD	Barrels of Oil Equivalent Per Day
BPD	Barrels Per Day
CCF	Common Cause Factor
DBU	Danish Business Unit
DC	Diagnostic Coverage
DD	Dangerous Detected
DU	Dangerous Undetected
DUC	Danish Underground Consortium
E/E/PE	Electrical/Electronic/Programmable Electronic
ESDV	Emergency Shutdown Valve
EUC	Equipment Under Control
F&G	Fire and Gas
FE	Final Element subsystem
FMECA	Failure Mode, Effects and Criticality Analysis
FTA	Fault Tree Analysis
HAZOP	Hazard and Operability
HCV	Hand Control Valve
HIPPS	High Integrity Pressure Protection System
HR	Hydraulic Return
HS	Hydraulic Supply
HWA	Harald Platform module A
IC	Initiating Cause
IEC	International Electrotechnical Commission
IPL	Independent Protection Layer
LCV	Level Control Valve
LOPA	Layer of Protection Analysis
LS	Logic Solver subsystem

MMUSD	Millions United States Dollars
MooN	M out of N (voting logic)
MOTS	Maersk Oil Technical Standard
MRT	Mean Repair Time
MTBD	Mean Time Between Demand
MTBF	Mean Time Between Failures
MTTR	Mean Time To Restore
NTNU	Norwegian University of Science and Technology
P&ID	Piping and Instrumentation Diagram
PA	Pressure Alarm
PFD	Probability of Failure on Demand
PFD_{AVG}	Calculated Probability of Failure on Demand for the SIF
PFH	Probability of Failure on demand pr. Hour
PI	Pressure Indicator
PIT	Pressure Indicator Transmitter
PLC	Programmable Logic Controller
PSHH	Pressure Switch High High
PT	Pressure Transmitter
RAMS	Reliability, Availability, Maintainability, Safety
RBD	Reliability Block Diagram
RRF	Risk Reduction Factor
S	Sensor subsystem
S/D	Shut Down
SCADA	Supervisory Control And Data Acquisition
SD	Safe Detected
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Integrity System
SOV	Solenoid Operated Valve
SU	Safe Undetected
SVA	Svend Platform module A
TEC	Tyra East module C
TEF	Tyra East Platform module F
TMEL	Target Mitigated Event Likelihood
XCV	Unclassified Control Valve

Legends

Valve Symbols



Gate valve



Gate valve with flanges



Ball valve



Ball valve with flanges



Globe valve



Globe valve with flanges



Check valve



Check valve with flanges



Needle valve



Needle valve with flanges



Choke valve



Choke valve with flanges

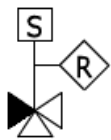


Axial on/off valve



Axial on/off valve with flanges

Instrument Symbols



Solenoid operated tree way
valve with manual reset



Solenoid operated tree way
valve with automatic reset



Locally mounted instrument



Local panel mounted (in
module) instrument



Spring

Fitting Symbols



Concentric reducer



Grayloc fitting

Line Styles



Main process lines



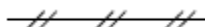
Flexible hose



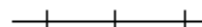
Instrument lines



Electric signal

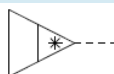


Pneumatic signal

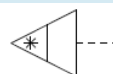


Hydraulic signal

Signal Conditioning Device Symbols



To signal



From signal



Part of computerized system

*** denotes**

C – SCADA

F – Fire & Gas System

M – Mimic

P – PLC

S – Shut Down System

T – Telemetry Signal

Z – HIPPS System

1, 2, 3, 4.... Shut Down Level

(This page is intentionally left blank)

Introduction Section

(This page is intentionally left blank)

1 Scope of Thesis

This chapter documents the motivation and objectives of the master thesis and method for documenting and answering the objectives. Some concepts are just used and not elaborated in this chapter but will be done in other chapters of the thesis.

1.1 Motivation

The reputation and performance of a company are measured by many different indicators e.g. quality, safety, and reliability of products and services. A hazardous incident in a company may have safety, environmental or commercial impact, which can damage the reputation and performance of the company depending on the severity of the incident. A conducted Layers Of Protection Analysis (LOPA) at Maersk Oil prior installation of a High Integrity Pressure Protection System (HIPPS) rated the severity of a hazardous incident at the Svend platform. Prior to the LOPA different hazard scenarios regarding over pressurizing of Svend were identified – see Appendix 12.1 page 80. During the LOPA a consequence assessment identified two possible consequences of the hazard scenarios and rated the severity as listed in Table 1-1.

Table 1-1: Severity rating of consequences [1]

Consequence	Safety	Environmental	Commercial
Leak at Svend	6-10 fatalities	Slight effect*	10-100 MMUSD
Leak at Tyra East F	2-5 fatalities	-	100-1.000 MMUSD

** Slight Effect in Maersk Oil terminology means risk of oil spill group 3 for Svend and group 2 for Harald. Both oil spills are more than 20 km from sensitive area and the severity is classified according to this – see Appendix 12.3 page 82.*

As illustrated in Table 1-1 a severe consequence of over pressurizing Svend could cost up to 1.000 MMUSD and cause several fatalities. In order to prevent the consequences of a hazardous incident a series of Independent Protection Layers (IPL) can be applied. A Safety Instrumented System (SIS) is an example of an IPL. The Emergency Shutdown (ESD) system is the primary SIS at the Svend platform but a HIPPS is considered installed as a secondary SIS in order to reduce the risk. To avoid any hazard incident and consequences it is crucial that the installed SIS works on demand. Reliability engineering gives a qualitative and/or quantitative indication of the SIS and certain measures can be taken to increase the reliability of avoiding a severe consequence.

1.2 Objective

Reliability and functional safety of safety instrumented systems is the topic of this master thesis. Within this topic the main objective of the thesis is to quantify the PFD_{Avg} with different approaches and compare selected methods. To obtain the main objective several sub objectives are identified in collaboration with Maersk Oil:

- outline the purpose of a SIS and describe the architecture of a HIPPS
- give an overall view of reliability assessment methods

- discuss different approaches to determine and quantify reliability of a SIS
- case study: analytical calculation of PFD, Availability, MTBF for Svend HIPPS
- compare results of different quantitative methods – are there any difference?
- does the calculated PFD fulfill the criteria of the Safety Integrity Level (SIL) analysis?
- illustrate the impact on PFD in changing the test interval of HIPPS instrumentation
- use relevant literature and recent research in the analysis

1.3 Limitations

Reliability analysis is a subpart of risk management as illustrated in Figure 1-1. Within reliability analysis different qualitative, quantitative, and semi-quantitative approaches can be used as outlined in Appendix 12.5 page 85 and Appendix 12.6 page 86. The objective of this thesis is to give a quantitative result of the reliability analysis with different modelling techniques and calculations, so qualitative approaches will not be considered.

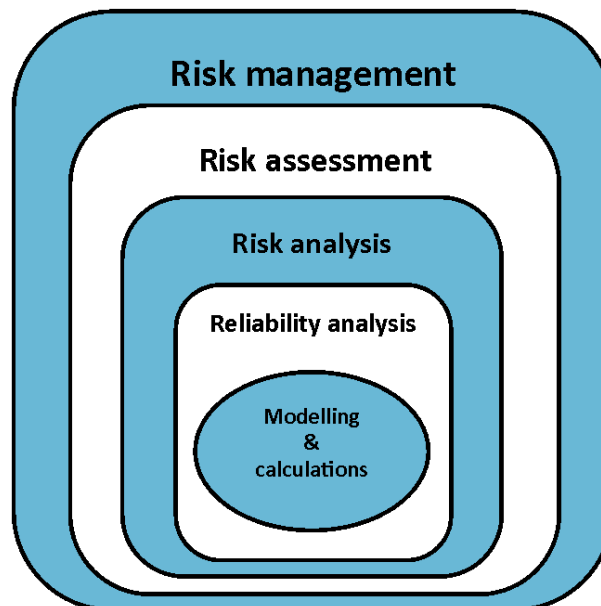


Figure 1-1: Framework of risk management [2]

Reliability analysis consists of three main branches:

- **Hardware reliability**
Reliability of technical components and systems can be divided into two approaches:
 - **Physical** – Will not be part of this thesis as it is mainly used for reliability analysis of structural elements and assessment of loads and stresses.
 - **Actuarial** – Main focus in this thesis as it is applicable to components and systems.
- **Software reliability**
Will not be treated in this master thesis due to the fact that this is not required to claim compliance with IEC 61508 and will often be performed by software specialists. [3]
- **Human reliability**
Though many technical components also involve human interactions it will not be a topic in this thesis. Whenever human interaction is required in calculations their interactions are considered 100 % reliable.

1.3.1 Quantitative approaches

Appendix 12.5 page 85 and Appendix 12.6 page 86 outlines different approaches in reliability analysis and in combination with the questions in Figure 1-2 they can be used as guidelines to choose an adequate approach to study a safety system. The “Modelling and calculations” part of “Reliability analysis” in Figure 1-1 is used when a quantitative approach is necessary as illustrated in Figure 1-2.

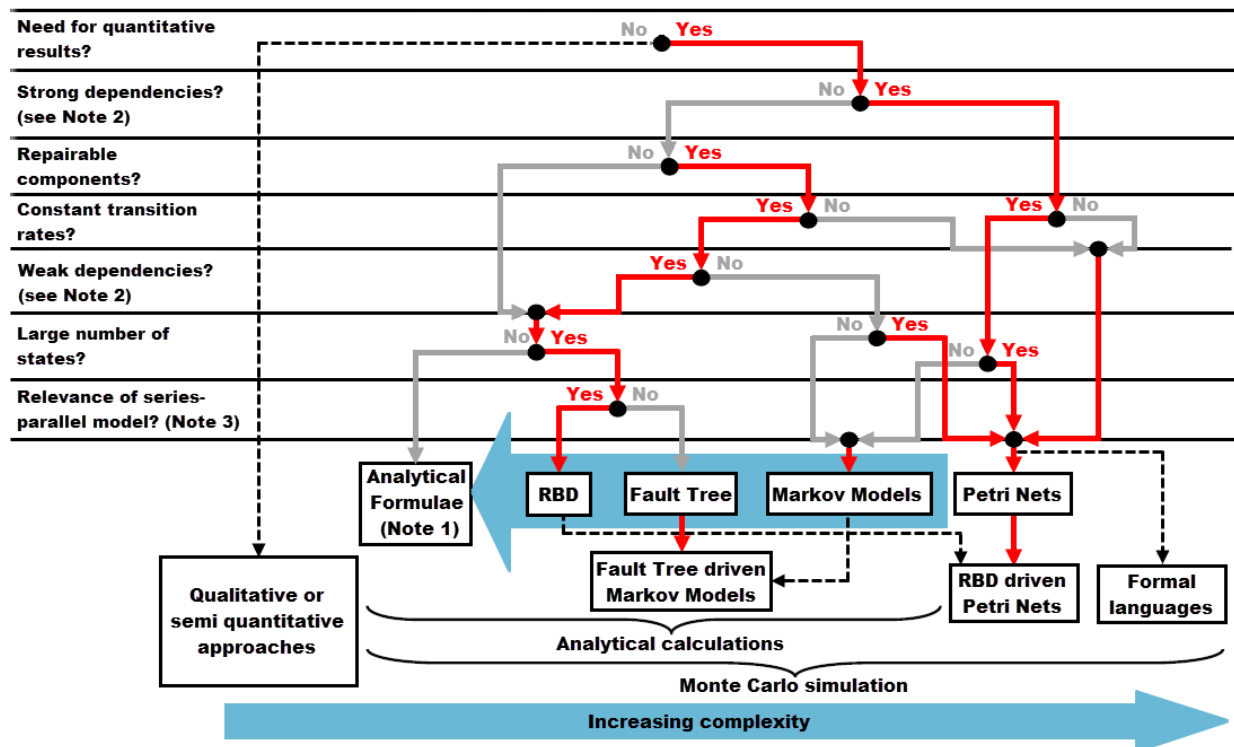


Figure 1-2: Overview of reliability modelling and calculation approaches [2]

- Note 1**
 Combination of Reliability Block Diagram (RBD), Fault Tree (FTA), and Markov models can be used to obtain the analytical formulae – illustrated with the blue arrow surrounding the three approaches.
- Note 2**
 Dependencies can either be weak or strong with either a negligible or strong impact on the probability of failure. Systems without dependencies do not really exist in the real world.
- Note 3**
 In “Series-parallel model” the logic of the system is only modelled with series or parallel structures.

The quantitative methods presented in Figure 1-2 can be sorted to two different views:

- Analytical calculations versus Monte Carlo Simulation**
- Static models versus dynamic models**
 Boolean models (RBD and FTA) versus states/transition models (Markovian)

According to IEC 61508 the choice of method is less important than the user's competence in using a specific method:

"All these methods can be used for the majority of safety related systems and, when deciding which technique to use on any particular application, it is very important that the user of a particular technique is competent in using the technique and this may be more important than the technique which is actually used...." [4]

1.3.2 Modes of operation

The mode of operation of a Safety Instrumented Function (SIF) is categorized according to how often the function is demanded. IEC 61508 defines three different modes of operation.

- **Low-demand mode**
Mean Time Between Demand (MTBD) > 1 year
- **High-demand mode**
MTBD < 1 year
- **Continuous mode**
Operates continuously and may be defined as a special case of high-demand mode

The main difference between a SIF in continuous mode and demand mode is that a SIF in continuous mode plays an active role in protecting the Equipment Under Control (EUC), while a SIF in demand mode is passive and will only operate when needed. IEC 61508 combines high-demand mode and continuous mode into one mode called *"high-demand mode/continuous mode"* [4]. IEC 61511 only distinguishes between demand mode and continuous mode [5]. A SIS can perform more than one SIF, so practically a SIS will be able to operate in low demand mode and high-demand mode.

1.3.3 Conclusion of limitations

Based on these considerations the thesis will be limited to quantitative analytical calculations of the reliability of Svend HIPPS with special focus on RBD, FTA, and Markov Model analysis. Svend HIPPS is defined to operate in low-demand mode of operation with a MTBD > 1 year.

1.4 Method

A literature review of books and research articles is used to describe the concepts of reliability analysis and safety instrumented systems. Analytical calculations of a case-study of Svend HIPPS will be performed after a literature review of RBD, FTA, and Markov Modelling.

1.5 Literature

The master thesis is based on a literature review of international IEC and ISO standards and reports, and internal Maersk Oil documents and standards. Some of the listed literature in the bibliography is only used as background knowledge and not referenced in the thesis. The comprehensive bibliography is established by a broad search on the reliability topic. Relevant literature was selected and their references used for further literature search. Multiple references of the chosen literature were used as a quality mark of the chosen literature.

1.5.1 IEC and ISO standards

For SIS in the process sector two main IEC standards apply and their relationship is illustrated in Figure 1-3.

- IEC 61508 – Functional safety of electrical/electronic/programmable electronic safety-related systems**
“This International Standard covers those aspects to be considered when electrical/electronic/programmable electronic (E/E/PE) systems are used to carry out safety functions. A major objective of this standard is to facilitate the development of product and application sector international standards by the technical committees responsible for the product or application sector. This will allow all the relevant factors, associated with the product or application, to be fully taken into account and thereby meet the specific needs of users of the product and the application sector. A second objective of this standard is to enable the development of E/E/PE safety-related systems where product or application sector international standards do not exist.” [6]
- IEC 61511 – Functional safety – safety instrumented systems for the process industry sector**
“This International Standard gives requirements for the specification, design, installation, operation and maintenance of a safety instrumented system, so that it can be confidently entrusted to place and/or maintain the process in a safe state. This standard has been developed as a process sector implementation of IEC 61508.” [5]

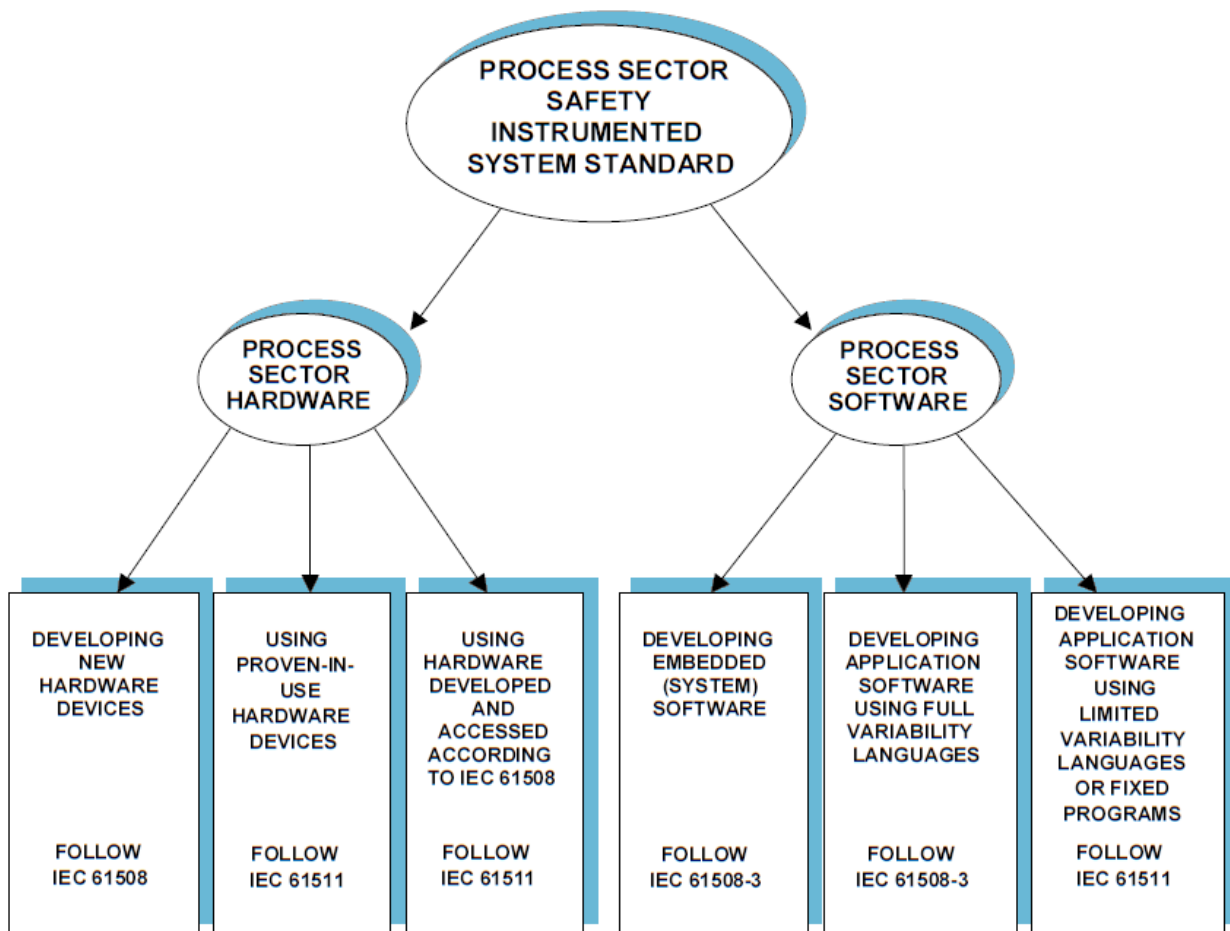


Figure 1-3: Relationship between IEC 61508 and IEC 61511 [5]

According to Figure 1-3 Maersk Oil must follow IEC 61511 as an operator while vendors must follow IEC 61508. In this master thesis the main focus will be on IEC 61508 because IEC 61511 gives a more general view on how to implement SIS. Appendix 12.4 page 84 gives an overall view of the framework of IEC 61508 – especially IEC 61508-6 is used as it gives guidelines to relevant reliability methods.

Other important used standards and technical reports include:

- **IEC 60300-3-1 – Dependability management – Part 3-1: Application guide – Analysis techniques for dependability – Guide on methodology**
- **IEC 61025 – Fault tree analysis (FTA)**
- **IEC 61078 – Reliability block diagrams**
- **IEC 61165 – Application of Markov techniques**
- **IEC 61703 – Mathematical expressions for reliability, availability, maintainability and maintenance support terms**
- **ISO/TR 12489 – Petroleum, petrochemical and natural gas industries – Reliability modelling and calculation of safety systems**

The bibliography contains more standards and technical reports used as background literature.

1.5.2 Maersk Oil documents

Internal Maersk Oil documents have been used including:

- **Maersk Oil Technical Standards (MOTS)**
- **Guidelines and Instructions**
- **Standards**
- **P&ID and Technical drawings**
- **Reports**
- **Vendor documentation**

Standards, guidelines, and instruction are based on IEC standards.

No further detailed description of Maersk Oil internal documents.

1.5.3 Books

Different views of certain topics are provided by different authors. The main authors and books used for this thesis are cited and referenced in used IEC standards and articles:

- **Birolini, Alessandro**
“Reliability Engineering: Theory and Practice” [7]
- **Goble, William**
“Control Systems Safety Evaluation and Reliability” [8]
- **Rausand, Marvin**
“System Reliability Theory: Models, Statistical Methods, and Applications” [9]
“Reliability of Safety-Critical Systems: Theory and Applications” [3]
“Risk Assessment: Theory, Methods, and Applications” [10]

- **Zio, Enrico**
 "An Introduction to the Basics of Reliability and Risk Analysis" [11]
 "Computational Methods for Reliability and Risk Analysis" [12]
 "Basics of Reliability and Risk Analysis Worked Out Problems and Solutions" [13]

Other books are used as supplementary literature.

Reliability data books with collected industry data are used for Reliability, Availability, Maintenance, and Safety (RAMS) analysis.

- **SINTEF – OREDA-2009**
 "Offshore Reliability Data Handbook: Volume 1 - Topside Equipment" [14]
- **SINTEF**
 "Reliability Data for Safety Instrumented Systems – PDS Data Handbook" [15]

SINTEF is a large independent research organization in Scandinavia, which has prepared the *Offshore & onshore RELiability DATA* (OREDA) handbook. OREDA is a project organization sponsored by eight worldwide oil and gas companies: BP, Total, Statoil, Petrobras, Shell, EN, ENI, Gassco. OREDA's main purpose is to collect and exchange reliability data between the participating companies. [14]

1.5.4 Articles

Many different articles within the topic of reliability analysis regarding RBD, Fault Tree, and Markov Analysis have been assessed to gain insight in recent research. The used articles will be cited when necessary.

A further review of articles will be given in Section 1.6 – State of the art Analysis.

1.6 State of the art Analysis

The topic of reliability assessment has attracted a lot of research interests and this section will introduce the articles used in this thesis.

The used articles are chosen from the following criteria:

- **Article relevance to subject of this thesis**
 The used articles are chosen within the following subject: SIL, PFD, RBD, FTA, Markov Modelling, Moon structures, and proof testing and failures.
- **Journal**
 The *'Reliability Engineering and Safety Systems'* journal is the main contributor of articles used in this thesis but other articles have been used if they were found valid and relevant.
- **Author of articles**
 The first gross selection of articles was filtered on author and only authors, which had many citations or publications of either articles or books were selected e.g. Rausand (a contributor of books used in this thesis – see Section 1.5.3 page 8).

- **Citations of articles**

The articles were also chosen with respect to the number of citations in other articles e.g. how many times have someone else cited the article.

1.6.1 ‘Reliability Engineering and Safety Systems’ Journal

The journal is the main contributor of articles used in this thesis. It is published by Elsevier in association with the *European Safety and Reliability Association*, and the *Safety Engineering and Risk Analysis Division*. The journal is an international journal devoted to development and application of methods in order to enhance the safety and reliability of complex technological systems, including offshore systems. Normally it only publishes articles that involve the analysis of substantive problems related to reliability of complex systems. An important aim of the journal is to achieve a balance between practical applications and academic material. The validity of the articles in the journal is considered high because of the criteria in order to have an article published in the journal i.e. peer review etc. Table 1-2 shows a list of used articles from the journal sorted by author and subject – the brackets [] refer to the bibliography. The PFD and SIL are main subjects of all articles.

Table 1-2: Articles in ‘Reliability Engineering and Safety Systems’ journal sorted by subject

Author	RBD/FTA	Markov	Testing/failures
Guo and Yang	[16]	[17]	
Lisnianski	[18]	[18]	
Torres-Echeverría et al.	[19] [20]	[19] [20]	[19] [20] [21]
Jin and Rausand	[22] [23]	[23]	[22] [23]

1.6.2 Other Articles

Other relevant articles chosen by the same criteria are listed in Table 1-3.

Table 1-3: Other articles sorted by subject and author

Author	RBD/FTA	Markov	Testing/failures
Hildebrandt et al.		[24]	[25]
Börcsök et al.	[26] [27]	[28]	[26] [27]
Kim	[29]		

As a supplement and inspiration, master theses supervised by the RAMS (Reliability, Availability, Maintainability/maintenance, and Safety) group at NTNU (Norwegian University of Science and Technology) have been read but not cited in this thesis. Only relevant theses were read but a complete list of the theses can be found at NTNU website: <https://www.ntnu.edu/ross/msc-theses-rams> [30]

No further description of used articles in this section but results from articles are highlighted and cited throughout this master thesis when relevant.

1.7 Structure of the Report

The master thesis report is initiated with a formal preamble followed by three main sections:

- Introduction Section
- Modelling Section
- Concluding Section

The reader should experience a smooth and relevant connection and guidance between the sections and chapters.

1.7.1 Introduction Section

This section will contain background, thoughts, and theory needed as guidance to understand the choices for the chapters in the Modelling Section. Some of the objective questions will be covered in this section including description of safety instrumented systems, general reliability assessment, and introduction to Svend platform and HIPPS architecture.

1.7.2 Modelling Section

This section will describe different modelling approaches to quantify reliability including case-study with analytical calculations of e.g. PFD, Availability, and impact of different test intervals. The rest of the objectives will be covered.

1.7.3 Concluding Section

This section will summarize and conclude on the theory and calculations presented in the preceding chapters. Furthermore the section will contain the bibliography and appendix.

2 Safety Instrumented Systems

Safety Instrumented Systems (SIS) have been used in the process sector, and especially the oil and gas industry, for many years as a protection layer to protect the Equipment Under Control (EUC) against hazardous incidents. Examples of SIS in the oil and gas industry and process sector:

- **PSD** – *Process Shutdown system*
- **ESD** – *Emergency Shutdown system*
- **HIP(P)S** – *High Integrity Protection System (e.g. against pressure (P), temperature, level etc.)*
- **F&G** – *Fire & Gas detection system*

A SIS may perform one or more Safety Instrumented Functions (SIF) – see Section 2.2.

IEC 61511 and IEC 61508 are the standards that address the application of SIS for the oil and gas industry, which are based on the use of electrical/electronic/ programmable electronic (E/EP/PE) technology.

2.1 Elements in SIS

A SIS consists of mainly three subsystems as illustrated in Figure 2-1. Each subsystem has different combinations of components depending on the necessity to perform the SIF and the Safety Integrity Level (SIL) required by the SIS.

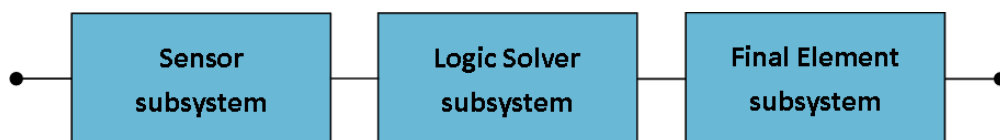


Figure 2-1: Subsystems of a SIS

2.1.1 Sensors

The components in the sensor subsystem monitor a certain process, e.g. pressure, temperature, level, fire detectors etc. The Svend HIPPS sensor subsystem consist of three smart pressure transmitters – see further description in Chapter 3 page 15. A smart sensor may be able to perform self-test and communicate any deviations to the logic solver.

2.1.2 Logic Solver

The main purpose of the logic solver subsystem is to receive, process, and act on signals from the sensor subsystem. Based on any abnormal signals from the sensor subsystem the logic solver subsystem initiates the required action of the final element subsystem. In this master thesis the logic solver components addressed are the input and output module and the logic module as illustrated in Figure 2-2.

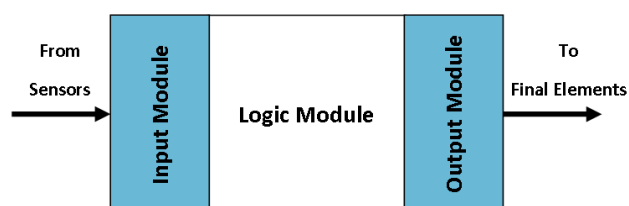


Figure 2-2: Logic Solver subsystem

2.1.3 Final Element

The final element subsystem reacts on the signal from the logic solver and the main purpose of the components in final elements subsystem is to protect the EUC. The Svend HIPPS final elements consist of a solenoid valve used to control the hydraulic supply to and from an actuating valve – see Chapter 3 page 15.

2.1.4 Design principle – fail safe

When choosing and implementing the different components in the subsystems the design can be made according to two principles:

- **Energize-to-trip**
The SIS component needs energy to perform the safety function, so if power or energy is lost the component fails to perform the safety function and a hazardous event may happen.
- **De-energize-to-trip**
In normal operation the SIS component is energized, so if power or energy is lost the component will trip and cause an activation of the safety function. This principle results in a fail-safe state where the components enter a safe state in case of a trip or malfunction due to e.g. loss of power. The Svend HIPPS system is designed as a fail-safe SIS.

2.2 Safety Instrumented Function

A Safety Instrumented Function (SIF) is designed to protect EUC against a specific demand, which in this thesis has been limited to low demand operation as described in Section 1.3.2 page 6. When operating in low demand mode the SIF is usually passive for a longer period of time. This may result in any failures being hidden in the Svend HIPPS when demand is required. Therefore it is necessary to perform regular testing:

- **Proof test**
The SIF is tested at regular time interval, τ , which might reveal dangerous undetected failures, λ_{DU} . A proof test requires man hours and could also be referred to as maintenance check.
- **Diagnostic test**
A smart component may be able to perform a self-test and reveal dangerous detected failures, λ_{DD}

More about failures in Chapter 4 page 23 and testing in Chapter 9 page 67.

The SIF is rated with a specific Safety Integrity Level (SIL) as described further in Section 2.3 and in order to quantify reliability requirements of the SIF the average Probability of Failure on Demand, PFD_{Avg} must be assessed. More about PFD_{Avg} in Chapter 5 page 29.

2.3 Safety Integrity Level

Safety integrity is a way to measure and compare performance of a SIF. In IEC 61508-4 safety integrity is defined as:

Safety Integrity

“probability of an E/E/PE safety-related system satisfactorily performing the specified safety functions under all the stated conditions within a stated period of time” [31]

The safety integrity of a component or system is divided into four different levels with level 4 being the most reliable level. Table 2-1 illustrates the four different Safety Integrity Levels (SIL) with corresponding range of Probability of Failure on Demand (PFD – see Chapter 5 page 29) and Risk Reduction Factor (RRF – see Eq. 2-1) for low-demand operation.

Table 2-1: SIL level with corresponding PFD and RRF for low-demand operation [4]

SIL	PFD range	RRF range
4	$\geq 10^{-5}$ to $< 10^{-4}$	10000-100000
3	$\geq 10^{-4}$ to $< 10^{-3}$	1000-10000
2	$\geq 10^{-3}$ to $< 10^{-2}$	100-1000
1	$\geq 10^{-2}$ to $< 10^{-1}$	10-100

where

$$RRF = \frac{1}{PFD_{Avg}} \quad \text{Eq. 2-1}$$

So if a SIF with SIL 2 fails to function then there is 100-1000 times higher risk of a hazardous event. After a system has been designed and before installation it is necessary to demonstrate that the SIL requirement is fulfilled.

The required SIL for Svend HIPPS is addressed in Section 3.2.3 page 18.

3 Svend Platform & HIPPS Installation

The normally unmanned Svend satellite platform is located in the Danish Underground Consortiums (DUC) sector of the North Sea as illustrated in Figure 3-1.

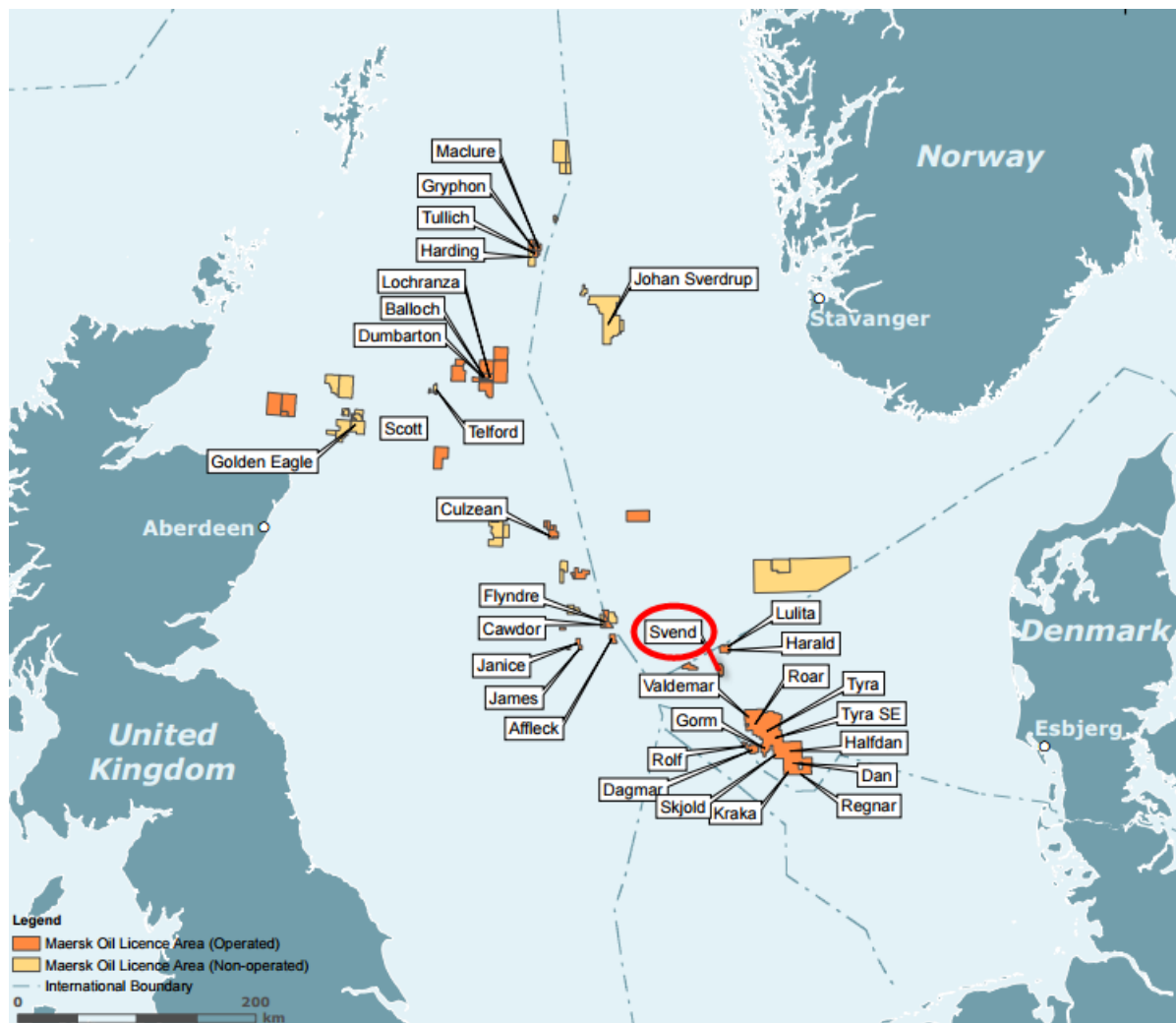


Figure 3-1: Maersk Oil in the North Sea [32]

Svend has seven drilled wells that produce crude oil and gas, which are transferred to Tyra East F (TEF) platform through pipeline P4001, a 65 km 16" subsea pipeline – see Appendix 12.7 page 87. The Tyra platforms are primarily gas production platforms but are also the export center for all gas produced in DUC to onshore gas handling – part of the connections to the Tyra platforms is illustrated in Figure 3-2 and more detailed in Appendix 12.8 page 88.

Currently Svend is shut-in due to well integrity issues. In order to drain the reservoir it is planned to re-drill new wells. Furthermore Maersk Oil has recently agreed with the Danish Government to invest and rebuild the Tyra field due to problems with sinking platforms. In order to protect the new Tyra Future project and the piping connecting Svend and Tyra it is necessary to implement a new secondary independent pressure protection system at Svend.

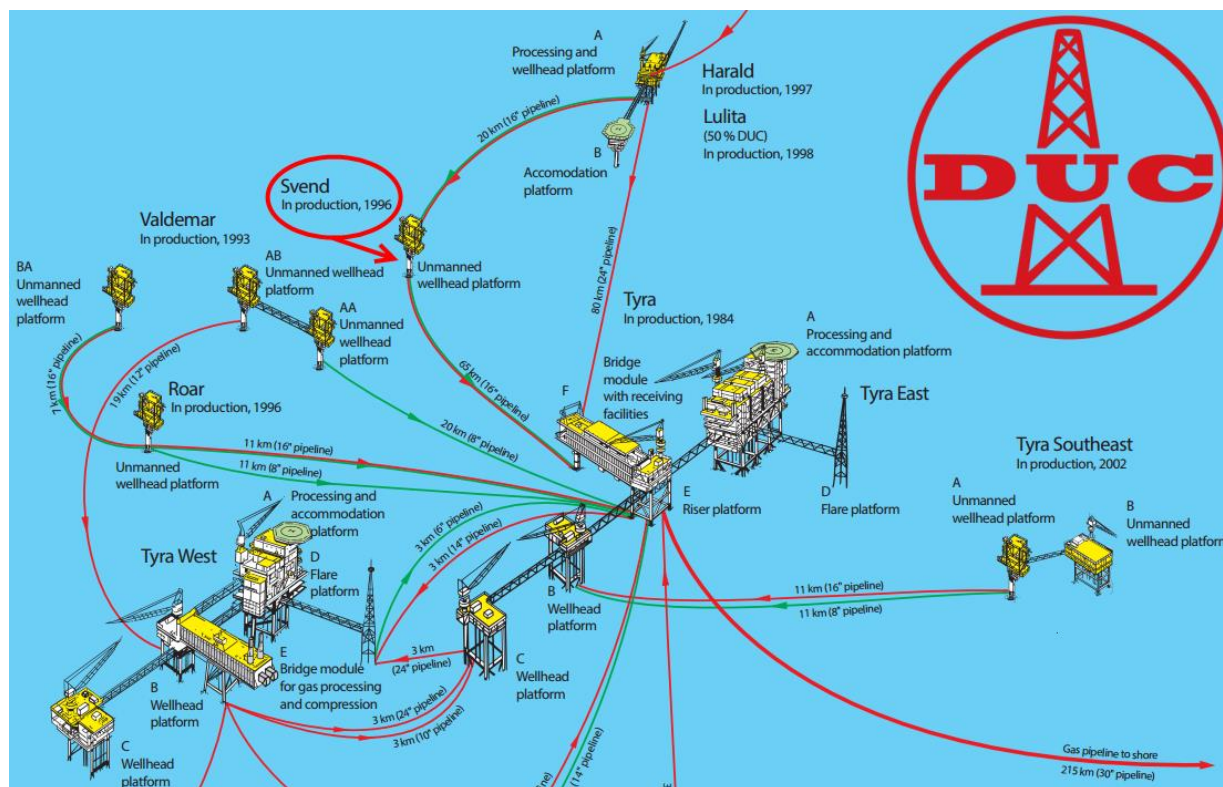


Figure 3-2: Platforms connected to Tyra field [33]

3.1 Equipment Under Control

Due to corrosion the original export riser is out of service and has been replaced with a 6" flexible hose/riser placed at the seabed as illustrated in Figure 3-3. The pressure rating of the hose is 76 barg and it is the lowest pressure rating on Svend. Svend is also a tie in point for the pipeline from Harald platform (HWA). The HIPPS shall protect the 6" flexible hose and the pipeline P4001 to TEF in order to avoid any of the hazard consequences assessed in the LOPA.

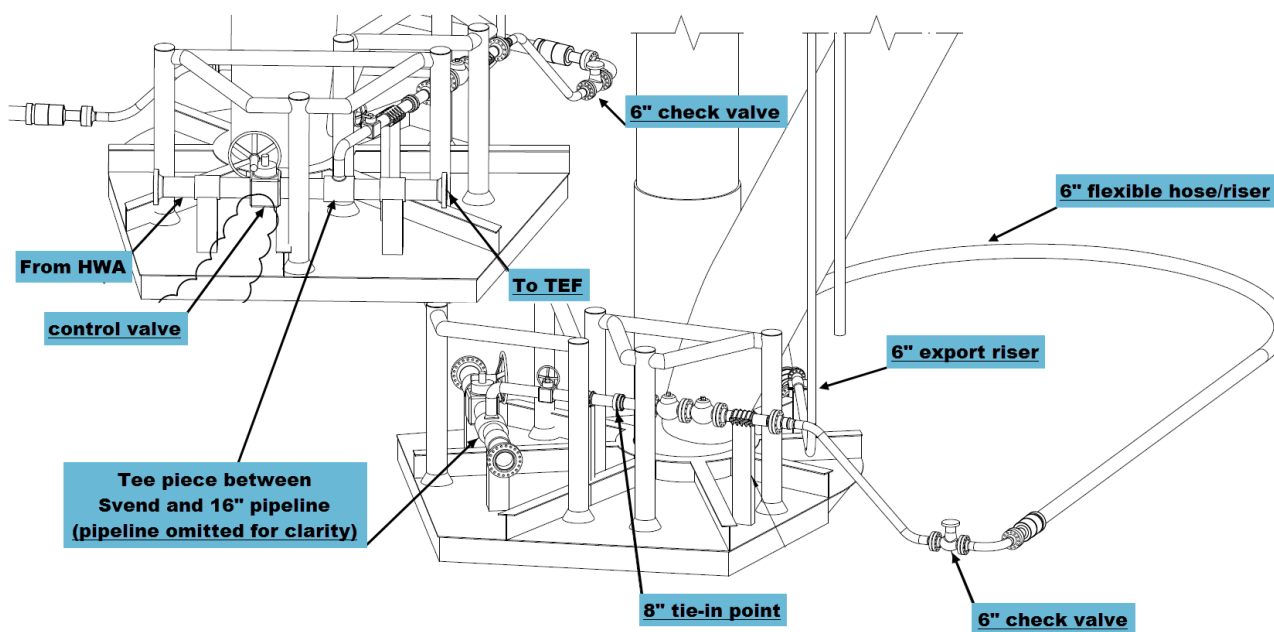


Figure 3-3: Two different views of the Svend piping at seabed [34]

3.2 HIPPS

3.2.1 Current Svend HIPPS

The current primary Emergency Shutdown (ESD) system is upgraded with extra sensors and final elements and is internally in Maersk Oil called a 1st generation High Integrity Pressure Protection System (HIPPS). According to international standards IEC61508/11 the current HIPPS does not fulfill the criteria of a HIPPS because it is not independent of the primary ESD protection system [35]. The two systems share sensors and final elements and an upgrade is needed. Table 3-1 lists the EUC of the current 1st generation HIPPS. See connection between EUC and SIS in Appendix 12.9 page 89.

Table 3-1: Equipment Under Control (EUC) and HIPPS components

EUC	Design Pressure	Sensors	Logic Solver	Final Elements
6" flexible hose/riser and	76 barg	SVA-PT-30X09		SVA-SOV-30X03 SVA-WCV-30X03
16" subsea pipeline, P-4001		SVA-PT-33004/5 SVA-PSHH-33008	SVA.FP-2201	SVA-SOV-33010 SVA-ESDV-33010

3.2.2 Future HIPPS

In order to comply with the IEC 61508/11 standards and internal MOTS-46 the HIPPS must be independent of the primary ESD system and the requirements include.

- Shall have dedicated sensors, logic solver and final elements so it is fully independent of the primary protection system.
 - Shall only handle a single Safety Instrumented Function (SIF)
 - Shall be fail safe
 - Shall generate an alarm when activated
- [36]

The considered design for Svend HIPPS is illustrated in Figure 3-4 and Appendix 12.10 page 91 illustrates the corresponding process flow diagram.

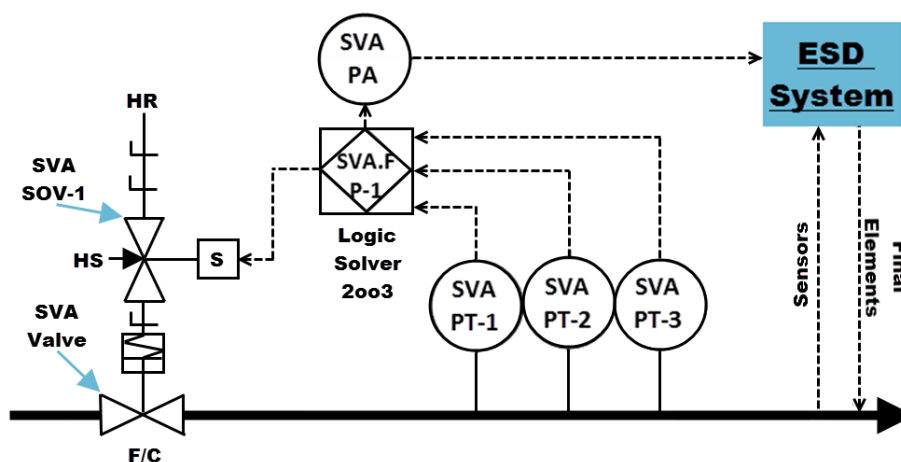


Figure 3-4: Proposed Svend HIPPS design

The pressure transmitters PT-1/3 are placed in a 2oo3 voting downstream the HIPPS valve because the EUC is downstream.

3.2.3 SIL requirement of future HIPPS

In the performed LOPA a semi-quantitative assessment of the PFD was performed using the Independent Protection Layers (IPL) to reduce the event frequency (F_E) risk of the different Initiating Causes (IC). The probabilities of each IPL can be calculated or assessed in Maersk Oil “*Standard - Safety Integrity Level (SIL) Analysis*” [37]. See Appendix 12.11 page 92 for used IC and IPL.

The event frequency pr. year (F_E) for each IC is calculated by multiplying the probability of the IC, F_{IC} with each of the probabilities of the IPLs (F_{IPL}) – as illustrated in Eq. 3-1.

$$F_E = F_{IC} \times \prod_{j=1}^n F_{IPL,j} \quad \text{Eq. 3-1}$$

The total event frequency pr. year ($F_{E,total}$) is the sum of F_E for each IC – as illustrated in Eq. 3-2.

$$F_{E,total} = \sum_{k=1}^m \left(F_{IC,k} \times \prod_{j=1}^n F_{IPL,j} \right) \quad \text{Eq. 3-2}$$

where

m = number of ICs
 n = number of IPLs

The severity of each consequence presented in Table 1-1 page 3 has a Target Mitigated Event Likelihood (TMEL) value as seen in Appendix 12.2 page 81. The TMEL is used in calculating the *PFD* for each of the different assessed consequences and associated *Safety, Environmental and Commercial Impact* – as illustrated in Eq. 3-3. [4]

$$PFD_{avg} = \frac{TMEL}{F_{E,total}} \quad \text{Eq. 3-3}$$

An example of SIL determination for *Safety Impact* of the consequence regarding over pressure at the Svend platform is illustrated in Table 12-1, Appendix 12.11 page 92.

The results for each impact are summarized in Table 3-2.

Table 3-2: SIL requirements to Svend HIPPS

Consequence	SIF	Safety SIL (PFD_{avg})	Environmental SIL (PFD_{avg})	Commercial SIL (PFD_{avg})	Total SIL (PFD_{avg})
Leak at Svend	Svend HIPPS	SIL 1 (2.8×10^{-2})	- (1.0)	SIL 1 (1.7×10^{-2})	SIL 1 (1.7×10^{-2})
Leak at TYE F	Svend HIPPS	SIL 1 (5.8×10^{-2})	- (1.0)	SIL 1 (1.4×10^{-2})	SIL 1 (1.4×10^{-2})

The highest calculated SIL is SIL 1 but according to MOTS-46 Section 7.3 the required SIL is raised to SIL 2 if the ESD system is credited as SIL 1.

“The design of the protective system shall be made such that_

- *The required SIL for the HIPS shall as a minimum be SIL 2 and as a maximum SIL 3.*
- *...*
- *If the hazard scenario overpressure is greater than the system design hydrotest pressure, then the combined SIL requirement for the protective system (primary and secondary) shall be minimum SIL 3.*
- *In the evaluation of the HIPS required SIL, credit may be taken for the presence of the ESD system to meet the overall SIL requirement for the overpressure scenario with the condition that the ESD system reacts fast enough to prevent the over-pressurisation scenario.....*
- *...”*

[36]

The PFD will be assessed with other methods in the Modelling Section page 21 and the reliability will be addressed.

(This page is intentionally left blank)

Modelling Section

(This page is intentionally left blank)

4 Failure Modes

Definition of different failure modes and rates is necessary for future modelling of reliability and will be presented in this chapter.

4.1 No Effect Failure

In IEC 61508-4 a No Effect failure is defined as:

“failure of an element that plays a part in implementing the safety function but has no direct effect on the safety function” [31]

According to the IEC definition a No Effect (or Non-critical) failure occurs when the main functions of the component are unaffected e.g. sensor imperfection.

4.2 Safe Failure

In IEC 61508-4 a safe failure is defined as:

“failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that:

- a) results in the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state; or*
- b) increases the probability of the spurious operation of the safety function to put the EUC (or part thereof) into a safe state or maintain a safe state” [31]*

According to the IEC definition a safe failure occurs when a component may operate without any demand e.g. a sensor provides a “false alarm” signal without a true demand. The safe failures can be split into:

- **Safe Detected (SD)**
SD failures are detected by automatic self-test and spurious trips are avoided.
- **Safe Undetected (SU)**
SU failures are not detected by automatic self-test and may results in spurious trips of the component.

4.3 Dangerous Failure

In IEC 61508-4 a dangerous failure is defined as:

“failure of an element and/or subsystem and/or system that plays a part in implementing the safety function that:

- a) prevents a safety function from operating when required (demand mode) or causes a safety function to fail (continuous mode) such that the EUC is put into a hazardous or potentially hazardous state; or*
- b) decreases the probability that the safety function operates correctly when required” [31]*

According to the IEC definition a dangerous failure occurs when a component does not operate as required on demand e.g. a sensor not measuring or a valve that does not close on demand. The dangerous failures can be split into:

- **Dangerous Detected (DD)**
DD failures are detected by automatic self-test.
- **Dangerous Undetected (DU)**
DU failures are not detected by automatic self-test but only by an operated performed functional proof test (maintenance) or upon demand.

4.4 Failure Rate

The individual independent failure rate $\lambda^{(i)}$ of the components can be defined based on the different failure modes and are divided in critical $\lambda_{critical}$ or non-critical $\lambda_{non-critical}$ failure rates.

$$\lambda^{(i)} = \lambda_{critical} + \lambda_{non-critical} \quad \text{Eq. 4-1}$$

$\lambda_{critical}$ are rates of failures that can cause a failure on demand or a spurious trip of the SIF, so it consist of both the safe and dangerous failures as presented in Eq. 4-2 and Table 4-1 :

$$\lambda_{critical} = \lambda_S + \lambda_D \quad \text{Eq. 4-2}$$

Table 4-1: Failure rates in critical failures

Detection	Safe Failures	Dangerous Failures
Detected	λ_{SD}	λ_{DD}
Undetected	λ_{SU}	λ_{DU}
SUM	λ_S	λ_D

The failure rates can also be expressed by the diagnostic coverage, DC which is given by the fraction:

$$DC = \frac{\lambda_{DD}}{\lambda_D} \quad \text{Eq. 4-3}$$

or

$$\lambda_{DU} = \lambda_D(1 - DC) \quad \text{Eq. 4-4}$$

A high DC value is preferred because the fraction of DU failures is small with a high DC value.

The failure rate of statistically identical and independent components follows a bathtub curve over time with three periods as illustrated in Figure 4-1:

- **Burn-in period** – early failures are often discovered at factory tests
- **Useful life period** – almost constant failure rate
- **Wear-out period** – aging equipment has an increasing failure rate

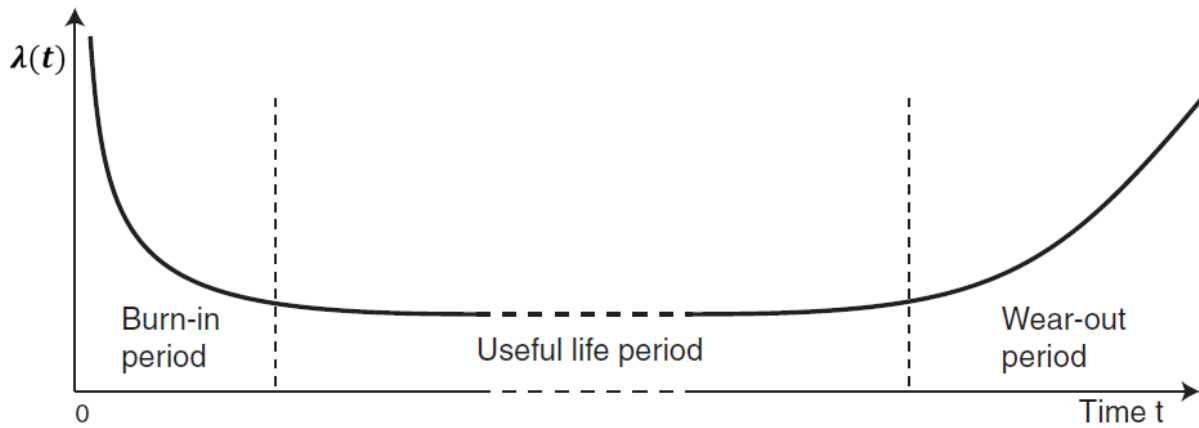


Figure 4-1: Failure rate development over time [9]

In this thesis the failure rate is assumed constant i.e. functioning in the useful life period.

4.5 Common Cause Failure (CCF)

In the quantification of reliability of a redundant SIS it is important to distinguish between independent and dependent failures.

- **Independent failures**
Random hardware failures that do not influence the failure rate of identical components in the SIS.
- **Dependent failures**
Systematic failures due to e.g. installation or operational failures, which can lead to a common cause failure.

In IEC 61508-4 a common cause failure is defined as:

“failure, that is the result of one or more events, causing concurrent failures of two or more separate channels in a multiple channel system, leading to system failure” [31]

According to the IEC definition a common cause failure is a simultaneous failure of at least two components in the SIS due to a shared cause. This may reduce the effect of a built-in redundancy.

4.5.1 β -factor standard

The CCF is accounted for in the β -factor model, presented by Fleming, in 1975 [38], where it is assumed that a certain fraction of the failures are common cause. The basic idea is to split the failure rate in two parts where

$$\lambda = (\lambda_{critical} + \lambda_{non-critical}) + \lambda_{CCF} = \lambda^{(i)} + \lambda_{CCF} \quad \text{Eq. 4-5}$$

The β -factor is the fraction of CCF failures of all the failures.

$$\beta = \frac{\lambda_{CCF}}{\lambda} \quad \text{Eq. 4-6}$$

and the failure rates can be expressed as

$$\lambda_{CCF} = \beta\lambda \quad \text{Eq. 4-7}$$

and

$$\lambda^{(i)} = (1 - \beta)\lambda \quad \text{Eq. 4-8}$$

It is relevant to distinguish between different CCF. If β_U represents the CCF rate of DU failures and β_D the DD failures, then the overall rate of dangerous CCF is:

$$\lambda_{D,CCF} = \beta_U\lambda_{DU} + \beta_D\lambda_{DD} \quad \text{Eq. 4-9}$$

The weakness in the β -factor model is the lack of credit for increased redundancy due to the fact that the individual failure rate in a high reliability SIS has almost no influence. Furthermore, the approach does not distinguish between any *moon* voting. The method described in this section only applies to identical components with constant failure rate, λ_{DU} – see Section 4.5.3 page 27 for non-identical components.

4.5.2 β -factor corrected

IEC 61508-6 Annex D.5 suggest an alternative method with a corrected β -factor, which is only applicable to hardware failures. The β -factor must be calculated for each subsystem of the SIS. This is done by answering 37 questions that each give a value for calculation of a score S_U or S_D . Each score S_U or S_D corresponds to a value for the β -factor depending on the type of subsystem – see Table 4-2 .

Table 4-2: Calculation of β_U or β_D [4]

S_U or S_D	Corresponding value of β_U or β_D for the	
	Logic Solver	Sensors or Final Elements
120 or above	0.5 %	1 %
70 to 120	1 %	2 %
45 to 70	2 %	5 %
Less than 45	5 %	10 %

For a conservative design it is possible to use the maximum β -factor values presented in Table 4-2 and still be in compliance with IEC 61508-6. In a system with redundancy IEC 61508-6 suggest to multiply the β -factor with a factor as presented in Table 4-3 in order to account for increased redundancy (MoonN voting – meaning M out of N components must react to predefined settings or conditions).

Table 4-3: Fraction of β -factor for systems with levels of redundancy greater than 1oo2 [4]

MoonN		N			
		2	3	4	5
M	1	1	0.5	0.3	0.2
	2		1.5	0.6	0.4
	3			1.75	0.8
	4				2

The numbers in Table 4-3 implies that the reduction of the β -factor is non-linear and at a certain point the effect of increased redundancy is negligible.

Other methods are applicable and the PDS method presented by Hauge et al. [39] suggests other values as presented in Table 4-4. They also suggest that it is possible to modify these factors based on personal experience and knowledge. Hauge et al. uses the symbol C_{MooN} in order to distinguish the factors from the factors presented in IEC 61508-6 in Table 4-3.

Table 4-4: C_{MooN} values for different voting logics greater than 1oo2 [39]

C_{MooN}		N				
		2	3	4	5	6
M	1	1	0.5	0.3	0.2	0.15
	2		2.0	1.1	0.8	0.6
	3			2.8	1.6	1.2
	4				3.6	1.9
	5					4.5

4.5.3 β -factor – non-identical components

Three different cases can be applicable when modelling non-identical components:

- Components with different failure rates
- Components with different β -factor
- Components with different test interval

It can be difficult to select the appropriate value for the different cases but a practical compromise is to use the geometric mean of the failure rates, the minimum β -factor, $\beta_{min} = \min_{i=1,2,...N}\{\beta_i\}$ and arithmetic mean of the proof test interval (maintenance requiring man hours), $\bar{\tau}$ as illustrated in Eq. 4-10.

$$PFD_{MooN}^{CCF} = C_{MooN} \cdot \beta_{min} \cdot \frac{\bar{\tau}}{2} \cdot \sqrt[N]{\lambda_1 \lambda_2 \lambda_3 \dots \lambda_N} \quad \text{Eq. 4-10}$$

An example of a proof test interval τ could be $\tau = 8760 \text{ hours}$, which means that a maintenance team will proof test the component each year. *DU* failures will be detected and repaired at this proof test.

4.6 Svend HIPPS Failure Modes

Components installed for a similar HIPPS at Roar platform are assumed as intended components for installation of the Svend HIPPS with the failure rates presented in Table 4-5. The values are vendor specific data delivered by Maersk Oil in connection to installation of HIPPS at Roar platform. The values will be used in calculations of the PFD_{Avg} but general formulas will be described in Chapter 5 page 29 so other values can be used if necessary.

Table 4-5: Failure rates and architecture for intended components at Svend HIPPS

Subsystem	Failure Rate [E-6/hr]				SFF [%]	Voting	β
	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}			
Pressure Transmitter	5.400E-02	0.00E+00	3.310E-01	3.900E-02	90.80	2oo3	0.02
Logic Solver Input	1.412E-01	1.412E-01	2.433E-01	1.232E-03	99.68	1oo1	0.01
Logic Solver	-	-	-	1.00E-05	99.84	1oo1	
Logic Solver Output	-	-	-	1.00E-05		1oo1	
Final Elements SOV	-	-	-	6.000E-1		1oo1	0.04
Valve	1.577	-	-	1.400E-2	91	1oo1	

The Safe Failure Fraction (SFF) is calculated as

$$SFF = \frac{\lambda_S + \lambda_{DD}}{\lambda_S + \lambda_D} \quad \text{Eq. 4-11} \quad [3]$$

The definitions of different failure modes presented in this chapter are needed in order to understand and calculate the Probability of Failure on Demand, which will be addressed in Chapter 5.

5 Probability of Failure on Demand

After introduction of Safety Instrumented Systems in Chapter 2 and different failure modes in Chapter 4 it is relevant to continue with a description of the Probability of Failure on Demand (PFD). The PFD is used as a quantitative value to distinguish different SIL from each other. Lower PFD value results in a higher SIL and a higher risk reduction factor (RRF) as described in Eq. 2-1 page 14. This chapter will describe the origin of the PFD and different analytical formulas that can be used to quantify the value for relevant architectures.

5.1 Definition of PFD

For a SIF the Probability of Failure on Demand is specified as the probability that the SIF cannot be performed at time t if a dangerous fault is present.

$$PFD(t) = \Pr(\text{The SIF cannot be performed at time } t) \quad \text{Eq. 5-1}$$

Most often it is not necessary to express the $PFD(t)$ as a function of time and an average value PFD_{Avg} is sufficient. If a SIF is proof tested as described in Section 2.2 page 13 with regular periodic time interval τ and considered as good as new after the proof test then:

$$PFD_{Avg} = \frac{1}{\tau} \int_0^{\tau} PFD(t) dt \quad \text{Eq. 5-2}$$

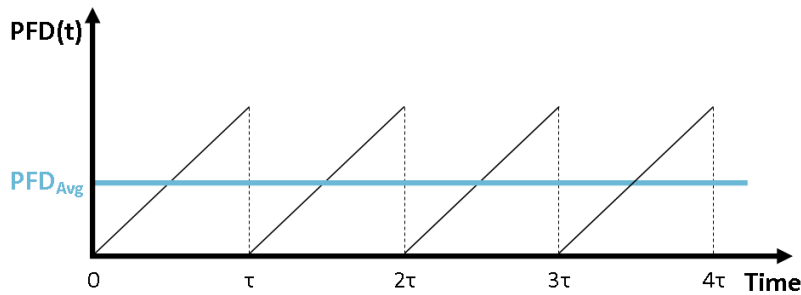


Figure 5-1: Illustration of PFD_{Avg} for periodically proof-tested components [39]

It can also be expressed as illustrated in Eq. 5-3.

$$PFD_{Avg} = 1 - \frac{1}{\tau} \int_0^{\tau} R(t) dt \quad \text{Eq. 5-3}$$

, where $R(t)$ is the reliability function or survivor function and

$$PFD(t) = F(T) = 1 - R(t) = 1 - e^{-\lambda_{DU}t} \quad \text{Eq. 5-4} \quad [3]$$

A SIL 2 with a $PFD_{Avg} = 5 \cdot 10^{-2}$ means that the SIF on average will fail 5 out of 1000 demands. The PFD_{Avg} value is used for low-demand operation but for high-demand operation it is necessary to express the Probability of Failures pr. Hour, PFH – this is not addressed further due to the limitations of the thesis.

5.2 Requirements

In a SIF it is possible to calculate the PFD_{Avg} separately for each independent subsystem and add them:

$$PFD_{Avg,SIF} = PFD_{Avg,S} + PFD_{Avg,LS} + PFD_{Avg,FE} \quad \text{Eq. 5-5}$$

[4]

In order to determine PFD_{Avg} for each subsystem the following information must be present:

- the system architecture and voting
- the diagnostic coverage, DC of each component/channel
- the failure rate (λ_{DU}) per hour for each component/channel
- the common cause factors β_U or β_D (see Section 4.5 page 25)

PFD_{Avg} can be evaluated with different methods and simplified equations based on different standards e.g. IEC 61508-6 or ISA-TR84.0.02. A study by HIMA Group demonstrated the difficulty of comparing different methods or standards because the calculation of the PFD_{Avg} -values are based on different parameters. They also concluded that IEC 61508 has a universal application approach [26] [27]. Based on this, the thesis will mainly focus on equations from IEC 61508-6 and if relevant compare results to simplified formulas.

5.3 PFD Formulas Relevant for Svend HIPPS

The Svend HIPPS architecture consists of three subsystems in series where the Sensor subsystem is a 2oo3 voting and the Logic Solver subsystem is a 1oo2 voting. IEC 61508-6 introduces different formulas for calculating the PFD_{Avg} . Only relevant formulas are presented in this thesis.

5.3.1 IEC 61508-6 Formulas

1oo1 Voting

If a SIF has more than one voted group of sensors or final elements then the $PFD_{Avg,S}$ or $PFD_{Avg,FE}$ is the sum of the average PFD for each of the voted groups, PFD_G .

$$PFD_{Avg,S} = \sum_i PFD_{G,i} \quad \text{Eq. 5-6}$$

or

$$PFD_{Avg,FE} = \sum_j PFD_{G,j} \quad \text{Eq. 5-7}$$

The Svend HIPPS architecture only has one voted group in each subsystem so $PFD_{Avg,FE} = PFD_G$ and the IEC formula is for a 1oo1 voting is:

$$PFD_{Avg,IEC}^{1oo1} = PFD_G = (\lambda_{DD} + \lambda_{DU})t_{CE} \quad \text{Eq. 5-8}$$

where t_{CE} is the combined down time in hours for all components in the subsystem.

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \left(\frac{\tau}{2} + MRT \right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \quad \text{Eq. 5-9}$$

MRT is Mean Repair Time in hours of a DU fault, and $MTTR$ is Mean Time To Restoration in hours of a DD fault.

1002 Voting

The Logic Solver subsystem in the Svend HIPPS consists of three components in series that are in a 1002 voting with three other components in series. The IEC formula for a 1002 voting is:

$$PFD_{Avg,IEC}^{1002} = 2((1 - \beta_D)\lambda_{DD} + (1 - \beta_U)\lambda_{DU})^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta_U \lambda_{DU} \left(\frac{\tau_1}{2} + MRT \right) \quad \text{Eq. 5-10}$$

Where t_{GE} is the combined down time in hours for all components in a voted group:

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D} \left(\frac{\tau_1}{3} + MRT \right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \quad \text{Eq. 5-11}$$

2003 Voting

The Sensor subsystem in the Svend HIPPS consists of three components in a 2003 voting. The IEC formula for a 2003 voting is:

$$PFD_{Avg,IEC}^{2003} = 6((1 - \beta_D)\lambda_{DD} + (1 - \beta_U)\lambda_{DU})^2 t_{CE} t_{GE} + \beta_D \lambda_{DD} MTTR + \beta_U \lambda_{DU} \left(\frac{\tau_1}{2} + MRT \right) \quad \text{Eq. 5-12}$$

5.3.2 Simplified Formulas

The formulas in IEC 61508-6 may be simplified by integrating the survivor function $R(t)$ as presented in this section.

1001 Voting

The $PFD_{Avg,Simpl.}^{1001}$ for a single component can be evaluated by integration of the survivor function, $R(t)$.

$$PFD_{Avg,Simpl.}^{1001} = 1 - \frac{1}{\tau} \int_0^\tau R(t) dt = 1 - \frac{1}{\tau} \int_0^\tau e^{-t\lambda_{DU}} dt = 1 - \frac{1}{\lambda_{DU}\tau} (1 - e^{-\tau\lambda_{DU}}) \quad \text{Eq. 5-13}$$

Using Taylor Series expansion (See Appendix 12.14 page 98) and a value $\lambda_{DU}\tau < 0.1$ reduces Eq. 5-13 to:

$$PFD_{Avg,Simpl.}^{1001} \approx \frac{\lambda_{DU}\tau}{2} \quad \text{Eq. 5-14}$$

The value of Eq. 5-14 is a conservative approximation and therefore a higher value than that of Eq. 5-13.

Series Structure Voting

In a series structure all components have to function in order for the system to function.

The survivor function is:

$$R(t) = e^{-(\sum_{i=1}^n \lambda_{DU,i})t} \quad \text{Eq. 5-15}$$

With integration, Taylor Series expansion, reduction and $\lambda_{DU,i}\tau < 0.1$ for all i , then

$$PFD_{Avg,Simpl.}^{noon} \approx \sum_{i=1}^n PFD_{Avg,i} \quad \text{Eq. 5-16}$$

1oo2 Voting

The Logic Solver components are placed in two series structures that are in a 1oo2 voting. The survivor function is

$$R(t) = e^{-t\lambda_{DU,1}} + e^{-t\lambda_{DU,2}} - e^{-t(\lambda_{DU,1} + \lambda_{DU,2})} \quad \text{Eq. 5-17}$$

With integration, Taylor Series expansion, and reduction [3]:

$$PFD_{Avg,Simpl.}^{1oo2} \approx \frac{\lambda_{DU,1}\lambda_{DU,2}\tau^2}{3} \quad \text{Eq. 5-18}$$

And for identical components

$$PFD_{Avg,Simpl.}^{1oo2} \approx \frac{(\tau\lambda_{DU})^2}{3} \quad \text{Eq. 5-19}$$

Furthermore the PFD_{CCF} must be added – see Eq. 5-22.

2oo3 Voting

It can be time consuming to integrate a survivor function of a 2oo3 architecture so a simplified approach may be used. The 2oo3 voting can be replaced by a series structure of 1oo2, so

$$\begin{aligned} PFD_{Avg,Simpl.}^{2oo3} &\approx \frac{\lambda_{DU,1}\lambda_{DU,2}\tau^2}{3} + \frac{\lambda_{DU,1}\lambda_{DU,3}\tau^2}{3} + \frac{\lambda_{DU,2}\lambda_{DU,3}\tau^2}{3} \\ &= \frac{(\lambda_{DU,1}\lambda_{DU,2} + \lambda_{DU,1}\lambda_{DU,3} + \lambda_{DU,2}\lambda_{DU,3})\tau^2}{3} \end{aligned} \quad \text{Eq. 5-20}$$

[3]

And for identical components:

$$PFD_{Avg,Simpl.}^{2oo3} \approx \frac{3(\tau\lambda_{DU})^2}{3} = 3PFD_{Avg}^{1oo2} \quad \text{Eq. 5-21}$$

5.3.3 CCF

The Common Cause Failures consist of a DD and a DU part as illustrated in Eq. 5-22.

$$PFD_{CCF} = PFD_{CCF,DD} + PFD_{CCF,DU} \approx \beta_D \lambda_{DD} MTTR + \beta_U \lambda_{DU} \left(\frac{\tau}{2} + MRT \right) \quad \text{Eq. 5-22}$$

5.4 Summary of Formulas

Table 5-1 summarizes the IEC 61508-6 and simplified formulas. In the simplified formulas only DU faults are considered. Furthermore the proof testing is assumed perfect and the MRT is assumed short so it can be neglected. Values for the Svend HIPPS will be addressed in Chapter 6.

Table 5-1: PFD_{Avg} IEC and simplified formulas for different architectures used in Svend HIPPS

Architecture	Simplified			IEC
	Identical	Non identical	CCF	
1oo1	$\frac{\lambda_{DU}\tau}{2}$	-	-	$(\lambda_{DD} + \lambda_{DU})t_{CE}$,
Series (noon)	$n \frac{\lambda_{DU}\tau}{2}$	$\sum_{i=1}^n PFD_{Avg,i}^{1oo1}$	-	$n(\lambda_{DD} + \lambda_{DU})t_{CE}$
1oo2	$\frac{(\tau\lambda_{DU})^2}{3}$	$\frac{\lambda_{DU,1}\lambda_{DU,2}\tau^2}{3}$	$\beta_U\lambda_{DU}\frac{\tau}{2}$	$2((1 - \beta_D)\lambda_{DD}$ $+ (1 - \beta_U)\lambda_{DU})^2 t_{CE}t_{GE}$ $+ \beta_D\lambda_{DD}MTTR$ $+ \beta_U\lambda_{DU}\left(\frac{\tau}{2} + MRT\right)$
2oo3	$(\tau\lambda_{DU})^2$	$\frac{(\lambda_{DU,1}\lambda_{DU,2})\tau^2}{3}$ $+ \frac{(\lambda_{DU,1}\lambda_{DU,3})\tau^2}{3}$ $+ \frac{(\lambda_{DU,2}\lambda_{DU,3})\tau^2}{3}$	$\beta_U\lambda_{DU}\frac{\tau}{2}$ or $C_{2oo3}\beta_{min}\frac{\tau^3}{2}\sqrt{\lambda_1\lambda_2\lambda_3}$	$6((1 - \beta_D)\lambda_{DD}$ $+ (1 - \beta_U)\lambda_{DU})^2 t_{CE}t_{GE}$ $+ \beta_D\lambda_{DD}MTTR$ $+ \beta_U\lambda_{DU}\left(\frac{\tau}{2} + MRT\right)$
with	$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{\tau}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D}MTTR$ and $t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{\tau}{3} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D}MTTR$			

6 Reliability Block Diagrams

As described in Figure 1-2 page 5 Reliability Block Diagrams (RBD) is one of the quantitative methods to evaluate the reliability of a SIS. This chapter will describe how RBD is used to determine the reliability of the Svend HIPPS.

A Reliability Block Diagram (RBD) shows the successful functioning of a system. It is important to emphasize that the pictorial representation of the individual components merely shows the functioning. This is not necessarily equivalent to the physical order of the components. The RBD can be used to represent logical equations of Boolean variables. RBD can be used for qualitative and quantitative analysis of a system.

6.1 Assumptions and Definitions

The RBD is used to model the functioning of the system based on some fundamental assumptions and definitions of states as described in this section 6.1. These assumptions have to be fulfilled in order to use analytical calculations presented in IEC 61078 [40]. Otherwise Monte Carlo simulations can be used but this master thesis has been limited to analytical calculations as described in Section 1.3 page 4.

6.1.1 State of system

The state of the whole system can be described by the structure function

$$\phi(\mathbf{X}) = \phi(x_1, x_2, x_3, \dots, x_n) \quad \text{Eq. 6-1}$$

$$\phi(\mathbf{X}) = \begin{cases} 1 & \text{if system is functioning} \\ 0 & \text{otherwise} \end{cases} \quad \text{Eq. 6-2}$$

The system has only two states:

- Functioning ("up" state)
- Failed ("down" state)

The RBD links the logic between the up state of the system and the up state of the individual components.

6.1.2 State of components

Each component in a system is modelled by independent working blocks in the RBD. Each component can have only two possible states:

- Functioning ("up" state)
- Failed ("down" state)

If the state i is represented by a state variable, then

$$x_i = \begin{cases} 1 & \text{if component } i \text{ is functioning} \\ 0 & \text{otherwise} \end{cases} \quad \text{Eq. 6-3}$$

The state vector is

$$\mathbf{X} = (x_1, x_2, x_3, \dots, x_n) \quad \text{Eq. 6-4}$$

6.2 Graphical & Mathematical Illustration of Boolean Logic [40]

With the defined state of the system and components the graphical RBD can be constructed and represent a Boolean logic and mathematical expression of the system structure. Different building blocks and Boolean logic operators for illustration of the system structure are presented in Figure 6-1.

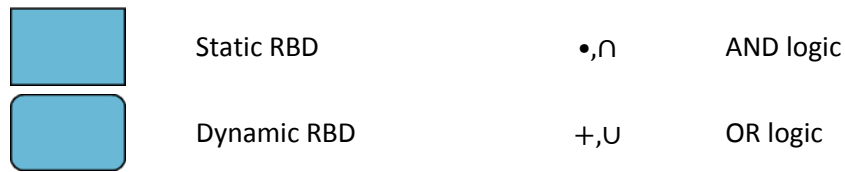


Figure 6-1: RBD type and Boolean logic operators

6.2.1 Series structures

In a series structure, as illustrated in Figure 6-2, all components need to function in order for the system to function.

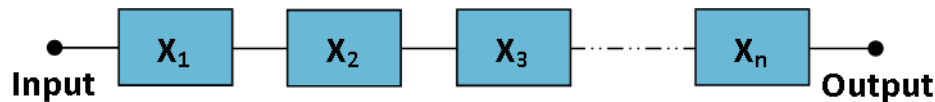


Figure 6-2: Series RBD

The series RBD represents the Boolean logic in Eq. 6-5 and mathematical expression in Eq. 6-6.

$$\phi(X) = x_1 \cdot x_2 \cdot x_3 \cdot \dots \cdot x_n = x_1 \cap x_2 \cap x_3 \cap \dots \cap x_n \quad \text{Eq. 6-5}$$

$$\phi(X) = x_1 x_2 x_3 \cdot \dots \cdot x_n = \prod_{i=1}^n x_i \quad \text{Eq. 6-6}$$

6.2.2 Parallel structures and *m* out of *n* (moon) structures

In a parallel structure, illustrated in Figure 6-3, only one component in up state is required for the system to be in up state. This structure is used when redundant components are implemented in the system.

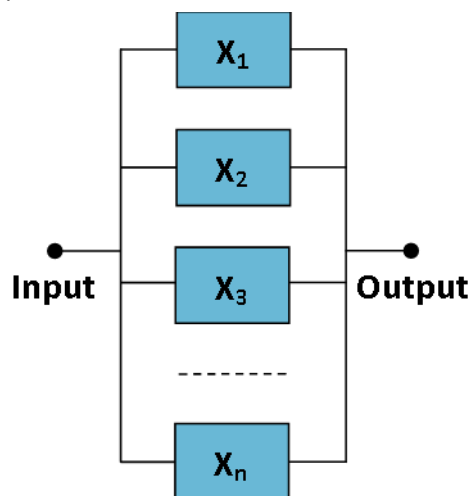


Figure 6-3: Parallel RBD

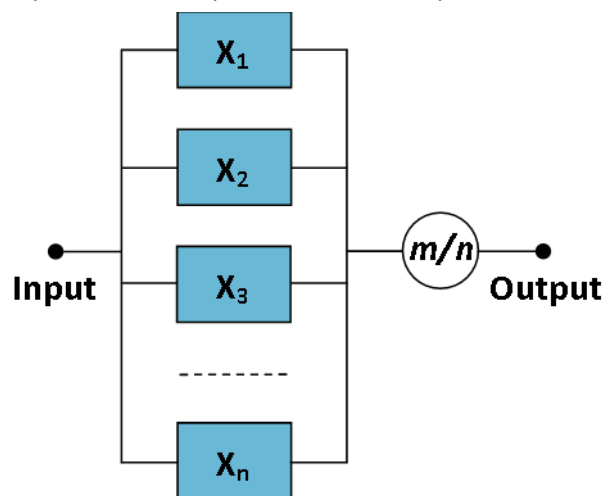


Figure 6-4: moon RBD

The parallel RBD represents the Boolean logic in Eq. 6-7 and mathematical expression in Eq. 6-8.

$$\phi(X) = x_1 + x_2 + x_3 + \dots + x_n = x_1 \cup x_2 \cup x_3 \cup \dots \cup x_n \quad \text{Eq. 6-7}$$

$$\phi(X) = 1 - (1 - x_1)(1 - x_2)(1 - x_3) \dots (1 - x_n) = 1 - \prod_{i=1}^n (1 - x_i) \quad \text{Eq. 6-8}$$

A special case of a parallel RBD is when a voting is implemented in the logic and m out of n components are required to be in up state in order for the system to be in up state. The RBD of this case is illustrated in Figure 6-4 and also illustrated with an example of a 2oo3 voting in Figure 6-5 and Figure 6-6.

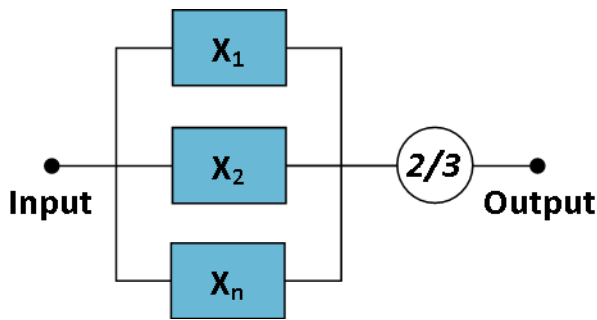


Figure 6-5: 2oo3 RBD

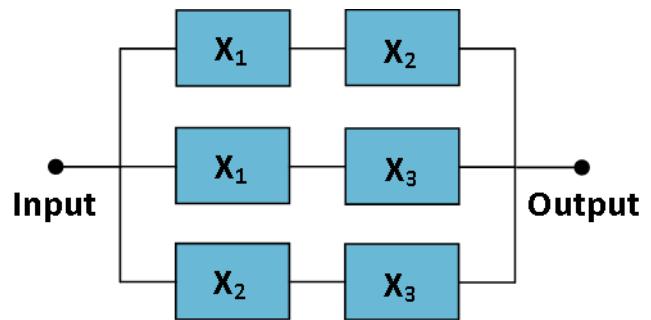


Figure 6-6: Equivalent 2oo3 RBD

The 2oo3 RBD represents the Boolean logic in Eq. 6-9 and mathematical expression in Eq. 6-10.

$$\phi(X) = x_1 \cdot x_2 + x_1 \cdot x_3 + x_2 \cdot x_3 = x_1 \cap x_2 \cup x_1 \cap x_3 \cup x_2 \cap x_3 \quad \text{Eq. 6-9}$$

$$\phi(X) = x_1x_2 + x_1x_3 + x_2x_3 - 2x_1x_2x_3 \quad \text{Eq. 6-10}$$

See Appendix 12.12 page 93 for derivation of Eq. 6-10.

6.2.3 Other structures

A complex system can be represented by a mix of subsystems of series, parallel, and *moon* structures. In large and complex systems it is possible to use transfer gates and it is also possible for systems to share blocks.

6.3 Probability Calculations

The state variable x_i defined in Section 6.1 page 34 is deterministic as it can be in either up state or down state. In reliability analysis the state variable is random and dependent on time, which is illustrated with the variable, $X_i(t)$. With a random variable it is possible to determine the probability, Pr , of a component, i , or system, s , to be in either up state $\Pr(X_{i/s}(t) = 1)$ or down state $\Pr(X_{i/s}(t) = 0)$.

$$\Pr(X_{i/s}(t) = 1) = \Pr(T > t) = p_{i/s}(t) \quad \text{Eq. 6-11}$$

$$\Pr(X_{i/s}(t) = 0) = \Pr(T < t) = 1 - p_{i/s}(t) \quad \text{Eq. 6-12}$$

6.3.1 Constant probability of failure or success

The reliability function $p_i(t)$ is equivalent to the survival function $R_i(t)$ if the component is non-repairable and equivalent to the availability function $A_i(t)$ if the component is repairable.

Using the probability formulas in Eq. 6-11 and Eq. 6-12 it is possible to derive formulas for series, parallel, and moon structures for non-repairable systems as presented in Table 6-1 [40].

Table 6-1: Probability Formulas [40]

Architecture	Constant Probability of Success
Series	$p_s = R_s = \prod_{i=1}^n p_i$
Parallel	$p_s = 1 - \prod_{i=1}^n (1 - p_i)$
moon (identical components)	$p_s = \sum_{j=m}^n \binom{n}{j} p^j (1-p)^{n-j}$ $p_s = \sum_{j=0}^{n-m} \binom{n}{j} p^{n-j} (1-p)^j$

6.3.2 Moon (non-identical components) IEC 11.8.2

If the components in a Moon structure are non-identical it is not possible to use the equations presented in Table 6-1. The availability of the system can be evaluated with use of different techniques:

- Probability Theorem
- Boolean Truth Tables
- Karnaugh Maps
- Shannon Decomposition
- Sylvester-Poincaré Formula

The use of these techniques is beyond the scope of this thesis but the interested reader can find Boolean Truth Tables and Karnaugh Maps calculations of a Zoo3 structure in Appendix 12.13 page 95.

6.4 Svend HIPPS – RBD and PFD Calculations

As presented in Chapter 5 page 29 the following information must be present in order to determine PFD_{Avg} for each subsystem:

- the system architecture and voting
- the diagnostic coverage (DC) of each component/channel
- the failure rate (λ_{DU}) per hour for each component/channel
- the common cause factors β_U or β_D (see Section 4.5 page 25)

The Svend HIPPS architecture and voting are presented in Figure 6-7.

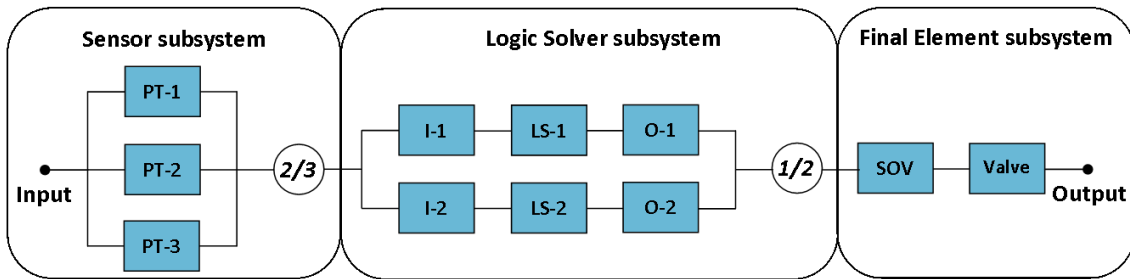


Figure 6-7: Svend HIPPS architecture and voting without CCF

The total Probability of Failure on Demand is the sum of the PFD from each subsystem:

$$PFD_{Avg,SIF} = PFD_{Avg,S} + PFD_{Avg,LS} + PFD_{Avg,FE} \quad \text{Eq. 6-13}$$

6.4.1 Sensor subsystem

The RBD of Svend HIPPS sensor subsystem is illustrated in Figure 6-8. The architecture is a 2oo3 voting with CCF factors β_U or β_D .

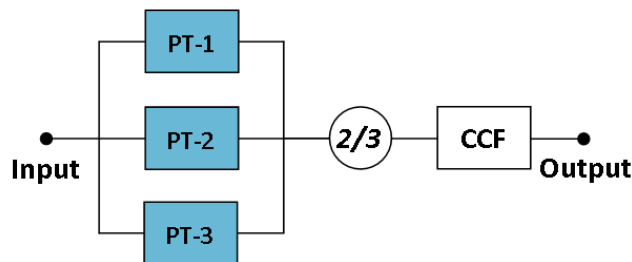


Figure 6-8: RBD of Svend HIPPS sensor subsystem

Using the IEC and simplified formulas presented in Table 5-1 page 33 with the failure rates and CCF factors β_U or β_D presented in Table 4-5 page 28 and $MTTR = MTR = 8 \text{ hours}$ and $\tau = 8760 \text{ hours}$ (standard IEC values for $MTTR$, MTR and τ) results in

$$PFD_{Avg,S}^{IEC} = 3.57E^{-6} \quad \text{Eq. 6-14}$$

$$PFD_{Avg,S}^{Simplified} = 3.53E^{-6} \quad \text{Eq. 6-15}$$

The results show a deviation of approximately 1% between the IEC and simplified formulas.

6.4.2 Logic Solver subsystem

The RBD of Svend HIPPS Logic Solver subsystem is illustrated in Figure 6-9. The architecture is a series structure in a 1oo2 voting with CCF factors β_U or β_D .

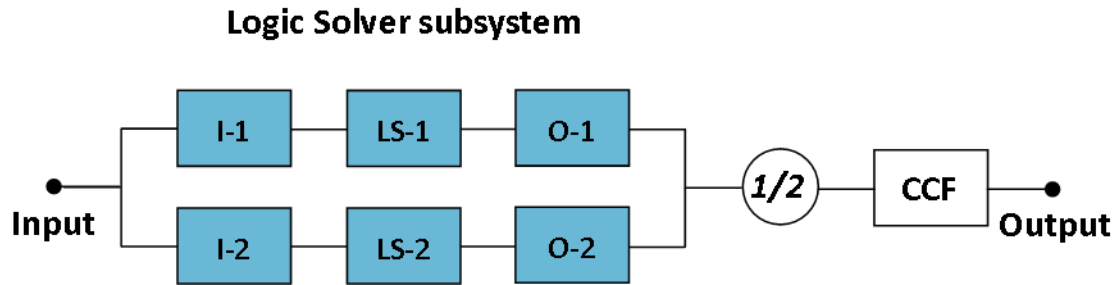


Figure 6-9: RBD of Svend HIPPS logic solver subsystem

Using the IEC and simplified formulas presented in Table 5-1 page 33 with the failure rates and CCF factors β_U or β_D presented in Table 4-5 page 28 and $MTTR = MTR = 8 \text{ hours}$ and $\tau = 8760 \text{ hours}$ results in

$$PFD_{Avg,LS}^{IEC} = 6.48E^{-8} \quad \text{Eq. 6-16}$$

$$PFD_{Avg,LS}^{Simplified} = 5.49E^{-8} \quad \text{Eq. 6-17}$$

The results show a deviation of approximately 15% between the IEC and simplified formulas.

6.4.3 Final Element subsystem

The RBD of Svend HIPPS Final Element subsystem is illustrated Figure 6-10. The architecture is a series structure.

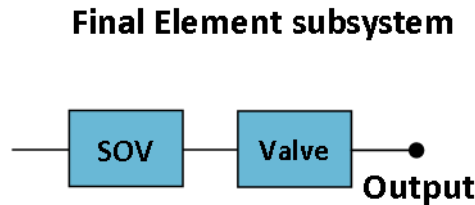


Figure 6-10: RBD of Svend HIPPS final element subsystem

Using the IEC and simplified formulas presented in Table 5-1 page 33 with the failure rates and CCF factors β_U or β_D presented in Table 4-5 page 28 and $MTTR = MTR = 8 \text{ hours}$ and $\tau = 8760 \text{ hours}$ results in

$$PFD_{Avg,FE}^{IEC} = 2.69E^{-3} \quad \text{Eq. 6-18}$$

$$PFD_{Avg,FE}^{Simplified} = 2.69E^{-3} \quad \text{Eq. 6-19}$$

6.5 Table Determination

If the diagnostic coverage DC , the dangerous failure rate λ_D , and the common cause beta factor β_U ($\beta_D = 0.5 \beta_U$) are known then IEC 61508-6 provides detailed tables for systems in low demand mode of operation. IEC 61508-6 Table B2-B5 gives a PFD_{Avg} value for different voting and with a proof test interval

τ ranging from 6 months to ten years. To give a more detailed version of the tables the MATLAB script in Appendix 12.15 page 99 was programmed and validated with the values presented in IEC 61508-6 Table B2-B5. The script produces a noon, 1oo2 and 2oo3 table as used in the Svend HIPPS architecture. The columns of the produced table represent increasing DC from 0-100% with a 1% step. The rows of the produced table represent beta factor β_U from 0-20% with a 1% step. The only user input is the dangerous failure rate λ_D and the proof test interval τ . The tables are exported to Excel for further data analysis.

6.5.1 Table Analysis

The figures in this section are based on exported Excel tables from the MATLAB script presented in Appendix 12.15 page 99. The values used for Figure 6-11 to Figure 6-13 are $\lambda_D = 5E^{-06}$ [1/hr] and $\tau=8760$ hours.

Figure 6-11 illustrates the PFD_{Avg} as a function of diagnostic coverage for five different values of common cause beta factor.

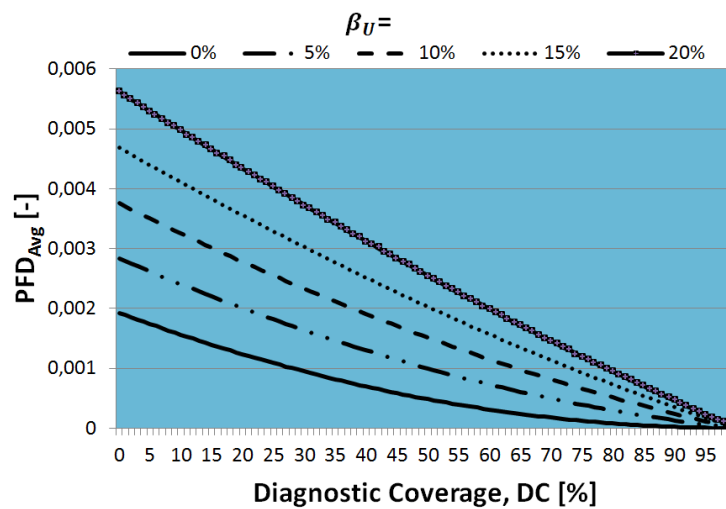


Figure 6-11: PFD_{Avg} for a 2oo3 voting with common cause beta factors from 0% to 20 % (step 5 %)

Figure 6-12 illustrates the PFD_{Avg} as a function of common cause beta factor for six different values of diagnostic coverage.

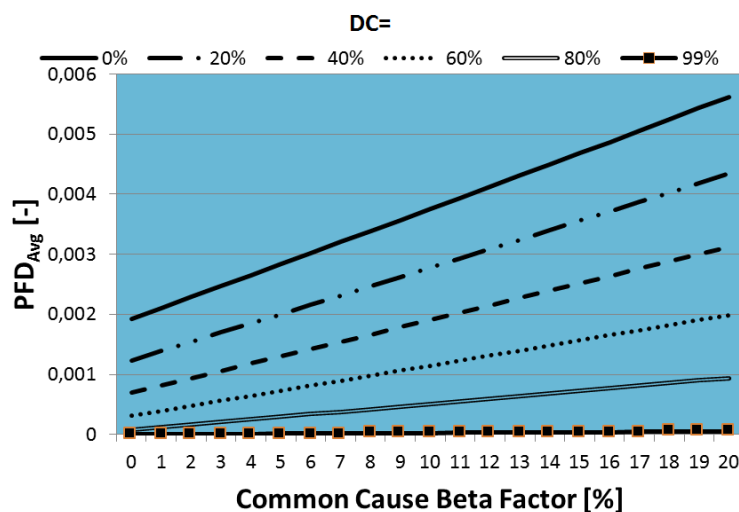


Figure 6-12: PFD_{Avg} for a 2oo3 voting with diagnostic coverages from 0% to 99 % (step 20 %)

Figure 6-13 illustrates the PFD_{Avg} as a function of diagnostic coverage for common cause beta factor $\beta_U = 5\%$ for a 1oo2 and 2oo3 voting system.

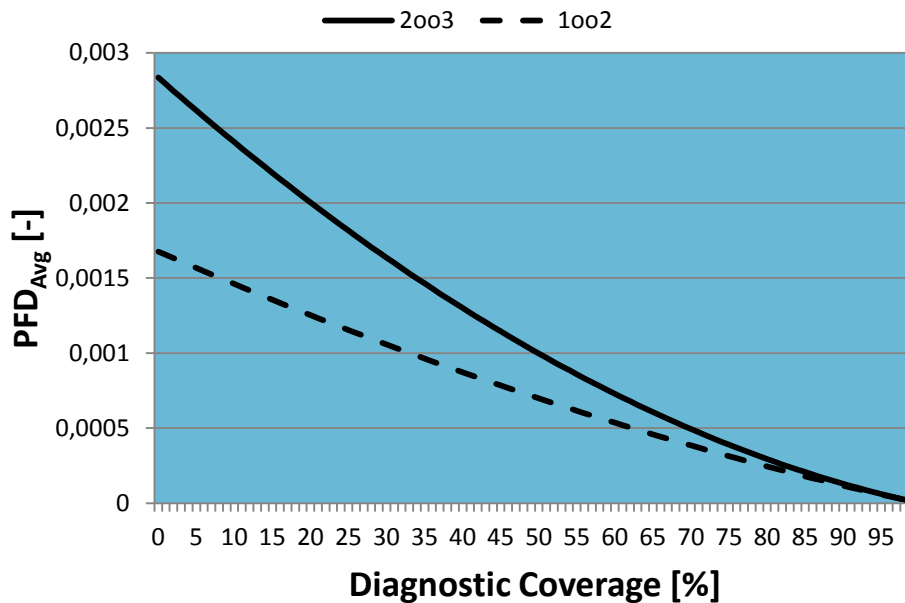


Figure 6-13: Difference between PFD_{Avg} for 1oo2 and 2oo3 voting (beta = 5 %)

Figure 6-14 illustrates the PFD_{Avg} as a function of diagnostic coverage for common cause beta factor $\beta_U = 5\%$ for three different values of dangerous failure rate λ_D (logarithmic scale).

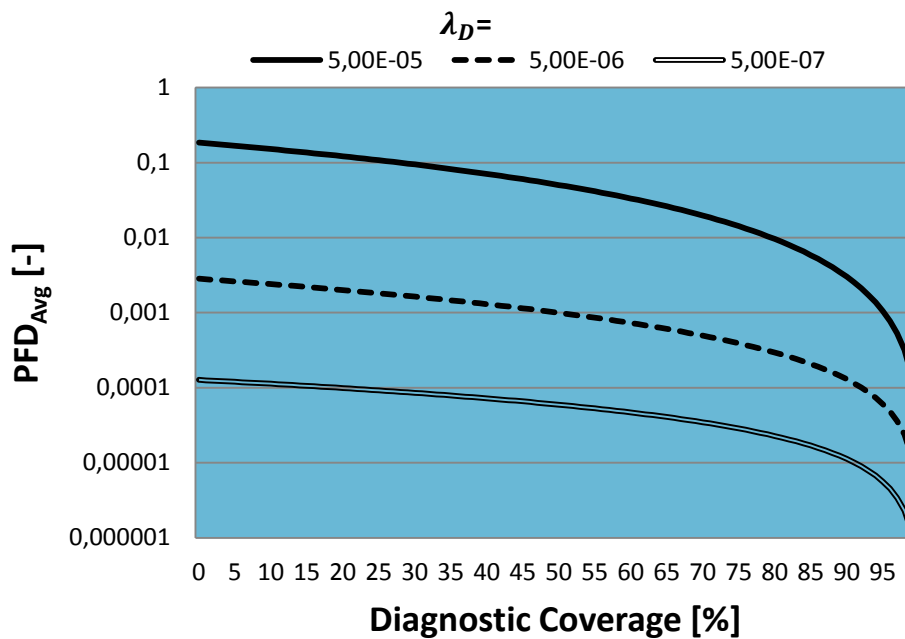


Figure 6-14: Difference between PFD_{Avg} for different values of dangerous failure rate (beta = 5 %)

6.5.2 Summary

The tables from the MATLAB script and IEC 61508 Table B2-B5 can be used as a quick reference for determining the PFD_{Avg} instead of performing calculations. The figures in Section 6.5.1 illustrate the importance of choosing components with a high diagnostic coverage and to implement components with a low common cause beta factor. A low dangerous failure rate also has a significant factor in the final value of PFD_{Avg} . Using the tables will give the same PFD_{Avg} value as IEC formula calculations.

6.6 Results of Svend HIPPS Calculations

The calculated values of PFD_{Avg} for each subsystem are listed in Table 6-2. The column with header $(1.5\beta_U)$ illustrates the value if the β -factor is corrected for as described in Section 4.5.2 page 26.

Table 6-2: Summary of PFD_{Avg} values for Simplified and IED calculations

Subsystem	Simplified	IEC	$1.5\beta_U$
Sensor	$3.53E^{-6}$	$3.57E^{-6}$	$5.29E^{-6}$
Logic Solver	$5.49E^{-8}$	$6.48E^{-8}$	$6.48E^{-8}$
Final Element	$2.69E^{-3}$	$2.69E^{-3}$	$2.69E^{-3}$
Total	$2.69E^{-3}$	$2.70E^{-3}$	$2.70E^{-3}$

The total Probability of Failure on Demand is the sum of the PFD from each subsystem so the total is

$$PFD_{Avg,SIF}^{RBD,IEC} = 2.70E^{-3} \quad \text{Eq. 6-20}$$

$$PFD_{Avg,SIF}^{RBD,Simplified} = 2.69E^{-3} \quad \text{Eq. 6-21}$$

This gives a risk reduction factor and SIL

$$RRF_{SIF}^{RBD,IEC} = 370 \quad SIL_{SIF}^{RBD,IEC} = 2 \quad \text{Eq. 6-22}$$

$$RRF_{SIF}^{RBD,Simplified} = 371 \quad SIL_{SIF}^{RBD,Simplified} = 2 \quad \text{Eq. 6-23}$$

The results in Table 6-2 illustrates the significance and importance of the Final Element subsystem in the total PFD_{Avg} . Furthermore the use of corrected β -factor gives a more conservative result for the Sensor subsystem even though the impact on the total PFD_{Avg} is insignificant. It is though still important to use voting and increased reliability of the sensor in order to avoid spurious trips and possible production loss due to shut down. It is important to choose components with a high DC and low β -factor but also with a low dangerous failure rate λ_D . The required MOTS-46 SIL 2 for the Svend HIPPS is achieved with the described configuration and architecture of the components.

6.6.1 Article Comparison

Furthermore the results show a small deviation whether the simplified or IEC formulas for RBD are used. This is also formulated in different articles about RBD and reliability e.g. Böröcsök [26] or Guo and Yang [16]. They compare different methods and example of results from Böröcsök is illustrated in Figure 6-15 to Figure 6-17

Fictive module	λ_b [1/h]	MTTF [years]	λ_S [1/h]	λ_D [1/h]	λ_{DD} [1/h]	λ_{DU} [1/h]	MTTR [h]	β_D	β
	1,700E-07	671,50	8,500E-08	8,500E-08	8,415E-08	8,500E-10	8	0,01	0,02

Figure 6-15: Values used in calculation by Böröcsök [26]

PFD-calculation for a 1oo2-system

Diagram of the different PFD-values for a 1oo2-system:

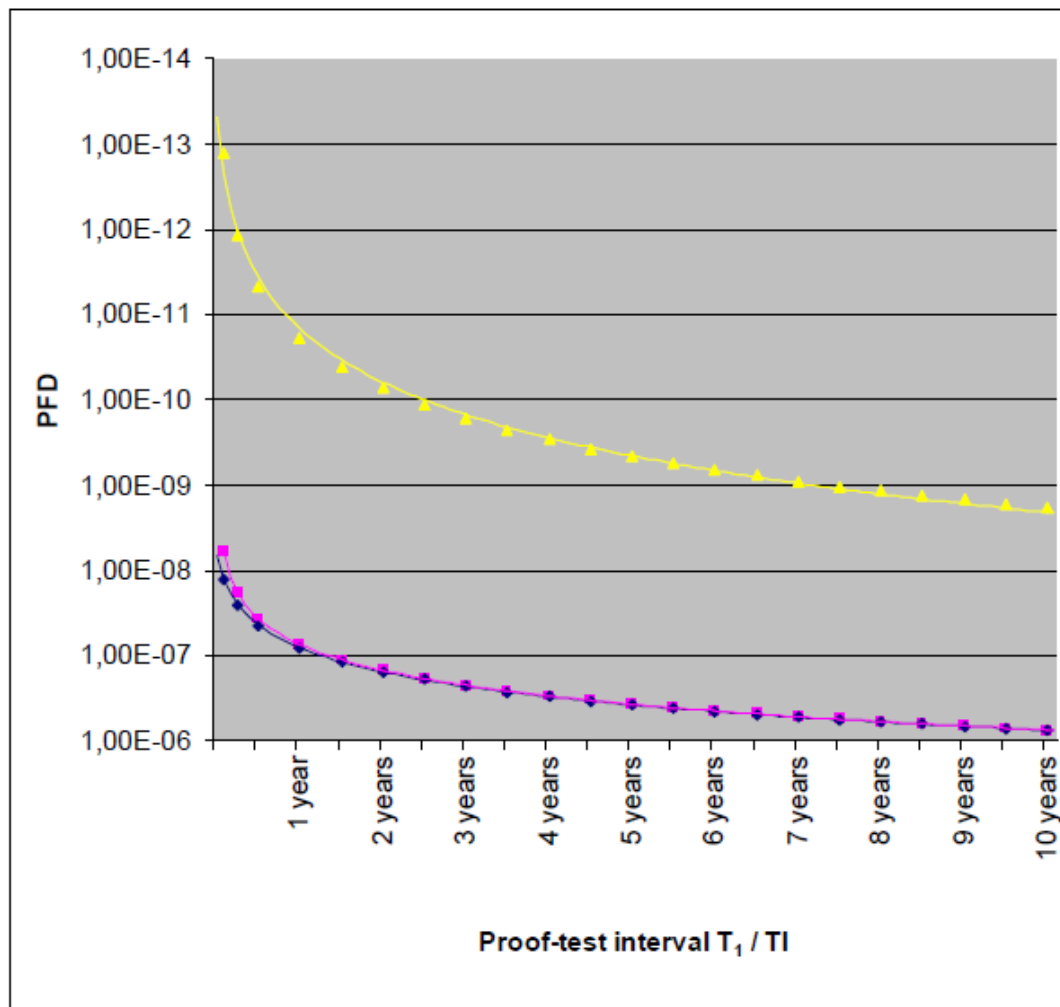


Figure 5: PFD-diagram for a 1oo2-system with DC = 99 %

Legend:




-  according to IEC 61508, with MTTR and common-cause-failure
-  according to ISA standard, with MTTR and common-cause-failure
-  according to ISA standard, without MTTR and without common-cause-failure

Figure 6-16: Figure from article by Böröcsök [26]

PFD-calculation for a 2oo3-system

Diagram of the different PFD-values for a 2oo3-system:

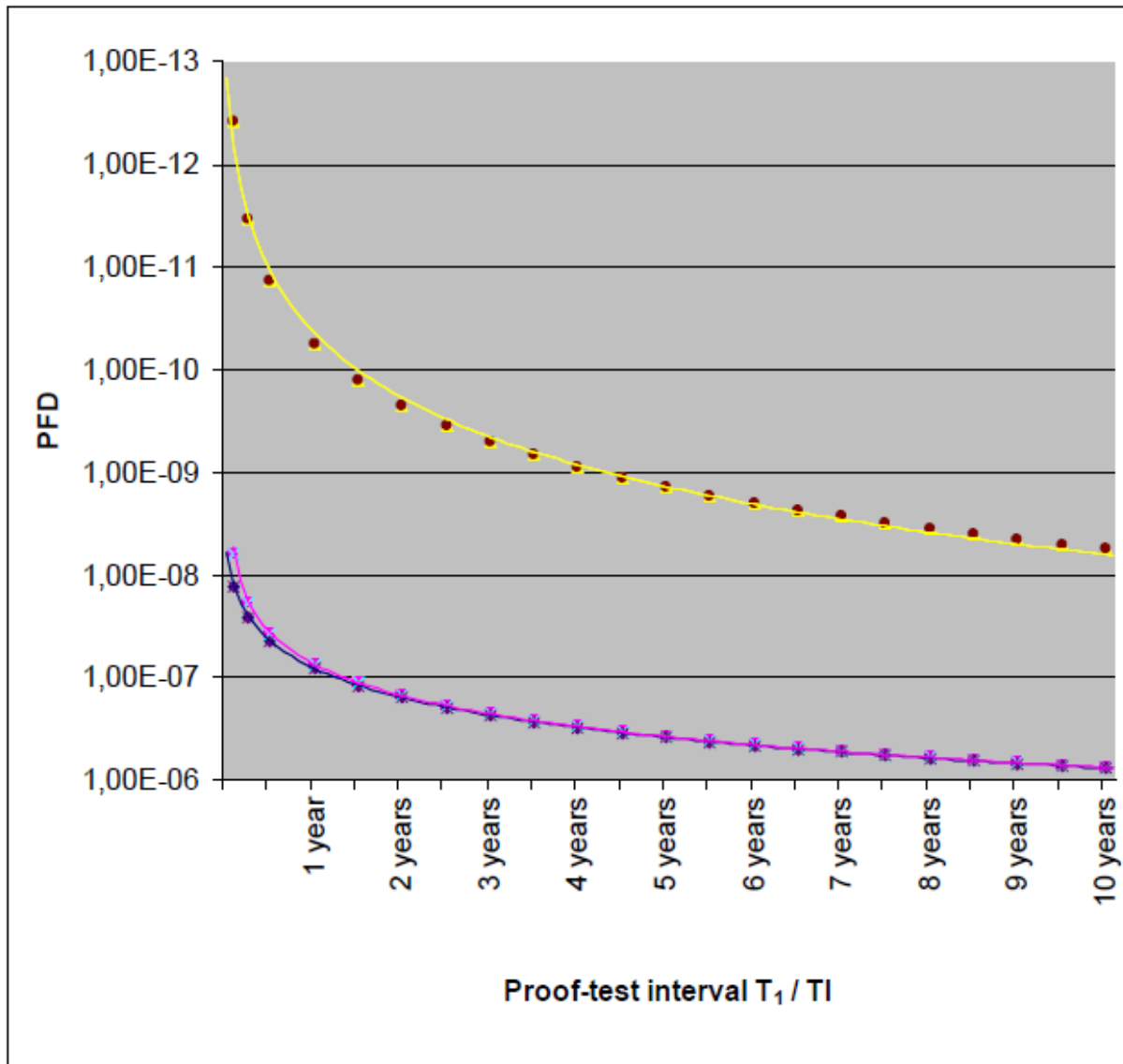


Figure 7: PFD-diagram for a 2oo3-system with $DC = 99\%$

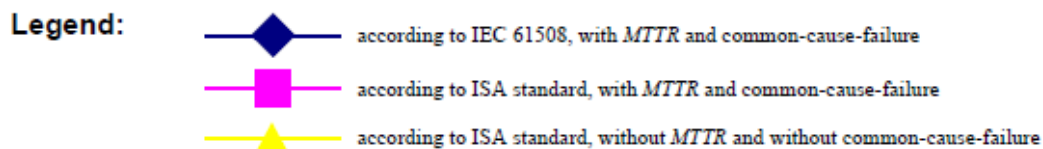


Figure 6-17: Figure from article by Börcsök [26]

Using the same values for dangerous failure rate as Börcsök gives a $PFD_{Avg,2oo3}^{IEC} = 1.22E^{-07}$ when using the $1.5\beta_U$ correction factor. The result is in compliance with the result on the graph in Figure 6-17 for a proof test interval of 1 year.

Guo and Yang presented the results in Figure 6-18 which for the IEC 61508 columns give the same results if same values are used in the calculation methods, which are used in this thesis. This validates the results of this thesis.

Table 2
Numeric comparison of t_{GE} and PFD_G

Sys.	Index	MTTR = 8 h, $\beta = 10\%$, $\beta_D = 5\%$, $\lambda_{SD} = \lambda_{DD}$, DC = 90%, $\lambda_{DD} = \lambda_D \cdot DC$					
		$\lambda_D = 5 \times 10^{-7} h^{-1}$, $T_1 = 4380 h$		$\lambda_D = 5 \times 10^{-7} h^{-1}$, $T_1 = 8760 h$		$\lambda_D = 2.5 \times 10^{-6} h^{-1}$, $T_1 = 8760 h$	
		This paper	IEC61508	This paper	IEC61508	This paper	IEC61508
1oo2	$t_{GE} (h)$	113.5	154	223	300	223	300
	PFD_G	1.1182×10^{-5}	1.1183×10^{-5}	2.2164×10^{-5}	2.2180×10^{-5}	1.1171×10^{-4}	1.1209×10^{-4}
2oo3	$t_{GE} (h)$	113.5	154	223	300	223	300
	PFD_G	1.1205×10^{-5}	1.1217×10^{-5}	2.2253×10^{-5}	2.2299×10^{-5}	1.1393×10^{-4}	1.1508×10^{-4}
1oo2D	$t_{GE} (h)$	61	84.8421	119.2632	161.6842	119.2632	161.6842
	PFD_G	1.117×10^{-5}	1.117×10^{-5}	2.2121×10^{-5}	2.2122×10^{-5}	1.1063×10^{-4}	1.1064×10^{-4}

Figure 6-18: Results presented by Guo and Yang [16]

7 Fault Tree Analysis [4] [3] [41]

As described in Figure 1-2 page 5 Fault Tree Analysis (FTA) is another one of the quantitative methods to evaluate the reliability of a SIS. This chapter will describe how FTA is used to determine the reliability of the Svend HIPPS.

IEC 61508-6 suggest the use of Fault Tree Analysis (FTA) as a relevant approach in reliability analysis of SIF. IEC 61025 is the international standard describing FTA and defines FTA as:

“Fault tree analysis (FTA) is concerned with the identification and analysis of conditions and factors that cause or may potentially cause or contribute to the occurrence of a defined top event....” [41]

FTA has been a common method in reliability and risk analysis since the 1960s and many computer aided programs have been developed to ease the FTA analysis. Because of the graphical illustration it is easy to understand and is a suitable communication tool for non-expert persons in reliability analysis. FTA is a top-down method and can be used for both qualitative and quantitative analysis – Appendix 12.5 page 85 and Appendix 12.6 page 86 describes when FTA is applicable. This thesis is concerned with the quantitative assessment though the qualitative and quantitative assessments are closely linked together.

The starting point of a FTA is often an existing Failure Mode, Effects and Criticality Analysis FMECA (not covered in this thesis) and a block diagram of the system. The FTA consists of basic events in combination with different Boolean operators as illustrated in Figure 7-1.

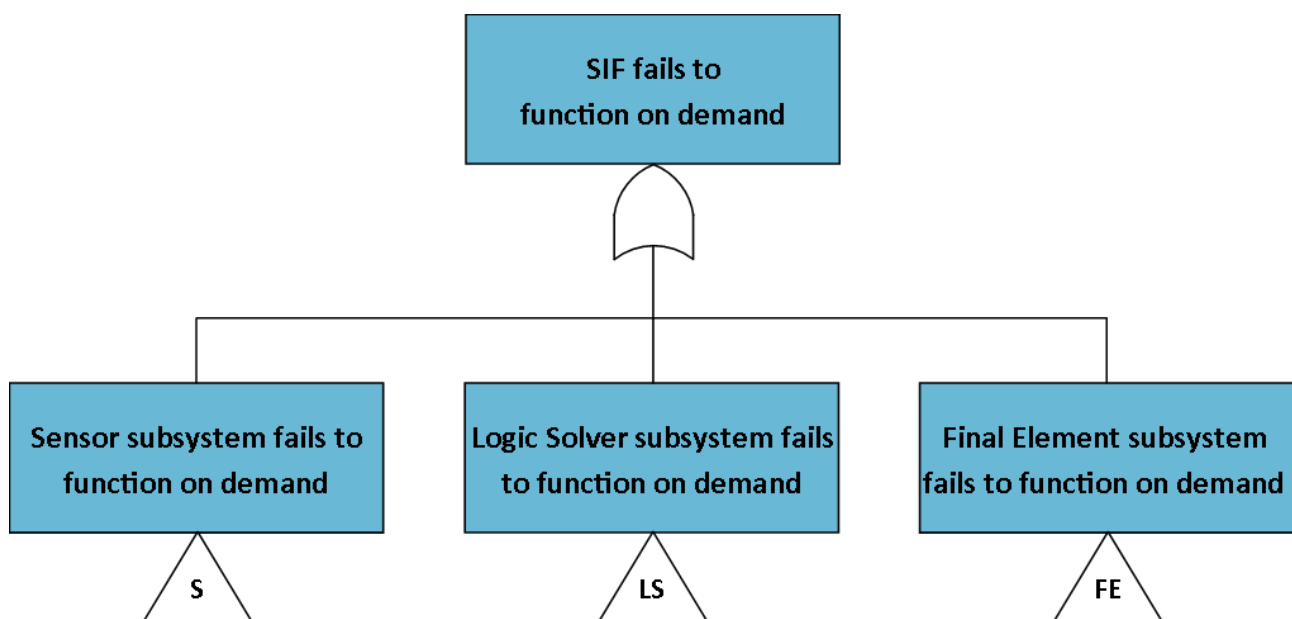


Figure 7-1: FTA of SIF failure as the top-event

Figure 1-2 page 5 illustrates a possible argument for choosing FTA compared to RBD when the system is built of other than series and parallel structures. When a FTA is constructed solely by AND- and OR-gates the FTA can be converted to a RBD and vice versa and should therefore give the same results. FTA mainly focuses on component failures where RBD is constructed in a way that the components must function in order for the SIF to perform [3].

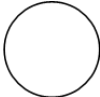
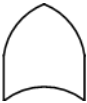
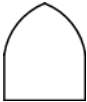

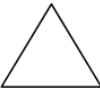
7.1 FTA Boolean Operators and Symbols

The graphical representation of a FTA requires that symbols and operators are used in a consistent manner. A fault tree has the following main modelling blocks and symbols:

- **Top Event**
Potential undesirable event caused by lower level events
- **Basic Event**
Individual or combined lower level failures or events
- **Logic Gates**
The causes or events are combined with logic gates
- **Transfer Gates**
In complex systems it can be necessary to use transfer gates to ease the interpretation

These symbols are presented in the international standard IEC 61025 and commonly used operators are presented in Table 7-1. More logic gates are available but not presented in this thesis.

Table 7-1: Commonly used Boolean operators and symbols [41]

Symbol	Name	Description
	Basic Event	Component failure mode or a failure mode cause. The lowest level event for which probability of occurrence or reliability information is available
	OR gate	Used for series systems. The output event occurs if any of the input events occur i.e. the system fails if any of the input fails.
	AND gate	Used for parallel systems. The output event occurs only if all of the input events occur i.e. the system fails if all of the input fails.
	Majority Vote gate	Used for MooN systems. The output occurs if m or more inputs out of a total of n inputs occur
	Transfer gate	Indicates that part of the system is described elsewhere.

7.1.1 Events

Different types of events can occur depending on the component characteristics

- **Non-repairable components**

The components are not repaired when a failure occurs. The basic event probability is $q_i(t) \approx \lambda_i t$

- **Repairable components**

The components are repaired when a failure occurs and is as good as new. The basic event probability is $q_i(t) \approx \lambda_i MTTR_i$

- **Periodically tested components**

Components are tested periodically with test interval τ . The basic event probability is $q_i(t) \approx \frac{\lambda_i \tau_i}{2}$

The basic event probabilities are similar to simplified formulas presented in Table 5-1 page 33 and the failure rate is the dangerous detected failures λ_{DD} for repairable components and dangerous undetected failures λ_{DU} for periodically tested components.

7.2 FTA Mathematics

The quantitative mathematics for FTA is much similar to the one presented for RBD in Section 6.3 page 36. For FTA the notation in Eq. 7-1-Eq. 7-4 is used.

$$Q_0(t) = \Pr(\text{Top event occurs at time } t) \quad \text{Eq. 7-1}$$

$$q_i(t) = \Pr(\text{Basic event } i \text{ occurs at time } t) \quad \text{Eq. 7-2}$$

$$\check{Q}_j(t) = \Pr(\text{Minimal Cut Set } j \text{ fails at time } t) \quad \text{Eq. 7-3}$$

A Minimal Cut Set will fail when all the basic events occur at the same time.

$E_i(t)$ is a basic event i that occurs at time t and it means that component i is in failed state at time t .

The mathematics is divided in AND-gate, OR-gate, and Minimal Cut Sets.

7.2.1 AND-gate

For an AND-gate with two independent basic events the probability of a top event is

$$Q_0(t) = \Pr(E_1(t) \cap E_2(t)) = \Pr(E_1(t)) \cdot \Pr(E_2(t)) = q_1(t) \cdot q_2(t) \quad \text{Eq. 7-4}$$

and for n basic events

$$Q_0(t) = \prod_{i=1}^n q_i(t) \quad \text{Eq. 7-5}$$

Eq. 7-5 is illustrating the failure function. Comparing with RBD the AND-gate reliability calculations are similar to a parallel RBD system as presented in Section 6.2-6.3 from page 35.

7.2.2 OR-gate

For an OR-gate with two independent basic events the probability of a top event is

$$\begin{aligned} Q_0(t) &= \Pr(E_1(t) \cup E_2(t)) = \Pr(E_1(t) + \Pr(E_2(t) - \Pr(E_1(t) \cap E_2(t))) \\ &= q_1(t) + q_2(t) - q_1(t) \cdot q_2(t) = 1 - (1 - q_1(t))(1 - q_2(t)) \end{aligned} \quad \text{Eq. 7-6}$$

and for n basic events

$$Q_0(t) = 1 - \prod_{i=1}^n (1 - q_i(t)) \quad \text{Eq. 7-7}$$

Eq. 7-7 is illustrating the failure function. Comparing with RBD the OR-gate reliability calculations are similar to a series RBD system as presented in Section 6.2-6.3 from page 35.

7.2.3 Minimal Cut Sets

A cut set is a set of components that by failing puts the system in down state. In a MoonN system the number of minimal cut set can be calculated as

$$\text{minimal cut set} = \binom{n}{n - m + 1} \quad \text{Eq. 7-8}$$

The system fails if $n - m + 1$ cut sets fail.

When calculating the probability of a minimal cut set occurring in a time interval t the main approach is

$$\check{Q}_j(t) = \prod_{i=1}^{n-m+1} q_i(t) \quad \text{Eq. 7-9}$$

The use of minimal cut sets for FTA in MoonN voted groups lead to a non-conservative answer and must be multiplied with a correction factor, CF .

$$CF = \frac{2^k}{k + 1} \quad \text{Eq. 7-10}$$

For a minimal cut set with $k = n - m + 1$ components

7.2.4 Average Probability of Failure on Demand

After finding the basic event failure function $Q_0(t)$ then the average probability of failure on demand can be calculated.

$$PFD_{Avg} = \frac{1}{\tau} \int_0^{\tau} Q_0(t) dt \quad \text{Eq. 7-11}$$

Most software programs use the basic event function to calculate the PFD_{Avg} [3].

7.3 FTA of Svend HIPPS

A SIF failure presented in Figure 7-1 page 46 can be elaborated further through the transfer gates. The Svend HIPPS SIF will fail on demand if any of the subsystems fails. This section illustrates a FTA of each subsystem.

7.3.1 Sensor Subsystem

The FTA of Svend HIPPS Sensor subsystem is illustrated in Figure 7-2.

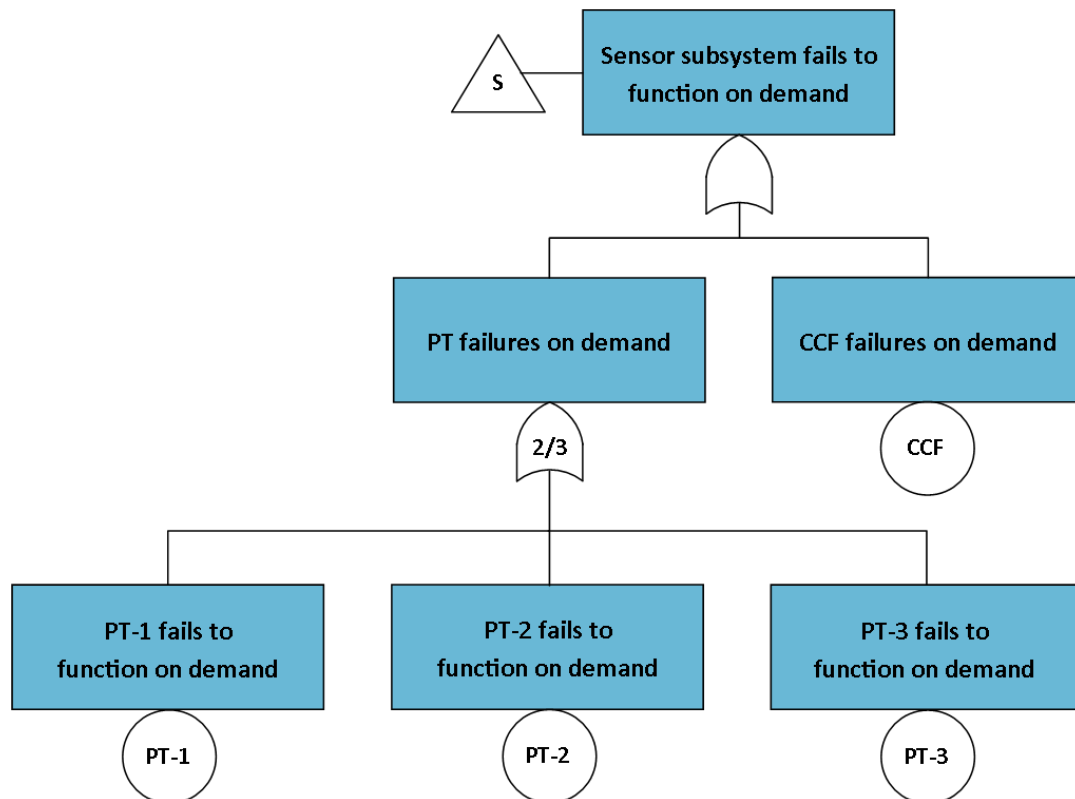


Figure 7-2: FTA of Svend HIPPS Sensor subsystem

The 2oo3 voting can be replaced with Minimal Cut Sets as illustrated in Figure 7-3.

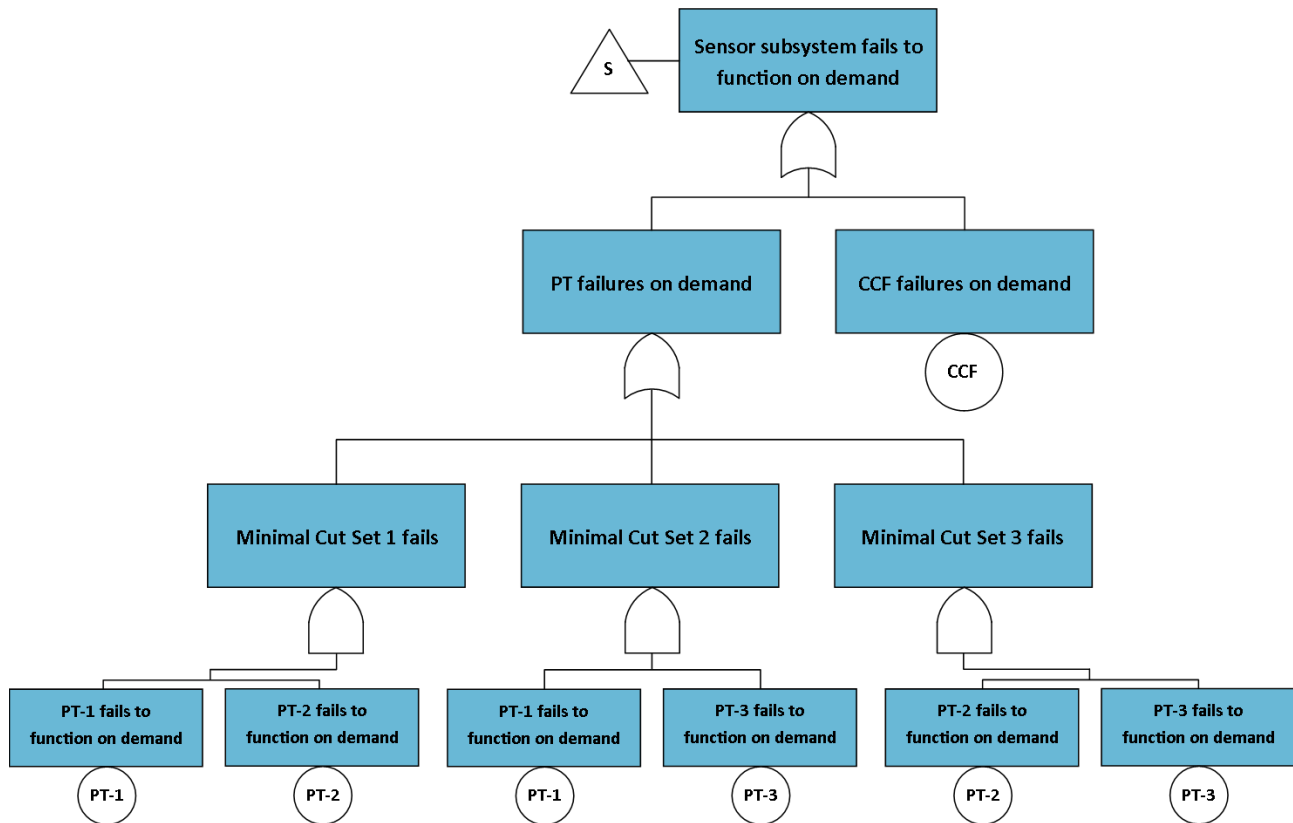


Figure 7-3: FTA of Svend HIPPS Sensor subsystem with minimal cut sets

7.3.2 Logic Solver Subsystem

The FTA of Svend HIPPS Logic Solver subsystem is illustrated in Figure 7-4.

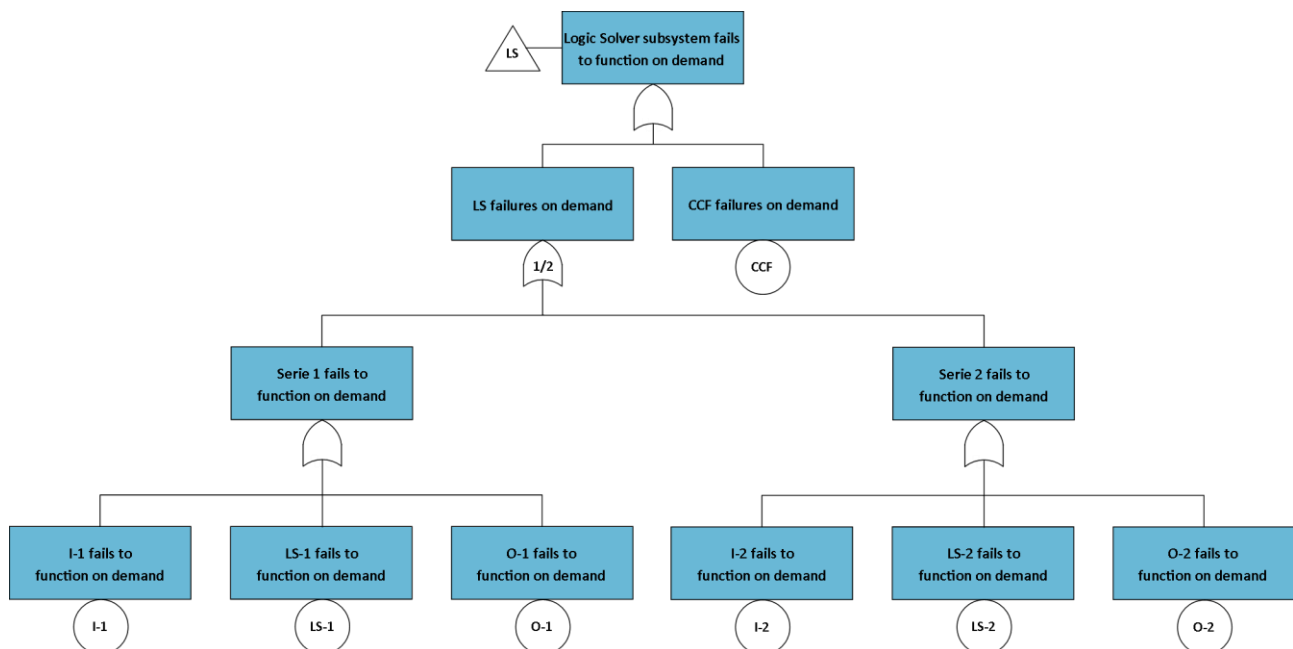


Figure 7-4: FTA of Svend HIPPS Logic Solver subsystem

7.3.3 Final Element Subsystem

The FTA of Svend HIPPS Final Element subsystem is illustrated in Figure 7-5.

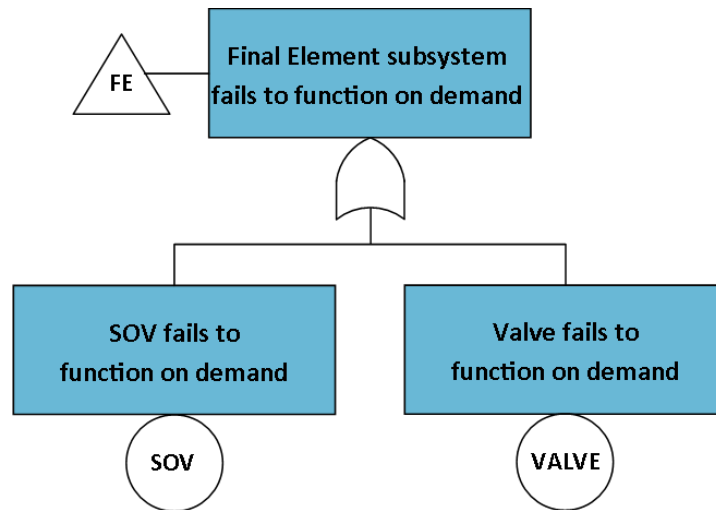


Figure 7-5: FTA of Svend HIPPS Final Element subsystem

7.4 Results: Svend HIPPS Basic Events

Table 7-2 list the basic events and dangerous undetected failures λ_{DU} used in calculating the PFD_{Avg} . Values of λ_{DU} are the same as presented for RBD in Table 4-5 page 28.

Table 7-2: List of Basic Events and calculations

Description	λ_{DU} [E-6/hr]	$q_i(t)$
PT-1 fails to function on demand	3.900E-02	1.711E-04
PT-2 fails to function on demand	3.900E-02	1.711E-04
PT-3 fails to function on demand	3.900E-02	1.711E-04
Sensor subsystem: CCF failures on demand		3.416E-06
I-1 fails to function on demand	1.232E-03	5.406E-06
LS-1 fails to function on demand	1.000E-05	4.388E-08
O-1 fails to function on demand	1.000E-05	4.388E-08
I-2 fails to function on demand	1.232E-03	5.406E-06
LS-2 fails to function on demand	1.000E-05	4.388E-08
O-2 fails to function on demand	1.000E-05	4.388E-08
Logic Solver subsystem: CCF failures on demand		5.484E-08
SOV fails to function on demand	6.000E-01	2.633E-03
Valve fails to function on demand	1.400E-02	6.143E-05

The CCF values are calculated with Eq. 5-22 page 32.

The basis event probabilities $q_i(t)$ in Table 7-2 are calculated with Eq. 7-12.

$$q_i(t) = \frac{\lambda_{DU,i}\tau_i}{2} + \lambda_{DU,i}MTTR \quad \text{Eq. 7-12}$$

with $\tau_i = 8760 [h]$ and $MTTR = 8 [h]$ (standard IEC values – other can be used)

Using the basis event probabilities and the FTA Boolean math presented in this chapter to calculate the top event $Q_0(t)$ gives a

$$PFD_{Avg,SIF}^{FTA} = 2.71E^{-03} \quad \text{Eq. 7-13}$$

and

$$RRF_{SIF}^{FTA} = 369 \quad SIL_{SIF}^{FTA} = 2 \quad \text{Eq. 7-14}$$

The result for FTA is as expected much similar to the one presented for RBD in Section 6.6 page 42.

8 Markov Modelling

Markov modelling is the last quantitative method presented in this thesis. The reliability of Svend HIPPS will be evaluated using this dynamic method. The Boolean models presented by RBD and FTA are static models while Markov models are dynamic. The Markov models are illustrated with state/transition diagrams, which this chapter will describe in detail. Markov Modelling are described in IEC 61508-6 and in a specific standard IEC 61165. The standards provide guidelines for using Markov Modelling.

The basic approach can be divided into five steps [3], which will be presented in this chapter.

- Define system states
- Draw transition diagram
- Define the transition rates
- Build the transition matrix
- Perform calculations (either time dependent analysis or steady state)

8.1 Basic Markov Modelling

The state/transition diagrams are a representation of reliability, availability or safety behaviors of a system which can be used to calculate the performance of the system. A system is built by a number of components, which can be in either up state or down state. The states of an arbitrary component can be defined as illustrated in Table 8-1

Table 8-1: State Description, example

State	State Description
0	The component is functioning (Up state)
1	The component has a DD fault (Down state)
2	The component has a DU fault (Down state)

The defined states are represented in a transition diagram where the states are represented by a circle and the transition between states with a transition arrow. If the guiding rules for development and representation presented in IEC 61165 Section 8.2 page 15 are followed the transition diagram could be illustrated as in Figure 8-1.

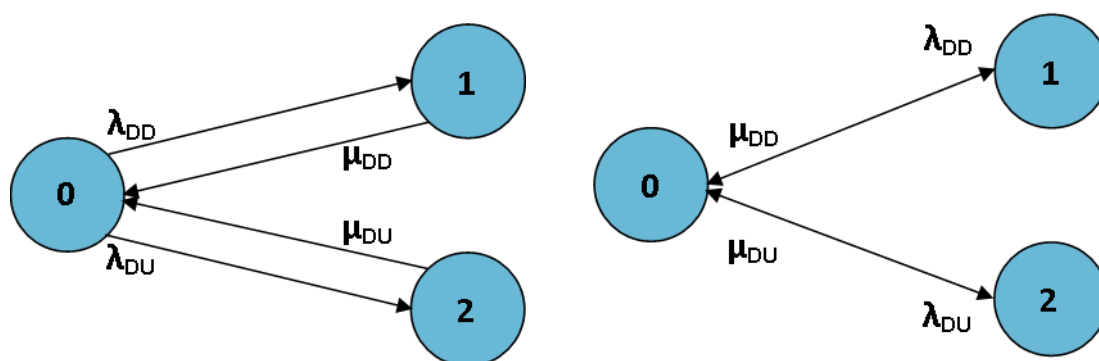


Figure 8-1: Transition diagram – Simple Markov Model

Furthermore the transition rates must be defined where λ is failure rate and μ is restoration or repair rate as illustrated in Table 8-2.

Table 8-2: Transition rates for Markov example

Transition Rate	Description	Comment
λ_{DU}	Dangerous Undetected failure rate	Described in Section 4.3 page 23 and Section 4.4 page 24
λ_{DD}	Dangerous Detected failure rate	Described in Section 4.3 page 23 and Section 4.4 page 24
μ_{DU}	Repair rate of DU failure	$\mu_{DU} = \frac{1}{\frac{\tau}{2} + MRT}$
μ_{DD}	Repair rate of DD failure	$\mu_{DD} = \frac{1}{MTTR}$

8.2 Markov Mathematics

After definition of system states and transition rates and drawing of transition diagram the next step is to build the transition rates matrix and perform calculation to obtain the PFD_{Avg} . This section will describe these last two steps in Markov Modelling.

In a Markov model the transition probabilities are given by Eq. 8-1

$$P_{ij}(t) = Pr(X(t) = j \mid X(0) = i) \quad \text{Eq. 8-1}$$

and for all $i, j \in X$ these probabilities can be arranged in a matrix \mathbb{P}

$$\mathbb{P}(t) = \begin{bmatrix} P_{00} & P_{01} & \cdots & P_{0(n-1)} \\ P_{10} & P_{11} & \cdots & P_{1(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ P_{(n-1)0} & P_{(n-1)1} & \cdots & P_{(n-1)(n-1)} \end{bmatrix} \quad \text{Eq. 8-2}$$

In matrix \mathbb{P} the subscript i denotes the current state, j denotes the state that the transition is to and n is the total number of states (the notation of the entries are numbered according to state but note that this is abuse of normal mathematical notation). As an example P_{23} (mathematical entry (3,4)) means the probability that the state will move from state 2 to state 3. A process in state i at time 0 must either be in state i at time t or make a transition to another state. Therefore the sum of probabilities in the entries in row i is always equal to 1.

$$\sum_{j=0}^{n-1} P_{ij}(t) = 1 \quad \text{Eq. 8-3}$$

Besides the probability matrix the transition rates from state to state is also presented in a transition rate matrix \mathbb{Q} :

$$\mathbb{Q} = \begin{bmatrix} q_{00} & q_{01} & \cdots & q_{0(n-1)} \\ q_{10} & q_{11} & \cdots & q_{1(n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ q_{(n-1)0} & q_{(n-1)1} & \cdots & q_{(n-1)(n-1)} \end{bmatrix} \quad \text{Eq. 8-4}$$

q_{ij} is the rate of leaving from state i to state j . The sum of transition rates in the entries in row i is always equal to 0.

$$\sum_{j=0}^{n-1} q_{ij}(t) = 0 \quad \text{Eq. 8-5}$$

8.2.1 Kolmogorov Differential Equation [3]

In order to find P_{ij} the Chapman-Kolmogorov equations can be used and expressed in simple form as presented in Eq. 8-6.

$$\dot{P}_{ij}(t) = \sum_{k=0}^{n-1} P_{ik}(t)q_{kj} \quad \text{Eq. 8-6}$$

Eq. 8-6 is also known as the Kolmogorov forward equations and may be presented in matrix form:

$$\dot{\mathbb{P}}(t) = \mathbb{P}(t)\mathbb{Q} \quad \text{Eq. 8-7}$$

When solving these equations it is known that the Markov process starts in state i at time 0, so the subscript i is suppressed and the probability matrix $\mathbb{P}(t)$ is reduced to a row vector with the subscript j :

$$\mathbb{P}(t) = [P_0(t) \quad P_1(t) \quad P_2(t)] \quad \text{Eq. 8-8}$$

There are two main ways to solve the differential equations:

- Solving for time dependent probabilities
- Solving for steady state probabilities

When solving the equations it is essential to use the fact presented in Eq. 8-3 in order to have same number of equations as variables.

The following steps can be used for a specific transition model

- Set up the transition matrix
- Set up differential equations
- Solve differential equations, either by hand or using MATLAB or similar tool

8.2.2 Time-dependent Solution

The main benefit of solving for time-dependent probabilities is the possibility to study how the probabilities change with time e.g. during a proof test interval $(0, \tau)$. In this proof test interval DU failures are not detected and no repair will be performed until the end of the interval, so $\mu_{DU} = 0$.

The transition model presented in Figure 8-1 page 54 and the transition rates presented in Table 8-2 page 55 are used to set up the transition matrix \mathbb{Q} in Eq. 8-9, but with the exception that $\mu_{DU} = 0$.

$$\mathbb{Q} = \begin{bmatrix} -(\lambda_{DD} + \lambda_{DU}) & \lambda_{DD} & \lambda_{DU} \\ \mu_{DD} & -\mu_{DD} & 0 \\ 0 & 0 & 0 \end{bmatrix} \quad \text{Eq. 8-9}$$

In this solution it is relevant to investigate the possibility of moving to a specific state j , so the probability matrix $\mathbb{P}(t)$ is reduced to a row vector with the subscript j :

$$\mathbb{P}(t) = [P_0(t) \quad P_1(t) \quad P_2(t)] \quad \text{Eq. 8-10}$$

The time-dependent differential matrix equation is therefore:

$$\dot{\mathbb{P}}(t) = \mathbb{P}(t)\mathbb{Q} \quad \text{Eq. 8-11}$$

and the equations from Eq. 8-11 that must be solved are:

$$\dot{P}_0(t) = -(\lambda_{DD} + \lambda_{DU})P_0(t) + \mu_{DD}P_1(t) \quad \text{Eq. 8-12}$$

$$\dot{P}_1(t) = \lambda_{DD}P_0(t) - \mu_{DD}P_1(t) \quad \text{Eq. 8-13}$$

$$\dot{P}_2(t) = \lambda_{DU}P_0(t) \quad \text{Eq. 8-14}$$

This can be done by hand or preferable with a MATLAB script as illustrated in Appendix 12.16 page 101 with the initial condition that the system is in state 0. If values are inserted in the obtained results from the MATLAB script the instantaneous *PFD* can be calculated with Eq. 8-15, where $P_0(t)$ is the initial state.

$$PFD(t) = 1 - P_0(t) \quad \text{Eq. 8-15}$$

and PFD_{Avg} over the proof test interval $(0, \tau)$ with Eq. 8-16

$$PFD_{Avg}(0, \tau) = \frac{1}{\tau} \int_0^\tau \sum_{i \in \mathcal{D}} P_i(t) dt = 1 - \frac{1}{\tau} \int_0^\tau \sum_{i \in \mathcal{U}} P_i(t) dt \quad \text{Eq. 8-16}$$

\mathcal{D} is the set of Down states, so $\mathcal{D} = \{1, 2\}$

\mathcal{U} is the set of Up states, so $\mathcal{U} = \{0\}$

The method described can be used for calculating time-dependent values of PPD_{Avg} in the Svend HIPPS architecture.

8.2.3 Steady State Solution

A Markov model often enters a steady-state after a few hours, approximate 2-3 times the MRT . So it may be more interesting to study the steady-state probabilities rather than the time-dependent [3].

The transition model presented in Figure 8-1 page 54 and the transition rates presented in Table 8-2 page 55 are used to set up the transition matrix.

$$\mathbb{Q} = \begin{bmatrix} -(\lambda_{DD} + \lambda_{DU}) & \lambda_{DD} & \lambda_{DU} \\ \mu_{DD} & -\mu_{DD} & 0 \\ \mu_{DU} & 0 & -\mu_{DU} \end{bmatrix} \quad \text{Eq. 8-17}$$

In this solution it is relevant to investigate the possibility of being in a specific state so the probability matrix \mathbb{P} is reduced to a row vector with the subscript j :

$$\mathbb{P} = [P_0 \quad P_1 \quad P_2] \quad \text{Eq. 8-18}$$

The steady state equations in matrix form are presented in Eq. 8-19:

$$\mathbb{P}\mathbb{Q} = [0] \quad \text{Eq. 8-19}$$

The equations derived from the matrix are:

$$-(\lambda_{DD} + \lambda_{DU})P_0 + \mu_{DD}P_1 + \mu_{DU}P_2 = 0 \quad \text{Eq. 8-20}$$

$$\lambda_{DD}P_0 - \mu_{DD}P_1 = 0 \quad \text{Eq. 8-21}$$

$$\lambda_{DU}P_0 - \mu_{DU}P_2 = 0 \quad \text{Eq. 8-22}$$

Eq. 8-20 to Eq. 8-22 are NOT independent because if Eq. 8-21 is inserted in Eq. 8-20 then Eq. 8-22 is obtained. The last equation needed is Eq. 8-3 that gives the information presented in Eq. 8-23.

$$P_0 + P_1 + P_2 = 1 \quad \text{Eq. 8-23}$$

Solving Eq. 8-20 to Eq. 8-23 by hand results in the values for P_0, P_1, P_2 as presented in Eq. 8-24-Eq. 8-26:

$$P_0 = \frac{1}{\frac{\lambda_{DD}}{\mu_{DD}} + \frac{\lambda_{DU}}{\mu_{DU}} + 1} \quad \text{Eq. 8-24}$$

$$P_1 = \frac{\lambda_{DD}}{\mu_{DD}} P_0 \quad \text{Eq. 8-25}$$

$$P_2 = \frac{\lambda_{DU}}{\mu_{DU}} P_0 \quad \text{Eq. 8-26}$$

Appendix 12.18 page 105 illustrates an example of how to solve the steady state equations using MATLAB. The steady state system is functioning in state 0 and is failed when a dangerous fault in state 1 or state 2 is present. The PFD_{Avg} is therefore the sum of probabilities being in a failed state, as presented in Eq. 8-27.

$$PFD_{Avg} = \sum_{i \in \mathcal{D}} P_i = P_1 + P_2 \quad \text{Eq. 8-27}$$

The MATLAB script in Appendix 12.18 page 105 illustrates an example of this and the method described will be used for calculating steady state values of PFD_{Avg} in the Svend HIPPS architecture.

8.3 Results: Svend HIPPS – Markov Modelling

This section describes the results of PFD_{Avg} for the Svend HIPPS system when using Markov modelling.

8.3.1 Sensor Subsystem

The state definitions in Table 8-3, state diagram in Figure 8-2 and transition matrix in Eq. 8-28 represent a 2oo3 voting system as the Sensor subsystem.

Table 8-3: State definition in 2oo3 voted Sensor Subsystem

State	State Description
0	Three PT are functioning (Up state)
1	Two PT are functioning and one is failed (Up state)
2	One PT is functioning and two are failed (Down state)
3	Three PT are failed (Down state)

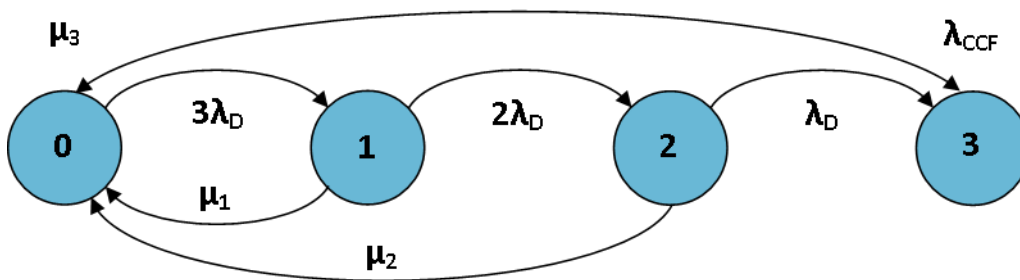


Figure 8-2: State transition diagram 2oo3 voting

$$\mathbb{Q}_S = \begin{bmatrix} -(3\lambda_D + \lambda_{CCF}) & 3\lambda_D & 0 & \lambda_{CCF} \\ \mu_1 & -(\mu_1 + 2\lambda_D + \lambda_{CCF}) & 2\lambda_D & 0 \\ \mu_2 & 0 & -(\mu_2 + \lambda_D) & \lambda_D \\ \mu_3 & 0 & 0 & -\mu_3 \end{bmatrix} \quad \text{Eq. 8-28}$$

with the failure rates from Table 4-5 page 28, $\beta_u = 0.02$ and $MTTR = MTR = 8 \text{ hours}$ and $\tau = 8760 \text{ hours}$

$$\lambda_D = \lambda_{DU} = 3.90E^{-08} \qquad \mu_1 = \mu_2 = \mu_3 = \mu_{DU} = \frac{1}{\frac{\tau}{2} + MRT}$$

$$\lambda_{CFF} = \beta_u \lambda_{DU}$$

Steady State solution

In the steady state solution it is relevant to investigate the possibility of being in a specific state so the probability matrix \mathbb{P} is defined as:

$$\mathbb{P} = [P_0 \quad P_1 \quad P_2 \quad P_3] \qquad \text{Eq. 8-29}$$

The steady state equations in matrix form are presented:

$$\mathbb{P}\mathbb{Q}_S = [0] \qquad \text{Eq. 8-30}$$

Equations in Eq. 8-30 are NOT independent so Eq. 8-3 page 55 must be used together with Eq. 8-30.

Appendix 12.17 page 103 presents a MATLAB script to the steady state solution of the 2oo3 voting of the Sensor subsystem. Running the script results in the PFD_{Avg} value in Eq. 8-31, which is the sum of probabilities being in a failed state, $\mathcal{D} = \{2,3\}$.

$$PFD_{Avg,S}^{Markov} = \sum_{i \in \mathcal{D}} P_i = P_2 + P_3 = 3.596E^{-06} \qquad \text{Eq. 8-31}$$

It is important to mention that the result in Eq. 8-31 is obtained without DD failures and $MTTR$ of these components. A 27x27 transition matrix must be built in order to account for both DD and DU failures but this has been omitted from this thesis. Table 12-4 in Appendix 12.20 page 109 illustrates the State Definitions of the three components in the 2oo3 voting in the Sensor subsystem. Using the definitions in Table 12-4 will assumedly results in a more precise $PFD_{Avg,S}^{Markov}$ value.

Time-dependent solution

See MATLAB script Appendix 12.16 page 101. The time-dependent solution is not elaborated further as it is expected to give the same result for the same proof test interval. The MATLAB script takes a while to run and execute, so the steady state solution is preferable.

8.3.2 Logic Solver Subsystem

Intuitively the state definitions in Table 8-4, state diagram in Figure 8-3 and transition matrix in Eq. 8-32 would represent a 1oo2 voting system as the Logic Solver subsystem

Table 8-4: State definition in 1oo2 voted Logic Solver Subsystem

State	State Description
0	Two Logic Solvers are functioning (Up state)
1	Logic Solver 1 is functioning and Logic Solver 2 is failed (Up state)
2	Logic Solver 2 is functioning and Logic Solver 1 is failed (Up state)
3	Two Logic Solvers are failed (Down state)

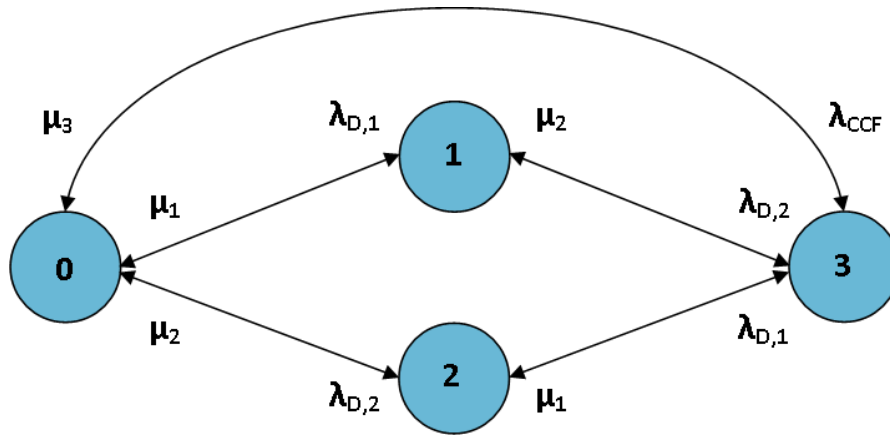


Figure 8-3: State transition diagram 1oo2 voting

$$Q_{LS} = \begin{bmatrix} -(\lambda_{D,1} + \lambda_{D,2} + \lambda_{CCF}) & \lambda_{D,1} & \lambda_{D,2} & \lambda_{CCF} \\ \mu_1 & -(\mu_1 + \lambda_{D,2}) & 0 & \lambda_{D,2} \\ \mu_2 & 0 & -(\mu_2 + \lambda_{D,1}) & \lambda_{D,1} \\ \mu_3 & \mu_2 & \mu_1 & -(\mu_1 + \mu_2 + \mu_3) \end{bmatrix} \quad \text{Eq. 8-32}$$

If the transition rates $\lambda_{D,1}$ and $\lambda_{D,2}$ are substituted with sum of *DU* failures for the Logic Solver, so $\lambda_{D,1} = \lambda_{D,2} = 1.252E^{-9}$ (refer to Table 4-5 page 28). Furthermore the components are only repaired at proof test interval, so $\mu_1 = \mu_2 = \mu_3 = \frac{1}{\frac{\tau}{2} + MRT}$ with $MRT = 8$ and $\tau = 8760$ [h].

With this information the result is $PFD_{Avg,1oo2}^{Markov} = 1.833E^{-8}$. It has not been possible to match the result of the PFD_{Avg} as calculated with the RBD and FTA methods. The reason for this must be because of the lack of states, difference between *DU* and *DD* failures and their repair time, which are not detailed enough. An example of the calculations for the transition matrix in Eq. 8-32 are not presented here but saved for a more detailed calculation of state definitions of a 1oo2 voting, which are presented in Table 8-5.

Table 8-5: Detailed state definition in 1oo2 voted Logic Solver Subsystem

State	State Description		Up/Down
0	Logic Solver (LS) ok,	Logic Solver (LS) 2 ok	(Up state)
1	LS 1 DU fault,	LS 2 ok	(Up state)
2	LS 1 DD fault,	LS 2 ok	(Up state)
3	LS 1 ok,	LS 2 DU fault	(Up state)
4	LS 1 ok,	LS 2 DD fault	(Up state)
5	LS 1 DU fault	LS 2 DU fault	(Down state)
6	LS 1 DD fault,	LS 2 DU fault	(Down state)
7	LS 1 DU fault,	LS 2 DD fault	(Down state)
8	LS 1 DD fault, CCF fault	LS 2 DD fault	(Down state)
9	CCF fault		(Down state)

The state definitions lead to the detailed state transition diagram in Figure 8-4.

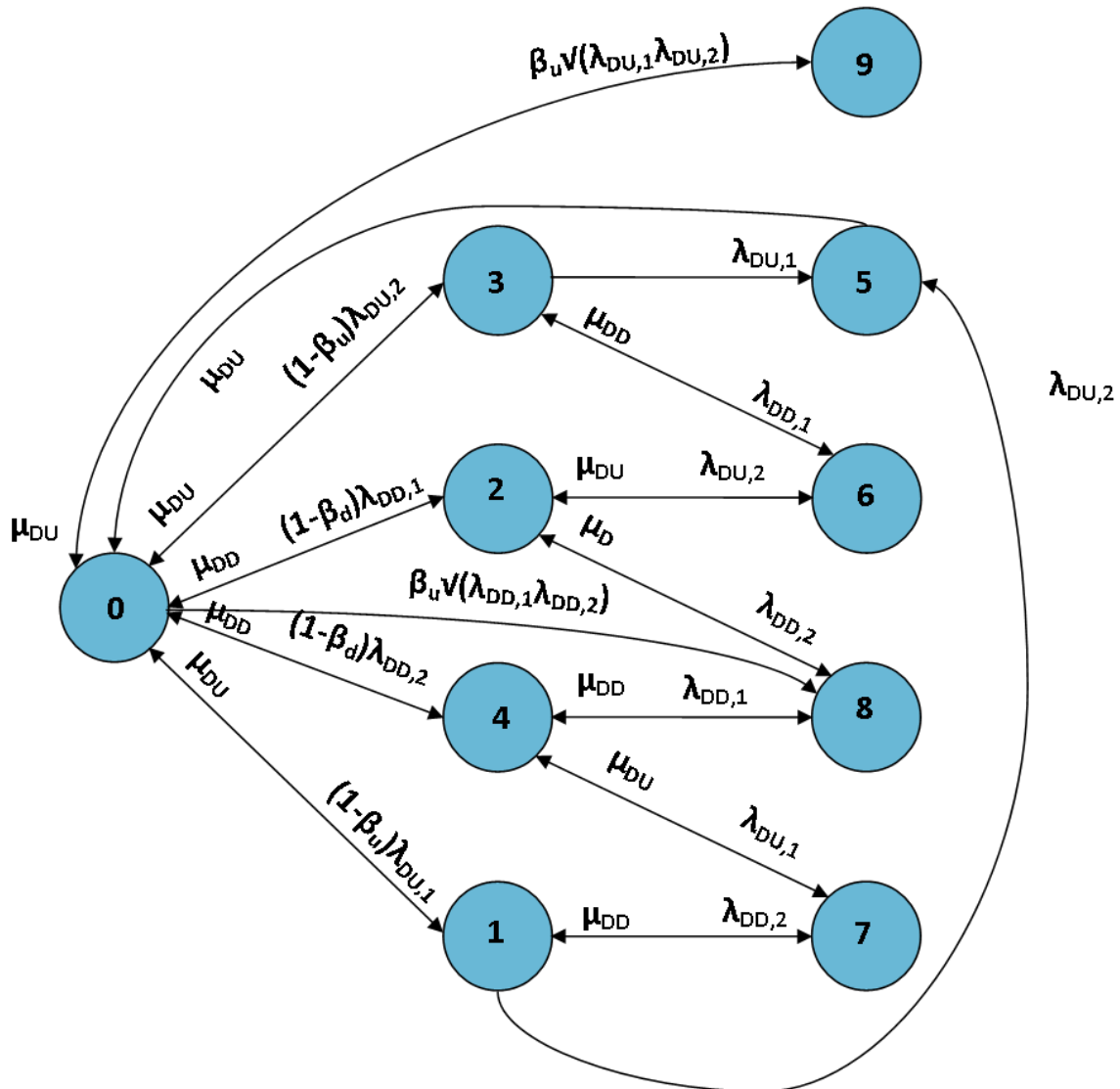


Figure 8-4: Detailed state transition diagram 1oo2 voting Logic Solver subsystem

From the state transition diagram the 10x10 transition matrix \mathbb{Q}_{LS} in Eq. 8-33 can be derived.

θ is short for the sum of the other entries in the same row, so Eq. 8-5 page 56 is fulfilled. Other abbreviations used: $\phi = (1 - \beta_U)$, $\psi = (1 - \beta_D)$, $\gamma = \sqrt{\lambda_{DD,1}\lambda_{DD,2}}$, $\varepsilon = \sqrt{\lambda_{DU,1}\lambda_{DU,2}}$

$$\mathbb{Q}_{LS} = \begin{bmatrix} -\theta & \phi\lambda_{DU,1} & \psi\lambda_{DD,1} & \phi\lambda_{DU,2} & \psi\lambda_{DD,2} & 0 & 0 & 0 & \beta_D\gamma & \beta_U\varepsilon \\ \mu_{DU} & -\theta & 0 & 0 & 0 & \lambda_{DU,2} & 0 & \lambda_{DD,2} & 0 & 0 \\ \mu_{DD} & 0 & -\theta & 0 & 0 & 0 & \lambda_{DU,2} & 0 & \lambda_{DD,2} & 0 \\ \mu_{DU} & 0 & 0 & -\theta & 0 & \lambda_{DU,1} & \lambda_{DD,1} & 0 & 0 & 0 \\ \mu_{DD} & 0 & 0 & 0 & -\theta & 0 & 0 & \lambda_{DU,1} & \lambda_{DD,1} & 0 \\ \mu_{DU} & 0 & 0 & 0 & 0 & -\theta & 0 & 0 & 0 & 0 \\ 0 & 0 & \mu_{DU} & \mu_{DD} & 0 & 0 & -\theta & 0 & 0 & 0 \\ 0 & \mu_{DD} & 0 & 0 & \mu_{DU} & 0 & 0 & -\theta & 0 & 0 \\ 0 & 0 & \mu_{DD} & 0 & \mu_{DD} & 0 & 0 & 0 & -\theta & 0 \\ \mu_{DU} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -\theta \end{bmatrix} \quad \text{Eq. 8-33}$$

The failure rates from Table 4-5 page 28 and $MTTR = MTR = 8 \text{ hours}$ and $\tau = 8760 \text{ hours}$ are used.

$$\lambda_{DD} = 2.433E^{-07} \quad \lambda_{DU} = 1.252E^{-09} \quad \mu_{DD} = \frac{1}{MTTR} \quad \mu_{DU} = \frac{1}{\frac{\tau}{2} + MRT}$$

It can be argued that entry (6,1) in matrix \mathbb{Q}_{LS} (represent the transition from state 5 to state 0), should be corrected with a factor because two DU failures have to be repaired.

Steady State solution

In this solution it is relevant to investigate the possibility of being in a specific state so the probability matrix \mathbb{P} is defined as:

$$\mathbb{P} = [P_0 \quad P_1 \quad P_2 \quad P_3] \quad \text{Eq. 8-34}$$

The steady state equations in matrix form are presented:

$$\mathbb{P}\mathbb{Q}_{LS} = [0] \quad \text{Eq. 8-35}$$

Equations in Eq. 8-35 are NOT independent so Eq. 8-3 page 55 must be used together with Eq. 8-35.

Appendix 12.19 page 107 presents a MATLAB script to the steady state solution of the 1002 voting of the Logic Solver subsystem. Running the script results in the PFD_{Avg} value in Eq. 8-36, which is the sum of probabilities being in a failed state, $\mathcal{D} = \{5,6,7,8,9\}$.

$$PFD_{Avg,LS}^{Markov} = \sum_{i \in \mathcal{D}} P_i = P_5 + P_6 + P_7 + P_8 + P_9 = 5.989E^{-08} \quad \text{Eq. 8-36}$$

Time-dependent solution

See MATLAB script Appendix 12.16 page 101. The time-dependent solution is not elaborated further as it is expected to give the same result for the same proof test interval. The MATLAB script takes a while to run and execute, so the steady state solution is preferable from.

8.3.3 Final Element Subsystem

The Final Element subsystem with the SOV and valve is similar to the example given in Section 8.2 page 55. For simplicity, the two components are illustrated as one with added failure rates in the calculations. The state definitions for the two components are presented in Table 8-6 and the transition diagram is illustrated in Figure 8-5.

Table 8-6: State definition in 1oo1 voted Final Element Subsystem

State	State Description
0	The SOV/Valve is functioning (Up state)
1	The SOV/Valve has a DD fault (Down state)
2	The SOV/Valve has a DU fault (Down state)

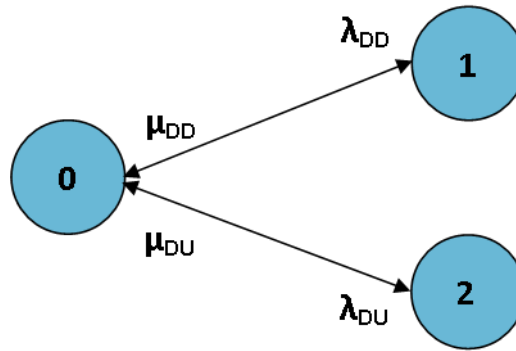


Figure 8-5: State transition diagram 1oo1 voting

Based on Figure 8-5 the transition matrix \mathbb{Q}_{FE} takes the form in Eq. 8-37.

$$\mathbb{Q}_{FE} = \begin{bmatrix} -(\lambda_{DD} + \lambda_{DU}) & \lambda_{DD} & \lambda_{DU} \\ \mu_{DD} & -\mu_{DD} & 0 \\ \mu_{DU} & 0 & -\mu_{DU} \end{bmatrix} \quad \text{Eq. 8-37}$$

with the failure rates from Table 4-5 page 28 and $MTTR = MTR = 8 \text{ hours}$ and $\tau = 8760 \text{ hours}$

$$\lambda_{DD} = 0 \quad \lambda_{DU} = 6.14E^{-07} \quad \mu_{DD} = \frac{1}{MTTR} \quad \mu_{DU} = \frac{1}{\frac{\tau}{2} + MRT}$$

Steady State solution

In this solution it is relevant to investigate the possibility of being in a specific state so the probability matrix \mathbb{P} is defined as:

$$\mathbb{P} = [P_0 \quad P_1 \quad P_2] \quad \text{Eq. 8-38}$$

The steady state equations in matrix form are presented:

$$\mathbb{P}\mathbb{Q}_{FE} = [0] \quad \text{Eq. 8-39}$$

Equations in Eq. 8-39 are NOT independent Eq. 8-3 page 55 must be used together with Eq. 8-39.

The equations derived from the matrix as described in Section 8.2.3 page 58:

$$P_0 = \frac{1}{\frac{\lambda_{DD}}{\mu_{DD}} + \frac{\lambda_{DU}}{\mu_{DU}} + 1} = 0.9973 \quad \text{Eq. 8-40}$$

$$P_1 = \frac{\lambda_{DD}}{\mu_{DD}} P_0 = 0 \quad \text{Eq. 8-41}$$

$$P_2 = \frac{\lambda_{DU}}{\mu_{DU}} P_0 = 2.687E^{-03} \quad \text{Eq. 8-42}$$

The PFD_{Avg} is the sum of probabilities being in a failed state.

$$PFD_{Avg,FE}^{Markov} = P_1 + P_2 = 2.687E^{-03} \quad \text{Eq. 8-43}$$

Appendix 12.18 page 105 presents a MATLAB script to the steady state solution of the 1oo1 voting of the Final Element subsystem.

Time-dependent solution

See MATLAB script Appendix 12.16 page 101, which will lead to the result in Eq. 8-44.

$$PFD_{Avg,FE}^{Markov}(0, \tau) = 1 - \frac{1}{\tau} \int_0^{\tau} P_0(t) dt = 2.685E^{-03} \quad \text{Eq. 8-44}$$

The time-dependent solution is not elaborated further as it is expected to give the same result for the same proof test interval.

8.4 Summary of Results

The PFD_{Avg} values obtained in this chapter are summarized in Table 8-7.

Table 8-7: Obtained PFD_{Avg} for different subsystems using Markov modelling

$PFD_{Avg,**}^{Markov}$	DU failures	DU and DD failures
Sensor	$3.596E^{-06}$	-
Logic Solver	$1.833E^{-08}$	$5.989E^{-08}$
Final Element	$2.687E^{-03}$	-
SIF	$2,691E^{-03}$	-

The value for the Final Element is placed under *DU* failures as no *DD* failures were available for the Final Element. None of the calculations, whether it was RBD or FTA, have used *DD* failures for the Final Element subsystem. The results are also based on a sum of the failure rates in the series connected systems.

Using the Markov modelling presented in this chapter gives a

$$PFD_{Avg,SIF}^{Markov} = 2.69E^{-03} \quad \text{Eq. 8-45}$$

and

$$RRF_{SIF}^{Markov} = 370 \quad SIL_{SIF}^{Markov} = 2 \quad \text{Eq. 8-46}$$

The result for Markov modelling is as expected much similar to the one presented for RBD in Section 6.6 page 42. The paper by Börcsök et al. [28] and the paper by Hildebrandt [24] give a general introduction to Markov modelling and examples of 1oo1 and 1oo2 architecture models. They conclude that using Markov modelling is in accordance with the values obtained from IEC 61508-6 formulas, which is confirmed in the results in Eq. 8-45 and Eq. 8-46. They also conclude that the number of states can rapidly increase depending on the details needed in the model, which will make the model more complex. This was also shown in this thesis by the number of states needed for result for *DU* and *DD* failures for 2oo3 (Table 12-4 page 109) and 1oo2 (Table 8-5 page 62) systems.

Guo and Yang [17] also describes how explosively the size of Markov models can increase as the system becomes a little more complicated. They have developed a flowchart for generating a Markov model and a computer program to automatically realize the technique they present in their paper.

9 Proof Test Interval

This chapter will describe how different proof test intervals impact the PFD_{Avg} , SIL and RRF. Furthermore it is described how to model imperfect proof testing.

Proof testing is performed as a periodic activity that shall verify the SIL of the SIS. Furthermore the proof test shall detect *DU* failures. Periodic proof testing contributes to achieve and improve the SIS without making modifications to the design. However, proof testing also involves man hours and it is therefore necessary to find an optimal test plan throughout the lifetime of the SIS, to keep a good balance between benefits and costs. The IEC 61508-4 defines a proof test as a

“periodic test performed to detect dangerous hidden failures in a safety-related system so that, if necessary, a repair can restore the system to an “as new” condition or as close as practical to this condition”

[31]

9.1 Perfect Proof Testing

Through this thesis it has been assumed that all *DU* failures were detected and repaired during proof testing, so the PFD_{Avg} could be assumed constant during proof test interval τ , as illustrated in Figure 9-1

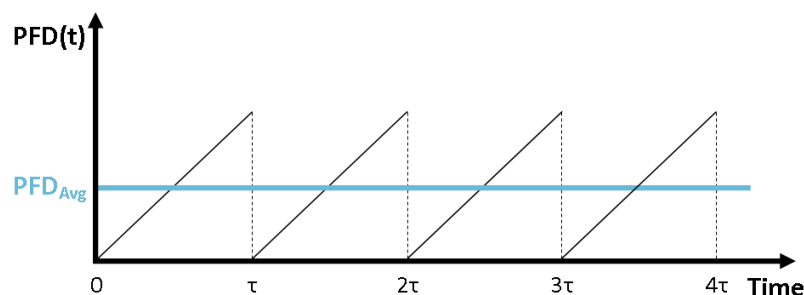


Figure 9-1: Illustration of PFD_{Avg} for periodically proof-tested components [39]

The proof test interval τ is usually allocated to one year (8760hrs). However this value should be determined by the end user of the SIS as it is a function of the site testing routine and if another RRF should be achieved. If a subsystem has a significantly higher PFD_{Avg} than other subsystems, then it could be considered to decrease the proof test interval for this subsystem. Table 9-1 illustrates the impact of changing the proof test interval of the Final Element subsystem in the Svend HIPPS.

Table 9-1: Impact of different proof test interval of the Final Element subsystem at Svend HIPPS

Reliability Parameter	RBD (IEC formulas)		
	$\tau = 8760$ [h]	$\tau = 4380$ [h]	$\tau = 2190$ [h]
$PFD_{Avg,SIF}$	$2.70E^{-03}$	$1.35E^{-03}$	$6.81E^{-04}$
RRF_{SIF}	370	738	1468
SIL_{SIF}	2	2	3

Torres-Echeverría et al. concluded in their paper that proof testing is very relevant for achieving and maintaining high SIL. Lower proof test intervals generally affect the PFD_{Avg} positively, which is also illustrated in Table 9-1. This is, however, in conflict with the system life cycle cost [21].

9.2 Imperfect Proof Testing

If any DU failures in the components are not detected during proof test the test is imperfect and will lead to an increasing PFD_{Avg} over time as illustrated in Figure 9-2.

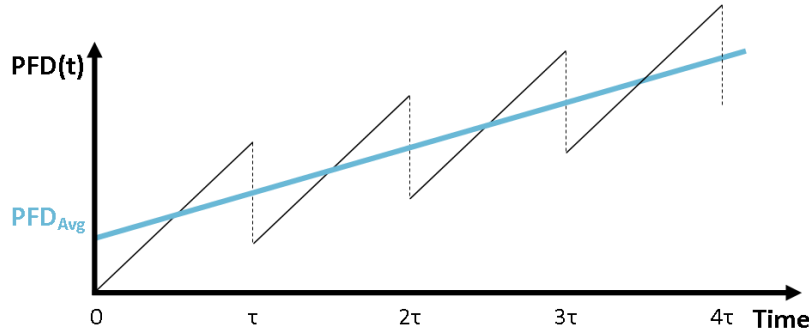


Figure 9-2: Illustration of PFD_{Avg} for periodically imperfect proof-tested components [39]

The contribution of imperfect proof testing can be modelled by introducing Proof Test Coverage (PTC) i.e. the fraction of detected DU failures during a proof test. The DU failures then consist of two parts:

- Detected DU failures during proof test is $PTC \cdot \lambda_{DU}$ with proof test interval τ
- Undetected DU failures during proof test is $(1 - PTC) \cdot \lambda_{DU}$ with complete test interval T , where the DU failure is detected

An example on how to model this for a 1001 voting is illustrated in Eq. 9-1-Eq. 9-2, which is the IEC formulas presented in Eq. 5-8-Eq. 5-9

$$PFD_{Avg,IEC}^{1001} = (\lambda_{DD} + \lambda_{DU})t_{CE} \quad \text{Eq. 9-1}$$

where t_{CE} is the combined down time in hours for all components in the subsystem.

$$t_{CE} = PTC \frac{\lambda_{DU}}{\lambda_D} \left(\frac{\tau}{2} + MRT \right) + (1 - PTC) \frac{\lambda_{DU}}{\lambda_D} \left(\frac{T}{2} + MRT \right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \quad \text{Eq. 9-2}$$

If all DU failures are detected and repaired, then the SIS can be considered as new during the useful life period (see Figure 4-1 page 25).

Concluding Section

(This page is intentionally left blank)

10 Conclusion

The main objective of the thesis was to quantify the PFD_{Avg} , for the SIS related to the Svend HIPPS, with different approaches and compare selected methods. Through a comprehensive literature review of books, articles, Maersk Oil documents, and international IEC standards the following three analytical reliability assessment methods were chosen to quantify the PFD_{Avg} :

- Reliability Block Diagrams (RBD)
- Fault Tree Analysis (FTA)
- Markov Modelling

The methods were chosen among many different qualitative and quantitative analysis methods (presented in Appendix 12.5 page 85 and Appendix 12.6 page 86) with respect to the limitations and objectives set up in the thesis.

Though Availability and MTBF were part of the sub objectives, they have not been addressed because literature review of internal Maersk documents has shown that these concepts are not used. Merely the SIL and PFD_{Avg} values are used in evaluating the reliability of a SIS. Furthermore, the thesis has shown how changing of the proof test interval affects the reliability of the SIS. A more frequent proof test interval increases the reliability but at the cost of increased lifetime cost of the SIS.

10.1 SIS of Svend HIPPS

The three methods were used as tools to analyze the three subsystems in the SIS of Svend HIPPS architecture, illustrated in Figure 10-1 and Figure 10-2.

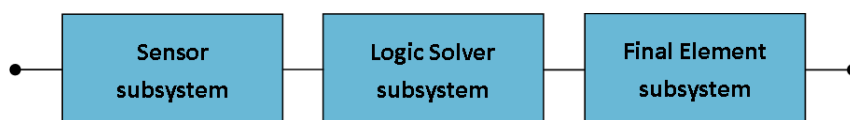


Figure 10-1: Subsystems of a SIS

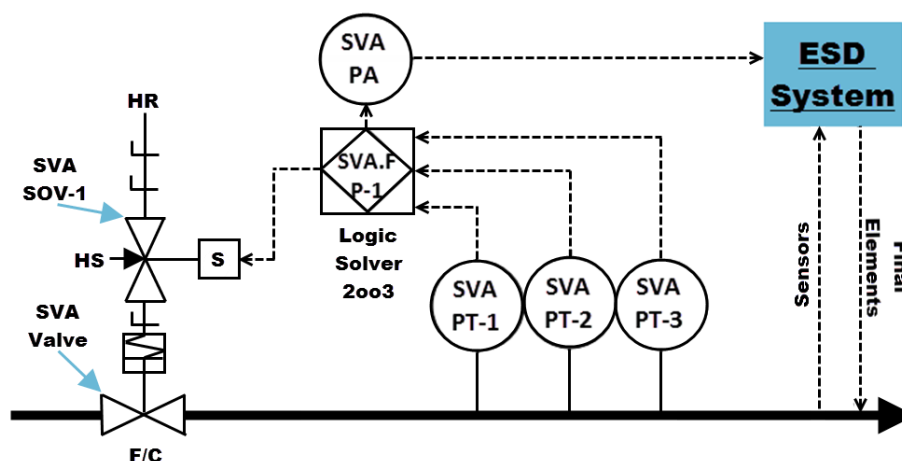


Figure 10-2: Proposed future Svend HIPPS architecture

Each subsystem in the SIS consist of different components from the Svend HIPPS, which are presented in Table 10-1

Table 10-1: Svend HIPPS components divided by subsystem

Sensors	Logic Solver	Final Elements
SVA-PT-1	SVA.F.P-1	SVA-SOV-1
SVA-PT-2		SVA-Valve
SVA-PT-3		

10.2 Comparison of RBD, FTA, and Markov Modelling

FTA and RBD are similar in their approach but more superficial than Markov modelling. The three methods each have benefits and limitations in their approach to calculate the reliability and PFD_{Avg} . The benefits and limitations encountered in this thesis are summarized in Table 10-2.

Table 10-2: Benefits and limitations to RBD, FTA, and Markov modelling

Method	Benefits	Limitations
RBD	<ul style="list-style-type: none"> Can be constructed almost directly from the functional diagram of the system Can be used for almost all types of system configuration including series, parallel, and redundant paths. Can be used to set up models for evaluation of overall system reliability Results in compact and concise diagrams of the system. 	<ul style="list-style-type: none"> Does not provide a specific fault analysis, i.e. the cause-effect(s) paths or the effect-cause(s) Requires a probabilistic model of performance for each element in the diagram. Is primarily success analysis and does not deal effectively with complex repair and maintenance strategies
FTA	<ul style="list-style-type: none"> Can be started in early stages of a design and developed in detail concurrently with design development. Can systematically identify and record the fault paths from a specific event, back to the prime causes by using Boolean algebra. Can easily be converted from logical model into corresponding probability measures. 	<ul style="list-style-type: none"> FTA is not able to represent time or sequence dependency of events correctly. Can have limitations with respect to reconfiguration or state-dependent behavior of systems. Limitations can be compensated by combining FTA with Markov models, where Markov models used as basic events.
Markov	<ul style="list-style-type: none"> Can provide a flexible probabilistic model for analyzing system behavior. Can be used for complex redundant configurations, complex maintenance policies, and common cause failures. Can provide probabilistic solutions that can be used modules in other models such as block diagrams and fault trees. 	<ul style="list-style-type: none"> When the number of components increases, the number of states increases exponential resulting in labor intensive analysis. Can be difficult to construct and verify Requires specific software for the analysis. Can only provide a numerical solution with constant transition rates.

10.3 Results of PFD_{Avg}

The overall results showed small deviations in the PFD_{Avg} value obtained for the Sensor and Final Element subsystem regardless of the used assessment method, as illustrated in Table 10-3. The values for the Svend HIPPS were obtained with reliability information from similar components used in similar installation at Roar HIPPS.

Table 10-3: Summary of results obtained by RBD, FTA, and Markov modelling

Subsystem PFD	RBD		FTA	Markov	
	IEC	Simplified		DU failures	DD + DU failures
Sensor	$3.53E^{-06}$	$3.57E^{-06}$	$3.42E^{-06}$	$3.60E^{-06}$	-
Logic Solver	$5.49E^{-08}$	$6.48E^{-08}$	$5.48E^{-08}$	$1.83E^{-08}$	$5.99E^{-08}$
Final Element	$2.69E^{-03}$	$2.69E^{-03}$	$2.69E^{-03}$	$2.69E^{-03}$	-
$PFD_{Avg,SIF}$	$2.70E^{-03}$	$2.69E^{-03}$	$2.71E^{-03}$	$2.69E^{-03}$	-
RRF_{SIF}	370	371	369	370	-
SIL_{SIF}	2	2	2	2	-

The largest deviation in result is for the PFD_{Avg} value for the Logic Solver subsystem. The calculations for the simplified RBD and $DU + DD$ failures of the Markov modelling are as described in the literature more conservative and therefore useful in the assessment of the final SIL. The deviations are caused by included details in the calculations.

The calculated $PFD_{Avg,SIF}$ is within 1 % deviation regardless of chosen method and the required SIL 2 is obtained with the proposed components and architecture for Svend HIPPS.

10.4 Conclusive Summary

The final conclusion of which of the presented quantitative assessment method to be used can be summarized in a citation from IEC 61508-6:

“All these methods can be used for the majority of safety related systems and, when deciding which technique to use on any particular application, it is very important that the user of a particular technique is competent in using the technique and this may be more important than the technique which is actually used....” [4]

11 Bibliography

1. **ORS Consulting.** LOPA of Svend HIPPS (47.1000.263_R1-A01). s.l. : ORS Consulting, 2016.
2. **ISO.** *ISO/TR 12489:2013 Petroleum, petrochemical and natural gas industries — Reliability modelling and calculation of safety systems.* s.l. : ISO, 2013.
3. **Rausand, Marvin.** *Reliability of Safety-Critical Systems.* s.l. : Wiley, 2014. ISBN: 978-1-118-11272-4-90000.
4. **IEC.** *IEC 61508-6:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3.* s.l. : IEC, 2010.
5. —. *IEC 61511-1:2003 Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements.* s.l. : IEC, 2003.
6. —. *IEC 61508-1:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements.* s.l. : IEC, 2010.
7. **Birolini, Alessandro.** *Reliability Engineering: Theory and Practice.* 5th ed. s.l. : Springer, 2007. 978-3-540-493884.
8. **Goble, William M.** *Control Systems Safety Evaluation and Reliability.* s.l. : ISA, 2010. 978-1-934394-80-9.
9. **Rausand, Marvin and Høyland, Arnljot.** *System Reliability Theory: Models, Statistical Methods and Applications.* 2nd ed. s.l. : Wiley, 2004. ISBN: 978-0-471-47133-2.
10. **Rausand, Marvin.** *Risk Assessment: Theory, Methods, and Applications.* s.l. : Wiley, 2011. 978-0-470-63764-7.
11. **Zio, Enrico.** *Series on Quality, Reliability and Engineering Statistics - Vol. 13: An Introduction to the Basics of Reliability and Risk Analysis.* s.l. : World Scientific, 2007. 978-981-270-639-3.
12. —. *Series on Quality, Reliability and Engineering Statistics - Vol. 14: Computational Methods for Reliability and Risk Analysis.* s.l. : World Scientific, 2009. 978-981-283-901-5.
13. —. *Series on Quality, Reliability and Engineering Statistics - Vol. 15: Basics of Reliability and Risk Analysis Worked Out Problems and Solutions.* s.l. : World Scientific, 2011. 978-981-4355-03-02.
14. **OREDA-2009.** *Offshore Reliability Data Handbook: Volume 1 - Topsides Equipment.* s.l. : OREDA, 2009. 978-82-14-04830-8.
15. **Hauge, Stein.** *Reliability Data for Safety Instrumented Systems - PDS Data Handbook.* s.l. : SINTEF, 2010.

16. *A simple reliability block diagram method for safety integrity verification.* **Guo, Haitao and Yang, Xianhui.** s.l. : Elsevier, October 2nd, 2006, Reliability Engineering and System Safety, Vol. 92, pp. 1267–1273.
17. *Automatic creation of Markov models for reliability assessment of safety instrumented systems.* **Guo, Haitao and Yang, Xianhui.** s.l. : Elsevier, 2008, Reliability Engineering and System Safety, Vol. 98, pp. 807–815.
18. *Extended block diagram method for a multi-state system reliability assessment.* **Lisnianski, Anatoly.** s.l. : Elsevier, 2007, Reliability Engineering and System Safety, Vol. 92, pp. 1601-1607.
19. *Modeling safety instrumented systems with MooN voting architectures addressing system reconfiguration for testing.* **Torres-Echeverría, A.C., Martorell, S. and Thompson, H.A.** 2011 : Elsevier, Reliability Engineering and System Safety, Vol. 96, pp. 545-563.
20. *Multi-objective optimization of design and testing of safety instrumented systems with MooN voting architectures using a genetic algorithm.* **Torres-Echeverría, A.C., Martorell, S. and Thompson, H.A.** s.l. : Elsevier, 2012, ReliabilityEngineeringandSystemSafety, Vol. 106, pp. 45-60.
21. *Modelling and optimization of proof testing policies for safety instrumented systems.* **Torres-Echeverría, A.C., Martorell, S. and Thompson, H.A.** s.l. : Elsevier, 2009, Reliability Engineering and System Safety, Vol. 94, pp. 838-854.
22. *Reliability of safety-instrumented systems subject to partial testing and common-cause failures.* **Jin, Hui and Rausand, Marvin.** s.l. : Elsevier, 2014, Reliability Engineering and System Safety, Vol. 121, pp. 146-151.
23. *Reliability performance of safety instrumented systems: A common approach for both low- and high-demand mode of operation.* **Jin, Hui, Lundteigen, Mary Ann and Rausand, Marvin.** s.l. : Elsevier, 2011, Reliability Engineering and System Safety, Vol. 96, pp. 365-373.
24. **Hildebrandt, Andreas.** *Calculating the "Probability of Failure on Demand" (PFD) of complex structures by means of Markov Models.* s.l. : Pepperl+Fuchs GmbH.
25. *PFD Calculation Considering Imperfect Proof Tests.* **Gabriel, Thomas, Hildebrandt, Andreas and Menck, Udo.** [ed.] Eddy de Rademaeker and Peter Schmelzer. s.l. : AIDIC, 2016, CHEMICAL ENGINEERING TRANSACTIONS, Vol. 48, pp. 637-642.
26. **Börcsök, Josef.** *Comparison of PFD calculation.* s.l. : HIMA Paul Hildebrandt GmbH + Co KG.
27. *Considering and comparing safety parameters — Using different calculation approaches of PFD/PFH/HR.* **Börcsök, Josef and Holub, Petr.** s.l. : IEEE, 2011.
28. *Calculation of MTTF values with Markov Models for Safety Instrumented Systems.* **Börcsök, J., Ugljesa, E. and Machmur, D.** [ed.] Department of Computer Architecture and System Programming, University of Kassel. 2007. 7th WSEAS International Conference on APPLIED COMPUTER SCIENCE, Venice, Italy.

29. *Reliability block diagram with general gates and its application to system reliability analysis*. **Kim, Man Cheol**. s.l. : Elsevier, 2011, Annals of Nuclear Energy, Vol. 38, pp. 2456-2461.
30. **NTNU**. ROSS Gemini Centre/ Publications/ MSc Theses/ MSc from RAMS group. [Online] [Cited: May 29th, 2017.] <https://www.ntnu.edu/ross/msc-theses-rams>.
31. **IEC**. *IEC 61508-4:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 4: Definitions and abbreviations*. s.l. : IEC, 2010.
32. **Maersk Oil - website**. Maersk > Maersk Oil > Operations. *North Sea map*. [Online] [Cited: February 21st, 2017.] <http://www.maerskoil.com/operations/Pages/operations.aspx>.
33. —. Maersk Oil > Operations > Denmark > Oil and gas production. *Map of DUC production facilities*. [Online] [Cited: February 21st, 2017.] http://www.maerskoil.com/operations/Denmark/Documents/DUC%20feltkort_UK_2015_01_mar%20.pdf.
34. **Maersk Oil - document control**. SVAY-14-00042-0001 - rev. 1, Isometric Views. s.l. : Maersk Oil, February 7th, 2012.
35. **IEC**. *IEC 61511-3:2003 Functional safety – Safety instrumented systems for the process industry sector – Part 3: Guidance for the determination of the required safety integrity levels*. s.l. : IEC, 2003.
36. **Maersk Oil - document control**. Standard - MOTS-46 High Integrity Protection System (MOG-FP-SAF-STD-0046 Rev. 2.0). s.l. : MAersk, September 1st, 2016.
37. —. *Standard - Safety Integrity Level (SIL) Analysis (MOG-FP-SAF-STD-0102 Rev 1.0)*. s.l. : Maersk Oil, January 3rd, 2014.
38. **Fleming, K. N.** *A reliability model for common cause mode failures in redundant safety systems, Technical Report GA-A13284*. San Diego, Ca. : General Atomic Company, 1975.
39. **Hauge, Stein, et al., et al.** *Reliability Prediction Method for Safety Instrumented Systems: PDS Method Handbook 2013 Edition*. s.l. : SINTEF, 2013. 978-82-536-1333-8.
40. **IEC**. *IEC 61078:2016 Reliability block diagrams*. s.l. : IEC, 2016.
41. —. *IEC 61025:2006 Fault Tree Analysis (FTA)*. s.l. : IEC, 2006.
42. **Glæsner, Jacob**. *Case-based report: Maersk Oil Svend Platform HIPPS Upgrade*. s.l. : Jacob Glæsner, 2017.
43. **Maersk Oil - document control**. SVAY-04-00014-0002 - rev. 11, SVA P&ID export riser. s.l. : Maersk Oil, June 14th, 2016.
44. —. *Svend General Documentation*. s.l. : Maersk Oil, June 2012.
45. **ITOPF**. *Fate of Marine Oil Spills - Technical Information Paper*. London : ITOPF, 2011.

46. **Maersk Oil - document control.** DBU Oil Spill Risk Assessment (DK-HSE-PRD-0001 Rev 1.0). s.l. : Maersk Oil, April 26th, 2015.
47. **IEC.** *IEC 61508-7:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of techniques and measures.* s.l. : IEC, 2010.
48. —. *IEC 60300-3-1:2003 Dependability management – Part 3-1: Application guide – Analysis techniques for dependability – Guide on methodology.* 2003.
49. **Maersk Oil - document control.** SVAY-03-00023-0000 - rev. 3, SVA HIPPS Schematic export pipeline. s.l. : Maersk Oil, September 8th, 2015.
50. **Wakerly, John F.** *Digital Design: Principles and Practices.* 4th. s.l. : Pearson, 2006. pp. 179-234. ISBN: 978-81-317-1366-2.
51. **IEC.** *IEC 60300-3-2:2004 Dependability management – Part 3-2: Application guide – Collection of dependability data from the field.* s.l. : IEC, 2004.
52. —. *IEC 60300-3-4:2007 Dependability management – Part 3-4: Application guide – Guide to the specification of dependability requirements.* s.l. : IEC, 2007.
53. —. *IEC 60812:2006 Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA).* s.l. : IEC, 2006.
54. —. *IEC 61508-2:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems.* s.l. : IEC, 2010.
55. —. *IEC 61508-3:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 3: Software requirements.* s.l. : IEC, 2010.
56. —. *IEC 61508-5:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 5: Examples of methods for the determination of safety integrity levels.* s.l. : IEC, 2010.
57. —. *IEC 61511-2:2003 Functional safety – Safety instrumented systems for the process industry sector – Part 2: Guidelines for the application of IEC 61511-1.* s.l. : IEC, 2003.
58. —. *IEC 62551:2012 Analysis techniques for dependability – Petri net techniques.* s.l. : IEC, 2012.
59. —. *IEC 60050-351:2013 International electrotechnical vocabulary – Part 351: Control technology.* s.l. : IEC, 2013.
60. —. *IEC 60050-151:2001 International Electrotechnical Vocabulary – Part 151: Electrical and magnetic devices.* s.l. : IEC, 2001.

61. —. *IEC/TR 62380:2004 Reliability data handbook – Universal model for reliability prediction of electronics components, PCBs and equipment.* s.l. : IEC, 2004.
62. **ISO.** *ISO 10418:2003 Petroleum and natural gas industries — Offshore production installations — Basic surface process safety systems.* s.l. : ISO, 2003.
63. —. *ISO 13702:2015 Petroleum and natural gas industries — Control and mitigation of fires and explosions on offshore production installations — Requirements and guidelines.* s.l. : ISO, 2015.
64. —. *ISO 14224:2016 Petroleum, petrochemical and natural gas industries — Collection and exchange of reliability and maintenance data for equipment.* s.l. : ISO, 2016.
65. —. *ISO 17776:2000 Petroleum and natural gas industries — Offshore production installations — Guidelines on tools and techniques for hazard identification and risk assessment.* s.l. : ISO, 2000.
66. **IEC.** *IEC 61703:2016 Mathematical expressions for reliability, availability, maintainability and maintenance support terms.* s.l. : IEC, 2016.
67. —. *IEC 61165:2006 Application of Markov techniques.* s.l. : IEC, 2006.
68. **Limnios, Nikolaos.** *Fault Trees.* s.l. : ISTE, 2007. ISBN: 978-1-905209-30-9.

12 Appendix

(This page is intentionally left blank)

12.1 Hazard Scenarios [42]

Eight hazard scenarios were identified prior to the LOPA study and merged into following five initiating causes:

a) Stuck pig

A blockage due to a stuck pig occurs in the sub-sea tee piece downstream the Svend riser or further downstream in the export pipeline to Tyra East. Pigging facilities are present on Svend, however pigging might be difficult as the pig historically has been difficult to drive to Tyra East due to the sub-sea tee piece. Notice that there is a check valve installed in the riser prior to entering the sub-sea tee piece according to the P&ID SVAY-04-00014-0002 rev 11 [43]. Pigging occurs regularly from Harald to Tyra East (approx. once per month).

b) Hydrate formation

A blockage due to hydrate formation occurs just downstream the hose on Svend riser or further downstream in the export pipeline to Tyra East. Hydrate formation is unlikely in normal situations as well fluid is relatively warm from Svend. However well fluid coolers are installed and could cool down to hydrate formation temperature if control does not work properly [44].

c) Wax plug

A blockage due to a wax plug occurs downstream the hose or in the pipeline downstream the sub-sea tee-piece since Lulita, Trym and Svend fluid is waxy [44].

d) Closed Tyra East inlet

Path into Tyra East gets closed, while Svend is still producing to the pipeline. This could be due to riser ESDV closure (ESDV-18010) or inlet ESDV closure (ESDV-18101).

e) Stuck check valve

Stuck check valve downstream flexible hose.

12.2 TMEL Values for existing installations [37]

SEVERITY RATING	HEALTH and SAFETY CONSEQUENCES	ENVIRONMENTAL CONSEQUENCES	COMMERCIAL CONSEQUENCES	TMEL (existing installations)
1	Minor injury or minimal health effect.	Minimal effect	na	na
2	Injury requiring medical treatment or short term health effect.	Slight effect	<USD10,000	$1 \times 10^{-1}/\text{yr}$
3	Lost workday injury or medium term health effect.	Minor effect	USD10,000 to USD100,000	$1 \times 10^{-2}/\text{yr}$
4	2 or more lost work day cases or 1 or more permanent disability cases allowing return to work or 1 permanent disability case preventing return to work.	Pollution near the asset, remediation within a matter of days	USD100,000 to USD10 million	$1 \times 10^{-3}/\text{yr}$
5	1 fatality or 2-5 permanent disability cases preventing return to work.	Significant pollution beyond the asset, potential to affect third-parties	USD10 million to USD100 million	$1 \times 10^{-4}/\text{yr}$
6	2 to 5 fatalities or 6 or more permanent disabilities preventing return to work.	Significant pollution requiring more than 6 months for remediation	USD100 million to USD1 billion	$1 \times 10^{-5}/\text{yr}$
7	6 to 10 fatalities	Extensive pollution affecting land and/or third party facilities requiring more than 2 years for remediation	USD1 billion to USD10 billion	$1 \times 10^{-6}/\text{yr}$

12.3 Oil Group Classification [45] [46]

Group 1 oils

A: °API > 45 (Specific gravity < 0.8)
B: Pour point °C
C: Viscosity @ 10–20°C: less than 3 cSt
D: % boiling below 200°C: greater than 50%
E: % boiling above 370°C: between 20 and 0%

	A	B	C	D	E
Asgard	49	-28	2 @ 10°C	58	14
Arabian Super Light	51	-39	2 @ 20°C		
Cossack	48	-18	2 @ 20°C	51	18
Curlw	47	-13	2 @ 20°C	57	17
F3 Condensate	54	<-63	1 @ 10°C	81	0
Gippsland	52	-13	1.5 @ 20°C	63	8
Hidra	52	-62	2.5 @ 10°C	60	11
Terengganu condensate	73	-36	0.5 @ 20°C	>95	0
Wolffbutt	49	-53	2 @ 20°C	55	4
Gasoline	58		0.5 @ 15°C	100	0
Kerosene	45	-55	2 @ 15°C	50	0
Naptha	55		0.5 @ 15°C	100	0

Group 2 oils

A: °API 35–45 (Specific gravity 0.8–0.85)
B: Pour point °C
C: Viscosity @ 10–20°C: between 4 cSt and semi-solid
D: % boiling below 200°C: between 20 and 50%
E: % boiling above 370°C: between 15 and 50%

Low pour point <6°C

	A	B	C	D	E
Arabian Extra Light	38	-30	3 @ 15°C	26	39
Azeri	37	-3	8 @ 20°C	29	46
Brent	38	-3	7 @ 10°C	37	33
Draugen	40	-15	4 @ 20°C	37	32
Dukhan	41	-49	9 @ 15°C	36	33
Liverpool Bay	45	-21	4 @ 20°C	42	28
Sokol (Sakhalin)	37	-27	4 @ 20°C	45	21
Rio Negro	35	-5	23 @ 10°C	29	41
Umm Shaif	37	-24	10 @ 10°C	34	31
Zakum	40	-24	6 @ 10°C	36	33
Marine Gas oil (MGO)	37	-3	5 @ 15°C		

High pour point >5°C

	A	B	C	D	E
Amna	36	19	Semi-solid	25	30
Beatrice	38	18	32 @ 15°C	25	35
Bintulu	37	19	Semi-solid	24	34
Escravos	34	10	9 @ 15°C	35	15
Sarir	38	24	Semi-solid	24	39
Statfjord	40	6	7 @ 10°C	38	32

Note: High pour point oils only behave as Group 2 at ambient temperatures above their pour point. Below this treat as Group 4 oils.

Group 3 oils

A: °API 17.5–35 (Specific gravity 0.85–0.95)
B: Pour point °C
C: Viscosity @ 10–20°C: between 8 cSt and semi solid
D: % boiling below 200°C: between 10 and 35%
E: % boiling above 370°C: between 30 and 65%

Low pour point <6°C

	A	B	C	D	E
Alaska North Slope	28	-18	32 @ 15°C	32	41
Arabian Heavy	28	-40	55 @ 15°C	21	56
Arabian Medium	30	-21	25 @ 15°C	22	51
Arabian Light	33	-40	14 @ 15°C	25	45
Bonny Light	35	-11	25 @ 15°C	26	30
Iranian Heavy	31	-36	25 @ 15°C	24	48
Iranian Light	34	-32	15 @ 15°C	26	43
Khafji	28	-57	80 @ 15°C	21	55
Sirri	33	-12	18 @ 10°C	32	38
Thunder Horse	35	-27	10 @ 10°C	32	39
Tia Juana Light	32	-42	500 @ 15°C	24	45
Troll	33	-9	14 @ 10°C	24	35
IFO 180	18–20	10–30	1,500–3,000 @ 15°C		–

High pour point >5°C

	A	B	C	D	E
Cabinda	33	12	Semi-solid	18	56
Coco	32	21	Semi-solid	21	46
Gamba	31	23	Semi-solid	11	54
Mandji	30	9	70 @ 15°C	21	53
Minas	35	18	Semi-solid	15	58

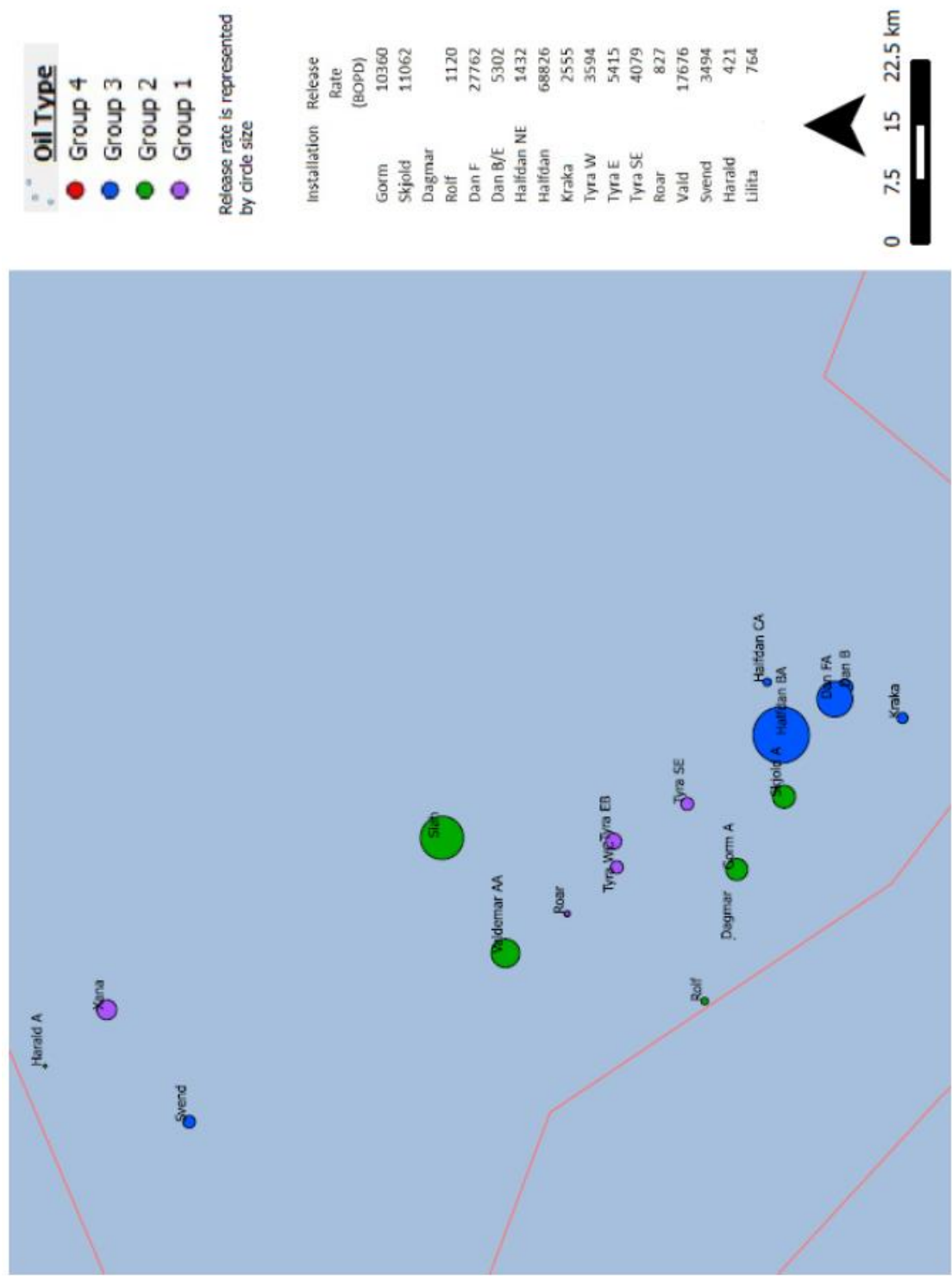
Note: High pour point oils only behave as Group 3 at ambient temperatures above their pour point. Below this treat as Group 4 oils.

Group 4 oils

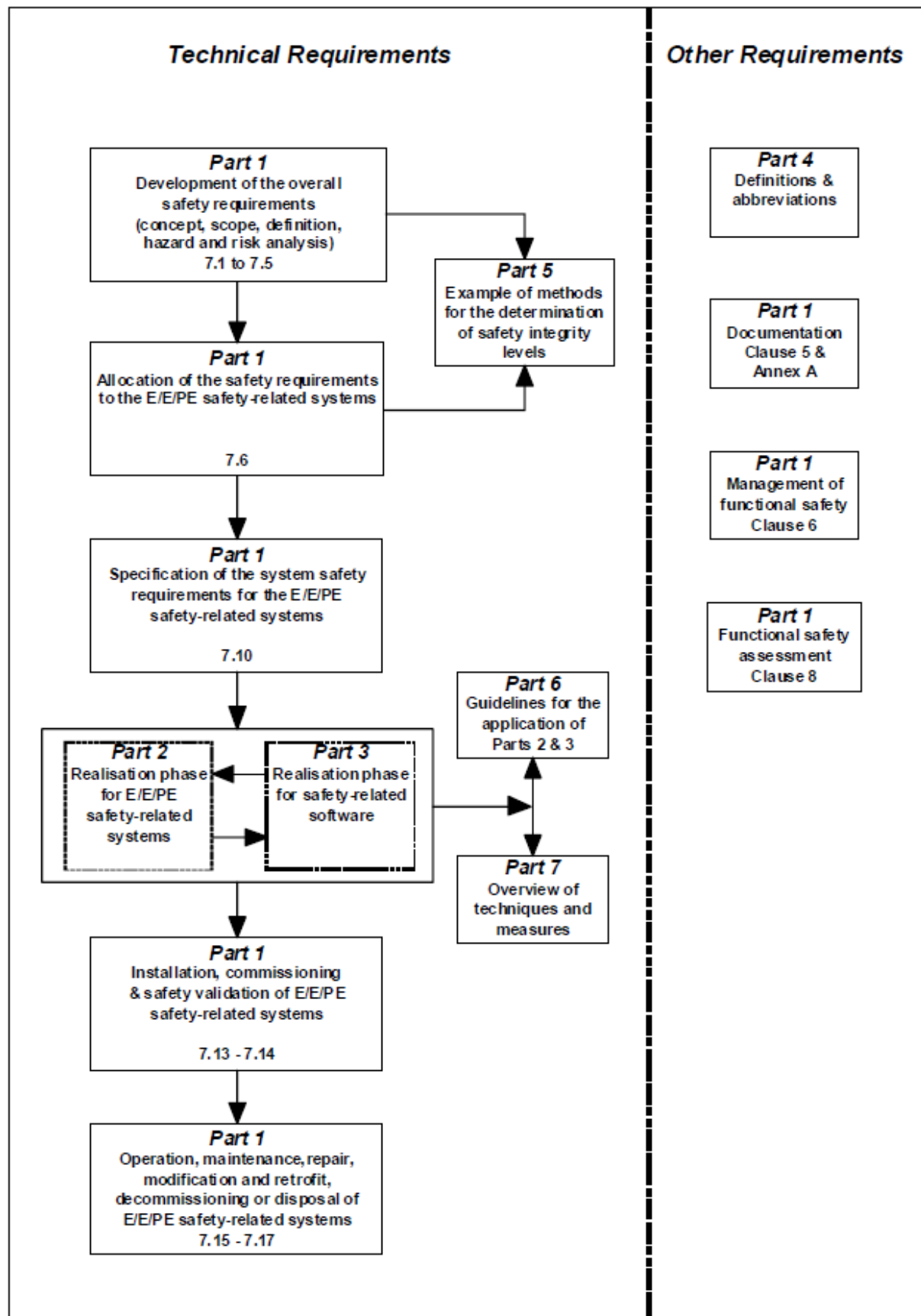
A: °API <17.5 (Specific gravity >0.95) or
B: Pour point >30°C
C: Viscosity @ 10–20°C: between 1500 cSt and semi-solid
D: % boiling below 200°C: less than 25%
E: % boiling above 370°C: greater than 30%

	A	B	C	D	E
Bachaquero 17	16	-29	5,000 @ 15°C	10	60
Boscan	10	15	Semi-solid	4	80
Cinta	33	43	Semi-solid	10	54
Handil	33	35	Semi-solid	23	33
Merey	17	-21	7,000 @ 15°C	7	70
Nile Blend	34	33	Semi-solid	13	59
Pilon	14	-3	Semi-solid	2	92
Shengli	24	21	Semi-solid	9	70
Taching	31	35	Semi-solid	12	49
Tia Juana Pesado	12	-1	Semi-solid	3	78
Widuri	33	46	Semi-solid	7	70
IFO 380	11–15	10–30	5,000–30,000 @ 15°C		

Table 2: Example oils classified according to their °API (American Petroleum Institute gravity). The colours of each group relate to Table 1 and to Figures 1, 2, 12 and 13. Generally, persistence when spilled increases with group number.



12.4 Overall framework of IEC 61508 [47]



12.5 Use of methods for general dependability analysis tasks [48]

Analysis method	Allocation of dependability requirements/goals	Qualitative analysis	Quantitative analysis	Review and recommendations	Annex
Failure rate prediction	Applicable for serial systems without redundancy	Possible for maintenance strategy analysis	Calculation of failure rates and MTTF for electronic components and equipment	Supporting	A.1.1
Fault tree analysis	Applicable, if system behaviour is not heavily time- or sequence-dependent	Fault combinations	Calculation of system reliability, availability and relative contributions of subsystems to system unavailability	Applicable	A.1.2
Event tree analysis	Possible	Failure sequences	Calculation of system failure rates	Applicable	A.1.3
Reliability block diagram analysis	Applicable, for systems where independent blocks can be assumed	Success paths	Calculation of system reliability, availability	Applicable	A.1.4
Markov analysis	Applicable	Failure sequences	Calculation of system reliability, availability	Applicable	A.1.5
Petri net analysis	Applicable	Failure sequences	To provide the system description for Markov analysis	Applicable	A.1.6
Failure modes and effects (and criticality) analysis; FME(C)A	Applicable for systems where independent single failure is predominant	Effects of failures	Calculation of system failure rates (and criticality)	Applicable	A.1.7
HAZOP studies	Supporting	Causes and consequences of deviations	Not applicable	Supporting	A.1.8
Human reliability analysis	Supporting	Impact of human performance on system operation	Calculation of error probabilities for human tasks	Supporting	A.1.9
Stress-strength analysis	Not applicable	Usable as a means of fault avoidance	Calculation of reliability for (electro) mechanical components	Supporting	A.1.10
Truth table (structure function analysis)	Not applicable	Possible	Calculation of system reliability, availability	Supporting	A.1.11
Statistical reliability methods	Possible	Impact of faults	Quantitative estimation of reliability with uncertainties	Supporting	A.1.12

NOTE The particular wording in the table is used as follows:

'Applicable' means that the method is generally applicable and recommended for the task (possibly with the mentioned restrictions).

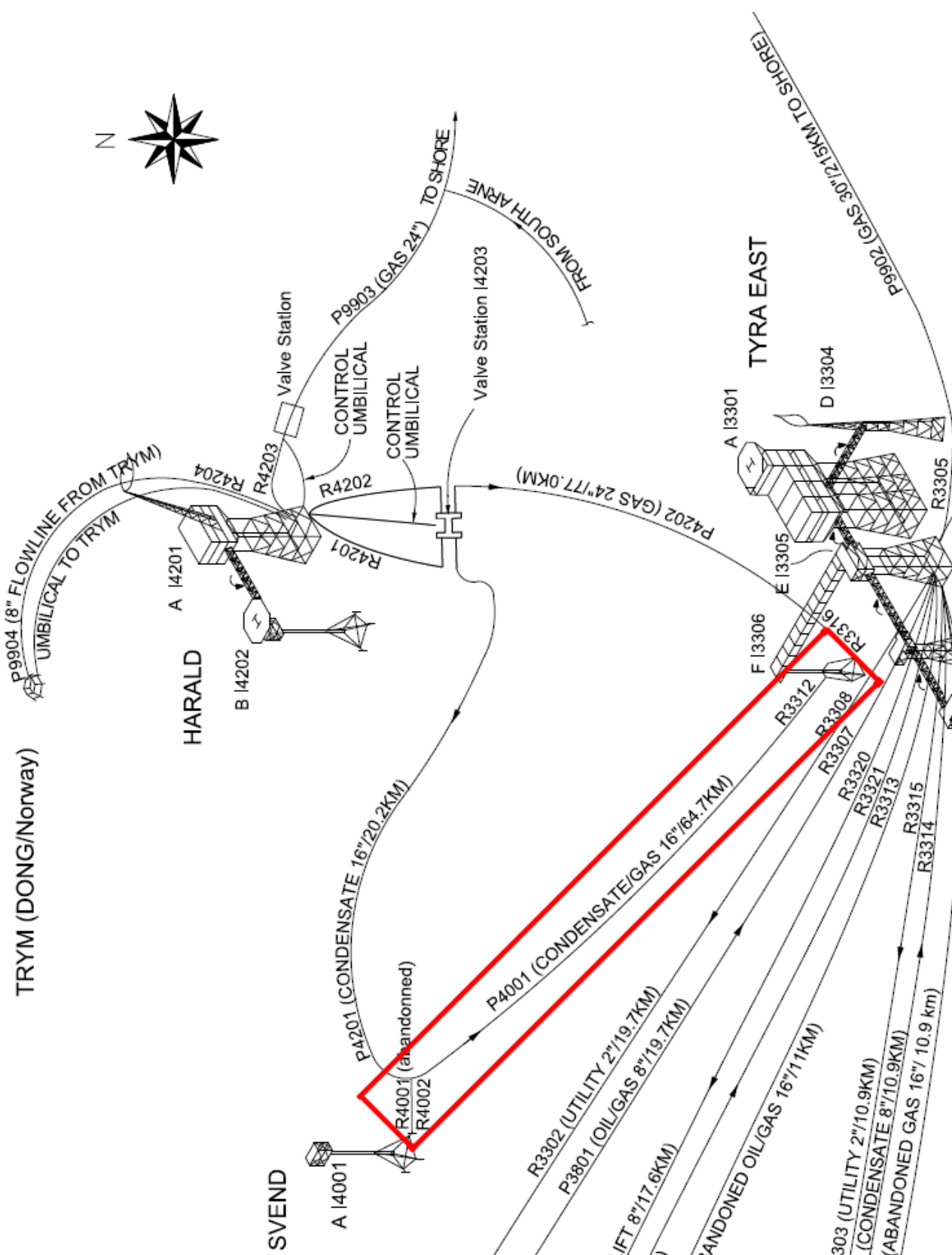
'Possible' means that the method may be used for this task but has certain drawbacks compared to other methods.

'Supporting' means that the method is generally applicable for a certain part of the task but not as a stand-alone method for the complete task.

'Not applicable' means that the method cannot be used for this task.

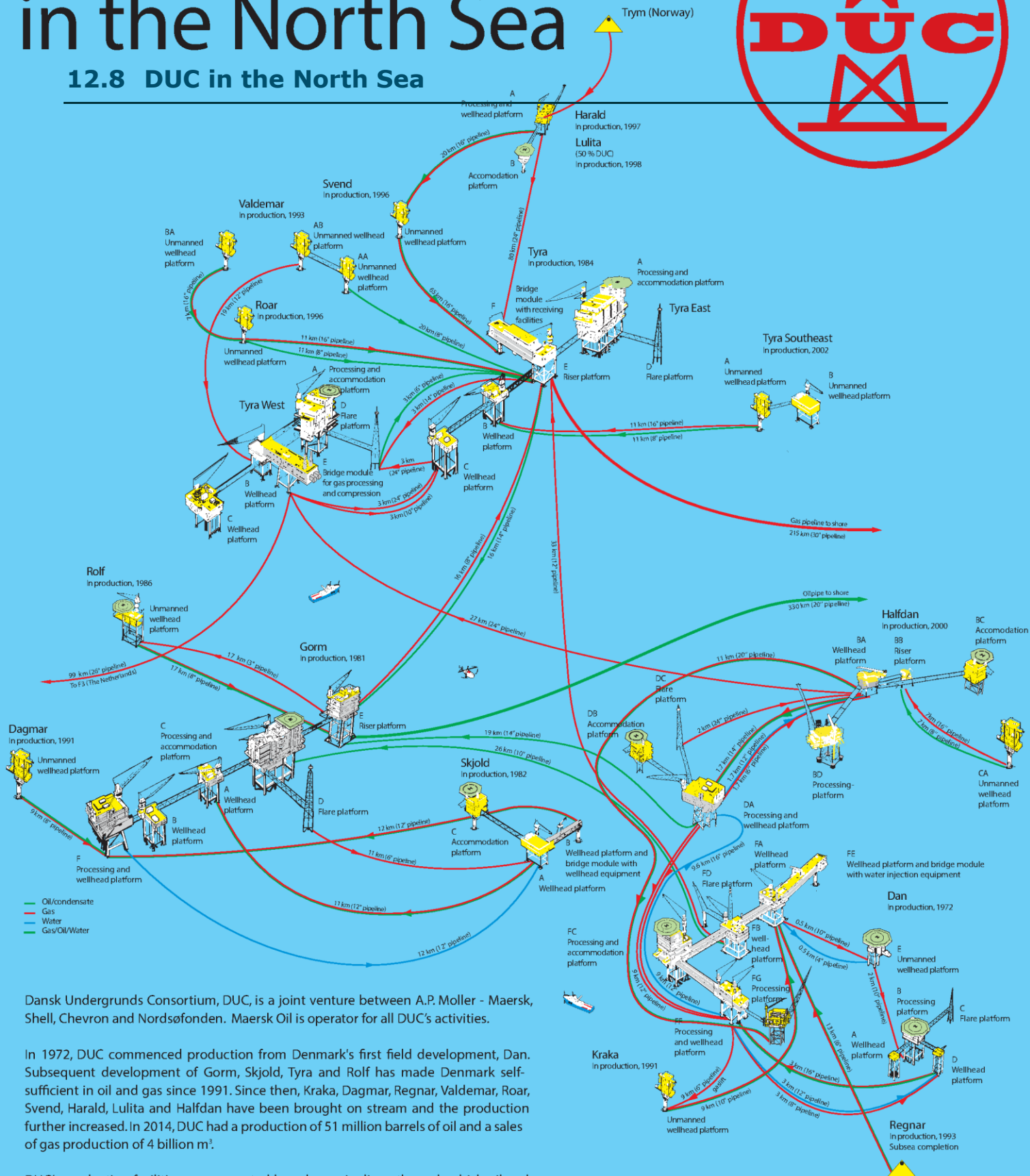
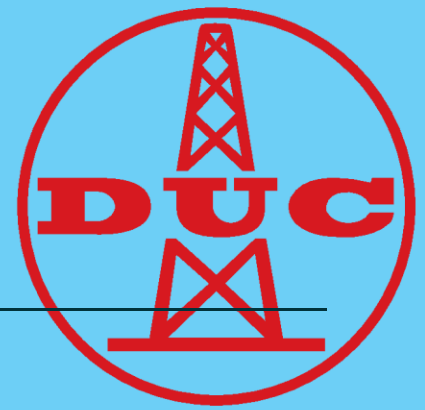
12.6 Characteristic of selected dependability analysis method [48]

Method	Suitable for complex systems	Suitable for novel system designs	Quantitative analysis	Suitable for combination of faults	Suitable to handle sequence-dependence	Can be used for dependent events	Bottom-up or top-down	Suitable for dependability allocation	Mastery required (from low to high)	Acceptance and commonality	Need for tool support	Plausibility checks	Availability of tools	IEC standard
Failure rate prediction	No	Yes	Yes	No	No	No	BU	Yes	Low	High	Avg	Yes	High	61709
Fault tree analysis (FTA)	Yes	Yes	Yes	Yes	No	No	TD	Yes	Avg	High	Avg	Yes	High	61025
Event tree analysis (ETA)	NR	NR	Yes	NR	Yes	Yes	BU	NR	High	Avg	Avg	Yes	Avg	
Reliability block diagram analysis (RBD)	NR	NR	Yes	Yes	No	No	TD	Yes	Low	Avg	Avg	Yes	Avg	61078
Markov analysis	Yes	Yes	Yes	Yes	Yes	Yes	TD	Yes	High	Avg	High	No	Avg	61165
Petri net analysis	Yes	Yes	Yes	Yes	Yes	Yes	TD	Yes	High	Low	High	No	Low	
Failure mode and effects analysis (FMEA)	NR	NR	Yes	No	No	No	BU	NR	Low	High	Low	Yes	High	60812
HAZOP studies	Yes	Yes	No	No	No	No	BU	No	Low	Avg	Low	Yes	Avg	61882
Human reliability analysis	Yes	Yes	Yes	Yes	Yes	Yes	BU	No	High	High	Avg	Yes	Avg	
Stress-strength analysis	NA	NA	Yes	NA	NA	No	NA	No	High	Avg	High	Yes	Avg	
Truth table	No	Yes	Yes	Yes	No	No	NA	Yes	High	Avg	High	No	Low	
Statistical reliability methods	Yes	Yes	Yes	Yes	Yes	Yes	NA	NR	High	Avg	High	Avg	Low	60300-3-5
NR May be used for simple systems, Not recommended as a stand-alone method, to be used jointly with other methods. TD Top-down. BU Bottom-up. Avg Average. NA The criterion is not applicable with respect to this method.														



DUC in the North Sea

12.8 DUC in the North Sea



Dansk Undergrunds Consortium, DUC, is a joint venture between A.P. Møller - Maersk, Shell, Chevron and Nordsøfonden. Maersk Oil is operator for all DUC's activities.

In 1972, DUC commenced production from Denmark's first field development, Dan. Subsequent development of Gorm, Skjold, Tyra and Rolf has made Denmark self-sufficient in oil and gas since 1991. Since then, Kraka, Dagmar, Regnar, Valdemar, Roar, Svend, Harald, Lulita and Halfdan have been brought on stream and the production further increased. In 2014, DUC had a production of 51 million barrels of oil and a sales of gas production of 4 billion m³.

DUC's production facilities are connected by subsea pipelines, through which oil and gas are transported to Gorm and Tyra. From here the processed oil and gas are sent to shore.

Please visit www.maerskoil.com for further information.



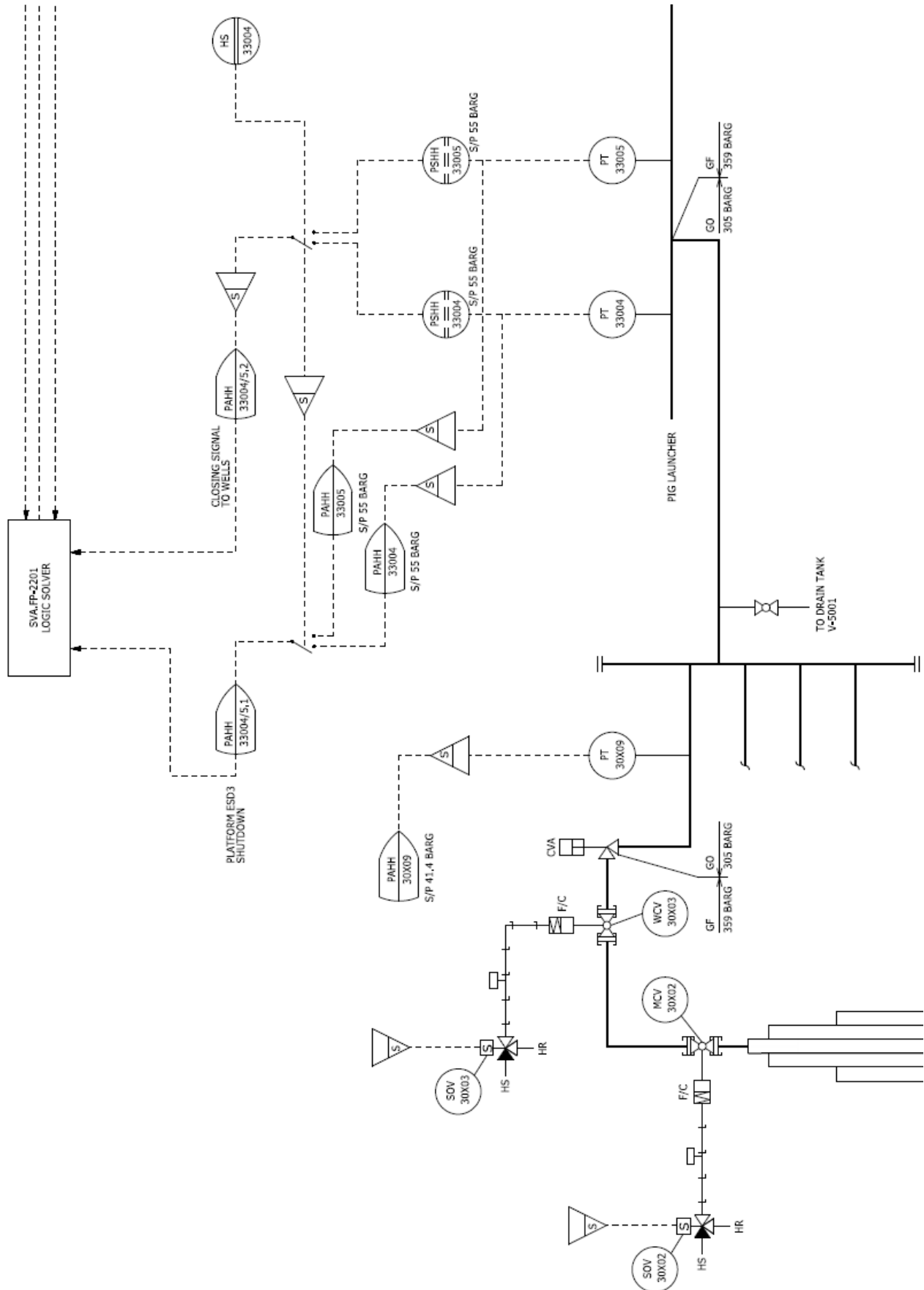


Figure 12-2: Part of Process Flow Diagram (PFD) HIPPS Schematic Export Pipeline, upstream pig launcher [49]

12.11 PFD and SIL determination

12.11.1 Initiating Cause (IC)

See Appendix 12.1 page 80.

12.11.2 Independent Protection Layers (IPL)

1) Primary Safety Instrumented Function (SIF)

ESD system

2) Probability of ignition

Conservatively assumed > 50 kg/s of gas emerging from subsea, migrating up to the installation and engulfing it

3) Occupancy

Probability of persons on installation calculated based on normal occupancy

12.11.3 TMEL

See Appendix 12.2 page 81.

12.11.4 Example of SIL determination of Safety Impact

Table 12-1: Example of SIL determination of Safety Impact

IC	Frequency (years)	Independent Protection Layers			F_E
		1	2	3	
A	0.01	0.1	0.3	0.02	6.0E-6
B	0.01	0.1	0.3	0.02	6.0E-6
C	0.01	0.1	0.3	0.02	6.0E-6
D	0.02	0.1	0.3	0.02	1.2E-5
E	0.01	0.1	0.3	0.02	6.0E-6
Total Event Frequency ($F_{E,total}$)					3.6E-5
TMEL (Appendix 12.2 page 81)					1.0E-6
PFD _{avg} ($TMEL/F_{E,total}$)					2.8E-2
SIL					1

12.12 2oo3 Structure Function

12.12.1 Minimal Path Set

The structure function for 2oo3 voting as represented in Eq. 6-10 page 36 is derived using a combination of series and parallel structures and the Minimal Path Sets, which is the minimal path through the system that still secures the system in up state. The different paths are illustrated in Figure 12-3.

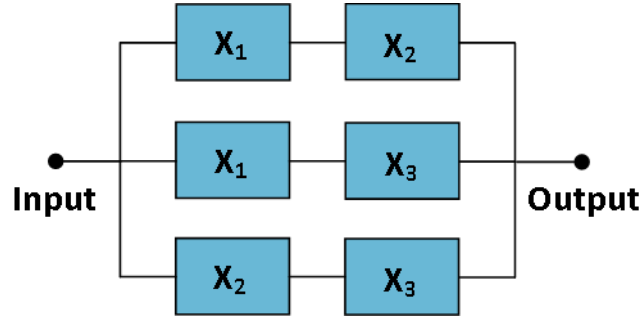


Figure 12-3: Minimal Path Set of a 2oo3 RBD

The approach is similar for other *moon* structures.

$$\begin{aligned}
 \phi(\mathbf{X}) &= x_1 \cap x_2 \cup x_1 \cap x_3 \cup x_2 \cap x_3 \\
 &= x_1 x_2 \cup x_1 x_3 \cup x_2 x_3 \\
 &= 1 - (1 - x_1 x_2)(1 - x_1 x_3)(1 - x_2 x_3) \\
 &= 1 - (1 - x_1 x_2 - x_1 x_3 + x_1^2 x_2 x_3)(1 - x_2 x_3) \\
 &= 1 - (1 - x_1 x_2 - x_1 x_3 + x_1^2 x_2 x_3 - x_2 x_3 + x_1 x_2^2 x_3 + x_1 x_2 x_3^2 - x_1^2 x_2^2 x_3^2) \\
 &= x_1 x_2 + x_1 x_3 + x_2 x_3 - x_1^2 x_2 x_3 - x_1 x_2^2 x_3 - x_1 x_2 x_3^2 + x_1^2 x_2^2 x_3^2 \\
 x_i \text{ is binary so } x_i^m &= x_i \\
 &= x_1 x_2 + x_1 x_3 + x_2 x_3 - x_1 x_2 x_3 - x_1 x_2 x_3 - x_1 x_2 x_3 + x_1 x_2 x_3 \\
 &= x_1 x_2 + x_1 x_3 + x_2 x_3 - 2x_1 x_2 x_3 = \text{Eq. 6-10 page 36}
 \end{aligned}$$

12.12.2 Minimal Cut Set

Another approach to derive Eq. 6-10 page 36 is by following a Minimal Cut Set. A cut set is a set of components that by failing puts the system in down state. The RBD of this is illustrated in Figure 12-4.

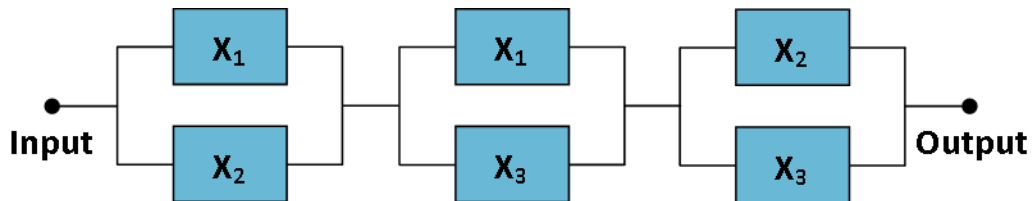


Figure 12-4: Minimal Cut Set of a 2oo3 RBD

The approach is similar for other moon structures.

$$\begin{aligned}
 \phi(X) &= x_1 \cup x_2 \cap x_1 \cup x_3 \cap x_2 \cup x_3 \\
 &= (x_1 \cup x_2)(x_1 \cup x_3)(x_2 \cup x_3) \\
 &= (1 - (1 - x_1)(1 - x_2))(1 - (1 - x_1)(1 - x_3))(1 - (1 - x_2)(1 - x_3)) \\
 &= (x_1 + x_2 - x_1x_2)(x_1 + x_3 - x_1x_3)(x_2 + x_3 - x_2x_3) \\
 &= (x_1^2 + x_1x_3 - x_1^2x_3 + x_1x_2 + x_2x_3 - x_1x_2x_3 - x_1^2x_2 - x_1x_2x_3 + x_1^2x_2x_3)(x_2 \\
 &\quad + x_3 - x_2x_3)
 \end{aligned}$$

x_i is binary so $x_i^m = x_i$

$$= (x_1 + x_2x_3 - x_1x_2x_3)(x_2 + x_3 - x_2x_3)$$

$$= x_1x_2 + x_1x_3 - x_1x_2x_3 + x_2^2x_3 + x_2x_3^2 - x_2^2x_3^2 - x_1x_2^2x_3 - x_1x_2x_3^2 + x_1x_2^2x_3^2$$

x_i is binary so $x_i^m = x_i$

$$= x_1x_2 + x_1x_3 + x_2x_3 - 2x_1x_2x_3$$

$$= \text{Eq. 6-10 page 36}$$

12.13 moon non-identical components

12.13.1 Boolean Truth Table

It can be a tedious task to calculate the structure function of a *moon* structure, so a Boolean Truth table can be helpful in reducing the necessary terms.

A 2oo3 system is represented in Eq. 12-1 and Eq. 12-2.

$$\phi(X) = x_1 \cdot x_2 + x_1 \cdot x_3 + x_2 \cdot x_3 = x_1 \cap x_2 \cup x_1 \cap x_3 \cup x_2 \cap x_3 \quad \text{Eq. 12-1}$$

$$\phi(X) = x_1x_2 + x_1x_3 + x_2x_3 - 2x_1x_2x_3 \quad \text{Eq. 12-2}$$

Table 12-2 illustrates the corresponding truth table with disjointed terms. The disjointed terms can be reduced using switching algebra theorems, which are illustrated in Figure 12-5 and Figure 12-6.

Table 12-2: Boolean Truth Table of 2oo3 RBD

State Number	Block State			System State	Disjointed Terms	Reduction
X1	X2	X3				
0	0	0	0	0	$\bar{x}_1 \cdot \bar{x}_2 \cdot \bar{x}_3$	$\bar{x}_1 \cdot \bar{x}_2$
1	0	1	0	0	$\bar{x}_1 \cdot \bar{x}_2 \cdot x_3$	
2	0	1	0	0	$\bar{x}_1 \cdot x_2 \cdot \bar{x}_3$	$\bar{x}_1 \cdot x_2 \cdot \bar{x}_3$
3	0	1	1	1	$\bar{x}_1 \cdot x_2 \cdot x_3$	$\bar{x}_1 \cdot x_2 \cdot x_3$
4	1	0	0	0	$x_1 \cdot \bar{x}_2 \cdot \bar{x}_3$	$x_1 \cdot \bar{x}_2 \cdot \bar{x}_3$
5	1	0	1	1	$x_1 \cdot \bar{x}_2 \cdot x_3$	$x_1 \cdot \bar{x}_2 \cdot x_3$
6	1	1	0	1	$x_1 \cdot x_2 \cdot \bar{x}_3$	$x_1 \cdot x_2$
7	1	1	1	1	$x_1 \cdot x_2 \cdot x_3$	

(T1)	$X + 0 = X$	(T1 ^)	$X \cdot 1 = X$	(Identities)
(T2)	$X + 1 = 1$	(T2 ^)	$X \cdot 0 = 0$	(Null elements)
(T3)	$X + X = X$	(T3 ^)	$X \cdot X = X$	(Idempotency)
(T4)	$(X ^)' = X$			(Involution)
(T5)	$X + X' = 1$	(T5 ^)	$X \cdot X' = 0$	(Complements)

Figure 12-5: Switching Algebra Theorems with one Variable [50]

(T6)	$X + Y = Y + X$	(T6')	$X \cdot Y = Y \cdot X$	(Commutativity)
(T7)	$(X + Y) + Z = X + (Y + Z)$	(T7')	$(X \cdot Y) \cdot Z = X \cdot (Y \cdot Z)$	(Associativity)
(T8)	$X \cdot Y + X \cdot Z = X \cdot (Y + Z)$	(T8')	$(X + Y) \cdot (X + Z) = X + Y \cdot Z$	(Distributivity)
(T9)	$X + X \cdot Y = X$	(T9')	$X \cdot (X + Y) = X$	(Covering)
(T10)	$X \cdot Y + X \cdot Y' = X$	(T10')	$(X + Y) \cdot (X + Y') = X$	(Combining)
(T11)	$X \cdot Y + X' \cdot Z + Y \cdot Z = X \cdot Y + X' \cdot Z$			(Consensus)
(T11')	$(X + Y) \cdot (X' + Z) \cdot (Y + Z) = (X + Y) \cdot (X' + Z)$			

Figure 12-6: Switching Algebra Theorems with two of three Variables [50]

The structure function for success can be reduced to

$$\phi(X) = \bar{x}_1 \cdot x_2 \cdot x_3 + x_1 \cdot \bar{x}_2 \cdot x_3 + x_1 \cdot x_2$$

Eq. 12-3

The structure function for failure can be reduced to

$$\phi(X) = \bar{x}_1 \cdot x_2 \cdot \bar{x}_3 + x_1 \cdot \bar{x}_2 \cdot \bar{x}_3 + \bar{x}_1 \cdot \bar{x}_2$$

Eq. 12-4

12.13.2 Karnaugh Maps

A Karnaugh map is a simplified representation of a truth table. Figure 12-7 illustrates a Karnaugh map of the Boolean truth Table 12-2 with block state in the blue quadrants and system state in the white quadrants.

		X ₂			
		00	01	11	10
X ₂ X ₃	X ₁				
0	0	0	0	1	0
1	1	0	1	1	1

X₃

Figure 12-7: Karnaugh map of 2oo3 Boolean truth table

A circle around a 2^i system state 1-cells may be combined if there are i variables of the logic function that take on all 2^i possible combinations within that set

- If a circle covers only areas of the map where the variable is 0, then the variable is complemented in the product term.

- If a circle covers only areas of the map where the variable is 1, then the variable is uncomplemented in the product term.
- If a circle covers areas of the map where the variable is 0 as well as areas where it is 1, then the variable does not appear in the product term.

[50]

The rules are used in interpretation of the Karnaugh map and the 1-cells may be combined to Eq. 12-5 and Eq. 12-6

$$\phi(X) = x_1 \cdot x_2 + x_1 \cdot x_3 + x_2 \cdot x_3 \quad \text{Eq. 12-5}$$

$$\phi(X) = x_1x_2 + x_1x_3 + x_2x_3 - 2x_1x_2x_3 \quad \text{Eq. 12-6}$$

12.14 Taylor Series Expansion

The Taylor Series expansion of $e^{-\tau\lambda_{DU}}$ are presented in Eq. 12-7

$$e^{-\tau\lambda_{DU}} = \sum_{n=0}^{\infty} \frac{(-\tau\lambda_{DU})^n}{n!} = 1 - \frac{\tau\lambda_{DU}}{1!} + \frac{(\tau\lambda_{DU})^2}{2!} - \frac{(\tau\lambda_{DU})^3}{3!} + \frac{(\tau\lambda_{DU})^4}{4!} - \dots \quad \text{Eq. 12-7}$$

When $0 < \tau\lambda_{DU} < 0.1$ then each extra term in Eq. 12-7 becomes smaller and less important and the approximation in Eq. 12-8 can be used.

$$\begin{aligned} e^{-\tau\lambda_{DU}} &\approx 1 - \tau\lambda_{DU} \\ \Updownarrow \\ \tau\lambda_{DU} &\approx 1 - e^{-\tau\lambda_{DU}} \end{aligned} \quad \text{Eq. 12-8}$$

Table 12-3 illustrates the approximation values for small values of $\tau\lambda_{DU}$

Table 12-3: Approximation values and difference

$\tau\lambda_{DU}$	$1 - e^{-\tau\lambda_{DU}}$	Difference [%]
0.01	0.00995	0.5
0.05	0.04877	2.5
0.10	0.09516	4.8
0.15	0.13929	7.1
0.20	0.18127	9.4

12.15 MATLAB – PFD Table Determination

```
% % P10 master project - spring 2017 - PFD Table Determination
%
% Aalborg University Esbjerg
% 10th Semester Energy Study Program
% Group OES10-2-F17
% Jacob Glæsner
%
% =====
%% 01. Instructions and information about script
%
% The script is programmed to run locally on the computer of the
% programmer. Change the values for dangerous failure rate, test interval
% MRT, MTTR and if necessary the noon value. Table will be written to
% Excel with increasing diagnostic coverage from 0-100% in the columns
% and increasing beta-factor from 0-20% in the rows. The tables comply with
% IEC 61508-6 table B2-B5.
%
% =====

clear all
close all
clc

% =====
%% 02. Inputs needed for the script
% =====

lamp_D = 5e-6;           % dangerous failure rate
tau     = 8760;          % test interval [h]
noon     = 1;
MRT      = 8;            % Mean Repair Time [h]
MTTR     = MRT;          % Mean Time To Restore [h]

% =====
%% 03. Constants and variables needed for the script
% =====

% Beta factor for Common Cause Failures
beta     = 0.0:0.01:0.2; % undetected - range from 1-20%
beta_D   = 0.5*beta;      % detected - assumed 0.5 of undetected

% Diagnostic Coverage, DC
DC        = 0.00:0.01:1.00; % Range from 0-100%

% =====
%% 04. Calculations needed for the script
% =====

% Failure rates
lamp_DD = DC.*lamp_D;      % detected failures
lamp_DU = lamp_D - lamp_DD; % undetected failures

t_CE     = lamp_DU./lamp_D * (tau/2 + MRT) + DC.*MTTR;
t_GE     = lamp_DU./lamp_D * (tau/3 + MRT) + DC.*MTTR;
```

```
% =====
%% 05. Architectures
% =====

% noon
PFD_noon      = lamp_D*t_CE*noon;

% 1oo2
PFD_1oo2 = 2.*(((1-beta_D).*lamp_DD' + (1-beta).*lamp_DU').^2)'.*t_CE.*t_GE...
            + (beta_D.*lamp_DD'.*MTTR + beta.*lamp_DU'.*(tau/2 + MRT))';

% 2oo3
PFD_2oo3 = 6.*(((1-beta_D).*lamp_DD' + (1-beta).*lamp_DU').^2)'.*t_CE.*t_GE...
            + (beta_D.*lamp_DD'.*MTTR + beta.*lamp_DU'.*(tau/2 + MRT))';

% =====
%% 06. Write Tables
% =====

% Predefine table size
row(2:22,1)      = 0:1:20;                % beta factor range in rows
column(1,2:102) = 0:1:100;                % DC range in columns
header_noon      = zeros(2,102);
header_noon      = column;
header_moon      = zeros(22,102);
header_moon(:,1) = row;
header_moon(1,:) = column;

header_noon(2,2:end)      = PFD_noon;      % Fill PFD_noon table
xlswrite('PFD_noon.xlsx',header_noon,1) % Write to Excel

header_moon(2:end,2:end) = PFD_1oo2;      % Fill PFD_1oo2 table
xlswrite('PFD_1oo2.xlsx',header_moon,1) % Write to Excel

header_moon(2:end,2:end) = PFD_2oo3;      % Fill PFD_2oo3 table
xlswrite('PFD_2oo3.xlsx',header_moon,1) % Write to Excel

% ====  END =====  END =====  END =====  END =====  END =====  END =====
```

12.16 MATLAB – Solving Time-Dependent Diff. Equations

```
% % P10 master project - spring 2017 -
% Solving time-dependent differential equations, example
%
% Aalborg University Esbjerg
% 10th Semester Energy Study Program
% Group OES10-2-F17
% Jacob Glæsner
%
% =====
%% 01. Instructions and information about script
%
% The script is programmed to run locally on the computer of the
% programmer. Change the values for dangerous failure rate, test interval
% MRT, MTTR and if necessary section 2. Set up transition rate matrix and
% probability vector in section 3. Set up initial conditions in section 4
% The example only works for a 3x3 transition matrix. If more
% differential equations are needed follow the logic in building more
% equations.
%
% =====

clear all
close all
clc

% =====
%% 02. Variables needed for the script
% =====

% set up symbolic variables
syms ldu ldd udu udd p0(t) p1(t) p2(t)

% If values are needed - remove % from inputs below
% ldd      = 0;           % lampda DD (dangerous detected failure)
% ldu      = 6.14e-7;     % lampda DU (dangerous undetected failure)
% tau      = 8760;        % proof test interval
% MRT      = 8;           % Mean Repair Time
% MTTR     = 8;           % Mean Time To Restore
% udd      = 1/MTTR;      % my DD (repair rate of detected failure)
% udu      = 0;           % my DU (repair rate of detected failure)

% =====
%% 03. Set up transition matrix and probability vector
% =====
Q      = [-(ldd+ldu) ldd ldu; udd -udd 0; udu 0 -udu]; % Transition Rate
P      = [p0(t) p1(t) p2(t)]; % Probability Matrix

% Calculate differential matrix equation
P_dot = P*Q; % Differential Matrix Equation

% =====
%% 04. Set up differential equations and initial conditions
% =====
ode1   = diff(p0,t) == P_dot(1,1); % Differential Equation 1
ode2   = diff(p1,t) == P_dot(1,2); % Differential Equation 2
ode3   = diff(p2,t) == P_dot(1,3); % Differential Equation 3
odes   = [ode1;ode2;ode3];
```

```
cond1 = p0(0) == 1;           % Initial Condition 1
cond2 = p1(0) == 0;           % Initial Condition 2
cond3 = p2(0) == 0;           % Initial Condition 3
conds= [cond1; cond2;cond3];

% =====
%% 04. Solve unknowns ans calculate PFD_Avg
% =====
[p0S(t), p1S(t), p2S(t)] = dsolve(odes,conds);

PFD_ins = abs(1 - vpa(abs(p0S(8760)),6));
PFD_Avg = vpa(1-int(abs(p0S(t)),0,8760)/8760,6);
PFD_Avg= vpa(PFD_Avg,6)

% ==== END ===== END ===== END ===== END ===== END =====
```

12.17 MATLAB – Solving Steady State Diff. Eqns. 2003 voting

```
% % P10 master project - spring 2017 -
% Solving steady state equations, example voting 2003
%
% Aalborg University Esbjerg
% 10th Semester Energy Study Program
% Group OES10-2-F17
% Jacob Glæsner
%
% =====
%% 01. Instructions and information about script
%
% The script is programmed to run locally on the computer of the
% programmer. Set up symbolic variables and define transition matrix Q
% and probability vector P in section 2-3. The example only works for a
% 2003 voting with corresponding transition matrix. If more equations are
% needed follow the logic in building more equations in the variable
% 'eqns', section 4.
% For numeric evaluation change the values for dangerous failure rate,
% test interval, MRT, MTTR in section 5.
% Results are calculated in section 6.
%
% =====

clear
close all
clc

% =====
%% 02. Variables needed for the script
% =====

% set up symbolic variables
syms p0 p1 p2 p3 ldu u1 u2 u3 bu

P = [p0 p1 p2 p3];

% =====
%% 03. Set up transition matrix
% =====

Q = [-(3*ldu+bu*ldu) 3*ldu 0 bu*ldu;
     u1 -(u1+2*ldu+bu*ldu) 2*ldu bu*ldu;
     u2 0 -(u2+ldu) ldu;
     u3 0 0 -u3];

P_dot = P*Q;

% =====
%% 04. Equations and solving of these
% =====

eqns = [sum(P)==1,P_dot(1)==0,P_dot(2)==0,P_dot(3)==0,P_dot(4)==0];
sol = solve(eqns,P);
```

```
% =====  
%% 05. Inputs for evaluation  
% =====  
  
ldu = 3.90e-8;  
  
MRT = 8;  
MTTR = 8;  
tau = 8760;  
  
udu = 1/(tau/2+MRT);  
u1 = udu;  
u2 = udu;  
u3 = udu;  
bu = 0.02;  
  
% =====  
%% 06. Results  
% =====  
  
% Display symbolic equations  
p0 = sol.p0;  
p1 = sol.p1;  
p2 = sol.p2;  
p3 = sol.p3;  
  
% Display numeric evaluation  
p0S = eval(sol.p0);  
p1S = eval(sol.p1);  
p2S = eval(sol.p2);  
p3S = eval(sol.p3);  
  
% Calculate PFD_Avg  
PFD_Avg = vpa(p2S+p3S,5);  
  
% ==== END ===== END ===== END ===== END ===== END =====
```


12.18 MATLAB – Solving Steady State Diff. Eqns. 1001 voting

```
% % P10 master project - spring 2017 -
% Solving steady state differential equations, example 1001
%
% Aalborg University Esbjerg
% 10th Semester Energy Study Program
% Group OES10-2-F17
% Jacob Glæsner
%
% =====
%% 01. Instructions and information about script
%
% The script is programmed to run locally on the computer of the
% programmer. Set up symbolic variables and define transition matrix Q
% and probability vector P in section 2. The example only works for a 3x3
% transition matrix. If more equations are needed follow the logic in
% building more equations in the variable 'eqns', section 3.
% For numeric evaluation change the values for dangerous failure rate,
% test interval, MRT, MTTR. Results are calculated in section 5.
%
% =====

clear
close all
clc

% =====
%% 02. Variables needed for the script
% =====

% set up symbolic variables
syms p0 p1 p2 ldd ldu udu udd
Q = [-(ldd+ldu) ldd ldu; udd -udd 0; udu 0 -udu];

P = [p0 p1 p2];

P_dot = P*Q;

% =====
%% 03. Equations and solving of these
% =====

eqns = [sum(P)==1, P_dot(1)==0, P_dot(2)==0, P_dot(3)==0];
sol = solve(eqns, P);

% =====
%% 04. Inputs for evaluation
% =====

ldd = 0;
ldu = 6.14e-7;
MRT = 8;
MTTR = 8;
tau = 8760;
udd = 1/MRT;
udu = 1/(tau/2+MTTR);

% =====
```

```
%% 05. Results
% =====

% Display symbolic equations
p0 = sol.p0;
p1 = sol.p1;
p2 = sol.p2;

% Display numeric evaluation
p0S = eval(p0);
p1S = eval(p1);
p2S = eval(p2);

% Calculate PFD_Avg
PFD_Avg = vpa(p1S+p2S,5);

% ==== END ===== END ===== END ===== END ===== END ===== END =====
```

12.19 MATLAB – Solving Steady State Diff. Eqns. 1002 voting

```
% % P10 master project - spring 2017 -
% Solving steady state differential equations, example voting 1002
%
% Aalborg University Esbjerg
% 10th Semester Energy Study Program
% Group OES10-2-F17
% Jacob Glæsner
%
% =====
%% 01. Instructions and information about script
%
% The script is programmed to run locally on the computer of the
% programmer. Set up symbolic variables and define transition matrix Q
% and probability vector P in section 2-3. The example only works for a
% 1002 voting with corresponding transition matrix. If more equations are
% needed follow the logic in building more equations in the variable
% 'eqns', section 4.
% For numeric evaluation change the values for dangerous failure rate,
% test interval, MRT, MTTR in section 5.
% Results are calculated in section 6.
%
% =====

clear
close all
clc

% =====
%% 02. Variables needed for the script
% =====

% set up symbolic variables
syms bu bd ldu1 ldu2 ldd1 ldd2 udd udu
syms p0 p1 p2 p3 p4 p5 p6 p7 p8 p9

P = [p0 p1 p2 p3 p4 p5 p6 p7 p8 p9];

% =====
%% 03. Set up transition matrix
% =====

Q = [-( (1-bu)*ldu1 + (1-bd)*ldd1 + (1-bu)*ldu2 + (1-bd)*ldd2 + ...
bd*sqrt(ldd1*ldd2) + bu*sqrt(ldu1*ldu2)) (1-bu)*ldu1 (1-bd)*ldd1 ...
(1-bu)*ldu2 (1-bd)*ldd2 0 0 0 bd*sqrt(ldd1*ldd2) bu*sqrt(ldu1*ldu2); ...
udu (-udu-ldu2-ldd2) 0 0 0 ldu2 0 ldd2 0 0; ...
udd 0 (-udd-ldu2-ldd2) 0 0 0 ldu2 0 ldd2 0; ...
udu 0 0 -(udu+ldu1+ldd1) 0 ldu1 ldd1 0 0 0; ...
udd 0 0 0 -(udd+ldu1+ldd1) 0 0 ldu1 ldd1 0; ...
udu 0 0 0 0 -udu 0 0 0 0; ...
0 0 udu udd 0 0 -udu-udd 0 0 0; ...
0 udd 0 0 udu 0 0 -udd-udu 0 0; ...
0 0 udd 0 udd 0 0 0 -2*udd 0; ...
udu 0 0 0 0 0 0 0 0 -udu];

P_dot = P*Q;

% =====
```

```

%% 04. Equations and solving of these
% =====

eqns = [sum(P)==1,P_dot(1)==0,P_dot(2)==0,P_dot(3)==0,P_dot(4)==0,...
        P_dot(5)==0,P_dot(6)==0,P_dot(7)==0,P_dot(8)==0,P_dot(9)==0,...
        P_dot(10)==0];

sol = solve(eqns,P);

% =====
%% 05. Inputs for evaluation
% =====

ldd1    = 2.433e-7;
ldd2    = 2.433e-7;
ldu1    = 1.252e-9;
ldu2    = 1.252e-9;
MRT     = 8;
MTTR    = 8;
tau     = 8760;
udd     = 1/MRT;
udu     = 1/(tau/2+MTTR);
bd      = 0.005;
bu      = 0.01;

% =====
%% 06. Results
% =====

% Display symbolic equations
p0 = sol.p0;
p1 = sol.p1;
p2 = sol.p2;
p3 = sol.p3;
p4 = sol.p4;
p5 = sol.p5;
p6 = sol.p6;
p7 = sol.p7;
p8 = sol.p8;
p9 = sol.p9;

% Display numeric evaluation
p0S = eval(sol.p0);
p1S = eval(sol.p1);
p2S = eval(sol.p2);
p3S = eval(sol.p3);
p4S = eval(sol.p4);
p5S = eval(sol.p5);
p6S = eval(sol.p6);
p7S = eval(sol.p7);
p8S = eval(sol.p8);
p9S = eval(sol.p9);

% Calculate PFD_Avg
PFD_Avg = p5S+p6S+p7S+p8S+p9S;

% ==== END ===== END ===== END ===== END ===== END =====

```

12.20 State Definition of a 2oo3 voting system

Table 12-4: State Definition of a 2oo3 voting system

State	Component			Up/Down
	1	2	3	
0	ok	ok	ok	Up
1	DU	ok	ok	Up
2	DD	ok	ok	Up
3	ok	DU	ok	Up
4	ok	DD	ok	Up
5	ok	ok	DU	Up
6	ok	ok	DD	Up
7	DU	DU	ok	Down
8	DU	DD	ok	Down
9	DD	DU	ok	Down
10	DD	DD	ok	Down
11	ok	DU	DU	Down
12	ok	DU	DD	Down
13	ok	DD	DU	Down
14	ok	DD	DD	Down
15	DU	DU	DD	Down
16	DU	DU	DU	Down
17	DU	DD	DU	Down
18	DU	DD	DD	Down
19	DD	DU	DU	Down
20	DD	DU	DD	Down
21	DD	DD	DU	Down
22	DD	DD	DD	Down
23	DU	ok	DU	Down
24	DU	ok	DD	Down
25	DD	ok	DU	Down
26	DD	ok	DD	Down