University of Stavanger

Faculty of Science and Technology

MASTER'S THESIS

Study program/ Specialization: Master in Risk Management – Offshore Safety	Spring semester, 2012 Open / ~~Restricted access~~
Writer: Karl Henry Eikeskog	…… (Writer's signature)
Faculty supervisor: Eirik Bjorheim Abrahamsen (University of Stavanger) External supervisor(s): Anniken Alsos and Stig Berg (Odfjell Drilling and Technology)	
Title of thesis: Reliability as a decision tool against SIL requirements	
Credits (ECTS): 30 SP	
Key words: Safety Instrumented Systems Safety Integrity Level Low Demand System Blowout Preventer Control System Probability of Failure on Demand IEC 61508 PDS OLF 070	Pages: 74 + enclosure: 8 pages Stavanger, 07.06.2012 Date/year

Preface

This master thesis represents the end of my master degree in Risk Management – Offshore Safety at the University of Stavanger and it was executed over a period of 18 weeks, during spring 2012. The thesis was carried out at the Department of Industrial Economics, Risk Management and Planning in collaboration with Odfjell Drilling and Technology.

First of all I would like to thank Anniken Alsos in OD&T for integrating me in their QHSE and Technical Safety department as early as possible. A special thanks to her, because she also gave me the opportunity to take part in SINTEF PDS forum in Trondheim 17th– 18th April 2012. A special thanks goes also to Stig Berg in OD&T for always taking time when I needed help, for showing interest in my thesis, and for all the advises I got along the way. In OD&T I would also like to thank Atle Lerum and Jack Bremer for helping me understand the technical part of a BOP control system.

I would like to use this opportunity to thank Stein Hauge in SINTEF PDS forum, because he has showed a lot of interest in my work.

Finally, I will give a special thanks to my internal supervisor at the University of Stavanger, Eirik Bjorheim Abrahamsen. This thesis would simply not be the same, if it was not for all the advices and guidance I received.

Stavanger

June 2012

Karl Henry Eikeskog

Abstract

Safety Instrumented Systems (SISs) is used in the oil and gas industry to detect the onset of hazardous events and/or to mitigate their consequences to humans, material assets, and the environment. International standards have been developed to ensure that a SIS is designed, implemented and operated according to the specified needs. Safety and reliability assessments play an important role in SIS design, construction and operation.

In this thesis there is carried out a reliability study of the BOP control system on Deepsea Atlantic (DSA) with use of the international IEC 61508 standard and the Norwegian PDS guidelines. All the results show that the BOP control system is within the requirements given by OLF 070.

The results from a reliability study will vary because of different interpretations in the guidelines. Factors that contribute to a change in the unavailability is identified in both methods and highlighted with examples throughout this thesis. The major difference between the two methods is that PDS guidelines include more details in the calculation of Common Cause Failure (CCF). In a calculation example given in this thesis, the two guidelines conclude against different Safety Integrity Levels (SILs).

If decision makers are not aware of assumptions and conditions in the methods, they may misinterpret the results and select a SIS design that is either too complex or too simple to provide necessary risk reduction.

In the oil and gas industry it is common to define and describe risk using probabilities and probability distributions. The Probability of Failure on Demand (PFD) gives a useful insight for decision makers. After presenting several examples of how different interpretations in the methods results in different SIL verification, I argue that there is a need for broader reflection of robustness and uncertainties, which can support decision makers when verifying against SIL requirements. Therefore, I present some new ideas of how one can merge existing approaches to support decision making. Today, it seems to exist no overall agreement or guidelines of how one can verify the PFD against the SIL requirements.

Figure of contents

Table of contents

Abbreviations

BOP	Blowout Preventer
BSR	Blind Shear Ram
CCF	Common Cause Failure
DWH	Deep Water Horizon
DSA	Deepsea Atlantic
EUC	Equipment Under Control
E/ E/ PE	Electrical/ Electronic/ Programmable Electronic
GOM	Gulf Of Mexico
Lambda (λ_{DU})	Dangerous Undetected Failure Rate
MFDT	Mean Fractional Dead Time
MooN	M-out-of-N
NCS:	Norwegian Continental Shelf
OD&T	Odfjell Drilling and Technology
OREDA	Offshore Reliability Data
PFD	The average Probability of Failure on Demand
PSA	Petroleum Safety Authority
PTIF	Probability of Test Independent Failure
RBD	Reliability Block Diagram
SIL	Safety Integrity Level
SIS	Safety Instrumented System

Terminology and concepts

Average Probability of Dangerous Failure On Demand	Mean unavailability of an E/E/PE safety- related system to perform the specified safety function when a demand occurs from Equipment Under Control (EUC) or EUC control system (IEC 61508-4 2010).
Blowout Preventer control system	A Blowout Preventer control system comprises a number of valves that should be closed during an emergency to prevent uncontrolled well-fluid to flow onto the platform during drilling operations (Bai 2010).
Common Cause Failure	Failure, which can result in one or more events, causing coincident failures of two or more separate channels in a multiple channel system, leading to system failure (IEC 61508-4 2010).
Dangerous undetected	Dangerous failures not detected by automatic self- test or incidentally by personnel (I.e. revealed only by functional test or upon a demand) (Hauge et al. 2010).
E/E/PE system	System for control, protection, or monitoring based on one or more electrical/electronic/programmable electronic (E/E/PE) devices, including all elements of the system such as power supplies, sensors, and other input devices, data highways and other communication paths, and actuators and other output devices. (IEC 61508-4 2010).

Generic data	Data that represent a property, for example the failure rate, for a group of similar components. Generic data may be based on experience data or predicted data (Lundteigen 2009).
Low demand system	A low demand safety system operates only upon a demand, can often be seen as an add-on to the basic control system, and shall only be called upon when something goes wrong or starts to go wrong. Typical examples are a Process Shutdown system (PSD), Blowout Preventer (BOP) control system, or an Emergency Shutdown system (ESD) (Hauge et al. 2010).
Model	The model represents our interpretation of some real phenomena (Lundteigen 2009).
MooN	A MooN voting (M<N) means that at least M of the N redundant modules have to give a shutdown signal for a shutdown to be activated (Hauge et al. 2010).
Probability of Test Independence Failure	The probability that the component/system will fail to carry out its intended function due to a (latent) failure not detectable by functional testing (Hauge et al. 2010).
Random Hardware failure	Failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware (IEC 61508-4 2010).
Redundancy	In an item, the existence of more than one means for performing a required function (IEC 61508-4 2010).

Reliability	The ability of a system to function as planned, and is expressed by probabilities and expected values (Aven 2006).
Risk	The two- dimensional combination of (i) events A and the consequences of these events C, and (ii) the associated uncertainties U (about what will be outcome), i.e. (C,U). For simplicity, we write only C, instead of A and C (Aven 2008).
Risk acceptance criteria	If the calculated risk is lower than a pre- determined value, then the risk is acceptable (tolerable) (Aven 2008).
Safety barrier	A safety barrier is often interpreted as a function which must be fulfilled in order to reduce the risk, and such a function can be implemented in terms of different systems and elements, both technical and operational (OLF 2004).
Safety Instrumented Systems	A Safety Instrumented System (SIS) comprises input elements (e.g. pressure transmitters and gas detectors), logic solvers (e.g. relay-based logic and programmable logic controllers) and final elements (e.g. valves, circuit's breakers) for the purpose of bringing the plant or equipment to a safe state if a hazardous event occurs (Lundteigen 2009).

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 (IEC 61508-4 2010).
Safety Integrity Level	Discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest level of safety integrity and safety level 1 has the lowest (IEC 61508-4 2010).
Systematic failure	Failure, related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factor (IEC 61508-4 2010).
Vendor data	Is in this thesis vendor data is defined as supplier and contactor specific data.
Voting	The number of redundant means that need to operate for the function to be accomplished (IEC 61508-4 2010).

1.0 Introduction

1.1 Background

Safety instrumented systems (SISs) are used in the oil and gas industry to detect the onset of hazardous events and/or to mitigate their consequences to humans, material assets, and the environment (Lundteigen 2009). The main purpose of a SIS is to bring the plant or equipment to a safe state if a hazardous event occurs. If the SIS fails to perform the intended functions, the event may develop into an accident. Safety and reliability assessments play an important role in SIS design, construction and operation.

In this thesis there will be performed a reliability study of the low demand Blowout Preventer (BOP) control system on Deepsea Atlantic (DSA), where the system will be analyzed against requirements given by OLF 070. International standards have been developed to ensure that SIS is designed, implemented and operated according to the specified needs. The international standard, IEC 61508 and the Norwegian PDS method will be used as guidelines in the reliability calculations.

Several examples will be presented to highlight the different interpretations in the guidelines, and to show how this can influence the PFD results and verification against Safety Integrity Level (SIL).

In the oil and gas industry it is common to define and describe risk using probabilities and probability distributions (Aven 2010). However, these perspectives have been challenged in recent literature (Rosa 1998) (Aven 2009a, 2009b) (Mosleh & Bier 1996). The PFD calculations give a useful insight for decision makers, but making conclusion against SIL only based on probability calculations, could produce poor and in some scenarios misleading results (Aven 2010).

1.2 Objective

The purpose of this assignment is to take a closer look at how the different reliability interpretations are covered in IEC 61508 and PDS, and how this can influence the calculations, which again can lead to different conclusions. A simplified BOP control system model for Deepsea Atlantic will be built and used in a reliability study to verify and conclude against specific SIL requirements.

For a reliability analyst and decision makers it is seen as important to have some background knowledge of factors that will and can influence the reliability calculation. Therefore the thesis also aims to identify the most critical factor that can influence the reliability result.

The thesis also aims to develop and discuss some new ideas that can be used when the reliability result is verified against the requirements.

The four objectives in this thesis are summarized under:

1. Highlight with examples that with use of IEC 61508 and PDS method the result can differ, and this may lead to different conclusion based on SIL verification.
2. Determine if the BOP control system on DSA is within SIL requirements given by OLF 070.
3. Identify factors that influence the PFD calculation in the reliability guidelines.
4. Develop new ideas to an approach that aim to support decision making when SIL is verified.

All the objectives will be concluded against in chapter 9.

1.3 Limitations

In this section the limitations in the assignment is presented.

- The IEC 61508 guideline presents Safe Failure Fraction (SFF), Test Coverage (TC) and Hardware Fault Tolerance (HFT), when the PFD is verified against SIL requirements. In this thesis these aspect are left out.
- An application specific calculation with use of IEC 61508 guidelines has not been performed. The approach is to complex and in some extent unclear.
- Both IEC 61508 and PDS guidelines present downtime due to known repair or test. In the IEC standard this is given by the PFDk, while in PDS as Downtime unavailability. A BOP control system can be seen as a non- reparable system, which means that faults only can be identified by testing or demands. Therefore the Mean Time To Repair (MTTR) is seen as low and can be neglected.
- The PFD results on the BOP control system will only be presented in a table in chapter 5.2, which means that all the calculation will not be showed or explained in a detailed way. For further information on those topics, the reader is referred to OLF (2004), Onhus (2010), Stein Hauge (2010), Lundteigen (2010) and IEC (2010, part 6 and 7).
- The original BOP control system model (Chapter 4) includes an independent acoustic control system and 3 ram preventers (OD&T 2010). In the RBD only 1 ram preventer is considered and the acoustic system is not considered. If the acoustic control system and all ram preventers were considered in the reliability study, the system PFD would be lower. This is because the acoustic system and ram preventers would give more redundancy to the system.

1.4 Structure of the report

This section includes a short presentation of the chapters in this thesis.

CHAPTER 2
Important theoretical background information is presented. For a more detailed description see the corresponding references.

CHAPTER 3
An introduction to the IEC 61508 and PDS guidelines is given, with focus on the different interpretations in the guidelines.

The chapter also includes a simplified example of how common cause failures are calculated by use of the different methods.

CHAPTER 4
A reliability block diagram (RBD) of the BOP control system on Deepsea Atlantic is made and presented.

CHAPTHER 5
The reliability of the BOP control system is calculated with use of both the IEC 61508 and PDS guidelines.

The results also include an application specific approach by PDS.

CHAPTER 6
This chapter aims to highlight assumptions and limitations in reliability calculations.

It demonstrates with several examples that with use of the different reliability guidelines (PDS and IEC 61508) the result and conclusion against SIL can differ.

The chapter also includes an overview of which factors that can influence the reliability calculations.

CHAPTER 7
New ideas of how one can merge existing approaches to help decision makers when SIL is verified against the requirements are presented. The new ideas are then illustrated by use of an example.

Strengths and weaknesses with the new ideas and existing approaches is also discussed.

CHAPTER 8

Reflection around topics that need to be studied and addressed more in reliability research is highlighted.

This chapter also includes an overview of the most important findings in this thesis.

CHAPTER 9

This chapter includes conclusion against all the objectives which was stated in chapter 1.2.

Reflections, examples, results and conclusions which are seen as important to the reader will be marked in outside borders (boxes) throughout this thesis.

2.0 Theory

This chapter includes an introduction to reliability and risk analysis with a main focus on risk perspective, SISs and SILs. A BOP control system will also be described from a SIS perspective and the associated SIL requirements will be presented.

2.1 Reliability and Risk Analysis

The overall requirements for barrier and safety functions are in Norway provided by the national authorities. The offshore industry shall adhere to the Petroleum Safety Authority (PSA) regulations. The main requirements for the Safety Instrumented Systems (SIS) are found in the PSA activity regulation, the management regulation, the facility regulation and in OLF 070.

Analysis of reliability and risk is an important and integrated part of planning, construction and operation of all technical systems. The primary objective of reliability and risk analysis is to provide a basis for decisions regarding choice and actions (Aven 2006).

Safety and reliability assessments are used to provide SIS designers, SIS manufacturers, and end users with decision support regarding SIS design, construction, and follow-up. The assessments build on a number of assumptions about the system and under what conditions it is to be operated. If decision makers are not aware of those assumptions and conditions, they may misinterpret the results and select a SIS design that is either too complex or too simple to provide necessary risk reduction (Lundteigen 2009).

Aven (2009) argue that the traditional quantitative approach in risk and reliability analysis provide a rather narrow risk picture, through calculated probabilities and expected values. Aven (2009) conclude that the approach should be used with care, in particular for problems with large uncertainties. This traditional reliability (quantification) approach is the leading approach when it comes to reliability analysis (IEC 61508 and PDS guidelines) on the NCS.
Therefore Aven (2009) argue that it is important to look beyond these assigned probabilities when making important decisions.

Both uncertainty and sensitivity are two topics that are commonly referred to in the concept of reliability engineering. Sensitivity analysis is often mentioned in the same context as uncertainty analysis, but the two types of analysis have slightly different meaning (Lundteigen 2009). While uncertainty analysis is a tool for evaluating the degree of knowledge or confidence in the results, the sensitivity analysis is used to improve the way to interpret the results (Lundteigen 2009). When performing sensitivity analysis, it is investigated how variations in input data (model input parameters, assumptions) cause changes to the model output parameters (Lundteigen 2009).

2.1.1 Risk perspective

Many definitions and description of risk exists in an engineering context. Therefore, I have chosen to describe which risk perspective that is used in this thesis. Most of the existing definitions and descriptions of risk include the following three components (Aven 2011):

- A: What can go wrong (the initiated events)
- C: The consequences of these events if they should occur
- P: The probabilities of A and C

There are basically two ways of interpreting the probability P:

- (a) as a relative frequency, i.e. the relative fraction of times the event occurs if the situation analyzed were hypothetically "repeated" an infinite number of times.
- (b) as a subjective measure of uncertainty, conditional on the background knowledge.

In this thesis I adopted the ACP perspective from Aven (2008, 2011) which means that there are not uncertainties associated with the results from probability calculation, but in the background knowledge, which can produce surprising outcomes ($P\{failure\ on\ demand|K\}$).

2.2 Safety Instrumented System

Safety instrumented systems are used in the oil and gas industry to detect the onset of hazardous events and/or to mitigate their consequences to humans, material assets, and the environment (Lundteigen 2009).

Our safety is increasingly taken care of by SISs, where electrical, electronic and/or programmable (E/E/PE) devices interact with mechanical, pneumatic and hydraulic systems.

A SIS comprises input elements (e.g. pressure transmitters and gas detectors), logic solvers (e.g. relay- based logic and programmable logic controllers) and final elements (e.g. valves, circuit's breakers) for the purpose of bringing the plant or equipment to a safe state if hazardous event occurs (Lundteigen 2009) (Figure 1).

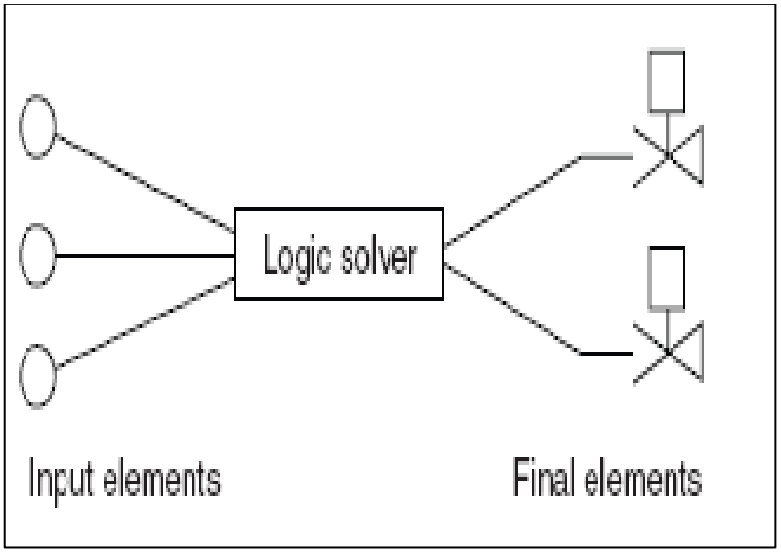


Figure 1. Example of a SIS

If the SIS fails to perform the intended functions, an incident or event may develop into an accident.

It can in some situations be important to distinguish between a SIS and a Safety Instrumented Function (SIF). The system is the technology (and human) elements, while the function describes the acts performed by the system. The relationship between a SIF and a SIS is illustrated in Figure 2 (Lundteigen 2011).

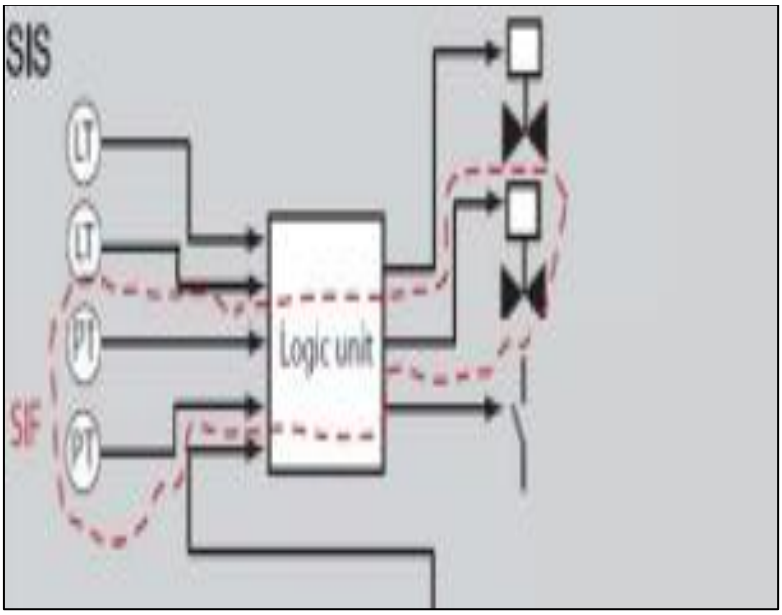


Figure 2. Illustration of the difference between a SIS and a SIF

2.2.1 BOP control system as a SIS

With the increased recognition of the IEC standards, many oil companies assign SIL requirements to other safety critical systems, such as well intervention and drilling systems. For those systems, it is often important to also focus on the rate of spurious[1] activations as they may lead to hazardous events. Whereas traditional SISs often have a well defined safe state, this is not always the case for other safety critical systems (Lundteigen 2009).

Theoretically, a BOP control system is not defined as a SIS because the system does not include all the aspect in the definition. But in "real" life the BOP control system is a safety critical system with regards to well control and therefore treated like a SIS. It is more correct to define a BOP control system as a SIF within a SIS.

The BOP control system is an example of a system where manual activation is normally preferred to automatic. When there is sufficient time for human judgment or in cases where an unintended or spurious activation may have very severe consequences, a manual activation may be preferred to automatic. The reason is that a spurious operation of the BOP during a drilling operation may create new hazardous events. To make sure that manual activation is possible in different types of critical events, there are pushbuttons installed in several locations in and near the drilling area.

[1] *Spurious Activations: A collective term used to characterize an improper, false, or non-genuine transaction from one state to another (Lundteigen 2009)*

2.3 Safety Integrity

In IEC 61508 the safety integrity are divided into four requirement levels, called SIL. Table 1 shows the SILs for safety functions operating on demand and in a continuous demand mode (IEC 61508-1 2010).

Safety Integrity Level	Demand Mode of Operations (average probability of failure to perform its design functions on demand-PFD)	Continuous / High Demand Mode of Operation (probability of a dangerous failure per hour)
4	≥ 10-5 to < 10-4	≥ 10-9 to < 10-8
3	≥ 10-4 to < 10-3	≥ 10-8 to < 10-7
2	≥ 10-3 to < 10-2	≥ 10-7 to < 10-6
1	≥ 10-2 to < 10-1	≥ 10-6 to < 10-5

Table 1.SIL intervals for systems operating on low demand and/or high demand

A SIS is defined as operation in high demand mode if demanded more than once per year, and as low demand mode if demanded less than once per year. If the safety function is a part of normal operations, it is defined as operating in the continuous mode (IEC 61508-1 2010).

A BOP control system can be defined as a low demand operation system, because the main function of the system is to close relevant valves on demand and the frequency is less than once per year.

2.3.1 SIL requirements for BOP a control system

SIL requirements for BOP/ BOP control system are presented in the application of IEC 61508 and IEC 61511 in the Norwegian Petroleum industry by OLF 070 (2004).

Table 2 shows the minimum SIL requirements for drilling related safety functions.

Safety functions	SIL	Functions boundaries for given SIL requirement / comments
Drilling BOP	2[2]	Annular/ pipe ram functions
Closing of relevant BOP valve(s) in order to prevent blowout and/or well leak	2[2]	Blind shear ram function

Table 2.SIL requirements for BOP control system and BOP stack

It is important to emphasis that the tabulated SIL requirements are minimum values, and therefore need to be verified with respect to overall risk level (OLF 2004).

[2] *The total safety functions include activation from drillers console or tool pusher console, and the remotely operated valves needed to close the BOP sufficiently to prevent blowout and/ or well leaks (OLF 2004)*

3.0 Reliability guidelines

Both the international standard IEC 61508 and the Norwegian PDS guidelines introduce the aspect Probability of Failure on Demand (PFD) for low demand systems. Verification of the quantitative part (PFD) of the SIL for a safety instrumented function is usually done by a calculation of PFD and then by a comparison with the criterion established (Abrahamsen & Røed 2011).

The PFD is a central aspect in both methods, and therefore the deduction and limitation of the approximate PFD formula is presented in Appendix A.

The average probability of failure on demand (PFD) is a reliability measure which is often used for systems that take actions when a dangerous condition is detected (Aven 2006).

For a more detailed description of the two reliability guidelines, than what is given in chapter 3, the reader is referred to the corresponding references.

3.1 IEC 61508 Method

The international standard IEC 61508 has been widely accepted as the basis for specification, design and operation of SISs (OLF 2004). The standard sets out a risk- based approach for deciding the SIL and the standard are split into seven parts.

The approach is complex and has been difficult to handle by the oil and gas industry. OLF has therefore made an application of the IEC standards for the Norwegian Petroleum Industry (OLF 2004). The overall purpose of OLF 070 is to issue a guideline on the application of IEC 61508 and IEC 61511 and thereby simplify the use of the standards.

The performance measures for loss of safety in the IEC 61508 are for low demand systems the average probability of failure on demand (PFD). IEC 61508 then require that SILs for the different safety instrumented functions are verified.

The approximate formula for a 1oo1 system for independent failure is shown below:

$$PFD\ IEC\ (Independent) = \frac{\lambda_{DU} * \tau}{2}$$

, were λ_{DU} are dangerous undetected failures (failures per hours), and τ the test interval in hours.

Both IEC and PDS give identical approaches when independent failure is calculated.

When common cause failure (CCF) are introduced the PFD for a M-out-of-N (MooN) system are as followed:

$$\text{PFD IEC (CCF)} = \beta * \lambda_{DU} * \frac{\tau}{2}$$

, were β is the certain fraction of failure for CCF that will cause all the redundant components to fail simultaneously or within a short time interval.

CCF shall only be considered when the analyzed system compromise of components which are in a parallel structure. An example of a parallel structure is given in chapter 3.4

If the calculated PFD is higher than the target value (SIL) (Table 2), it indicates that risk reducing measures should be implemented.

3.1.1 Interpretations in the IEC 61508 guidelines

The traditional way of accounting for CCF has been the β-factor model in IEC 61508. In this model it is assumed that a certain fraction of the failures (equal to β) are common cause, i.e. failures that will cause all the redundant components to fail simultaneously or within a short time interval.

If λ_{DU} is the components failure rate, the MooN voted system have a CCF contribution equal to β. Hence, this approach does not explicit distinguish between different voting logics, and the same result is obtained e.g. for 1oo2, 1oo5 and 3oo4 voted systems. The simplified example in chapter 3.4 demonstrates this interpretation.

Determining values for the β-factor is not a straightforward approach, one problem being the limited access to relevant data. Checklists in IEC 61508-6 (2010) has therefore been developed to support the estimation of this parameter. The checklist, or score card as it is referred to in the IEC 61508 part 6, contains several topics that must be analyzed to determine the β factor.

The IEC 61508 distinguishes between random hardware failure and systematic failure. However, systematic failures are not quantified and therefore not considered in the PFD calculations. By implementing design principles and risk reduction the systematic failure should be avoided and therefore not needed to be taken into account.

IEC 61508 also considers non-perfect testing in part 6, section B.3.2.5 (Effects of non-perfect proof test) of the final draft version of the 2.0 edition of the standard. Here, a Test Coverage (TC) factor is introduced, which is defined as the fraction of dangerous undetected failures that are revealed by a functional test.

The residual fraction (1-TC) of failures remains unrevealed until a more thorough proof test is performed or till the next real demand (Hauge et al. 2010). When the total PFD of a system is calculated the TC is not considered (see Figure 3).

3.2 PDS Method

The Norwegian PDS method is in line with the main principles advocated in the IEC 61508 standard, and together with the PDS data (Onshus et al. 2010) and method handbook (Hauge et al. 2010) it offers an effective and practical approach towards implementing the quantitative aspects of the standards.

The PDS method has been applied in numerous projects and in many different contexts. The main application, however, has been related to computer-based safety systems in the offshore and onshore oil and gas industry (Hauge et al. 2010).

PDS uses a slightly different interpretation and approach when quantify failures and for calculating CCF. Failures are categorized according to failure cause and the PDS standard differentiates between random hardware failures and systematic failures, were also the systematic failures is quantified. PDS introduce in addition a CMooN (see chapter 3.2.1) value when CCF is calculated, while IEC only consider the β-factor.

Note that splitting λ_{DU} (dangerous undetected failure rate) is not necessary when performing standard reliability calculations. However, when application specific calculations are performed (local safety systems) it is required to have an estimate of the fractional split between random hardware failures and systematic failures.

The potential contributors to loss of safety (safety unavailability) are in PDS been split into three main categories:

- *PFD*: Unavailability due to dangerous undetected (DU) failures.
- *PTIF*: Unavailability due to TIF failures (test independent failures)
- *DTU*: Unavailability due to known or planned downtime

In PDS the measure Critical Safety Unavailability (CSU) [3] is used to quantify the loss of safety, while the IEC method only consider the PFD when quantify the loss of safety.

Thus the relation is as followed:

CSU = PFD + PTIF

If the calculated CSU is higher than the target value (SIL) (Table 2), it indicates that risk reducing measures should be implemented.

[3] *CSU: The probability that the component/system will fail to automatically carry out a successful safety action on the occurrence of a hazardous/accidental event, and it is not known that the safety system is unavailable (Hauge et al. 2010)*

3.2.1 Interpretations in the PDS guidelines

CCF in PDS is based on an extension of the beta factor model in IEC, called the multiple beta factor model. The model considers different multiplicities of failures and has therefore introduced a configuration factor, CMooN that modifies the contribution of CCFs for different voting configurations. This means that β_{MooN} equals:

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

These CMooN values suggested by PDS are based on expert judgments supported by data related to the effect of adding redundancy to a system. These values are regularly updated, last back in 2010, and are presented in Appendix B.

PDS acknowledges that most tests are not 100% perfect and that the SIS, for this reason, may not be able to function shortly after a test. Therefore a PTIF factor is introduced, which takes into account the probability that certain failures are not identified during functional testing.

The PDS method also introduces a simplified application specific approach that should be used when local safety systems are analyzed.

3.3 Illustration of differences in safety unavailability

Figure 3 shows the different contributions to safety unavailability in the IEC 61508 guidelines (Hauge et al. 2010).

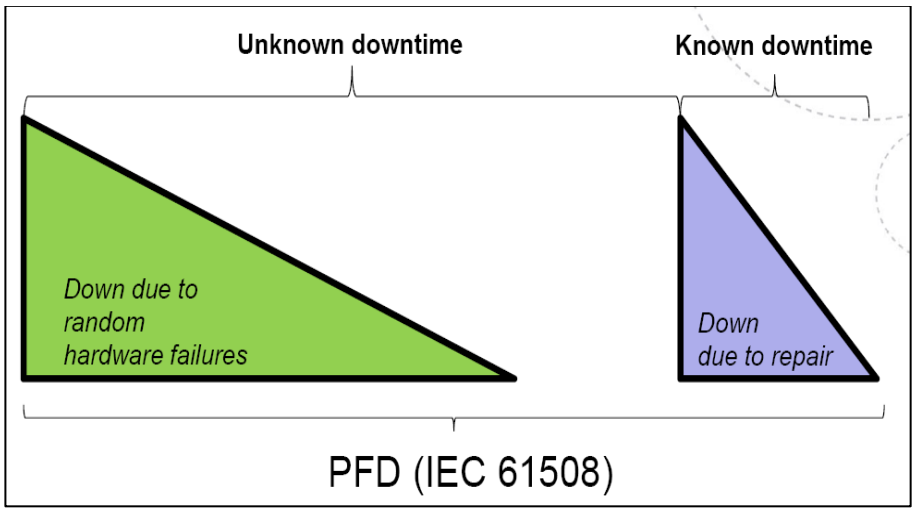


Figure 3.Contribution to safety unavailability in the IEC 61508 method

Figure 4 shows the different contributions to safety unavailability in the PDS guidelines (Hauge et al. 2010).

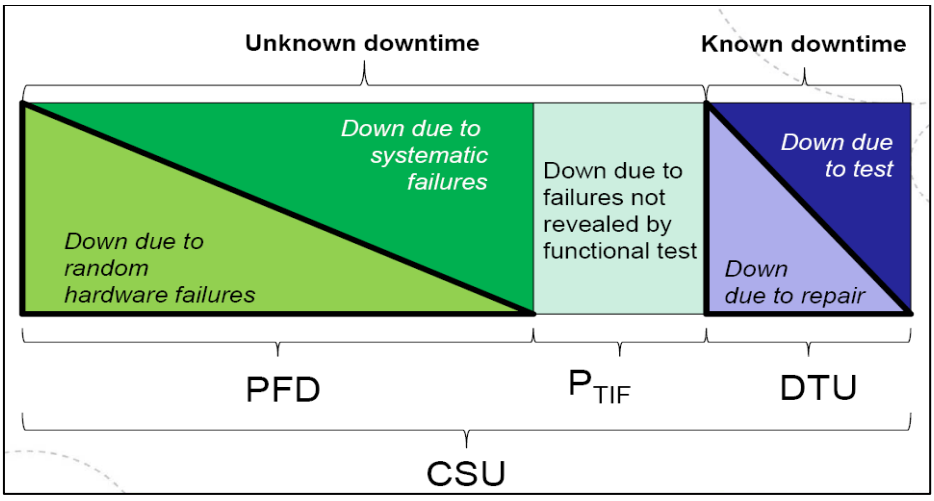


Figure 4.Contribution to safety unavailability in the PDS method

The reliability calculations, with use of PDS and IEC 61508 guidelines will differ because of different interpretations in the methods.

3.4 Simplified example of PFD calculations

The purpose of this simplified example is to demonstrate how CCF is treated in the PDS and IEC 61508 guidelines. Remember that independent failures are in the two guidelines calculated by identical approaches, and therefore the contributions from those failures are the same in all calculations.

Example: Demonstration of modeling Common Cause Failure

The subsystem below is the Central Control Console (CCC) from the DSA BOP control system. The whole model is presented in chapter 4.2.

The CCC is a 1oo4 system, with four possible Programmable Logic Controller (PLC) signal lines (Figure 5).

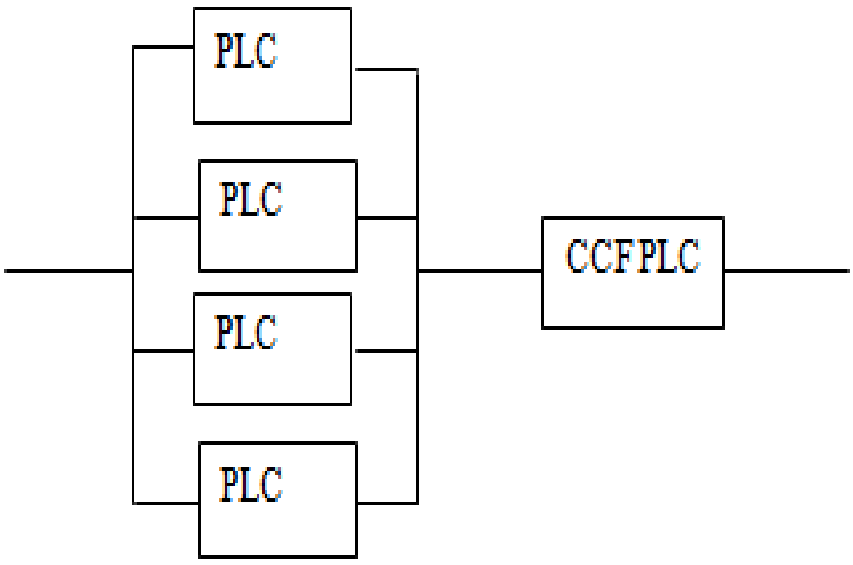


Figure 5.PLC system (RBD)

See appendix E for input data.

The results and the calculation approaches are shown below:

$$PDS\ PFD\ system\ 1oo4 \approx C_{1oo4} * \beta * \lambda_{DU} * \frac{\tau}{2} + \frac{[\lambda_{DU} * \tau]^4}{5} \approx 4{,}61\text{E} - 04$$

$$\rightarrow SIL\ 3$$

$$IEC\ 61508\ PFD\ system\ 1oo4\ \approx \beta * \lambda_{DU} * \frac{\tau}{2} + \frac{[\lambda_{DU} * \tau]^4}{5} \approx 1{,}53\text{E} - 03$$

$$\rightarrow SIL\ 2$$

In this simplified example, the CMooN factor is the only difference between the two approaches. The results show that the CMooN notification in the PDS method clearly has an impact on the system PFD.

In this example, the PDS method gives a much lower PFD than the IEC 61508 method. Actually, the results conclude against different SILs.
The PDS method concludes with SIL 3, while the IEC conclude with SIL 2.

For a 1oo4 system the PDS method will always result in a lower PFD than with use of the IEC guidelines. The reason is that the PDS introduces a CMooN value for voting systems. In this simplified example a CMooN value of 0, 3 (1oo4 system) is used, and by multiplying with 0,3 one will achieve a result which is 70 % less then IEC 61508 approach.

The outcome presented in the simplified example is not always the scenario, because the result in the PDS method depends on the voting of a system. Table 3 demonstrates how the CMooN value influence the PFD calculations in simple voting systems.

System	1oo2	1oo3	1oo4	2oo3	2oo4	3oo4
Corresponding CMooN value (PDS method)	**1,0**	**0,5**	**0,3**	**2,0**	**1,1**	**2,9**
PDS guidelines	Same PFD as IEC	Lower PFD than IEC	Lower PFD IEC	Higher PFD than IEC	Higher PFD than IEC	Higher PFD than IEC
IEC 61508 guidelines	Same PFD as PDS	Higher PFD than PDS	Higher PFD than PDS	Lower PFD than PDS	Lower PFD than PDS	Lower PFD than PDS

Table 3.PFD results with different voting system

If the CMooN value is higher than 1, the PDS guidelines will result in a higher PFD than with use of IEC 61508 guidelines. While if CMooN is lower than 1, PDS will result in a lower PFD than with use of IEC 61508.

4.0 Presentation of the case study - DSA BOP control system

This chapter includes some background information of the BOP control system on DSA and a RBD which are used in the reliability calculations.

See Bai (2010) for general information about a piloted hydraulic BOP control system, and Appendix C for a short description of the DSA platform.

4.1 System description of the BOP control system

The new and modified BOP control system on DSA is a Piloted Hydraulic Control System (OD&T 2010). The previous BOP control system was operated through a Multiplex (MUX) control system, which also was installed on DWH.

The principal function of the surface control system is to control and monitor the hydraulically operated subsea equipment. This surface control system controls both the main hydraulic pressure, as well as the hydraulic pilot signals. The hydraulic power for the system is supplied from a Hydraulic Power Unit (HPU) and associated accumulator bottle racks. All BOP functions can be controlled and monitored from either the Driller's or Tool pusher's panels (OD&T 2010).

Signals are sent from the Drill Floor Panel and Tool Pusher Panel to the CCC PLC's, where they are processed according to a predetermined set of logic instructions (OD&T 2010). Then the corresponding signals are transmitted to the Surface Electronics Panel (SEP) and initiates control signals to the hydraulic panel. Pressure switch inputs from the hydraulic panel confirm valve movements in response to control commands. The Hydraulic Control Module (solenoids) then gives pressure to two redundant umbilicals, which again transport pressure too respectively a yellow or a blue pod. The pod then gives pressure further to the BOP stack (OD&T 2010).

4.2 Case model- Reliability block diagram of the BOP control system

The BOP control system on Deepsea Atlantic will be used as a case example in the reliability analysis, and for this purpose a Reliability Block Diagram (RBD) is made and presented (Figure 6).

For those who are not familiar with RBD, a Fault Tree is constructed for the same system and could be found in Appendix D.

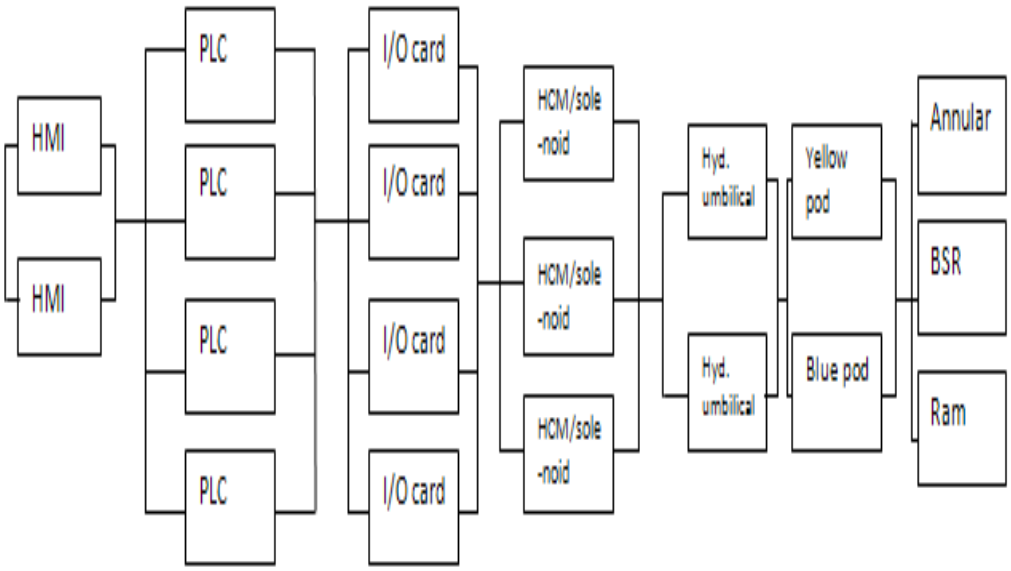


Figure 6.RBD of the BOP control system on DSA

In the process of making the model (interpretation of a real phenomena), a lot of work has been done to make the model as realistic as possible. But still, the model must not be taken as a blueprint of the DSA BOP control system.

Model uncertainty is a topic that is given a lot of attention in the literature of reliability and risk analysis (Aven & Nilsen 2002) (Zio & Apostolakis 1996) (Chatfield 1995) (Lundteigen 2009). It seems like an overall understanding of what model uncertainty is and how this influences the quantitative results does not exist.

The RBD used in the calculation is not uncertain; it is only a simplified phenomenon of the DSA BOP control system, but if the model is changed, the result will differ.

5.0 Results

In this chapter the results from the reliability study, by use of IEC 61508 and PDS guidelines will be presented.

The input data used in the calculations are mainly based on information from OREDA (OREDA 2009), PDS method Handbook (Hauge et al.2010), PDS data handbook (Onshus et al. 2010) and a SINTEF reliability study (Holand 1999).
An overview of input data used in the calculations can be found in Appendix E.

Several methods exist to verify an underlying lifetime distribution. Hazard plotting or Nelson estimator is a graphic method to identify the underlying lifetime distribution (Aven 2006).

Example: Verifying the underlying distributions

The input data used in the Hazard plotting is based on Mean Time To Failure (MTTF) values. The result from the Hazard plotting is presented in Appendix F and shows the plots fall roughly on a straight line, which indicates that the hazard line is linear. Based on this information one can conclude that the failure rate is approximate constant and that exponential distribution is a preferable distribution to assume.

5.1 SIL verification on the NCS

First of all, data from the Risk Level Project (RNNP 2010) on the NCS has been reviewed for the function "BOP isolation". The RNNP was initiated in 1999/2000 to develop and utilize a measuring tool which illustrates the development in the risk level on the NCS.

Based on the data collected from RNNP (PTIL 2010) the PFD has been calculated[4] to be 7.42E-03, which indicates a SIL 2 requirement for closing one valve in the BOP stack on the NCS.

5.2 Reliability analysis of the DSA BOP control system

In the calculations the approximate formulas given in PDS and IEC 61508 are used. The results from the reliability calculation are presented in the Table 4.

Deepsea Atlantic BOP Control System		
Reliability guidelines	**Result, PFD system (hours)**	**SIL level**
IEC 61508 guidelines (approximate formulas)	$4{,}9E-03$	SIL 2
PDS guidelines (approximate formulas)	$2{,}1E-03$	SIL 2
PDS guidelines – Application specific calculations	$4{,}9E-04$	SIL 3

Table 4.PDS and IEC results

The result shows that the BOP control system on DSA is within SIL 2 given by OLF 070 (2004).

[4] *In this exact scenario (1oo1) the IEC 61508 and PDS guidelines are identical*

6.0 Discussion

6.1 Reliability analysis of the DSA BOP control system

It is important to note that there is little relevant research published on reliability of a BOP control system, both in Norway and worldwide. Reliability assessment of offshore systems is often classified as restricted or internal information by the oil and gas companies. This is a problem when performing reliability studies, simply because these studies depend on having relevant input data available.

The BOP control system on DWH was one of the safety critical systems that failed and significantly contributed to escalate the accident (BP 2010). Therefore it is reasonable to believe that more studies and research will be prioritized in the years to come.

SINTEF has some relevant studies, mainly a joint industry project on behalf of the Minerals Management Services, which was conducted on data from the GOM (Holand 1999)(Holand & Skalle 2001). Scandpower also has some relevant research, and they recently initiated a new research project on the reliability of a BOP (Scandpower 2011).

The result in chapter 5.2 shows that the DSA BOP control system is within the SIL requirements given by OLF 070. The results are also in agreement with the calculated PFD based on data from PTIL RNNP (Chapter 5.1).

By use of IEC 61508 guidelines one achieved a higher system PFD than with use of PDS guidelines. The difference cannot be categorist as critical, simply because both methods conclude within the same SIL. In this exact model the PDS method give approximately 0,3 % lower PFD than with use of IEC guidelines.

In the simplified example presented in chapter 3.4 the results were more dramatic. Actually, the results concluded against different SIL. PDS concluded with SIL 3, while the IEC 61508 concluded with SIL 2.

An application specific [5]calculation of the BOP control system based on PDS guidelines has also been performed. The result from those calculations differs strongly from the other calculations presented in chapter 5.2. With use of the application specific calculation one will probably, in most scenarios, archive a lower PFD. The main reason is that generic failure rate is often higher than vendor data. In an application specific calculation of local safety system, the vendor data shall be used, if not, generic data should be modified to vendor data.

6.1.1 Assumptions and limitation in the PFD formula

The PFD formulas are based on the assumption that the lifetime of failure rates is exponentially distributed (see also proof in Appendix A). Thus, the exponential distribution is characterized by a constant failure rate. A unit having an exponential failure time distribution has a tendency to failure that does not depend on the age of the unit (Aven 2006). Other assumptions in the underlying distribution is that after a test the system is assumed to be as good as new and that the state of the system can only be identified by a test or a demand. If decision makers are not aware of the assumptions and conditions attended with the PFD formula, they may misinterpret the results.

An issue that is sometimes raised is whether to use the average or time dependent PFD. Some researchers argue that the average PFD is misleading since the PFD in approximately 50% of the time is higher than this value (Dutuit et al. 2008).

Currently, the IEC 61508 and the PDS method suggest using the average PFD, while a new ISO Technical Report (TR) (to be released 2012/2013), will recommend to use the time dependent PFD (ISO TR 12489).

[5] *Local safety systems or specific systems*

Example: Underlying distribution in the PFD formula

You are given a choice to select between two identical light bulbs. Light bulb A have been in use for 5 months and light bulb B have been in use only for a couple of days. Then it is reasonable to think that most of us would choose light bulb B. Simply, because light bulb B is newer and probably will work for a longer period. Based on the information of exponential distribution the choice is not light bulb B, because the tendency of failure do not depend on the age of the unit.

The probability that the light bulb then will survive an additional "v" hours is given by (Aven 2006):

$$P(T > u + v | T > u) = \frac{P(T > u + v \cap T > u)}{P(T > u)} = \frac{P(T > u + v)}{P(T > u)} = \frac{e^{-\lambda_{DU}(u+v)}}{e^{-\lambda_U}}$$
$$= e^{-\lambda_{DU} v} = P(T > v)$$

The exponential distribution is the only distribution with this property, and this lack of memory simplifies the mathematical modeling.

The fact that the failure rate is constant for large values of "T" may seem unrealistic in the example above. However, remember that usually the interest is on studying the lifetime in a limited period of time. The failure rate assumed outside this period will then not be critical (Aven 2008).

6.2 Different interpretation in the IEC and PDS method

This section aims to demonstrate that with use of the different reliability guidelines (PDS and IEC 61508) the PFD and conclusion against SIL can differ.

Topics that will be focused on are:

- β modeling
- Hardware and Systematic failure
- Application specific calculations
- Calculation approaches (detailed or approximate formulas)
- Input data

The traditional approach (IEC and PDS) for verification of a quantitative SIL seems intuitively appealing. As Figure 7 shows, firstly, a SIL requirement for the probability of failure on demand is given. Then the probability of failure on demand is calculated for the specific system, before it is compared with the established criteria.
If the calculated PFD is higher than the target value (SIL), it indicates that risk reducing measures should be implemented. If the calculated PFD is lower or equal the SIL requirement the system is approved.

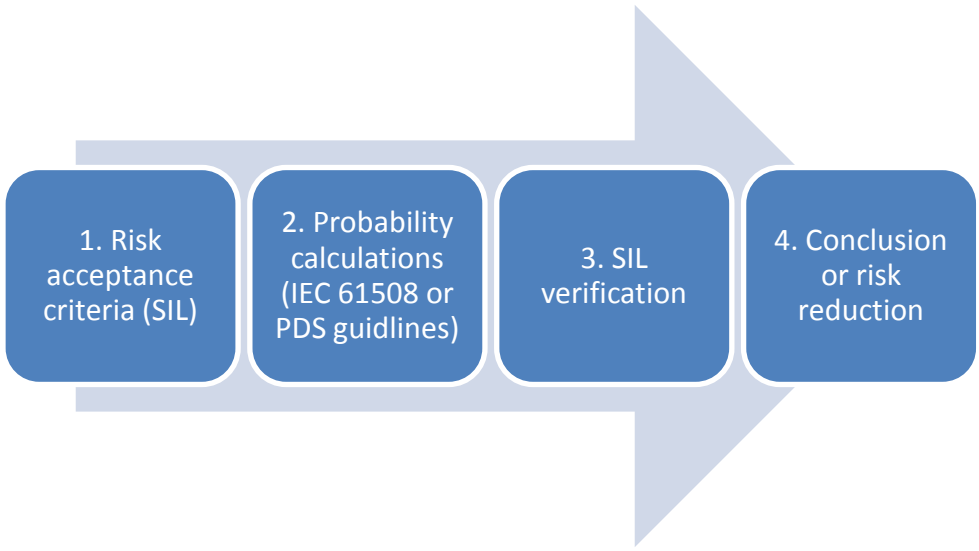


Figure 7.Traditional approach

Both methods are based on probability calculations when SIL requirement is verified. By jumping directly into probabilities, important uncertainty aspects are easily truncated, meaning that potential surprises could be left unconsidered (Aven, 2008).

Uncertainties are often hidden in the background knowledge, and restricting attention to the assigned probabilities could camouflage factors that could produce surprising outcomes (Aven 2008). Therefore researchers argue that it is important to look beyond the assigned probabilities (Aven 2010) (Abrahamsen & Røed 2011) (Flage & Aven 2009).

The point is that probability is a tool to express uncertainty. It is, however, not a perfect tool, and therefore verification against SIL should not only be based on the probabilistic world (Abrahamsen & Røed 2011). The probabilities (P) are conditional on specific background knowledge (K), and they could produce poor predictions (P{failure on demand|K}) (Abrahamsen & Røed 2011).

6.2.1 Beta modeling

The differences between the standard β-factor model in IEC 61508 and PDS are illustrated in Figure 8.

A circle (say A) represents the event of component A has failed. For a duplicated set of redundant components A and B (N=2), the standard IEC 61508 and PDS approach are identical for CCF calculations; Here, β represents the fraction of failures affecting both A and B, so that they fail simultaneously (Hauge et al. 2010).

For a triplicate set of components (N=3), the β-factor model in IEC 61508, assumes that whenever there is a failure affecting two components (say A and B) the third component (C) will also fail. According to PDS it will never happen that just two of the three components fail due to a CCF (Hauge et al. 2010). Using the PDS method and the updated CMooN factors, it is assumed that if A and B have failed due to a CCF, C may also fail (50% of the cases) (Hauge et al. 2010).

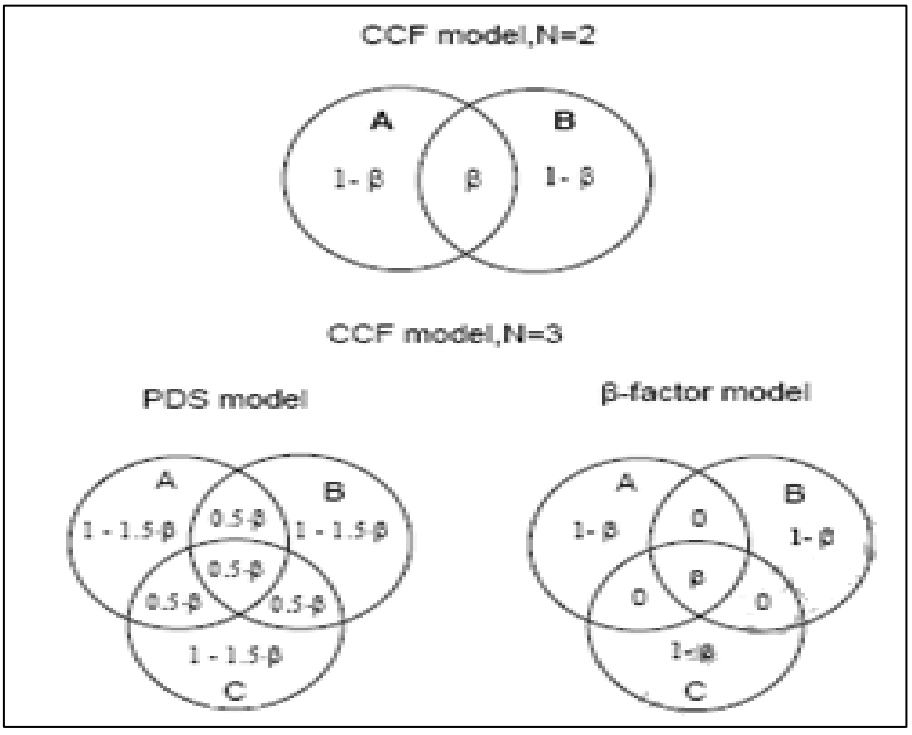


Figure 8.Illustration of differences in B model in IEC 61508 and PDS 2010

From Figure 8 it is also seen that the C2oo3 factor in the PDS method 2010 becomes 2.0, since the fraction of failures affecting 2 or 3 component is $0.5 \cdot \beta + 0.5 \cdot \beta + 0.5 \cdot \beta + 0.5 \cdot \beta = 2.0 \cdot \beta$.

In the 2006 edition of PDS method handbook, the CMooN values were slightly different. Using the PDS method 2006 it was assumed that if A and B have failed due to a CCF, C may also fail, but only in 30% of the situations. Based on this information the old PDS 2006 C2oo3 factor would be; $0.3 \cdot \beta + 0.7 \cdot \beta + 0.7 \cdot \beta + 0.7 \cdot \beta = 2.4 \cdot \beta$.

Example: Calculation of PFD with use of "old" and "new" CMooN factor given by PDS

Think of the simplified example in chapter 3.4. In those calculations the new CMooN values found in the PDS method handbook 2010 were used.

In this example the same system is analyzed, but instead of using CMooN of 0, 3 (as suggested in PDS 2010) a CMooN value of 0, 15 is used instead (as suggested in PDS 2006).

The system PFD in the simplified example is then calculated to be approximately 2.36 E-0.4. The PFD becomes slightly lower, but one can argue that the change is not very dramatic because both calculations conclude against the same SIL. If the example were more complex, the outcome could be greater and then the conclusion against SIL could differ.

Note that there is a new committee draft version of IEC 61508-6 (2010) that includes correction factors for modifying the β-factor for different MooN voting configurations. This approach is in line with the β model approach in PDS, even if some of the modification factors proposed by IEC deviate slightly from the suggested values in PDS.

6.2.2 Hardware and Systematic failure

In the PDS – project "Reliability Quantification of Computer-Based Safety Systems" it was documented that systematic failure is a major contributor towards unavailability of safety functions (Aarø 1997).

Because of this contribution OLF 070 recommends to use PDS guidelines when carrying out application specific calculations (See also chapter 6.2.3).

Example: Taking systematic failures into account - PDS

Again the simplified example in chapter 3.4 will be used. In this example to demonstrate how the systematic failure influences the total PFD calculations. The dangerous undetected failures have to be split[6] *into systematic and random hardware failure.*

When taking into account the split of dangerous undetected failures, the system PFD becomes 3.32 E-04. In this example the systematic failure has an impact on the PFD. The outcome in this example is that the PFD becomes slightly higher. If the example were more complex, the outcome could be greater and then the conclusion against SIL could differ.

[6] *In this specific example an r value of 0, 3 are chosen (Hauge et al. 2010). The "r" is the fraction of* λ_{DU} *originating from random hardware failures. See Lundteiegn (2010) for a more detailed description.*

6.2.3 Application specific calculations

For a given application of SIS, the appropriate data to use may deviate from the average data presented in handbooks or databases. PDS has therefore developed simple models in order to adapt or transform average parameter values into application specific values.

Example: Expert judgments in the application specific calculations - PDS

When performing application specific calculation by use of PDS, the parameters $\widehat{P_{TIF}}, \widehat{\beta}$ *and* $\widehat{\lambda_{DU-SYST}}$ *need to be treated and modified to local safety conditions. To support expert deal with the process, the PDS method presents guidelines that can support under the process.*

This approach can result in a lower or higher PFD, depending on how the guidelines are judged. It is reasonable to think that this approach will lead to a lower PFD, since the experts on its own system can or might have a tendency to overprotect the system they are working on daily.

The IEC standard gives an opportunity to carry out application specific calculations. Determining these β values (upgraded) is not a straightforward approach when following IEC guidelines. Therefore the main part of reliability researches uses the application specific approach presented by PDS. One problem being the lack of input data, relevance of the input data and the subjective or expert judgments in the scorecard [7]approach.

The scorecard consists of a number of questions that needs to be answered, and at the end these answer are summarized to a total score, which is the β that should be used when dealing with CCF.

[7] *The scorecard in the IEC method can be found in IEC 61508 –part 6 – table D.1 (IEC 61508-6 2010)*

A general weakness related to application specific calculations, both in IEC and PDS, is expert and human judgments. The result of this calculation approach is believed to differ strongly, depending on how well the reliability analyst knows the analyzed system. Therefore it is preferable that this application is performed in collaboration with technical experts. Still, expert judgments also have a tendency to vary.

Example: Variation in expert judgments

In Baraldi et al. (2009) five organizations with significant experience in explosion modeling performed numerical simulations of explosions in a specific tunnel. The expert judgments are in this scenario used as input data and to select the wanted approach in a Computational Fluid Dynamics (CFD) simulation.

The result shows that there was a significant difference in the conclusion.

The selected approach, based on the expert judgments, was believed to be one criterion that influenced the overall conclusion.

6.2.4 Calculation approach

In the reliability calculations (Chapter 5) the approximate formulas in the IEC 61508 and PDS method have been used.
The PDS guidelines give an opportunity to calculate the PFD with use of "more detailed formulas" (Hauge et al. 2010). According to Lunteigen (2009) the difference between the calculation approaches is not dramatic.

The PFD may also be calculated by using mathematically exact expressions (Markov modeling) (Høyland and Rausand 2004). Hauge et al. (2010) has carried out calculations with Markov for different voting system and compared the results with the approximate formulas in IEC 61508 and PDS. As expected, because of different interpretations, the results differ. For simplified models, the result is in reasonable agreement, but for complex systems the difference is greater.

In the example below (Figure 9) the PFD will be calculated for a 1oo3 Hydraulic Control Manifold system to determine the difference between approximate and "more detailed" formulas given by PDS. The system can be characterized as a 1oo3 and input data can be found in Appendix E.

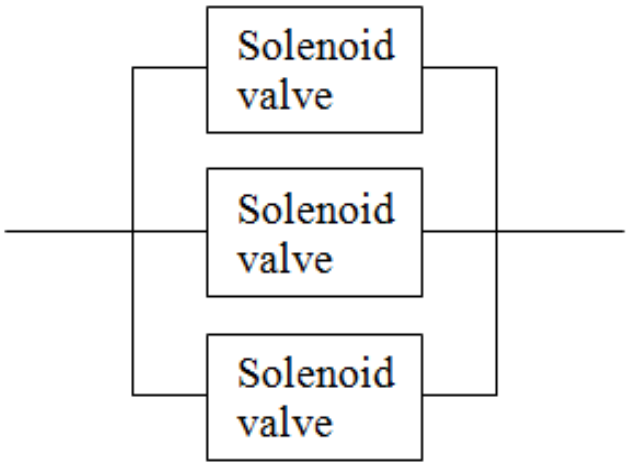


Figure 9.Hydraulic Control Manifold (RBD)

Example: Comparison of the approximate and more detailed formulas given by the PDS method

In this specific example the PDS approximate and PDS "more detailed" (not Markov modeling) formulas gives the same result.

To be precise, the PDS approximation formulas give a PFD of 1, 7520E-04, while the more detailed formulas give a PFD of 1, 7525E-04.

If the example were more complex the outcome could be greater.

It is important to note that the ISO TR 12489 includes new approaches and guidelines on how reliability analysis should be handled by the industry. The TR argues in some extent that for complex systems, the guidelines and approaches in PDS and IEC 61508 is not sufficient.

6.2.5 Input Data

All data sources used in this thesis are seen as credible data by the oil and gas industry. The best practice would probably be to use one data source, but in many situations, this is not possible because of lack of relevant input data.

The input data could be poor or less representative due to factors such as (Hauge et al. 2010):

- *The data collection itself*; inadequate failure reporting, classification or data interpretation.
- *Variations between installations*; the failure rates are highly dependent upon the operating conditions and also the equipment will vary between installations.
- *Relevance of data / equipment boundaries*; what components are included / not included in the reported data? Have equipment parts been repaired or simply replaced?
- *Assumed statistical model*; is the standard assumption of a constant failure rate always relevant for the equipment type under consideration?
- *Aggregated operational experience*; what is the total amount of operational experience underlying the given estimates?

The data sources presented in data bases are based on generic values. A generic failure rate is believed to be higher than vendor data, and will therefore result, in many cases, in a higher PFD result.

If the system that is being analyzed is based on new technology, the generic data could produce poor and unrealistic result. The reason is that generic data does not exist for new technology due to lack of field experience.

The vendor data is often collected from newer technology, but vendor data can also been collected during laboratory testing or limited field experience only. If so, important factors like human involvement, field environment, etc. are not reflected and may thus underestimate the failure rate (Janbu 2009).

Figure 10 illustrates in a simplified manner the compromise between the need for failure data and the relevance of the data (Lundteigen 2010). The broader the category of failure data becomes, the less representative the data can be for a particular component.

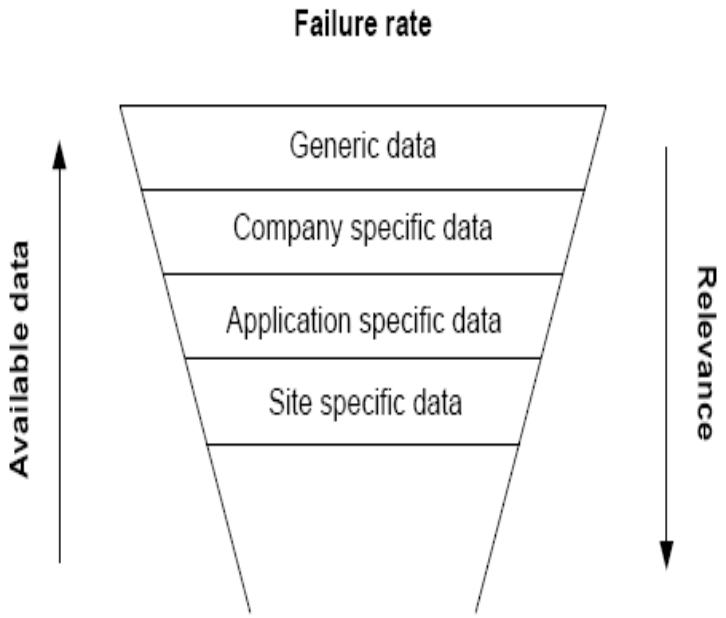


Figure 10.Illustration of availability and relevance of failure data

Example: Use of sensitivity study in the input data

In a sensitivity study presented by Janbu (2009,) two different failure rates (generic) for "level transmitter" resulted in significant differences between the estimated unavailability. The generic data which was used in the calculations were based on the exact same equipment, but was gathered from difference sources. In this exact study the data was gathered from OLF 070 and OREDA.

6.3 An overview and a summary of factors which influences the PFD result

Figure 11 aims to illustrate parameters that can influence the PFD calculations, and again can cause or mislead to wrong interpretation of the results.

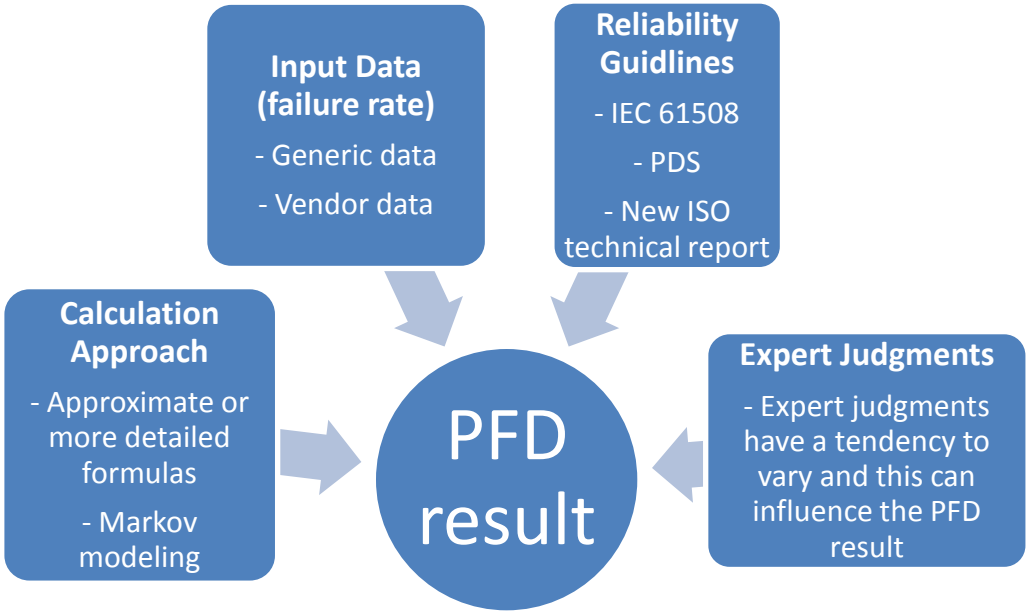


Figure 11. Factors which can influence the PFD result

The main factor is identified to be calculation approach, input data, reliability guidelines and expert judgments.

Lunteigen (2009) presents a similar overview and with underlying factors as well, but with slightly different main factors. These underlying factors can for example be time pressure, competence, regulations, standards and guidelines (Lundteigen 2009).

The reliability guidelines (IEC 61508 and PDS) are not defined as an underlying factor in Figure 11, as it is by Lundteigen (2009). The reason for this is that with use of different reliability guidelines one will achieve different system PFD for the same model, especially when a model is built up by different voting configuration. When making decisions it is important to have some background knowledge of how different reliability guidelines can influence the PFD.

Therefore, I argue that reliability guidelines are not an underlying factor, but a main factor.

7.0 Idea for an approach to support the verification of SIL

This chapter includes a presentation of new ideas for a method which aims to support decision makers after the PFD of the system is calculated and before SIL is verified. The presentation of the new method is given in chapter 7.1. An example in chapter 7.2 will then be presented to demonstrate the ideas in a practical example.

Chapter 7.3 includes a discussion of weaknesses and strengths associated with the new ideas and existing approaches.

It is important to note that the method presented in this chapter is not a new approach, but it includes some new ideas of how one can merge existing approaches to help decision makers when SIL is verified.

7.1 Overview of the method

An overview of the method is shown in the block diagram below (Figure 12). The method can be described as a semi quantitative/qualitative approach.

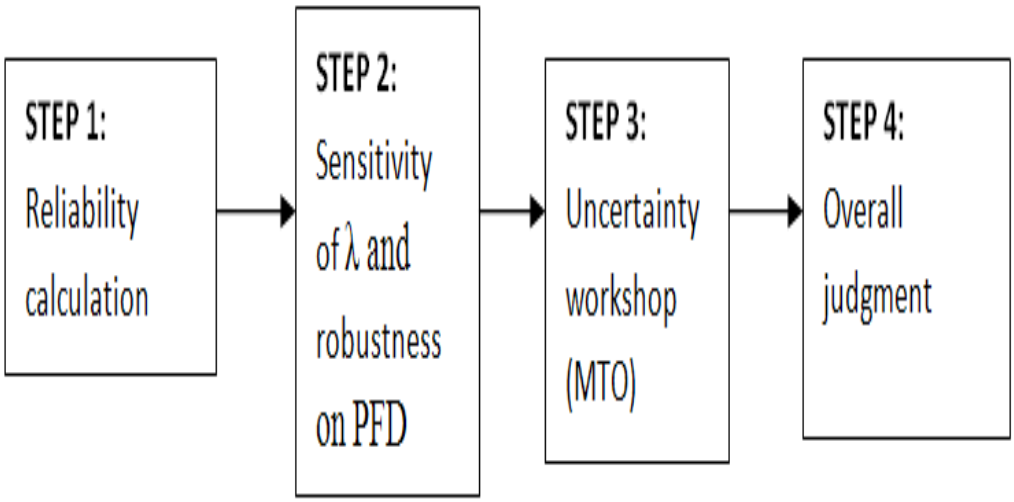


Figure 12.New idea of an approach to verify against SIL

The only new idea in the method is the use of a quantitative sensitivity analysis in Step 2.

7.1.1 Step 1: Reliability calculations

Step 1 consists of PFD calculation with use of IEC 61508 or PDS guidelines.

7.1.2 Step 2: Quantitative sensitivity study of the failure rate

Step 2 consists of a quantitative sensitivity study, which aim to find out how robust the system is against changes in the input data (λ).
I also identified the failure rate (Chapter 6.3) as a critical factor that will influence the PFD result.
The step is not in total agreement with the ACP perspective described in chapter 2.1.1, but the goal in the step is not to describe uncertainty in the failure rate. The goal is to conclude against robustness in the system.

The lower and upper limits of the estimated λ may be presented as a 90 % confidence interval (OREDA 2009). This is an interval (λ_L, λ_U), such that the "true value" of λ fulfils (OREDA 2009):

$$P(\lambda_L \leq \lambda < \lambda_U) = 90\%$$

With *n* failures during an aggregated time in service (τ) this 90% confidence interval is given by:

$$\left(\frac{n}{2\tau}Z_{0,95,2n}, \frac{n}{2\tau}Z_{0,05,2(n+1)}\right)$$

,were $Z_{0,95,\nu}$ and $Z_{0,05,\nu}$ denote the upper 95% and 5% percentiles, respectively, of the α^2 distribution with "ν" degrees of freedom. See Appendix G for percentage point for the CHI- square distribution.

Guidelines in step 2

The quantitative sensitivity study can conclude with two different outcomes:

- Low robustness: The different failure rates (Low and High) used in the PFD calculations conclude against DIFFERENT SIL.

- High robustness: The different failure rates (Low and High) used in the PFD calculations do conclude against the SAME SIL.

7.1.3 Step 3: Qualitatively uncertainty workshop

The ideas for Step 3 are adopted from Abrahamsen & Røed (2011).

Abrahamsen & Røed (2011) presents and discuss an alternative approach, acknowledging that the calculated probability should not be the only basis for verifying the established quantitative SIL requirements.

The approach consists of identifying sub-categories, from a human, technical and operational perspective (MTO). Then each sub-category is evaluated with respect to uncertainty and based on this evaluation the category is given an uncertainty classification. The uncertainty classifications are based on guidelines from Flage & Aven (2009).

Guidelines in step 3

The qualitatively workshop can conclude with low, medium or high uncertainty. This conclusion is based on subjective and expert judgments.

7.1.4 Step 4: Overall judgment

This step consist of an overall judgment were step 2 and 3 shall be seen in relation with step 1.

Guidelines in step 4

A general guideline for the overall judgment are made and described below:

- *High robustness and low uncertainty → Conclude against SIL.*

To simplify the verification against SIL, only one guideline is made. For all other outcomes risk reducing measures are needed before concluding.

7.2 Demonstration of the method with an example

The example that will be used to demonstrate the new method is based on failure data given by Holand (1999) on the GOM. The system that will be treated separately is a hydraulic pod[8] and is in this case seen as a 1oo1 system (Figure 13).

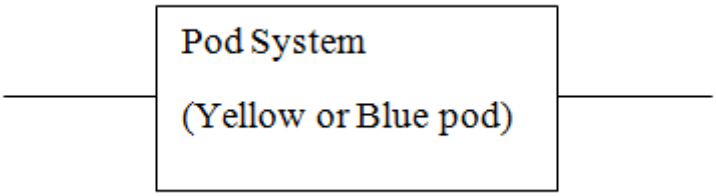


Figure 13.POD system (RBD)

7.2.1. Step 1

The PFD is calculated with use of IEC 61509 and PDS guidelines.

$$PFD_{IEC\ and\ PDS\ method} = 1{,}37E-01$$

Step 1 concludes against SIL 0.

[8] *Note that this pod system is not comparable with the hydraulic pod system on DSA*

7.2.2. Step 2

Based on the method given in chapter 7.1.2 the following confidence intervals are calculated:

$$Lower\ 90\ \%\ confidence\ limit = 2{,}71E-05$$
$$Higher\ 90\ \%\ confidence\ limit = 1{,}23E-04$$

The PFD for the 1oo1 pod system is then calculated by use of lower and higher failure rate to determine how this influences the system PFD.

$$PFD_{lower\ limit(chi\ square)} = 5{,}95E-02 \rightarrow SIL\ 1$$
$$PFD_{higher\ limit(chi\ square)} = 2{,}70E-01 \rightarrow SIL\ 0$$

Step 2 concludes with low robustness, because low and high failure rate conclude against different SILs.

7.2.3. Step 3

The MTO uncertainty workshop is presented in Table 5.

Uncertainty workshop: Pod system			
MTO perspective	**Sub- categories**	**Evaluation**	**Uncertainty classification**
Human aspects (M)	Training	Operators will be trained to recog-nize situations that need manual push down from panels	Medium
Technical aspects (T)	Hydraulic pres-sure in pod	Test interval and maintenance is required but not always followed	Low
Operational aspects (O)	Procedures	Poor quality management	Low

Table 5.Uncertainty Workshop

Based on a subjective judgment in collaboration with a technical expert, step 3 concludes with low uncertainty.

7.2.4 Step 4

This step is based on guidelines presented in chapter 7.1.4, were step 2 and 3 are seen in relation with step 1.

Steps 4 conclude that risk reducing measures are needed before verifying against SIL.

7.3 Strengths and weaknesses with new ideas and existing approaches

In this section I will both argue for and against the new ideas in the suggested approach and existing approaches.

It is important to note that there is a need for new ideas and approaches when verifying PFD against SIL. No overall agreement or guidelines exist to support decision makers when concluding against SIL.

7.3.1 Quantitative sensitivity study of the failure rate

To determine if a system have low or high robust, I argue that a quantify sensitivity study (step 2) is a good approach to use. This approach can be used to test the robustness and to determine how the failure rates influence the system PFD. It can also help to draw attention to those factors that requires especially careful assessment or management (New Zealand Treasury 2005). As mention earlier in this thesis, sensitivity analysis is given a lot of attention in nuclear power industry, while in the oil and gas industry the topic is often neglected.

The strength with implementing sensitivity studies in reliability guidelines (IEC 61508 and PDS) is that the input data (failure rate) will be given more attention. A PFD calculation, based on IEC and PDS guidelines, is mainly influenced by the input data. The failure rate was also a critical factor which I identified in chapter 6.3. Sensitivity studies are used as a powerful tool by economics to predict and highlight uncertainty to future cash flows in cost - benefit analysis.

By carrying out a quantify sensitivity study which aim to describe the robustness of a system, is therefore information that can be used to support decision makers.

Researches will and can probably in some extent argue that Step 2:

- do not take the MTO perspective into fully account
- that uncertainty from a ACP perspective is not given enough attention
- that sensitivity studies is time and cost consuming
- that sensitivity is already covered in the uncertainty workshop in step 3 (will be discussed in chapter 7.3.2)

I also believe that the MTO perspective must be taking more into account when performing sensitivity studies (Step 2), especially for technical systems that are manually activated (BOP, ESD). In some data, for example, historical failure rate, one can argue that the MTO perspective is more or less covered. Those failure rates have been influences by human errors and organizational failure over time. For other data, as for example, vendor data, the MTO is not covered in a preferable way in step 2. Simply because this input data is mainly based on new technology.

I agree that uncertainty from an ACP perspective is not given enough attention in step 2, but from a relative frequencies perspective, the uncertainty is covered by the sensitivity study. The goal in the step is not to describe uncertainty in the failure rate, but instead to conclude against robustness of the analyzed system. Robustness as a decision tool is frequently discussed in risk and reliability research. Barberies (2006) also argue that a quantify sensitivity analysis is a powerful and useful tool to support decision making processes.

Sensitivity studies can be time and cost consuming, especially when the analyzed system is complex. Therefore it can be practical to select a subsystem in a model which is seen as critical. A number of importance ranking measures have been developed to support sensitivity analyses, for example Birnbaum's and the Improvement potential measure (Lundteigen 2009).

These measures can be used in collaboration with the sensitivity study. Sometimes the relative reliability between components is a more important knowledge than the overall reliability itself since it might pinpoint vulnerabilities in the system that needs to be addressed (NASA 2011).

7.3.2 Qualitatively uncertainty workshop

In step 3 I adopted the uncertainty workshop presented by Abrahamsen & Røed (2011), while the uncertainty classification used in the approach is gathered from Flage & Aven (2009). The MTO perspective is well implemented in the approach and I believe that human involvement and organizational factor will be more covered than in a standard quantify approach.

I identified two weaknesses in Abrahamsen & Røed (2011) approach that need to be more addressed in reliability research:

- uncertainty categorizing of the sub categories (see table 5)
- a need to highlight and clarify the use of sensitivity

The uncertainty categorizing of the subsystems is preferred in collaboration with technical expert on the analyzed system. This is because the reliability experts, in many cases do not have the preferable knowledge of a complicated technical system. It is reasonable to think that the uncertainty workshop will more often conclude with low uncertainty instead of high uncertainty. The reason might be that some technical expert might have a tendency to overprotect the system they are working with daily. If this is the most likely outcome, the output from the suggested approach by Abrahamsen & Røed (2011) can lose some of its value.
Another point is that expert judgments also have a tendency to vary due to different background knowledge and experience. This is not reflected well enough in the suggested approach. This can lead to that the same analyzed system can result in two different results, if it is studied by two independent reliability experts.

One expert can for example conclude with low uncertainty, while another can conclude with high uncertainty. If the result then is seen is relation with the probabilities, the overall judgment will probably lead to a different conclusion. Again, if this is the most likely outcome, the output from the approach by Abrahamsen & Røed (2011) can lose some of its value.

Abrahamsen & Røed (2011) also take sensitivity into account (qualitative), where the sensitivity is seen in relation to uncertainty and assigned probabilities. My opinion is that sensitivity is not well documented or highlighted in the approach. Therefore, I also argue that the approach suggested by Abrahamsen & Røed (2011) in some extent lack the focus on sensitivity.

It is important to be aware of the limitations which is highlighted above, if not, the results can be misunderstood and the output from the approach can lose some of its value as a decision tool. Several misunderstandings can then lead to poor decision making, which again can cause to an incorrect conclusion against SIL.

I acknowledge that the quantitative sensitivity (step 2) and the approach suggested by Abrahamsen & Røed (2011) (step 3) is in some extent in resemble agreement.
The only difference is that I will introduce a quantitative sensitivity study which aim to conclude against robustness. In addition, I implemented the approach suggested by Abrahamsen & Røed (2011).
How these two steps can influence each other in the suggested approach (chapter 7.1) is not considered in a detailed way.
It is reasonable to think that my idea for an approach will in some extent consider the sensitivity of the failure rate two times, both in step 2 and in the implemented step 3. The outcome and the consequences of this scenario are not clear and must be addressed more in reliability research.

8.0 Further work

The PFD calculations give a useful insight for decision makers. After presenting several examples of how different interpretations in the methods result in different SIL verification, I argue that there is need for a broader reflection of robustness and uncertainties that can support decision makers. The reason for this is that both methods are based on probability calculations when SIL is verified or determined.

In the oil and gas industry it is common to define and describe risk using probabilities and probability distributions. This can and has probably led to misunderstandings and some misleading interpretation of the result in reliability analysis. This is a topic I believe must be more addressed in risk and reliability research.

I strongly believe that the MTO perspective must be more reflected in reliability assessments. This is a topic that has now been more or less implemented in risk analysis and accident investigation. Therefore it is reasonable to think that the perspective will be more addressed in future reliability assessments. More research is needed on the topic and on how the perspective can be implemented in reliability analysis.

As previously mentioned, reliability assessments is often classified as restricted information by the oil and gas companies. The consequences of this are that relevant experience is not transferred between companies. Therefore, I argue that there is a need for more collaboration between companies working on safety critical systems.

To get an overview of some of the most important findings in this thesis, Figure 14 is presented.

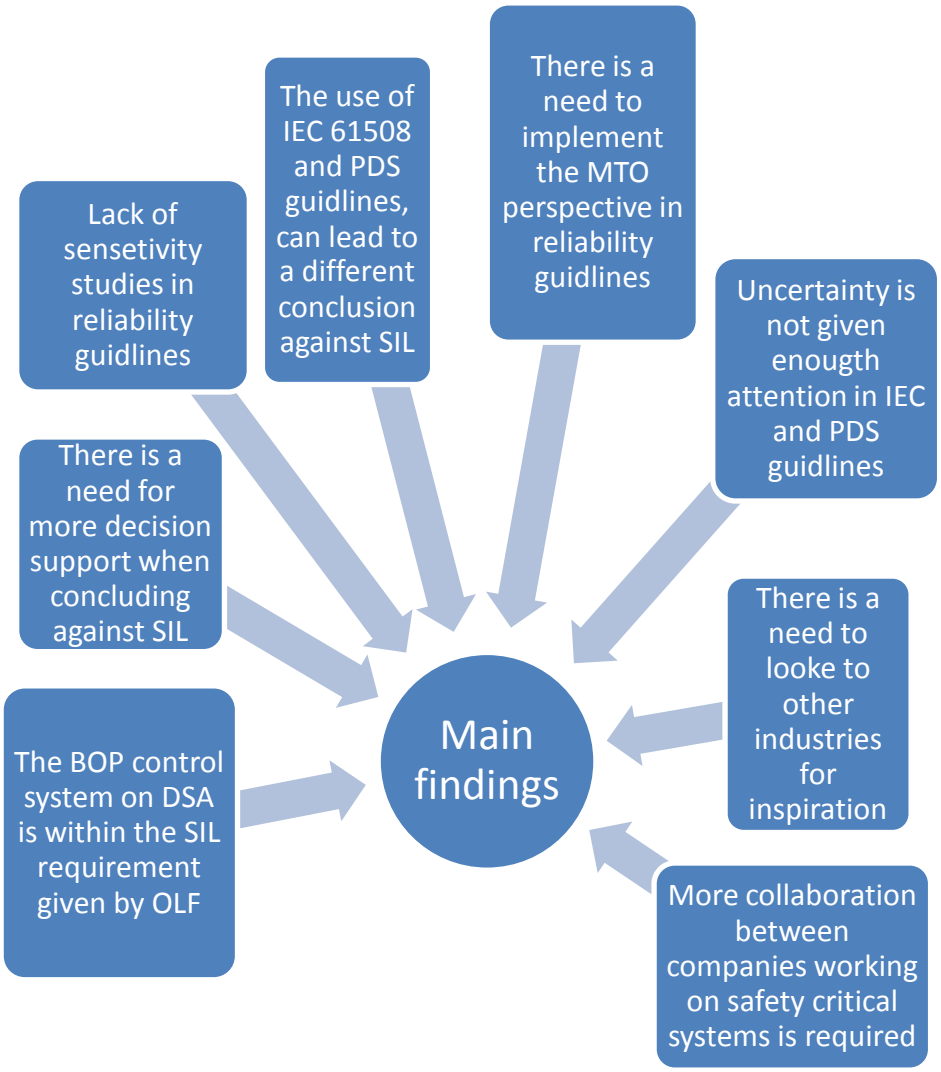


Figure 14. Main findings

9.0 Conclusion

The four goals which were stated in chapter 1.2 is concluded against below.

1. Highlight with examples that with use of IEC 61508 and PDS method the result can differ, and that this can lead to different conclusion based on SIL verifying.

The calculations in chapter 3.4 are one example that shows the PFD results differ strongly and that the guidelines conclude against different SIL for the same system.

2. Determine if the BOP control system on DSA is within SIL requirements given by OLF 070.

The calculations in this thesis (chapter 5) show that the BOP control system on DSA is within SIL 2 given by OLF.

3. Identify factors that influence the PFD calculation in the reliability guidelines.

The most critical factor which can influence the PFD result is identified to be: Calculation approaches (approximate vs. detailed formulas), Input data (vendor vs. generic data), Expert judgments (they have a tendency to vary) and the use of different reliability guidelines (IEC 61508 vs. PDS).

4. Develop new ideas to an approach that aim to support decision making when SIL is verified against the requirements.

I present some ideas on how one can merge existing approaches to support decision making, and I argue that it is important to look beyond assigned probabilities when SIL is verified. I believe that this is a topic that must be more addressed in risk and reliability research, because no overall agreement or guidelines to support decision makers when concluding against SIL exists.

10.0 References

Aarø, G. K. H. R. (1997). Reliability Quantification of Computer-Based Safety Systems. Safety and Reliability. SINTEF. Trondheim.

Abrahamsen. E.B. Røed.W (2011). A new approach for verification of safety integrity levels. Reliability: Theory & Applications. Volume 2.

Abrahamsen. E.B (2011). Lecture notes in risk and reliability analysis. UIS.

Aven, T. (2006). Reliability and Risk Analysis. OSLO. Universitetsforlaget.

Aven, T. (2008). Risk analysis: Assessing uncertainties beyond expected values and probabilities. Chichester, England, Wiley: N.J.

Aven, T (2009a). A new scientific framework for quantitative risk assessments. International Journal of Businesses Continuity and Risk Management, 1, 67-77.

Aven, T (2009b). On the interpretations of non- probalistic uncertainty representations in a reliability and risk analysis context. Submitted for possible publication.

Aven.T (2010). Misconceptions of risk. England, Wiley Flage R. Aven T. (2009). Expressing and communicating uncertainty in relation to quantitative risk analysis. Risk & Reliability – Theory & Application 2.

Aven.T. Nilsen.T (2002). Models and model uncertainty in the context of risk analysis. Reliability Engineering & System Safety. ELSEVIER.

Aven.T (2011). A risk concept applicable for both probabilistic and non-probabilistic perspectives. Safety Science. Elsevier.

Bai, Y. B. Q. (2010). Subsea Engineering Handbook, ELSEVIER.

Barberis. G.M. F (2006). Robustness Analysis: A Powerful Tool in the Multiple Criteria Decision Making Field. Quantitative method department. Madrid – Spain.

BP (2010). British Gas, Deepwater Horizon. Accident Investigation Report. Internal report.

Baraldi D (2009). A. Kotchourko, A. Lelyakin, J. Yanez, P. Middha, O.R. Hansen. An inter-comparison exercise on CFD model capabilities to simulate hydrogen deflagrations in a tunnel. International journal of hydrogen energy. ELSEVIER.

Chatfield C (1995). Model uncertainty, Data mining and Statistical inference. J R Statistical Society.

Dutuit, Y., Innal, F., Rauzy, A., and Signoret, J.-P. (2008). Probabilistic assessments in relationship with safety integrity levels by using fault trees. Reliability Engineering and System Safety.

Flage R, Aven T. 2009. Expressing and communicating uncertainty in relation to quantitative risk analysis. Risk & Reliability – Theory & Application 2(13): 9-18.

Holand, P. (1999). Reliability of Subsea BOP Systems for Deepwater Applications, Phase 2 DW. SINTEF.

Holand,P & Skalle,P (2001). Deepwater Kicks and BOP Performance, SINTEF.

Høyland. A & Rausand. M (2004). System Reliability Theory; Models, Statistical Methods, and Applications, Second Edition. England. Wiley.

IEC- International Electrotechnical Commission. IEC 61508-1, I. (2010). Functional safaty of electrical/electronic/programmable electronic safety-related systems. General requirements: Geneva.

IEC – International Electrotechnical Commission. IEC 61508-4, I. (2010). Functional safety of electric/electronic/programmable electronic safety-related systems. International Electrotechnical Commission. Definitions and Abbreviations: Geneva.

IEC- International Electrotechnical Commission. IEC 61508-6, I. (2010). Functional safaty of electrical/electronic/programmable electronic safety-related systems. Guidelines on the application: Geneva.

ISO - International Organization for Standardization. ISO TR 12489, Petroleum, petrochemical and natural gas industries –Reliability modeling and calculation of safety systems. Draft version. Received from the PDS forum 17.04.2012.

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

Lundteigen, M. A. (2009). Safety instrumented systems in the oil and gas industry. Concepts and Methods for safety and reliability assessments in design and operation. NTNU. Doctoral thesis.

Lundteigen, M. A. (2011). Lecture notes on reliability of safety critical systems.

Lundteigen, S. H. S. H. M. A. (2010). Reliability Predictions Method for Safety Instrumented Systems- PDS Example collection, 2010 Edition. S. T. a. Society.

Lundteigen, M. R. (2007). "Spurious activation of safety instrumented systems in oil and gas industry: Basic concepts and formulas." Reliability engineering & system safety. ELSEVIER.

Mosleh, A and Bier, V.M (1996). Uncertainty about probability: a reconciliation with the subjective viewpoint. IEEE Transactions on Systems, Man and cybernetics, Part A: System and Humans, 26, 419- 432.

NASA (2011). Probabilistic Risk Assessment Procedure Guid for NASA Managers and Practitioners second edition. NASA/SP- 2011-3421.

New Zealand Treasury (2005). Cost Benefit Analysis Primer. Business Analysis Team. Version 1.12.

NORSOK (2004). D-010. Well integrity in drilling and well operations.

Odfjell Drilling and Technology (OD&T). Overall system description. DSA well control system (2010). Internal document.

Odfjell Drilling and Technology (OD&T). Brochure of DSA (2009). Official document.

OLF – The Norwegian Oil Industry Associated (2004). Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry, The Norwegian Oil Industry association, Stavanger, Norway.

Onshus, S.H.T (2010). Reliability Data for Safety Instrumented Systems. PDS Data Handbook, 2010 Edition.PDS Forum. Trondheim, SINTEF.

OREDA – Offshore Reliability Data (2009). Subsea Equitment. DNV. Trondheim, SINTEF. Volume 2.

PTIL (2010). Main report - Trends in Risk Level (RNNP).

Rosa, E.A (1998). Metatheoretical foundations for post- normal risk. Journal of Risk Research, 1, 15-44.

Scandpower (2011). Article on homepage, Scandpower Risk Spectrum.Technology, O. D. (08.12.2011). "Overall System Descrption; DSA Well Control System." Internal Document OD&T.

Stein Hauge, M. A. L., Per Hokstad and Solfrid Håbrekke (2010). Reliability Prediction Method for Safety Instrumented Systems. PDS Method Handbook, 2010 Edition. SINTEF.

Zio E, Apostolakis GE (1996). Two methods for the structured assessment of model uncertainty by experts in performance assessments of radioactive waste repositories. Reliability Engineering & System Safety. ELSEVIER.

11.0 Appendix list

Appendix A. Deduction of the approximate formula for PFDavg/ MFDT

The average probability of failure on demand (PFDavg /MFDT) is mathematically expressed by (Abrahamsen 2011):

$$PFDavg = \frac{\int_0^\tau F(t)dt}{\tau}$$

The following assumption applies (Abrahamsen 2011):

- The components are put in operation at time t = 0
- The state of the system can only be identified at a test or at a demand
- The system is tested and if necessary repaired after regular time intervals of length τ
- After a test or a repair the system is assumed to be as good as new
- The time required to test and repair the item is considered to be negligible

The average unavailability is the mean proportion of time the system is not function. That is why PFDavg sometimes is called the mean fractional dead time (MFDT).

The unavailability at time t, $\bar{A}(t)$, denotes the probability that a system will fail to respond adequately to the demand at time t.

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

$$\bar{A}(t) = F(t) = PFD(t)$$

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

In the PFD calculation the exponential distribution is assumed:

$$F(t) \approx \sum_{j=1}^{M} \prod_{i \in kj} q_i(t) \ and \ q_i(t) \approx 1 - e^{-\lambda t}$$

, when $\lambda_\tau < 0{,}1$, we can write $F(t) \approx \sum_{j=1}^{M} \prod_{i \in kj} (\lambda_i t) dt$

, then the proof is as followed (Abrahamsen 2011):

$$PFD_{AVG} \approx \frac{\int_0^\tau \sum \prod (\lambda_i \, t) dt}{\tau} = \frac{\int_0^\tau \sum (\prod \lambda_i) t^{|kj|} dt}{\tau} = \frac{\sum (\prod \lambda_i) \int_0^\tau t_i^{|kj|} dt}{\tau}$$

$$= \frac{\sum (\prod \lambda_i) \left[\frac{t^{|kj|+1}}{|kj|+1} \right]_0^\tau}{\tau}$$

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

$$\approx \sum_{j=1}^{M} \frac{1}{|kj|+1} \prod_{i \in j} (\lambda_i \tau)$$

Appendix B. Voting factors - PDS

The PDS CMooN 2010 values are given in the table below.

Voting	1oo2	1oo3	2oo3	1oo4	2oo4	3oo4
C_{Moon}	1.0	0.5	2.0	0.3	1.1	2.9

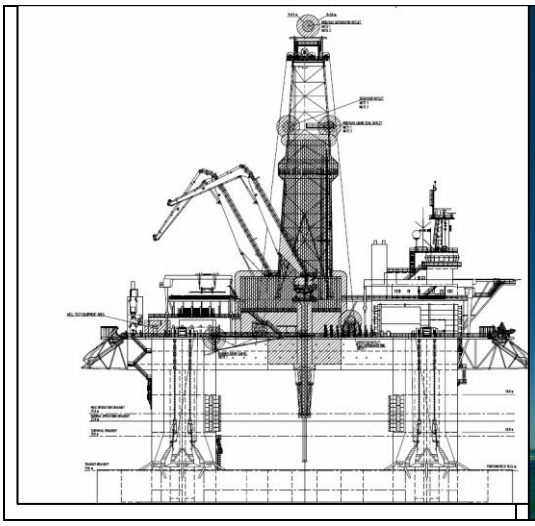
There also exist other sources for data on CMooN factors. The Swedish nuclear power inspectorate has through several reports investigated CCF. These values are in reasonable agreement with the PDS and IEC 61508 draft values, but in some voting configuration there is a major difference.

Appendix C. Deepsea Atlantic Platform

Deepsea Atlantic is a sixth generation deepwater and harsh environment semisubmersible (OD&T 2009). This unit, along with its sister platform Deepsea Stavanger, is a state of the art dual derrick, dynamic-positioned unit of enhanced GVA 7500 design. Deepsea Atlantic is designed for operations in water depths up to 3000 meters.

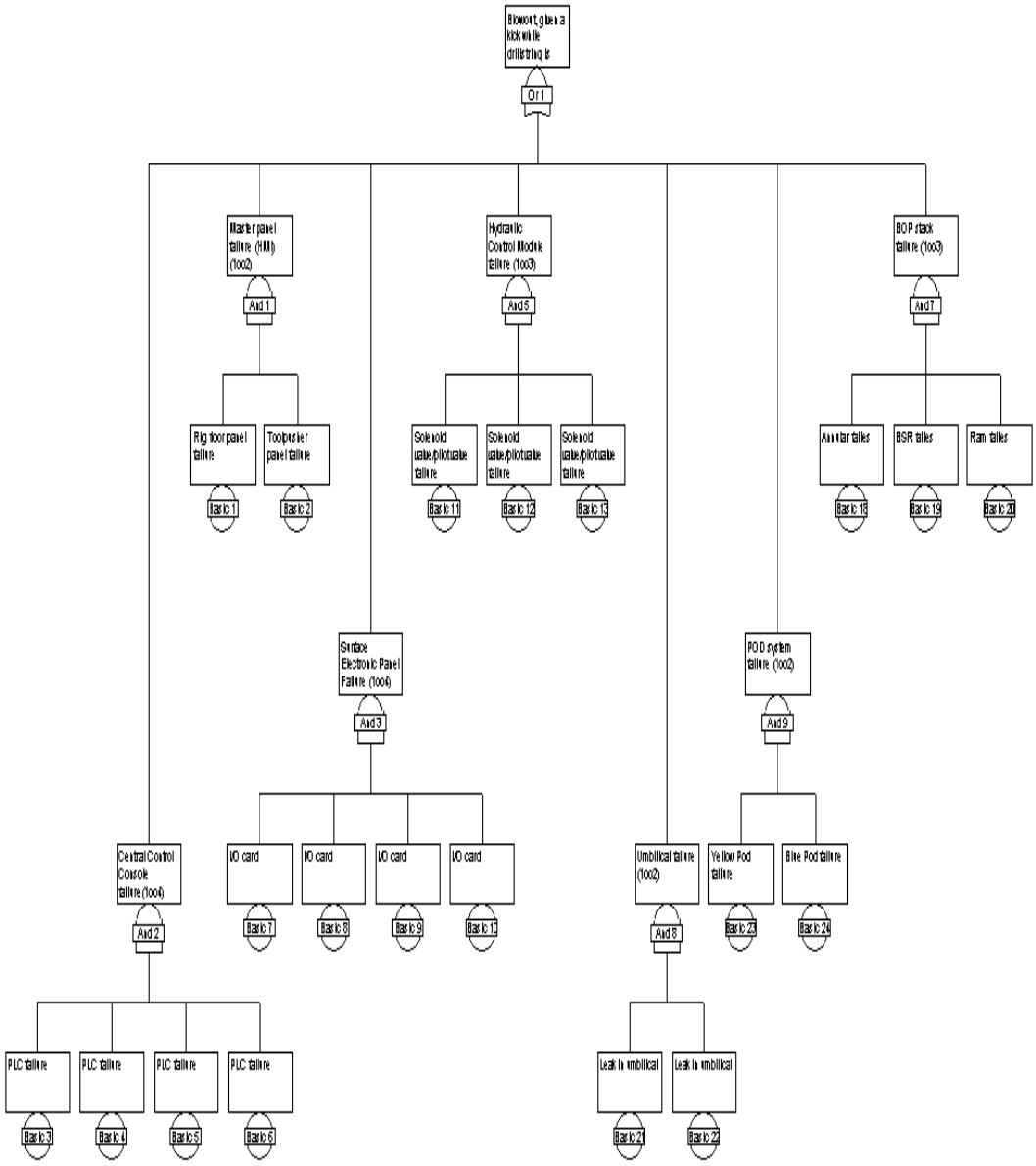
Daevoo Shipbuilding and Marine Engineering (DSME) are responsible for the engineering of the rig systems and the construction of the rig. (OD&T 2009).

See Figures below for a side view and real live picture of the rig.



Appendix D. Fault Tree of the BOP control system model on DSA

The fault Tree is constructed with use of CARA.



For further description of the symbols used in the fault tree, see Aven (2006) or Høyland & Rausand (2004).

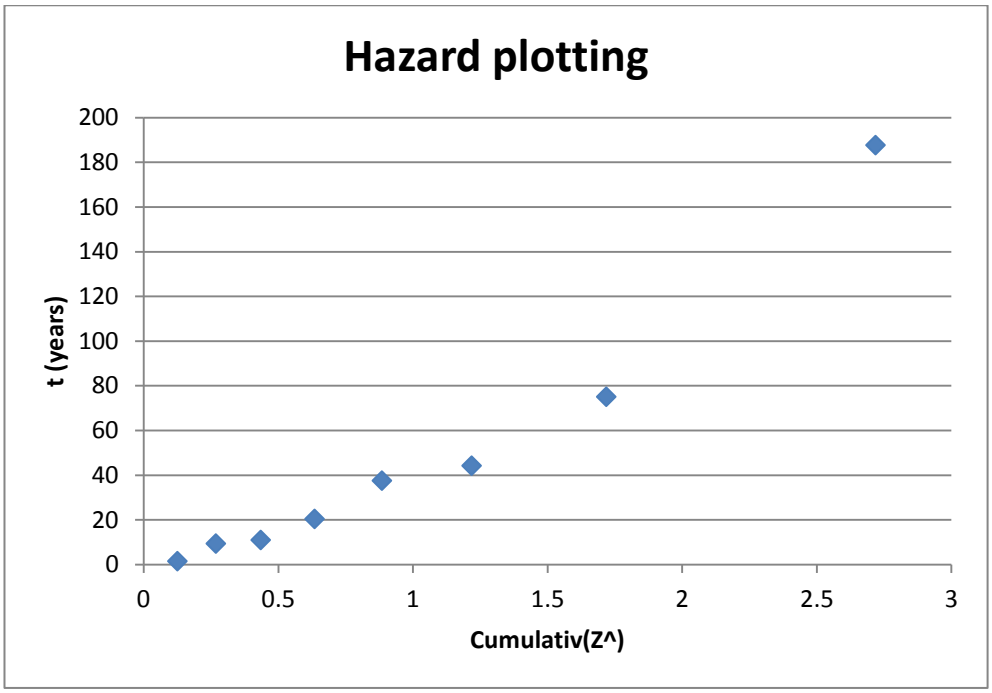
Appendix E. Input data

Components in the BOP control system	Undetected failure rate (hours)	B generic (PDS and IEC)	PTIF (hours) (PDS)	Reference
Rig Floor l and Tool Pusher Panel (1oo2)	2,00E-07	0,03	0,00001	OLF 070. ESD push down button
Standard industrial (PLC) - single system. CCC (1004)	5,00E-06	0,07	0,0005	PDS Data Handbook (2010)
Hardwired safety system-single system. (SEP).I/O (1oo4)	1,00E-07	0,03	0,000005	PDS Data Handbook (2010)
Hydraulic Control Module. Solenoid / pilot valve	8,00E-07	0,1	0,0001	PDS Data Handbook (2010)
Umbilical hydraulic/chemical line(per line) (1002)	4,00E-08	0,05	0,0005	OREDA (2009)
Yellow Pod/ Blue pod, loss of all function one pod	1,04E-05	0,03	0,0001	SINTEF-Reliability BOP study – Holand (1999)
Annular Preventer, failed to close	5,59E-06	0,03	0,0001	SINTEF-Reliability BOP study – Holand (1999)
Ram Preventer, failed to close	2,58E-06	0,03	0,0001	SINTEF-Reliability BOP study – Holand (1999)
Blind Shear Ram, function failure	2,58E-06	0,03	0,0001	SINTEF-Reliability BOP study – Holand (1999)

Appendix F. Hazard Plotting

The method is based on the estimation of the hazard Z(t) using so – called Nelson estimator, $\hat{Z}(t)$.

The result from the Hazard plotting is shown below.



For a more detailed description of the method, see Aven (2006) or Høyland & Rausand (2004).

Appendix G. Critical values of the Chi square distribution

Critical values of the χ^2-distribution

$$P(\mathcal{X}^2 > \chi^2_{\alpha,\nu}) = \alpha$$

$\nu \backslash \alpha$	.995	.990	.975	.950	.050	.025	.010	.005
1	.000	.000	.001	.004	3.841	5.024	6.635	7.879
2	.010	.020	.051	.103	5.991	7.378	9.210	10.597
3	.072	.115	.216	.352	7.815	9.348	11.345	12.838
4	.207	.297	.484	.711	9.488	11.143	13.277	14.860
5	.412	.554	.831	1.145	11.070	12.833	15.086	16.750
6	.676	.872	1.237	1.635	12.592	14.449	16.812	18.548
7	.989	1.239	1.690	2.167	14.067	16.013	18.475	20.278
8	1.344	1.646	2.180	2.733	15.507	17.535	20.090	21.955
9	1.735	2.088	2.700	3.325	16.919	19.023	21.666	23.589
10	2.156	2.558	3.247	3.940	18.307	20.483	23.209	25.188
11	2.603	3.053	3.816	4.575	19.675	21.920	24.725	26.757
12	3.074	3.571	4.404	5.226	21.026	23.337	26.217	28.300
13	3.565	4.107	5.009	5.892	22.362	24.736	27.688	29.819
14	4.075	4.660	5.629	6.571	23.685	26.119	29.141	31.319
15	4.601	5.229	6.262	7.261	24.996	27.488	30.578	32.801
16	5.142	5.812	6.908	7.962	26.296	28.845	32.000	34.267
17	5.697	6.408	7.564	8.672	27.587	30.191	33.409	35.718
18	6.265	7.015	8.231	9.390	28.869	31.526	34.805	37.156
19	6.844	7.633	8.907	10.117	30.144	32.852	36.191	38.582
20	7.434	8.260	9.591	10.851	31.410	34.170	37.566	39.997
21	8.034	8.897	10.283	11.591	32.671	35.479	38.932	41.401
22	8.643	9.542	10.982	12.338	33.924	36.781	40.289	42.796
23	9.260	10.196	11.689	13.091	35.172	38.076	41.638	44.181
24	9.886	10.856	12.401	13.848	36.415	39.364	42.980	45.559
25	10.520	11.524	13.120	14.611	37.652	40.646	44.314	46.928
26	11.160	12.198	13.844	15.379	38.885	41.923	45.642	48.290
27	11.808	12.879	14.573	16.151	40.113	43.195	46.963	49.645
28	12.461	13.565	15.308	16.928	41.337	44.461	48.278	50.993
29	13.121	14.256	16.047	17.708	42.557	45.722	49.588	52.336
30	13.787	14.953	16.791	18.493	43.773	46.979	50.892	53.672
40	20.707	22.164	24.433	26.509	55.758	59.342	63.691	66.766
50	27.991	29.707	32.357	34.764	67.505	71.420	76.154	79.490
60	35.534	37.485	40.482	43.188	79.082	83.298	88.379	91.952
70	43.275	45.442	48.758	51.739	90.531	95.023	100.425	104.215
80	51.172	53.540	57.153	60.391	101.879	106.629	112.329	116.321
90	59.196	61.754	65.647	69.126	113.145	118.136	124.116	128.299
100	67.328	70.065	74.222	77.929	124.342	129.561	135.807	140.169