University of Stavanger

Faculty of Science and Technology

MASTER'S THESIS

Study program/ Specialization:

Offshore Technology/ Risk Management

Spring semester, 2015

Open / ~~Restricted access~~

Writer:
Sharmin Sultana

…………………………………………
(Writer's signature)

Faculty supervisor: Eirik Bjorheim Abrahamsen (University of Stavanger)

External supervisor(s):

Thesis title:

A new approach of uncertainty treatment in the verification of safety integrity level of safety instrumented system

Credits (ECTS): 30

Key words:
Safety instrumented system
Safety integrity level
Uncertainty
IEC 61508
PDS
Monte Carlo

Pages: 71

+ enclosure: 7 pages

Stavanger, 15.06.2015

Date/year

A new approach of uncertainty treatment in the verification of safety integrity level of safety instrumented system

PREFACE

This master thesis is written, as a requirement to my master's degree in offshore technology in the specialization of Risk Management at the University of Stavanger during the spring semester of 2015. The title of the thesis is "A new approach of uncertainty treatment in the verification of safety integrity level of safety instrumented system".

The main objective is to investigate the treatment of uncertainty in SIL verification and the possible decision making process on the basis of the investigation. Basic knowledge of risk and reliability analysis, IEC standards and PDS method will help readers to better understand this thesis. However, it is tried to give these basic ideas in relevant sections.

I wish to thank my supervisor Professor Eirik Bjorheim Abrahamsen at the Department of Industrial Economics, Risk Management and Planning at the University of Stavanger for his invaluable suggestions, comments and advice throughout the entire master thesis project. Without his help and guidance, this intensive work would not have become possible.

Stavanger, June, 2015

Sharmin Sultana

ABSTRACT

Reliability is very important aspect of any safety instrumented system. The standard IEC 61508, widely accepted in field of reliability of instrumented systems, entails the quantification of achieved risk reduction to be expressed as a safety integrity level (SIL). The required SIL can be determined by various methods like risk graph method, risk matrix, markov process, petri-nets. The standard also instruct that reliability data uncertainty should be taken into account when calculating target PFD_{avg}.

Even in the recent past, it was common practice to overlook the existence of uncertainty. Uncertainty encountered during design, operation and maintenance should be an integral part of the decision making process, not an afterthought and should be treated with the same attention as the other requirements. The main objective of this research is to develop a systematic approach to assess the effect of uncertainty on SIL level, where SIL is determined by PDS method.

The research was motivated by five research questions: 1) How to propagate uncertainty in SIL level, where SIL is calculated by PDS method? 2) Is objective uncertainty analysis established in literature is adequate for modern system? 3) What are the limitations of this objective approach? 4) How can MTO perspectives and operational constraints be included in uncertainty analysis? 5) What should be the basis for overall decision making? To answer these questions, a literature study was performed to review existing theories, models and their prospects. The study attracts the focus to the point that there is a lack of objective along with subjective uncertainty analysis for PDS method. Few works has been done to verify uncertainty in SIL verification where SIL has been determined by reliability block diagram or risk graph method proposed by IEC standard.

PDS method uses approximated formula for SIL calculation and is said to follow conservative approach. This means calculated SIL value will show conservative result compared to the results determined by other methods. One may argue about the necessity of uncertainty analysis after getting such conservative result. Logic for this further study is to establish a structured framework for the analysis. Objective quantitative analysis is carried out with Monte Carlo simulation using @risk software applied to a practical case application of subsea well isolation system. The simulation case is checked with one programming language (Scilab) to check consistency of the result of @risk. However, this thesis does not focus on the accuracy of the result, rather more focus is given to the development of framework.

During the literature study, it is also observed that there is a lack of literature on the inclusion of MTO perspective and operational constraint in uncertainty analysis. It is termed as background knowledge in risk management point of view. Exception is the paper of Abrahamsen and Røed (2011) where the authors have proposed a qualitative uncertainty assessment of background knowledge in SIL verification. Schönbeck, Rausand, and Rouvroye (2010) in their paper also presented an approach to include human and organization factor in the operation phase of SIS. Part of this research is motivated by these two papers. Now a days wide spread research is going on to include human-organizational factors in risk analysis or others. Aramis project, bora approach, work process analysis method are such examples. A quantification method is proposed to take into account of uncertainty in background knowledge.

Final task in reliability analysis is decision making of SIL compliance. If it does not meet the requirement, one option is to modify SIS architectural configuration or modifying test interval, using highly reliable equipment. However the question may arise about the potential contribution of uncertainty result in decision making, use of suitable tool and proper phase to use. Is the result only carry significance or other factors need to be considered also? This thesis tries to cover answers of all these questions in a systematic way. Analysis are carried out with the help of a case study. To draw confident conclusions from the development, it is necessary to verify the methods with more case applications and see their effects applied in practice. Recommendations for further work are included in the final part of the thesis.

Uncertainty analysis should not be considered as an unnecessary burden, rather it should be thought as a mean to be informed about risk in the decision process that will be helpful in a broader sense to reduce risk.

Contents

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

Nothing can be more important than safety, whether it is related to our daily lives or industrial sector. Risk[1] cannot be reduced to zero level, which means absolute safety cannot be achieved, but can be reduced to a tolerable level (Redmill 1999). Safety instrumented systems are used to reduce risk to an acceptable level which is less hazardous for people, society and environment, in other word to balance between risk and profit.

Modern engineering systems and processes has become complex, both in their functionality and their interaction with environment. This growing complexity demands more capability and more advanced methodology instead of traditional methodologies. System failure does not evolve from single component failure, rather software element, human factor, operating conditions, and environmental factors play important role in the availability of safety systems.

Safety instrumented systems are comprised of input elements, logic solvers and final elements. SIL or safety integrity level is used to express the level of risk reduction. Various methods are established in industry in selecting the appropriate SIL, which is the foremost step in any safety specification. The challenge of system engineers are to design a user friendly, reliable and efficient system which is able to prevent dangerous failures/hazard. An example of such safety system is fire and gas detection system, which will give alarm on the detection of fire or gas to control room operator, so control room operator can take necessary step. In modern times, they are designed in such a way so that system can initiate further step for example controlling the process flow, prevention of material flow into the detected segment, initiation of process shutdown valve, vice versa. In such complex system, prediction of safety performance and system behavior on demand has become more difficult.

Various Methods were developed for identifying hazards and for quantifying the consequences of failures to help in decision making. Two standards IEC 61508 and IEC 61511 were established after through research and is accepted throughout the world by industry personnel. These two standard quantifies safety issue related to reliability engineering and give a direction about safety life cycle. The IEC standards define four safety integrity levels (1-4). to define safety integrity level IEC uses the terms 'Probability of failure on demand (PFD)' and 'Demand mode of operation' (Abrahamsen and Røed 2011). According to the IEC 61508 standard, PFD_{avg} should be used for low demand systems (one demand per year) (Hui Jin, Lundteigen, and Rausand 2011).

IEC standards entails that safety integrity levels for the different safety instrumented functions should be verified. In traditional approach, this verification is usually done by the calculation of PFD. If the calculated PFD is higher than the target value, risk reducing measures should be implemented (Abrahamsen and Røed 2011). In broader risk perspective, uncertainties and background knowledge should be taken into consideration. The assigned PFD is conditioned on a number of assumptions and suppositions (Abrahamsen and Røed 2011). A large number of qualitative criteria must be considered for

[1] Risk is defined as event (A), consequences (C) and associated uncertainty (U)

decision making. Many fields can be affected and the impact of a wrong decision would impact the organization.

1.1 Objective

In this thesis uncertainty treatment in SIL verification is presented and analysed with details. There are various methods for SIL calculation, established theoretically and in practice. Here, The PFD_{avg} is considered as a measure of safety integrity level. For PFD_{avg} calculation, PDS method, introduced by SINTEF, is used. Quantification of induced uncertainty in the PFD estimation is the main concern of the thesis.

To reach the main objective, sub-objectives are developed as below:

- To perform literature review for existing models and methods with the special attention to uncertainty treatment
- To propose methods for uncertainty treatment in SIL verification with focus for inclusion of MTO and operational perspectives
- To check the models with a case study of practical application
- To propose a strategy to help decision making about use of suitable model in proper phase and to propose possible risk reducing solutions

1.2 Limitations

It has been a great discussion on the industry of the best suitable method to deal with uncertainty for SIL verification. These assessments are beyond the scope of this thesis. Focus is given on uncertainty treatment for one specific method. PDS method is used for PFD calculation as it is well embraced by Norwegian oil and gas sector. A case study is chosen for better realization of the concept. System considered here is subsea well isolation system. This thesis tries to give a systematic structure in the inclusion of uncertainty in SIL estimation by PDS method. During the analysis, focus is given only to system safety. Environmental and asset protection are not focused. Hardware failure is only included in PFD calculation without taking into account of systematic failure. Only parameter uncertainty and its treatment is given importance without consideration of model and completeness uncertainty. Further is discussed in chapter 5.

The thesis focuses on the method and how to apply the mathematics, not so much on result. In semi-quantitative uncertainty assessment, uncertainty ratings and weight ratings are made anonymously, as no data exists for such type of evaluation. Uncertain factors are considered independent. Overlaps and interdependencies are not taken into account.

1.3 Structure of the report

Some prior knowledge about reliability analysis and the mathematical background of statistics and probability is beneficial when reading this report. Even so, some basic terms used in reliability analysis and SIL estimation along with uncertainty is described in relevant chapters.
Overall report have eight chapters. Chapter 1 introduces the concept of this research to the reader with its objective and limitation. Chapters 2 provides theoretical framework: the necessary background information to support the thesis work for the reader. This chapter

looks into details in some of the common terminology used in the field of reliability engineering that is related to the scope of this thesis. It also includes a review of the standards used in reliability field and a review of SIL calculation approach as described in PDS method.

Chapter 3 is the presentation of the concept of uncertainty and representation recognised in the field of risk analysis and related application. Chapter 4 identifies and discusses the existing models in literatures used in uncertainty analysis in reliability estimation. A systematic literature study is conducted and the relevant articles are sorted and selected to extract the concept. Uncertain parameters effecting the reliability estimation are also discussed in details in first part of this chapter.

In Chapter 5 possible work flow for SIL verification are presented. Models are proposed for uncertainty assessment with their framework and methodology. Of them one is semi-quantitative models and one is quantitative model. Monte Carlo simulation is proposed as quantitative analysis. Finally a strategy for decision making is proposed about the suitability of the specific method on specific situation. Chapter 6 makes a comparative study between proposed models presented in chapter 5 and existing models presented in chapter 4. Pros and cons of each models are also discussed.

Chapter 7 presents the SIL calculation for a case study of subsea well isolation system. PFD calculation are performed by making reliability block diagram following the method described in the PDS method handbook.   A description of all components used in the SIS are illustrated. Component reliability data, used is taken from PDS data handbook. At last uncertainty assessment are carried out for the case study following the methods described in chapter 5. Microsoft excel and @risk software was used for Monte Carlo simulation. a discussion is made on the results obtained from the analysis with its meaning and significance. Possible risk reducing measures are also proposed in short. Chapter 8 makes a conclusion on the achievement of this research and recommends on future work.

Appendix A presents the acronyms, mathematical notation and terminology used in the thesis.

Appendix B presents the results obtained from quantitative uncertainty analysis graphically along with the calculation procedure by @risk software. In appendix C programming codes are shown to run the simulation along with graphical result. These codes are executable with open-source Scilab software which is very closer to Matlab.

2 THEORETICAL FRAMEWORK

2.1 RELIABILITY THEORY

2.1.1 Safety instrumented systems

Safety instrumented system provides a protective layer around process system by implementing one or more safety instrumented functions. A SIS is composed of one or more sensor, logic solver and final element.

Sensors: It detects the potential or cause of an unwanted incident by producing appropriate electrical signal which is sent to logic solver (Redmill 1999). Examples are pressure transmitters, level transmitters, temperature gauges, and so on.

Logic Solver: It detects the electrical signals which exceed a given threshold and sends signal for action to the final elements (Redmill 1999). Logic solvers can be computers, programmable electronic controllers (PLCs), and relay circuits.

Final Control Element: It implements the required action as instructed by the logic system (Redmill 1999). This final control element is typically a pneumatically actuated on-off valve operated by solenoid valves.

2.1.2 Safety instrumented functions

A SIF, implemented by a SIS, detects a hazard and bring the process to a safe state (Redmill 1999).

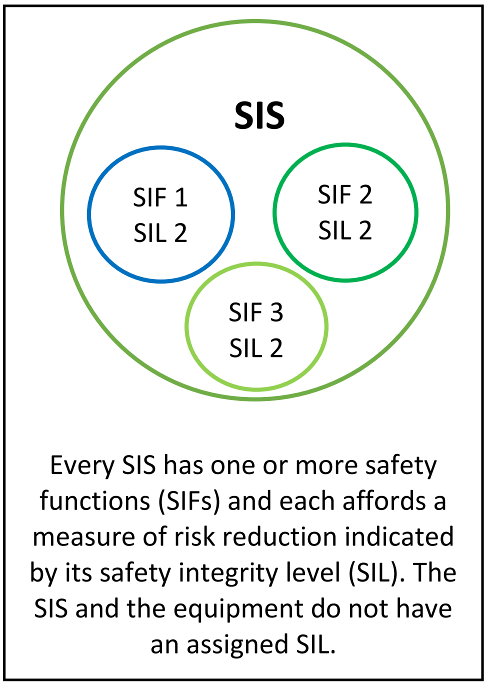

SIS
SIF 1
SIL 2
SIF 2
SIL 2
SIF 3
SIL 2
Every SIS has one or more safety functions (SIFs) and each affords a measure of risk reduction indicated by its safety integrity level (SIL). The SIS and the equipment do not have an assigned SIL.

Figure 1: SIS-SIF-SIL relationship *(Redmill 1999)*

2.1.3 Failure classification

Failures of SIS elements can be classified as dangerous and safe failures. Dangerous failure can be detected and undetected failures. Dangerous detected failures are revealed by regular diagnostic testing, but undetected failures are only revealed by proof testing. In sis reliability calculation often it is assumed that dangerous detected failures have a very less impact on the safety integrity (H. Jin, Lundteigen, and Rausand 2012).

A safe failure does not lead the SIF to an unsafe state when failed. Failures of SIS elements can also be classified as random hardware failures and systematic failures.

- A random hardware failure: Occurs due to one or more possible degradation in the hardware at a random time (H. Jin, Lundteigen, and Rausand 2012).
- A systematic failure: A systematic failure or a functional failure may be related to the design or operational procedures or other relevant factors. When systematic failure occurs, the item cannot perform its specified function though is able to operate. It cannot be easily detected by regular proof testing (H. Jin, Lundteigen, and Rausand 2012).

2.1.3.1 Common cause failure (CCF)

A CCF failure causes failure of more than one channel in a multiple channel system leading to system failure. Having same type of components or design deficiency or inadequate maintenance in redundant channel, or are located in the same area may be the reasons of CCF (H. Jin, Lundteigen, and Rausand 2012, Lundteigen and Rausand 2007). Several methods exist to describe CCFs in SIS. Beta factor model is most popular today. β is the conditional probability of a CCF, when a failure has occurred (Lundteigen and Rausand 2007).

2.1.3.2 Test-independent failures (TIF)

TIF were introduced in the PDS-method. TIF are those failures which passes the proof test, but still remain undetected. If TIF are present in the system, after proof test the system cannot retain to ‘as good as new’ condition (H. Jin, Lundteigen, and Rausand 2012).

2.1.3.3 Safety integrity requirements

Safety integrity level indicates achieved level of risk reduction implemented by safety function. Four discrete levels of safety is described in IEC standard. Each level represents the measure of risk reduction. IEC standards require that the SIS design, operation and maintenance choices must be verified against the target SIL (IEC 2000). SIL is not a measure of risk, it indicated reliability of a safety function/system required to achieve the necessary amount of risk reduction (Charlwood, Turner, and Worsell 2004).

A safety function can operate in low demand mode or high demand mode. In low demand mode, the frequency of demand of a SIS is not greater than one per year and no greater than twice the proof test frequency (Spellemaeker and Witrant 2007). In this mode, safety function is operated only when required to ensure that the equipment and environment remains in a safe state (e.g. gas detection system in boiler room). In case of high demand mode system, the frequency of demand of a SIS is greater than once per year or greater than twice the proof test frequency (Spellemaeker and Witrant 2007).

According to IEC, for these two modes of operation, the safety integrity level of a safety function should be expressed as (Spellemaeker and Witrant 2007):

- The PFD: the average Probability of Failure to perform its intended function on Demand, used in the case of low demand mode (Spellemaeker and Witrant 2007).

  The probability that a SIL 3 safety function will fail on demand is 0.1%-0.01% or in other words, it will work on demand in 99.9% to 99.99% case and associated risk reduction factor is 1000 to 10000.

- The PFH: the Probability of a dangerous Failure per Hour, used in the case of high demand or continuous mode (Spellemaeker and Witrant 2007).

Table 1: PFD and RRF (risk reduction factor) for SIL level as defined in IEC 61508 (Spellemaeker and Witrant 2007)

SIL	PFD: Low demand mode	PFH: high demand mode	Risk reduction
4	≥ 10^{-5} to < 10^{-4}	≥ 10^{-9} to < 10^{-8}	10000 - 100000
3	≥ 10^{-4} to < 10^{-3}	≥ 10^{-8} to < 10^{-7}	1000-10000
2	≥ 10^{-3} to < 10^{-2}	≥ 10^{-7} to < 10^{-6}	100-1000
1	≥ 10^{-2} to < 10^{-1}	≥ 10^{-6} to < 10^{-5}	10-100

2.1.4 Architectural constraint

For each part of the SIS, the architectural constraints are expressed by the hardware fault tolerance (HFT), which again is determined by the type of the components (type A or B), the safe failure fraction (SFF[2]), and the specified SIL.

2.1.5 Hardware fault tolerance (HFT)

The HFT expresses the maximum number of faults that a SIS can tolerate to perform the SIF. A HFT of M means that M+1 faults will cause a loss of the safety function. A KooN architecture tolerates N–K failures (faults) (Lundteigen and Rausand 2009).

The second parameter that is used to determine the HFT, is the component type. IEC 61508 defines them type A and type B components. A type component is characterized by: (i) well defined failure modes, (ii) well known behavior of the component under fault conditions and (iii) dependable field data to confirm the claimed failure rates. B type component does not fulfill one or more of these criteria.

2.1.6 Reliability block diagram

A Reliability Block Diagram (RBD) is a graphical presentation of a system showing the logical connections of functioning items needed to fulfil a specific function.

[2] SFF is the proportion of ‘‘safe’’ failures among all failures

Each component in the system is represented by a block. Reliability block diagrams are often applied to determine the PFD of a SIF.

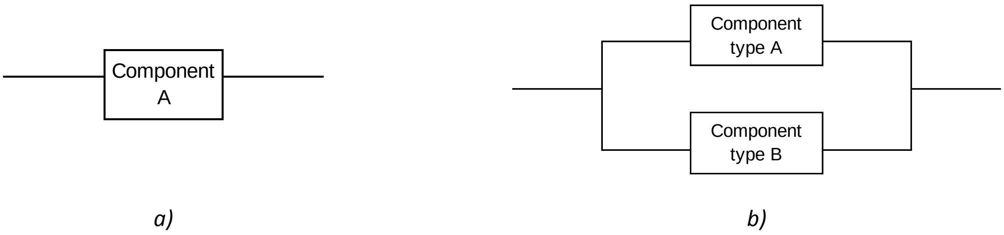


Figure 2: a) 1oo1 configuration b) 1oo2 configuration

2.1.7 Impact of testing

To keep the SIL level at the initial value, it is mandatory to perform a proof test to check the availability of the safety function. A proof test is assumed to lead the SIS to the normal situation. These tests are designed to detect random hardware failures. There is a link between the average PFD, proof test interval and the mean time to repair (Spellemaeker and Witrant 2007). A proof test can be manual or automatic.

2.1.7.1 Functional testing

Functional testing is manual test performed at definite time intervals, can be typically 3, 6 or 12 months intervals.

2.1.7.2 Automatic self-test

Modern system often have in-built-system to detect random hardware failures by automatic self-test. Moreover, as a part of self-test, the system may determine the failed modules by itself (PDS method 2013). But *all* random hardware failures cannot be detected automatically, its performance depends on voting logic and operating philosophy.

2.2 STANDARDS AND GUIDELINES

2.2.1 IEC

Various international standards are used to verify compliance with legal requirement for organization/system. IEC 61508 (generic standard applicable to all industries) and IEC 61511(applicable to only process industry) are used as a benchmark for acceptable good practice for industry by worldwide Safety regulators for industry. For estimating reliability of a SIS, the IEC standard describes a number of possible calculation approaches including analytical formula, reliability block diagrams, fault tree analysis, Markov modelling, petri nets (Innal 2008). IEC standard do not mandate one particular approach or a particular set of formulas , but leave it to the user to choose the most appropriate approach for quantifying the reliability of a given system or function (IEC 2000).

The standard specifies the risk and measures in the design of safety functions. It provides the functional safety requirements covering random hardware failure, systematic failure and common cause failures. IEC 61508 and IEC 61511 guides all necessary activities during the entire lifecycle of the systems for the *management of functional safety*. IEC 615081 entails to consider only random hardware failures in PFDavg calculations and further recommends a proper safety management program to control systematic failures. Since systematic failures do not follow the same failure processes as random hardware failures (H. Jin, Lundteigen, and Rausand 2012). The standard gives a number of requirements to reduce the systematic failures (OLF 2004).

2.2.2 OLF 70

This standard provides a guideline for minimum SIL requirements on the basis IEC 61508, IEC 61511 and gained experience with a purpose to gain adequate safety level for petroleum activities in Norway. In comparison to fully risk based perspective as described in IEC 61508, this standard will directly focus toward hazard identification and identification of deviations from minimum SIL requirement. To ensure a better performance level, stricter SIL requirement has been chosen.

OLF describe minimum SIL requirement instead of fully risk based approach as described in IEC 61508 for determining SIL requirement. It helps the organization to avoid time consuming calculations and documentation is possible. According to this guideline, in case of deviation from requirements due to technological advances or due to operational aspects, IEC 61508/61511 should be followed.

2.2.3 PDS method

The PDS method (developed by SINTEF AS, Norway) is said to account the major factors affecting system reliability during operation (PDS method 2013).

1. The model takes into account of random hardware and systematic failures and so on relevant failure causes such as:
    - Normal ageing or wear out
    - Software failures
    - Stress induced failures
    - Hardware related failures
    - Installation failures
2. The model accounts for common cause failures and the effect of testing.

2.2.3.1 Operational failures

PDS method counts safety unavailability due to systematic failures and random hardware failures. The PDS method uses extended β factor model which depends on the voting configuration (PDS method 2013).

2.2.3.2 Contributions to Loss of Safety

PDS identifies three main contributors to loss of safety or safety unavailability (PDS method 2013). They are:

- PFD: Unavailability due to dangerous undetected failures
- P_{TIF}: Unavailability due to TIF failures
- DTU: Unavailability due to known or planned downtime

2.3 PFD CALCULATION BY PDS METHOD

Main input parameters for the PFD calculation:

λ_{DU} = Rate of DU (Dangerous Undetected) failures
τ = Test period for manual functional testing
β = Beta factor value

For a single (1oo1) component the PFD can be approximated by: $PFD_{1oo1} \approx \lambda_{DU}.\tau/2$

2.3.1 Calculation of common cause failures and **β** factors

In PDS method uses an extended or modified version of beta factor model. Some assumptions in this version, are different from actual beta factor model. In this model, the rate of common cause failures explicitly depends on the configuration of system. Beta factor of a MooN voting logic may be expressed as:

$\beta\ (MooN) = \beta.C_{MooN}$ (M<N) (PDS method 2013)

Where, C_{MooN} is a modification factor for various voting configurations.

The system failure rate due to CCF of MooN configuration = $C_{MooN}.\beta.\lambda_{DU}$

For N different components voted MooN, PFD subjected to CCF then becomes (PDS method 2013):

$$PFD_{MooN}^{(CCF)} = C_{MooN}.\beta_{min}.\sqrt[N]{\lambda_1.\lambda_2 \ldots .\lambda_N}.\bar{\tau}/2$$

For a duplicated module, voted 1oo2, PFD, including common cause failure and contribution from independent failures (PDS method 2013):

$$PFD_{1oo2} \approx \beta.(\lambda_{DU}.\tau/2) + (\lambda_{DU}.\tau)^2/3$$

Table 2: Summary of formulas for PFD for duplicated system (PDS method 2013)

Voting	PFD calculation formulas		
	Common cause contribution		Contribution from independent failures
1oo1	-		$\lambda_{DU}.\tau/2$
1oo2	$\beta.(\lambda_{DU}.\tau/2)$	+	$((1-\beta)(\lambda_{DU}.\tau))^2/3$
2oo2	-		$(2-\beta).\lambda_{DU}.\tau/2$
1oo3	$C_{1oo3}.\beta.(\lambda_{DU}.\tau/2)$	+	$((1-1.5\beta).\lambda_{DU}.\tau).3/4$

Table 3: Numerical values for configuration factor, C_{MooN} (PDS method 2013)

M/N	N = 2	N = 3	N = 4	N = 5
M = 1	C_{1oo2} = 1.0	C_{1oo3} = 0.5	C_{1oo4} = 0.3	C_{1oo5} = 0.2
M = 2	-	C_{2oo3} = 2.0	C_{2oo4} = 1.1	C_{2oo5} = 0.8
M = 3	-	-	C_{3oo4} = 2.8	C_{3oo5} = 1.6
M = 4	-	-	-	C_{4oo5} = 3.6
M = 5	-	-	-	-

2.3.2 Calculation for multiple SIS

For a multiple SIS comprising of two layers, the average PFD of the multiple SIS can be calculated as:

PFDavg = CF . PFDavg(SIS1). PFDavg(SIS2)

Where CF is a correction factor and depends on a voting logic, Using CF will give a conservative result.

Table 4: Correction factors for multiple SIS (PDS method 2013)

Number of SISs	**CF**
1	1
2	1.33
3	2
4	3.2
N	$\frac{2^N}{N+1}$

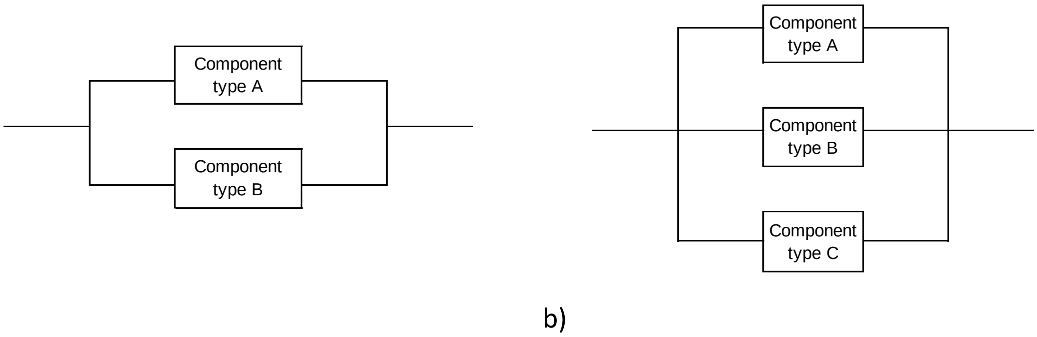


Figure 3: a) 1oo2 configuration b) 1oo3 configuration

Taking into consideration of common cause failures and independent failures, following formulas are applied to calculate PFD for multiple SIS:

$$PFD_{1oo2} = CF_{1oo2} * PFD_A * PFD_B + C_{1oo2}.\beta\sqrt{PFD_A * PFD_B}$$

$$PFD_{1oo3} = CF_{1oo3} * PFD_A * PFD_B * PFD_C + C_{1oo3}.\beta\sqrt[3]{PFD_A * PFD_B * PFD_C}$$

3 CONCEPT OF THE UNCERTAINTY AND REPRESENTATION

3.1 CONCEPT OF UNCERTAINTY

Uncertainty means the state of being uncertain or something that is uncertain or that causes one to feel uncertain. The term uncertainty is used different ways in different fields.

In the scientific world, representative model or theory is used to describe the real phenomena. To establish the model, several assumptions are made, which is done on the basis of background information. For modern complex applications the number of background assumptions increases. Often the analyst becomes unsure about the choice of theoretical model, adequacy and accuracy of the model.

Uncertainty arises due to the following facts (Oberkampf and Roy 2010):

- Lack of adequacy and level of detail to represent the physical system properly
- Lack of adequacy and accuracy of the model or theory for particular proposed application
- Deviation between the real world and simplified representations in models.

Before treatment of uncertainty, it is important to know the sources of uncertainty which can be evolved from Inherent uncertainty in random variables, from the selection of the probabilistic or physical sub model, measuring or observation error, computational or numerical error (Kiureghian and Ditlevsen 2009).

3.1.1 Classification

Uncertainty is classified in different ways in different fields. Scientists often distinguish uncertainty as aleatory and epistemic as they originate from different conditions. Aleatory, also referred as stochastic or objective uncertainty, arises due to randomness property in the inherent variability of the system or nature. Variables describing the system are not always known to the sufficient degree to possibly assign the variable to a constant.

Epistemic uncertainty evolves due to imprecise knowledge about the system. This type of uncertainty can be reduced by further analysis of the problem and experiments. Both types of uncertainty can be described by the probability distribution of the variable (Zio 2013).

Sometimes it is difficult to distinguish between these two types of uncertainties. With increment of new knowledge, the epistemic uncertainty will be reduced. While the aleatory uncertainty is inherent in system behavior and cannot be reduced. Different mathematical structures (probability or possibility or combination of both) can be used in the same analysis to represent aleatory and epistemic uncertainty (Helton et al. 2008 , Kiureghian and Ditlevsen 2009).

In nuclear industry uncertainty is classified as parameter uncertainty, model uncertainty and completeness uncertainty.

3.1.2 Parameter uncertainty

This uncertainty evolves due to imprecise knowledge about the parameters and other model input. It is related to the uncertainty in the computation of input parameter values to quantify the model or due to lack of accuracy of assigned parameter values in the physical model. In reliability application, such parameter can be component failure rates and probability.

These uncertainties are often characterized by probability distributions which expresses the analyst's degree of belief about the values of these parameters. Many methods are available for parameter estimation from experimental data, e.g. Bayesian, maximum likelihood.

3.1.3 Model uncertainty:

This uncertainty arises due to the difference between model and reality. This is related to the effectiveness of the model to reproduce the physics of the system due to limitation of computational model or coding error. (Oberkampf and Roy 2010)

3.1.4 Completeness uncertainty

This uncertainty can be known uncertainties (which were not included in the model) or unknown uncertainties. This uncertainty cannot be properly quantified and it is difficult to estimate its magnitude, because it represents those aspects of the system which was not addressed in the model.

In the following, there are some examples how this uncertainty can arise:

- Methods of analysis have not been developed for some issues or for specific application.
- Resources to develop the complete model is limited.
- Some phenomena, knowingly or unknowingly, was omitted because their existence was not recognized.

3.2 Representation

Scientist expresses different opinions for the presentation of uncertainty. Some scientists like Lindley, Oakley suggests only probabilistic approach for the representation of uncertainty. Whereas others (e.g. Terje Aven) proposes semi-quantitative approach, which postulates that risk and uncertainty cannot be expressed in full dimension by any mathematical or probability formula (Aven et al. 2014). Aven et al. (2014) identifies five measures for the uncertainty representation in the context of risk analysis:

- Probabilistic approach
- Non-probabilistic approach with help of interval probabilities
- Non-probabilistic approach with help of other than interval probabilities
- Hybrid approaches
- Semi-quantitative methods

3.2.1 Probabilistic approach

Probability is a measure of expressing uncertainty of the possible outcomes, on the basis of assessor's background information and knowledge. It is said to well represent aleatory uncertainty in the presence of lots of historical data or strong background knowledge.

3.2.2 Interval analysis

The interval analysis is useful when only the bounds of a quantity is known without any other knowledge which refers to weak background knowledge. It can be used to propagate uncertainty of input parameters with the help of a model. The analyst may reflect his limited knowledge and associated uncertainty through an interval specification (Aven et al. 2014).

Interval analysis may be represented as:

Xi = {xi : ai ≤ xi ≤ bi}

Where, Xi is set of possible value of variable xi, and [ai, bi] is the interval range that contains the possible values of xi.

Pros: This concept is computationally inexpensive and consistent which produces conservative result of an analysis. It is a straightforward method that generalizes the worst case analysis (Abrahamsson 2002).

Cons: Often in times, interval may become wide rages which will produce less useful result in real-life situations. More information of the parameters cannot be obtained except only the ranges, which often shows excessive conservative results (Abrahamsson 2002).

3.2.3 Probability interval or imprecise probability

Upper and lower probabilities are more appropriate than precise probabilities in case of poor knowledge. It is a generalization of probability theory through the use of a lower probability and an upper probability where 0 ≤ P(A) ≤l 1 where probabilistic model relies incomplete statistical information (where the mean value or the variance are ill-known , only a set of conditional probabilities is available) (Baudrit and Dubois 2006).

Pros: It can deal with uncertainty in parameter values, distribution shapes, dependencies and model form, which is very advantageous (Abrahamsson 2002).

Cons: In case of repeated occurrences of parameters, it is difficult to obtain optimal bounds. Different kinds of uncertainties cannot be analyzed separately by this method (Abrahamsson 2002).

3.2.4 Possibility theory

Possibility theory uses a pair of dual set functions called possibility and necessity measures. π(x) expresses the degree of the possibility of x. π(x) = 0 means that the outcome x is an impossible situation, whereas π(x) = 1 indicates that the outcome x is possible or normal (Aven and Zio 2011).

3.2.5 Evidence theory

The evidence theory (Shafer, 1976) provides two quantitative indicators to describe uncertainty. The belief ($Bel\ B$) and the plausibility ($Pl\ B$) functions both qualify the validity of the statement that the values of the variable X (with mass distribution (A)) fall into set B (Aven and Zio 2011). Mathematically, $Bel\ B$ and $Pl\ B$ are defined as:

$Bel\ B$ = (Ai),$\subseteq B$ and $Pl\ B$ = $v\ Ai\ Ai$,$Ai \cap B \neq \emptyset = 1 - Bel\ B$ (18)

3.2.6 Semi-quantitative approach

Semi-quantitative approach is a hybrid approach integrating both quantitative and qualitative framework to represent uncertainty. This approach represents a qualitative characterization of the background knowledge K of the output to capture aspects beyond quantitative numbers. This approach consumes the belief that uncertainty cannot be accounted in full scope by a quantitative probabilistic or any other formula. Uncertain factors concealed in the background knowledge should be assessed qualitatively (Aven and Zio 2011). The uncertainty can be characterized in the format Q= (P, U_F), where U_F denotes a qualitative characterization of uncertainty factors in the background knowledge K on which P is conditional (Aven et al. 2014).

3.3 Uncertainty propagation

Uncertainty propagation: methods for propagating the uncertainty in input parameters onto the output from the analysis.
If the model can be described such that, Y is the function of x:

$Y = \{y: x \in X \text{ and } y = F(x)\}, X= X_1, X_2\ldots X_n;$

An analysis outcome y = F(x) will have an uncertainty structure associated with uncertain structure x. If there is no uncertainty in the values of X, there is also no uncertainty in x and as a sequence to Y. the uncertainty associated with y may be represented by possibilistic or probabilistic method in consistent with the uncertainty representation of x. An exact determination of the uncertainty of y is usually not possible in a real analysis (Rausand 2005).

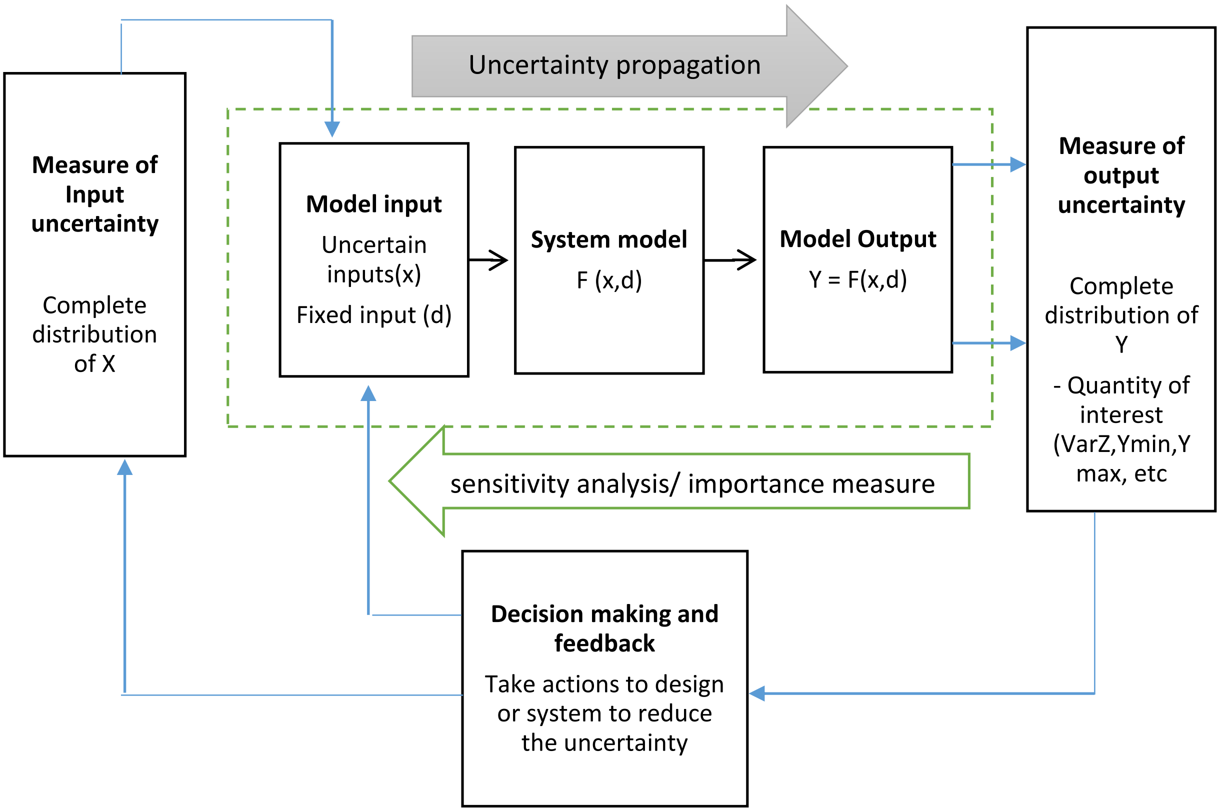

Uncertainty propagation
Measure of Input uncertainty
Complete distribution of X
Model input
Uncertain inputs(x)
Fixed input (d)
System model
F (x,d)
Model Output
Y = F(x,d)
Measure of output uncertainty
Complete distribution of Y
- Quantity of interest (VarZ,Ymin,Y max, etc
sensitivity analysis/ importance measure
Decision making and feedback
Take actions to design or system to reduce the uncertainty

Figure 4: Framework for uncertainty propagation (G. Rausand 2005)

Methods of uncertainty propagation can be classified as level 1 and level 2 setting depending on the type of uncertainty effecting the model input (Aven et al. 2014). For a level 1 setting, input quantities which are subjected to aleatory uncertainty are only considered for propagation in the output result. A level 2 uncertainty propagation setting applies if the input quantities X (subjected to aleatory uncertainty) are conditioned on parameter ϴ (subjected to epistemic uncertainty) (Aven et al. 2014). Aleatory uncertainties in X are described by frequentist probabilities. If the analyst has strong background knowledge about process or system, then all the epistemic uncertainties are removed and level 2 setting transforms to the level 1 setting (Aven et al. 2014).

Three setting are commonly discussed for uncertainty propagation in level 1 setting (Aven et al. 2014):

- Purely probabilistic framework
- Purely possibilistic framework
- Hybrid (probabilistic-possibilistic) framework

3.3.1 Sampling based approach

Sampling based uncertainty propagation can be a purely probabilistic framework or a purely possibilistic framework. Sampling-based procedures generates sample Xi= {X_1, X_2 … X_N,} for i = 1, 2... n. Uncertainty in with y = F(x) is derived by association with uncertain x.

Monte Carlo simulation or Latin hypercube sampling are two methods to carry out sampling based uncertainty propagation in a purely probabilistic framework.

3.3.1.1 Monte Carlo Simulation

MCS involves two steps. First, uncertain input variables, X, are generated according to their specified probability distributions which represents the random realization of X. Assuming there are n input variables, n random variables are generated and y are evaluated for these samples in the next step. This procedure is repeated N times yielding N values of y. These N values of y can be represented by the PDF or CDF where the mean and other statistical characteristics of interest can be calculated.

Pros: Implementation of this procedure is simple and user friendly software is available. The total distributions of the output can present the uncertainty of the model fully. One can use the information of correlations and dependencies between the variables to see the impact in the final results (Abrahamsson 2002).

Cons: To perform the analysis, a great deal of empirical information is necessary, e.g. the distributions of all variables and their correlations and dependencies, Lack of which may lead to make questionable assumptions (e.g. independence about system interaction) leading non-protective results. In this approach different kinds of uncertainties are not propagated separately.

3.3.1.2 Latin hypercube sampling

Latin hypercube sampling works in a quite similar way to Monte Carlo sampling. First probability distribution for xi set are constructed, where xi =[x1, x2… xn]. The range of xi is divided into equal probability interval and one random value of xi is selected from each interval (Helton et al. 2008). These randomly selected x1 values are paired with x2 values

without replacement. Again this pair is combined with x3 to form triplets. Process is continues in such a way to produce Latin hypercube sample (Helton et al. 2008).
Pros: It is a good choice to study computationally demanding models (Helton et al. 2006).
Cons: Less effective if large sample sizes are required to provide for appropriate coverage of low probability and high consequence (Helton et al. 2006).

3.3.1.3 Two-phase sampling procedures

Two-phase sampling procedures are suitable for level 2 propagation setting, where it is preferable to keep stochastic or epistemic uncertainties (stochastic or epistemic) separate in the analysis,. This can be based on traditional MC sampling or Latin hypercube procedure. The sampling is performed in two “loops”. For each iteration in the outer loop (the values are sampled for the parameters subjected to epistemic uncertainty), a specified number of iterations is performed in the inner loop (a value is drawn for the parameters subjected to aleatory uncertainty). In the problem of risk analysis where it is desirable to keep distinct the epistemic and aleatory uncertainty, this model is used. Normally, the variables which are subjected to epistemic uncertainty are sampled in the outer loop and the variables which are subjected to aleatory uncertainty are sampled in the inner loop.

Pros: The most obvious advantage is that it distinguishes between different kinds of uncertainty.

Cons: Not capable to handle uncertainty in distributional shapes. Calculations are quite complex and computational time increases rapidly in complex models.

3.3.2 Fuzzy set theory

Many studies have been carried out on the application of fuzzy sets theory which is based on purely possibilistic framework. A fuzzy probability, represented by a fuzzy number, can be 0 to 1 assigned according to the probability of an event occurrence. Membership function for fuzzy probability can be different, between [0, 1], where 0 represents less confidence and 1 indicates more confidence (Sallak, Simon, and Aubry 2008). Fuzzy arithmetic, another representation of possibility theory, is a generalization of interval analysis. Fuzzy number approach is appropriate when sufficient statistical data are not available.

Pros: Computations of fuzzy arithmetic is easy and does not require detailed empirical information. One can use subjectively assigned distributions in the event of sparse empirical information. Dependencies and correlations between parameters need not be specified as this method is fundamentally conservative (Abrahamsson 2002).

Cons: Some criticism has been raised in the risk analysis community about the fundamentals of the method. The level of conservatism is not clear. Repeated parameters may constitute a computational problem as the case of interval analysis. Different types of uncertainty cannot be separately analysis in this method (Abrahamsson 2002).

4 Uncertainty assessment in reliability estimation

4.1 Uncertain parameters in reliability estimation

Uncertainty expresses our degree of knowledge about the safety instrumented system. One input in SIS design is hardware safety integrity level (SIL) which can be expressed as the probability of failure on demand (PFD) for the low demand system (according to IEC 61508). Other inputs are related to systematic safety integrity and software safety integrity. Decision makers may have to balance safety requirements with production availability and maintenance strategies.

The calculated PFD is influenced by three main factors: (i) the model, (ii) the data, and (iii) the calculation approach. Our ultimate goal is to arrive at a decision regarding safety integrity level that will keep the system safe.

The PFD may be calculated by using mathematically exact expressions or approximation formulas. The Choice of the model is a great question concerning which model will be less uncertain. Level of uncertainty in various models is out of the scope of present work. In this thesis focus is limited to parameter uncertainty and PDS method.

In reliability estimation, uncertain parameters can be component failure rates, beta factors, functional test intervals, mean repair times, mean restoration time, diagnostic coverage[3] and so on (H. Jin, Lundteigen, and Rausand 2012)(Wang, West, and Mannan 2004) . The level of uncertainty in the input data may be influenced by many factors which is discussed here.

4.1.1 Failure rate data

- In reliability calculation, constant failure rates are assumed which means elements do not have any deterioration while operation. This assumption may be valid for some electronic and electrical components. But in offshore production or subsea where the components are left for a long time in the harsh environment with minimum maintenance, this assumption may become invalid (H. Jin, Lundteigen, and Rausand 2012, Hui Jin 2013)
- Database (e.g. OREDA), is based on data from components installed a long time ago. Failure rate estimates may become invalid due the advanced technology used in the new SIS (H. Jin, Lundteigen, and Rausand 2012, Hui Jin 2013)
- Database (e.g. OREDA) is based on recorded maintenance actions which may not cover those failures which was performed without any formal maintenance (H. Jin, Lundteigen, and Rausand 2012)
- Some failure rate data include items replaced during preventive maintenance which should be excluded, but not always possible in practice. This can affect failure rates (Smith. 2001)
- Failure rates may be affected by the tolerance of a design, as a consequence may vary from database value

[3] A fault coverage factor (Diagnostic coverage, DC) is introduced to quantify the efficiency of the self-test. This factor equals the fraction of failures being detected by the automatic self-test (PDS method 2013)

- It is assumed that standby units have identical constant failure rates similar to the main unit and do not fail when idle (Smith. 2001)

4.1.2 Availability

- For subsea, repair of a failed component may take several weeks depending on the system and weather conditions. Sometimes the team has to wait several months due to unavailability of the intervention rig. In this case repair time cannot be assumed as negligible (M. Rausand and Høyland 2004).
- While waiting for repair failed item may not function as a safety barrier. This unavailability is different from the unavailability in the test interval (M. Rausand and Høyland 2004). Restoration time should be considered in reliability calculation instead of repair time.
- For a safety system, failure of a single component may not lead to the unavailability of safety function for which it was installed. From maintenance data of failure record, it may not become always clear whether the component failure was the reason for system failure or not. Uncertainty may exist in the capability of the system to function after failure of one or more components.

4.1.3 The environmental condition

- Effect of environmental and quality assurance levels on the range of parameters are another source of variability (Smith. 2001).
- System condition or environment under study can be different from which data were collected (Smith. 2001).

4.1.4 Operational constraint

PFD may not cover all operation aspects of SIS failure, so in real situation experience may be different from theoretical assessment.

4.1.5 Common cause failure and β factor

Uncertainty increases with increasing complexity, due to the difficulty of constructing adequate architecture and reliability models. Systems are characterized by their degree of coupling[4]. In PFD calculations, a comprehensive set of data is needed to determine the degree of coupling. It is often difficult to collect detailed data, especially for the oil and gas industry where limited focus is given to CCFs in the data collection process. For this reason, it is assumed that uncertainty increases with increasing coupling. Other factors are as bellows:

- CCF rates are highly dependent on operational and environmental conditions. Therefore, it is difficult to claim that a CCF rate will be similar to all installation (H. Jin, Lundteigen, and Rausand 2012, Hui Jin 2013).
- The OREDA database does not distinguish between independent failures and common cause failures since data were collected from the single maintenance report (H. Jin, Lundteigen, and Rausand 2012).
- β-factor model seems adequate for parallel systems with two components but may not fit for more complex systems. A serious limitation is that it does not allow the

[4] The 'Coupling' expresses the degree of dependencies between system components, and may vary from loose to tight.

failures of a certain fraction of the components as common cause failures (M. Rausand and Høyland 2004).

- Dependency other than CCF (e.g. cascading failure, negative dependencies) are not covered in the calculation (H. Jin, Lundteigen, and Rausand 2012). systematic failure was not considered in the availability calculation (H. Jin, Lundteigen, and Rausand 2012).

4.2 RANKING UNCERTAIN PARAMETERS OR COMPONENTS

Dealing with uncertainty is one of major challenges in complex systems. One way to perform the uncertainty analysis used in the industry is to rank the parameters or components with respect to their contributions to the uncertainty in the model prediction. This approach identifies the most critical components which affect most on SIL level determination. The configuration of these critical components can be modified then to reduce the SIL uncertainty. PFD is computed for various possible configurations (e.g. series or parallel) and overall decision is made.

Sensitivity analysis illurstrates how the changes in one input parameter affect the output. It is used in industry to identify the critical parameters or components and to rank with respect to reliability and risk. Importance measures shows the relative contribution of the uncertainty in one input parameter in relation to the uncertainty in the output.

A number of importance ranking measures have been developed, for example Birnbaum's measure, the improvement potential measure, and the Fussel-Vesely's measure (T. Aven and Nøkland 2010).

Birnbaum measure is defined as the partial derivative of the system reliability with respect to component reliability. This measure ranks components according to the effect of a small change in component reliability to the system reliability (T. Aven and Nøkland 2010). It can be used if concerned about small changes in a component's reliability.

Importance measures are used to rank the importance of the components with respect to uncertainties. This measure expresses the maximum potential improvement in system reliability that can be obtained by improving the reliability of component i (T. Aven and Nøkland 2010). In general, birnbaum measure is used in operation whereas the improvement potential is typically used in a design phase (T. Aven and Nøkland 2010).

Risk achievement worth, Fussel vesely's importance measure are other two importance measure used in reliability applications (More details can be found in T. Aven and Nøkland 2010).

Advantage of Importance Measure is that, the knowledge of how input uncertainty influences the uncertainty in output advises to direct the limited resources to the most influential parameters or components in terms of reducing uncertainty and improving system safety (Aven and Nøkland 2010). For the new installation, especially in the design phase, this approach will give valuable direction for decision making.

However, situations may occur where the modification of the configuration of critical components are not possible (e.g. an existing platform installed a long time ago). In this case, this type of analysis will be useless. In fact, sensitivity analysis is a method to reduce uncertainty. By identifying critical components and by modifying architecture of components, uncertainty can be reduced from the system without being aware of the overall uncertainty. More detailed investigation is necessary for complete uncertainty analysis which will be able to give all information regarding the uncertainty in variables.

4.3 EXISTING MODEL FOR UNCERTAINTY ASSESSMENT IN RELIABILITY ANALYSIS

4.3.1 Standard Monte Carlo approach

Sampling based method- Monte Carlo is often used to investigate the effects of the uncertainties on SIL determination. Data sampling of uncertain input parameters is carried by assigning relevant probability density function. For each MC simulation run, random values for each uncertain parameter is obtained and then used as an input to calculate target SIL based on PFD. The uncertainties on input parameters (reliability data) can be modeled using relevant probability distributions. MC sampling presents the effects of uncertainty of input parameters to the final outcome (PFDavg). Analysis can be standard or two phase setting. Standard setting is used to deal with aleatory uncertainty.

Innal, Dutuit, and Chebila (2013) has used MC simulation to propagate uncertainty in SIL determination. They followed the following steps:

- Probability density function (pdf) is constructed for each input parameter which expresses the knowledge about the value of the parameter. Randomness of all input parameters are (λ_D, DC, β, β_D, MTTR and T_1) considered for each subsystem. seven different probability distributions (Uniform, Triangular, Normal, Lognormal, Chi-square, Beta and Gamma) are implemented for input parameters for comparison
- Random numbers for all variable input parameters are generated according to assigned pdfs
- The output function (PFDavg) is quantified using the set of random values which expresses the realization of a random variable (X)
- The steps are repeated n times. These *n* output values represent the probability distribution of the output function. Statistics are generated from this outcome e.g. mean, standard deviation, confidence interval, percentiles, etc.

4.3.2 Fuzzy set theory

Fuzzy set theory can be applied to propagate uncertainty in SIL estimation. *In Fuzzy Probabilistic Approach,* the uncertainty of components failure probabilities are expressed by fuzzy probabilities (Sallak, Simon, and Aubry 2008). Any shape (trapezoidal, peak, normal,) can be chosen to compute fuzzy probability. Fuzzy SIS PFD can be estimated from the fuzzy probabilities of components failure (Sallak, Simon, and Aubry 2008).

One can see the work of **Sallak, Simon, and Aubry (2008)** where they used fuzzy probabilistic approach to determine SIL of SIS applied to a process example and compared it with conventional probabilistic approach. Their finding was that the two approaches give similar result. To reduce uncertainty of SIS, they proposed a method called fuzzy probabilistic importance measure. This method finds the critical component is SIS and then uncertainty can be reduced by modifying component architecture.

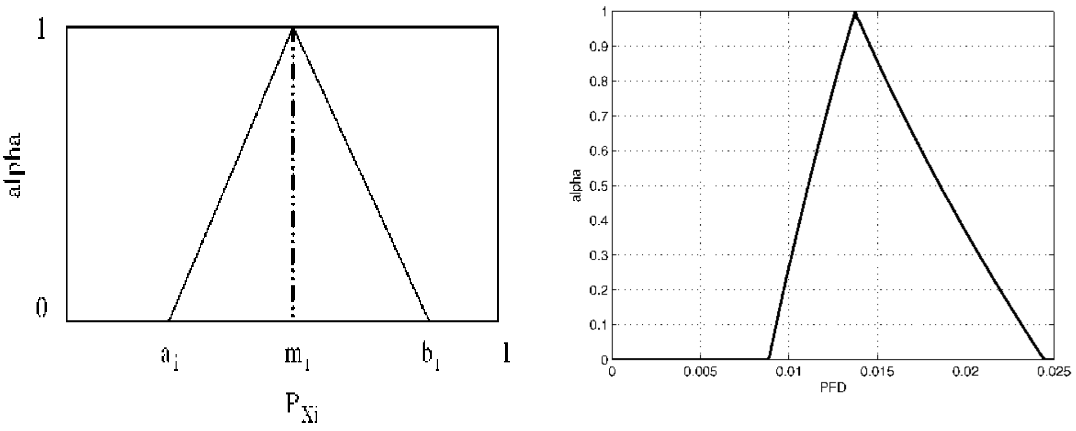


Figure 5: a) Fuzzy probability of component failure (Sallak, Simon, and Aubry 2008); b) The fuzzy SIS PFD (Sallak, Simon, and Aubry 2008)

Sungteak Kima and others (Kima et al. 2014) has performed uncertainty analysis, using fuzzy set approach and sampling-based method for two different SIL determination methods which are risk graph and OLF 070 minimum SIL requirement. Moreover, two PDS model has been used for comparison. The first PDS model, takes into account the probability of test independent failure (PTIF) to reflect the effect of incomplete testing and does not consider common cause failure. In the second PDS model, proof test coverage (PTC) is added as input parameters instead of PTIF.

Result show that Fuzzy set and sampling approach (applied to first PDS model) gives similar SIL output when uncertainties are considered. However for the same SIS, result gives different SIL output for 2nd PDS method. It is said that, reason for this difference is due to difference in model for PFD estimation. PTC shows much sensitivity and are more vulnerable than other parameters. Trustworthy and reliable database dealing with PTC does not exist yet.

Mechri, Simon, and Ben Othman (2011) in their paper studied uncertainty analysis in SIL qualification by fuzzy approach. Epistemic and aleatory uncertainties in the values of CCF factors in a SIS are modelled by fuzzy numbers. They compared the result with probabilistic approach (second order) and showed that this approach gives same result as MC sampling in a short computing time and with less effort.

Fuzzy set approach is appropriate for uncertainty analysis on SIL determination where SIL is determined by risk graph model in case of lack of sufficient data. Realistic approximate values can be modelled with help of Fuzzy number approach in case of lack of knowledge to choose precise values. For a fuzzy risk graph, a range of SIL value (SIL 1 to SIL 3) may be obtained from which dominant SIL value is taken as target SIL. However, limitation of this approach is that, a situation may occur when there is no dominant target SIL value (e.g., relative frequency of 35%, 35%, and 30% respectively for SIL 1 to SIL 3). For this case, target SIL is determined by using median or mean value. However, it is problematic for the decision makers to make a reasonable decision. The similar problem may evolve for MC sampling.

4.3.3 Recommendation in the guidelines

IEC 61508 recommends two procedures (Route 1H and Route 2H) to overcome the previously mentioned difficulties (in section 4.1) in the PFD calculation. Both ways helps to determine maximum SIL of the safety function. Route 2H is based on uncertainty analysis.

4.3.3.1 Route 2H: Uncertainty analysis

The IEC 61508 stipulates that If Route 2H is selected, then the reliability data uncertainties shall be taken into account when calculating the target failure measure (i.e. PFDavg) and the system shall be improved until there is a confidence greater than 90 % that the target failure measure is achieved (Innal, Dutuit, and Chebila 2013).

The requirement of this procedure is as below:

- “The failure rates data used should have a confidence level of at least 70%”. To meet this requirement, it is advised to express the failure rate with a probability distribution which expresses our belief in randomness of the failure rate (H. Jin, Lundteigen, and Rausand 2012, p-2).
- “A confidence level of at least 90% shall be demonstrated on the reliability estimates, in the selection of hardware architectures” (H. Jin, Lundteigen, and Rausand 2012,p-2) . Monte Carlo simulation or fuzzy set can be used to fulfil this objectives. Overall objective is to demonstrate that the obtained value for PFDavg of the SIS performing a specified safety function belongs to the required SIL zone with probability of 90% (H. Jin, Lundteigen, and Rausand 2012).

To reduce uncertainty, the PDS method considers some additional factors in the SIS reliability calculations: (i) Test independent failures (TIF) that remain unrevealed during proof testing, and (ii) consideration of systematic failures in failure rates (H. Jin, Lundteigen, and Rausand 2012). It is said that random hardware failures only represent a limited fraction of the actual failures, so systematic failures should be included to predict the real performance of SIS (Lundteigen and Rausand 2006, PDS method 2013)

Suppliers often add conservatism by making the SIL requirement stricter e.g. SIL3, is claimed when PFDavg ≤ $0.7\text{x}10^{-3}$ (H. Jin, Lundteigen, and Rausand 2012). This decision criteria is based on the precautionary or cautionary principle which ensures adequate system safety but lead to extra cost in terms of CAPEX and OPEX (Kima et al. 2014). This approach does not give any additional information about the level of uncertainty, hence scope is limited.

4.3.4 Hybrid approach

In hybrid approach, probabilistic and possibilistic methods are applied simultaneously. Here, uncertainties of some model input quantities are represented by probabilistic distribution whereas other model input quantities are represented by possibilistic distribution (Innal, Dutuit, and Chebila 2013). The logic behind this approach is that, sufficient historical data may be obtained for some input parameters or subsystem (e.g., failure rates of SIS that is used frequently). However, this may not be the case for some other parameters or subsystem (e.g., common cause failures). Moreover, in the case of new SIS elements, which are complex but highly reliable, relevant reliability data may not exist (Innal, Dutuit, and Chebila 2013). This combined approach is suitable to relieve these problems.

Innal, Dutuit, and Chebila (2013) has proposed a combined approach of Monte Carlo and fuzzy set for uncertainty analysis in SIL estimation. To carry out MC simulation and fuzzy sets simultaneously, a computer code is developed under the MATLAB environment.

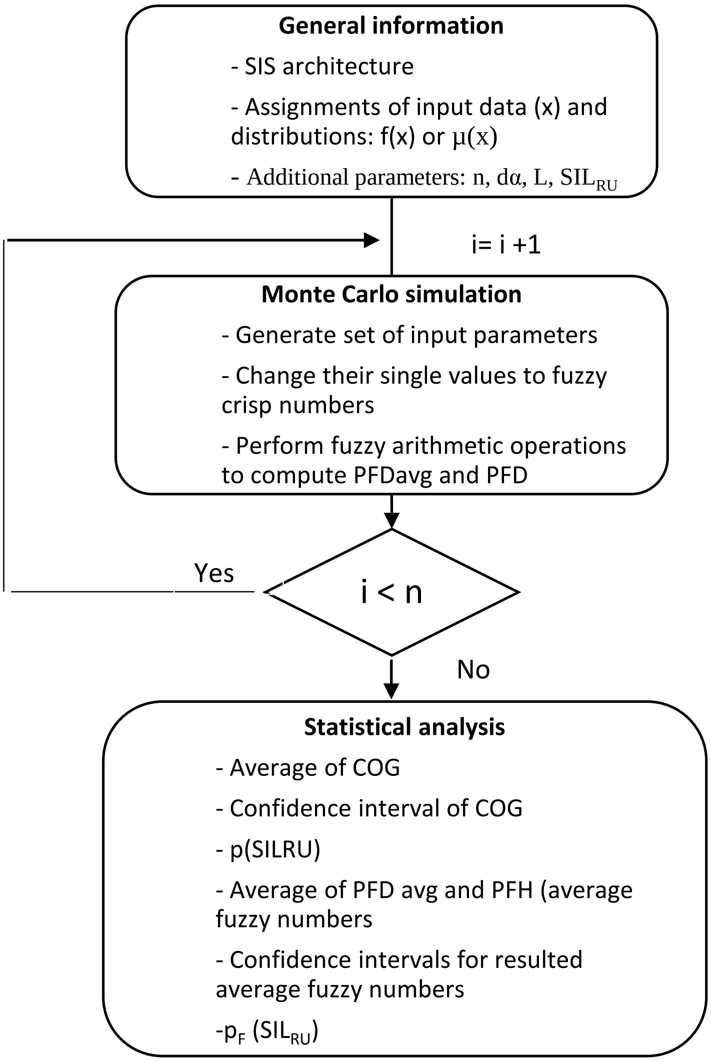

General information
- SIS architecture
- Assignments of input data (x) and distributions: f(x) or μ(x)
- Additional parameters: n, dα, L, SIL_{RU}
i= i +1
Monte Carlo simulation
- Generate set of input parameters
- Change their single values to fuzzy crisp numbers
- Perform fuzzy arithmetic operations to compute PFDavg and PFD
Yes
i < n
No
Statistical analysis
- Average of COG
- Confidence interval of COG
- p(SILRU)
- Average of PFD avg and PFH (average fuzzy numbers
- Confidence intervals for resulted average fuzzy numbers
-p_F (SIL_{RU})

Figure 6: Overall process for combining Monte Carlo and fuzzy sets (Innal, Dutuit, and Chebila 2013)

The problem of this approach is that, high competence is needed to carry out the computational simulation. Fuzzification of the probability parameters and defuzzification is not a simple process. To carry out the simulation properly is a time consuming process.

4.3.5 Semi-quantitative approach

This approach states that the calculation of probability of failure on demand should not be the only basis for verifying the established quantitative SIL requirements, rather uncertainty aspects hidden in the background knowledge should be given special attention in relation to the assigned probabilities.

The reason of this argument is that, the PFD number is conditional probability which can be expressed as P (failure on demand |K) where K is the background knowledge and information. The background knowledge includes system performance, characteristics, data and system knowledge. There are lots of assumptions and presumptions in the calculation of PFD, so decision making should not be based on the PFD number only.

Abrahamsen and Røed (2011) has proposed such an approach for SIL verification. Along with the qualitative assessment of background knowledge, they propose to add conservatism in decision making depending on the result of qualitative assessment. An example for the application of this approach can be illustrated like this: determined SIL is SIL 3 because the calculated probability number is within the range 10^{-4} to 10^{-3} without considering the uncertainty factors in the background knowledge. After uncertainty evaluation, it is found that considered case is highly uncertain considering all uncertainty factors. So the SIL for the safety function should be considered as SIL2 instead of SIL3. An uncertainty evaluation should take into account of human aspects, technical aspects and operational aspects.

The problem of this approach is that the uncertainty evaluation is quite difficult to judge for the decision makers and may be subjected to the analyst's different view of perspective.

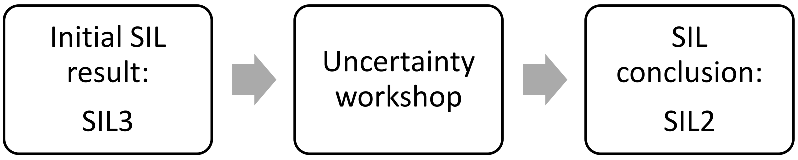


Figure 7: An application example illustrated by Abrahamsen and Røed (2011)

5 PROPOSAL FOR UNCERTAINTY ASSESSMENT AND DECISION MAKING

5.1 WORKFLOW OF SIL VERIFICATION

In reliability analysis, uncertainty analysis should be included in the SIL verification process. It is discussed earlier, that the uncertainties accompanying with system and process should be reported to the decision maker to make aware of the risks related to the decision. Decision context may be different due to the availability of resources for the assessment and purpose of analysis. Moreover, it may be greatly influenced by the interest of the stakeholder.

The SIL verification process should consist the following steps:
Step 1 is initiating the reliability assessment, which includes to define the scope, to select the suitable model to carry the reliability assessment, search for available data.
Step 2 is to carry out the reliability assessment based on the approach decided in the previous step
STEP 3 comprises uncertainty analysis, expert review and judgement and review of knowledge dimension. Each of the steps are described below:

- Uncertainty analysis

It can be quantitative or qualitative or both. A presentation of only quantitative results may become less valuable if the decision maker does not have the competence to interpret quantitative results from an uncertainty assessment.
The aim of the uncertainty analysis is to gain sufficient confidence to make the decision. Confidence is gained through critical evaluation of the information and methods used in modeling.

- Expert review and judgement

One SIL value cannot describe the system fully and there may remain uncertainty in the system which the analyst may become unaware of. Knowledge sharing among experts from different disciplines are very important therefore. The decision maker has not to fully trust in the single opinion of the technical person. Expert opinion includes technical background and consolidated experience. Analysis result should be presented to individuals or groups who have experience with a similar system, including other analysts, managers responsible for analysis, outside reviewers, and formal decision makers who must make the decisions on the basis of analysis. The final decision making can be made by brain storming session, eliciting expert opinions.

It should be kept in mind that, in practical application a mathematical or objective analysis cannot replace a management review and judgement. It is not desirable to develop tools that dictate the decision. Aim of analysis is to help make the decision processes more fact based and transparent.

- The review of knowledge dimension

  Strength of knowledge means the available knowledge dimension of the system and phenomenon being studied. Whether the analysis is based or poor or strong background knowledge, this should be informed to the decision maker.

Step 4 is decision making. The extracted conclusion from the uncertainty assessment, in step 3, should be included in the compliance report. Decision should be made based on the results of uncertainty analysis, limitation of tools, knowledge dimension and expert review.

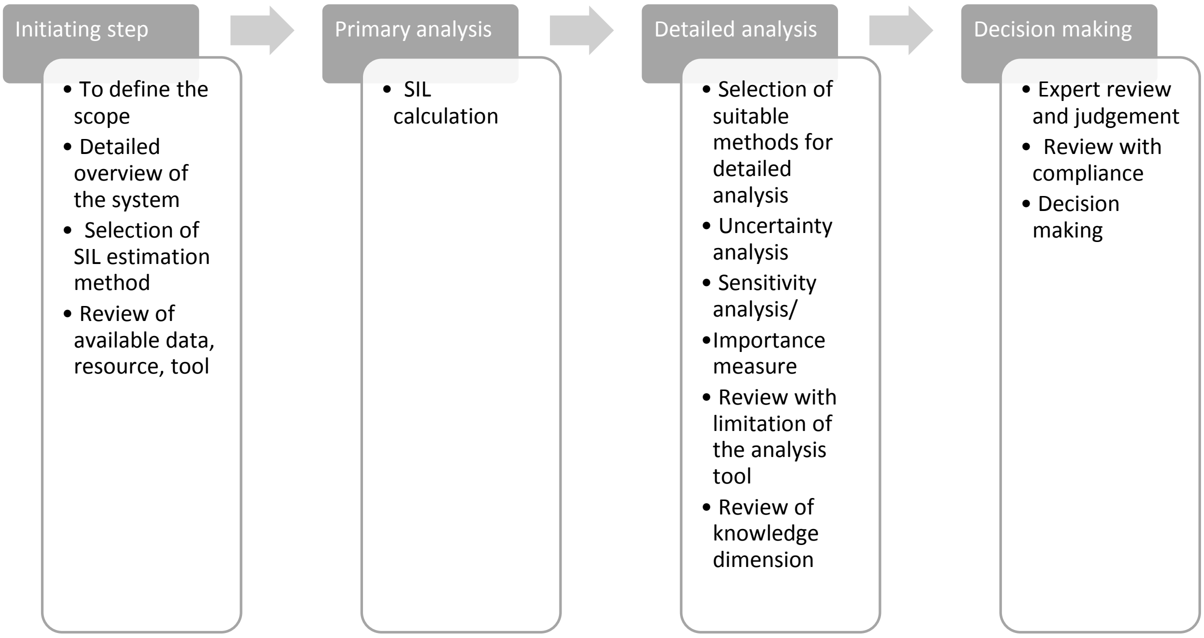

Initiating step
• To define the scope
• Detailed overview of the system
• Selection of SIL estimation method
• Review of available data, resource, tool
Primary analysis
• SIL calculation
Detailed analysis
• Selection of suitable methods for detailed analysis
• Uncertainty analysis
• Sensitivity analysis/
•Importance measure
• Review with limitation of the analysis tool
• Review of knowledge dimension
Decision making
• Expert review and judgement
• Review with compliance
• Decision making

Figure 8: Proposed steps for SIL verification and decision making

5.1.1 The need to consider of both uncertainty analysis and strength of knowledge

One may ask about the need to take account of both uncertainty and strength knowledge, as showed in presented workflow (Figure 8). Here it is tried to answer this question in details.

Uncertainty is an unavoidable part affecting the behavior of the system influenced by available information (Terje Aven and Krohn 2014). Uncertainty about input parameter X is propagated through the model F (figure 5), to get an uncertainty description of the result Y. The tool for analysis can be analytical approach (e.g. Monte Carlo simulation) (T. Aven 2011).

The issue is debatable in literature whether the knowledge dimension should be assesses after doing the uncertainty analysis. It is discussed earlier (section 3.2) that uncertainty can be represented by assigning probabilities. If the assessor assigns a probability based on background knowledge then why he should dispute his own assignment as this probability number is expressing his /her uncertainties. The aim of the assignment of this second order probability is not to express the belief of belief, rather to draw attention to the fact that probability or any other analysis tool has its own limitation to capture the relevant uncertainty aspects (Terje Aven 2010b).

Assumptions and suppositions onto which probabilities are based on could turn out to be wrong if background knowledge K is poor (Terje Aven 2011). K is generally omitted assuming K as unknown quantities and as it is the basis for assignments. Whereas the entire K cannot generally be removed by treating as unknown quantity.

Uncertainty representation based on a strong knowledge or based on poor knowledge can come out the same result. In a general sense, strong knowledge means the lower degree of uncertainty and poor knowledge indicates the higher level of uncertainty. One has to be careful when referring to both terms. The concept ‘strength of knowledge’ is considered more precise in reflecting the concept of the overall system (Terje Aven 2013). This term is described more clearly in the following paragraph with an example.

It is supposed that assessor has to assign the uncertainty interval as a mean of probability of a risk event e.g. a violent storm. This probability is conditional on a number of factors such as the location of the storm, time, and previous weather statistics. It reflects a degree of belief of the assessor based on his background knowledge. He can have lack of available data or sophisticated tool to predict the weather. If he assigns a probability number of 0.01 that means he is 1% sure that the storm will occur. By this number it is not reflected whether he had sufficient available data or tool during the analysis. An assignment of strength of knowledge can help the assessor to express his uncertainty about his belief, can show the weakness/strength of the analysis to the decision maker. In two situations, the uncertainty result can be same, but the strength of knowledge supporting the probabilities may be different. In case of new technology, where the proper prediction of system performance is difficult, the assignment of ‘strength of knowledge’ can nullify this concern.

Here the focus is the safety integrity level of a safety instrumented system which expresses a level of risk reduction from the system. Risk reduction is also about reducing uncertainties and strengthening knowledge. A probability (assigned based on the available knowledge) changes by gathering more knowledge. A broader risk perspective should be adopted which considers a set of methods, both qualitative and quantitative to reflect this knowledge level. Addressing uncertainties and knowledge we obtain a stronger focus on the resilient system (Veland and Aven 2013).

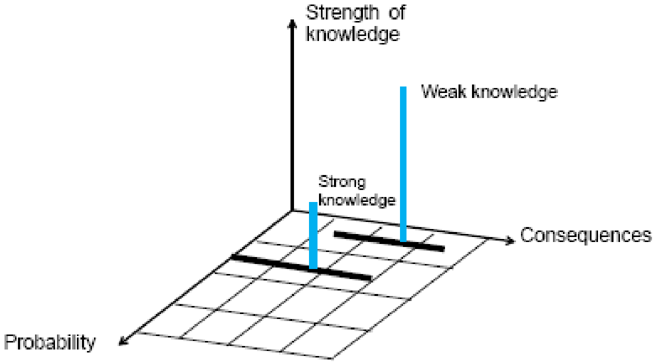


Figure 9: A way of representing risk with respect to a risk event taking into consideration of knowledge dimension (Terje Aven and Krohn 2014)

There are several procedures to quantify the ‘strength of knowledge’. One method is direct grading of knowledge supporting the uncertainty analysis. According to this method, knowledge will be considered as weak if following conditions are met (Terje Aven 2013):

- Strong simplifications were done to make assumptions
- The lack of sufficient data
- The lack of agreement among experts
- complex or little understood phenomena

This insight of the phenomena is not possible by uncertainty analysis, whether it is probabilistic or non-probabilistic representation.

This assessment of knowledge dimension can be viewed as a continuous improvement process. The goal is to focus on the overall performance of the activity that helps the continuous improvement, not only to be in compliance with stated regulation.

5.1.2 Difference between uncertainty analysis and sensitivity analysis

It is common in industry to perform sensitivity analysis as a requirement to uncertainty analysis. Though the actual fact is that sensitivity analysis in not a type of uncertainty analysis. Uncertainty analysis represents the determination of uncertainty in the analysis result that evolves due to uncertainty in the analysis input (Terje Aven 2010). Sensitivity analysis represents the determination of the contributions of individual uncertain inputs to the analysis results (Terje Aven 2010). Sensitivity analysis shows how the uncertainty in specific model input may affect the uncertainty in the output. Here it is tried to explain the difference of both with help of model notation.

Previously, it is shown (Figure 4) that model output Y= F(x,d) where, F(x,d) is the model, x is uncertain inputs and d is fixed input. Taking into consideration of uncertain input only, Y= F(x). An uncertainty analysis of Y represents an assessment of the uncertainties about X achieved by the uncertainty propagation through F (Terje Aven 2010). The uncertainties of these quantities can be expressed as subjective or objective probabilities. Sensitivity analysis shows how the variation of a quantity X affects Y or EY. The uncertainties about X are unknown in this analysis. Thus, the analysis is not an uncertainty analysis. In reliability application, the sensitivity analysis does not assess the uncertainties of safety integrity level.

Sampling-based approaches can be used both for uncertainty and sensitivity analysis. The focus is given here to Monte Carlo approaches. A framework is presented here to show the difference between both analyses.

Framework to perform standard MC sampling is as follows (Helton et al. 2006):

1. Output function is defined as $y(x) = [y_1(x), y_2(x)\ldots y_n(x)]$ where, $y_1(x), y_2(x)\ldots y_n(x)$ are functions of uncertain inputs $x = [x_1, x_2\ldots x_n]$. Uncertainty in x will induce uncertainty in y(x). Here arises two questions: (i) what is the uncertainty of y(x) due to uncertain input x? And (ii) How the individual elements of x effects the uncertainty in y(x)? Uncertainty analysis answers the first question and sensitivity analysis answers the second question.
2. Probability distributions are assigned to characterize the aleatory uncertainty in the elements xi of x where, i = 1, 2… n.
3. Samples xi are generated from the assigned distributions.

4. Sample is propagated through model from analysis inputs to analysis results. After each iteration model output is calculated. The result will be a distribution which is governed solely by the uncertainty in the stochastic parameters.
5. Uncertainty analysis results are presented by the distributions of the elements of y constructed from the corresponding elements of xi.
6. Sensitivity analysis results are determined by the exploration of the mapping [xi, y(xi)], i = 1; 2; . . . ; n)

This framework focuses only probabilistic characterizations of uncertainty. Presentation of uncertainty analysis results involves means and standard deviations of the obtained distribution, density functions, cumulative distribution functions, and box plots (Helton et al. 2006). Cumulative distribution and box plot are usually preferable to mean and standard deviation. Presentation of sensitivity analysis results involves the exploration of the mapping [xi, y(xi)], i = 1; 2; . . . ; n, to assess the effects of individual elements of x on the elements of y (Helton et al. 2006).

In reliability application birnbaum measure, improvement potential are widely used to identify critical components and to rank components with respect to reliability and risk where the criticality or importance of component are presented by a tornado chart.

5.2 Uncertainty assessment

Various models for uncertainty analysis in SIL estimation, established in literature and industry, is presented and discussed in details in the previous section. It is found that fully quantitative uncertainty analyses like sampling based approach, fuzzy probabilistic approach are well established in literature. However, in a complex system's reliability analysis, proper characterization, representation, and propagation of uncertainty is a critical task.

This thesis gives weight to the parameter uncertainty analysis adopting the idea of Nilsen and Aven. According to Nilsen and Aven (2003), the concept of model uncertainty does not add any value to the uncertainty analysis. Rather, it may divert the attention of the analyst away from what is uncertain and the outcome of the activity being studied. The aim of the uncertainty assessment is to clarify or to reduce the uncertainty related to activity or relevant information of the system. The quantification of model deviation may misguide the decision maker about the actual finding of the analysis (Nilsen and Aven 2003).

To propagate the parameter uncertainty in SIL verification two approaches are proposed in this thesis. Along with the presentation of already established quantitative uncertainty analysis, an approach is proposed for quantification of uncertain factors hidden in the background knowledge. The overall aim is to have a complete presentation of uncertainty in the system and the inter-connection between system and environment that will help the decision making on target SIL determination. Quantitative uncertainty analysis can be performed with MC sampling. For the uncertainty assessment of background knowledge, technical, operational and organizational aspects which may affect the safety integrity level should be taken into consideration. The uncertainty assessment of background knowledge is termed as the 'semi-quantitative' assessment in the rest part of the thesis.

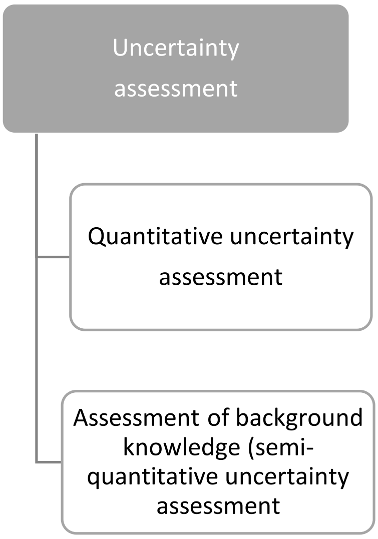

Uncertainty assessment
Quantitative uncertainty assessment
Assessment of background knowledge (semi-quantitative uncertainty assessment

Figure 10: The proposed uncertainty treatment for SIL verification

5.2.1 Quantitative uncertainty assessment

5.2.1.1 Introduction

The uncertainty factors in reliability estimation is discussed earlier with their causes. For quantitative uncertainty analysis MC approach is adopted here because it gives the flexibility on selecting different probability distribution or different interval in the input parameters and to observe their effect on the overall PFD result. Probability is regarded as a perfect tool to describe aleatory uncertainty. Uncertainty will not be a concern if subjective probabilities are allocated because the analyst is well known with his subjective belief. However, objective probabilities (known from observations) can be uncertain. As discussed earlier that, for PFD calculation, failure rate and common cause failure data is taken from observation (e.g., OREDA database).

5.2.1.2 Assumptions

As discussed earlier in section 3.3, depending on the type of uncertainty affecting model input quantities, methods of uncertainty propagation can be classified into level 1 and level 2 setting (Aven et al. 2014). For reliability estimation, case level 1 setting is adopted, assuming that only aleatory uncertainty will be dealt here. The rest of variables will be assumed as constant on the assumption of having sufficient system information and knowledge.

5.2.1.3 Procedure

The following framework is followed to perform MC simulation which resembles the standard MC sampling procedure and adopts the probabilistic approach:

1. Uncertain input are identified which may affect the SIL. If PDS method is adopted for SIL calculation, uncertain inputs are failure rate of components (λ), common cause failure (β factor) and proof test interval (τ). It is tried to find 'what is the uncertainty in SIL level given the uncertainty in these input parameter?' in the next steps.

2. Appropriate probability distribution are assigned to characterize aleatory uncertainty for each uncertain input. The distributions are typically defined through an expert review process.
3. Samples are generated for uncertain inputs according to the assigned probability distribution.
4. Sample is propagated through the analysis from analysis inputs to analysis results. After each iteration model output is calculated. The result will be a distribution which is governed solely by the uncertainty in the stochastic parameters.
5. The uncertainty analysis results are presented by the distributions of the elements of y constructed from the corresponding elements of xi. Other statistical properties (mean, percentiles value, standard deviation) are also presented to analyze the results of the analysis.

An example of how to perform this analysis is presented in chapter 8.

5.2.2 Semi-quantitative assessment

5.2.2.1 Introduction

The reason for the semi-quantitative assessment is due to the acknowledgement that it is not possible to quantify the uncertainty of PFD_{avg} estimate in any objective way. Rather Probability of failure on demand (PFD) is conditional on a background knowledge *K*, which includes assumptions of the model, data, expert statements and phenomenological understanding. All probabilities need to be considered in relation to *K*. If background knowledge changes, probability may also change.

All assessment of events, consequences and uncertainties are affected by the background knowledge. There may be inherent uncertainties hidden in the background knowledge. Screening background knowledge and identifying uncertainty factors in the background knowledge also provides the analyst with a clearer view of where special considerations should be taken.

The reliability analysis of modern complex systems demand an integrated approach in which the hardware, software, organizational and human elements are treated in a combined framework accounting their inter-dependencies. In the MC simulation framework for reliability analysis, the information about the system discrepancy of system behavior is hidden. The deviated result after the simulation may not be meaningful without the evolution of physical parameter which influence and characterize the system behavior. A model is required, which captures the behaviors of the physical system such as hardware, software, and environmental factors adequately affecting the safety integrity of safety instrumented system.

To focus on the safe system, a broader perspective should be taken which will include all the physical aspects influencing system behavior. Today's complex organizational system cannot be studied fully as a technical system, rather multidimensional approach should be taken into consideration to include other dimension such as organizational culture, organizational environment. For example, organizational factors influence local workplace conditions, which may increase failure events. Organizational factors includes organizational processes, organizational culture, time pressure, insufficient training, ambiguous procedures, etc. The increased complexity of engineering systems has increased the uncertainty in the system behavior and their modelling. The component failure rate collected from the existing database may be inconsistent due to improved maintenance practice and more reliable software.

The proposal, presented here, is motivated from previous work of Schönbeck, Rausand, and Rouvroye (2010). Schønbeck in his master's thesis has evaluated safety influencing factors on SIL of SIS. His proposal captures human and organizational factors along with their structural and behavioral aspects. He used eight failure types which considered human and organizational factors in the operation phase of safety instrumented systems and presented an equation to predict operational SIL which is different from design SIL. This thesis adopts the similar approach. However, this is further developed in order to include technical and operational aspects along with human and organizational aspects that may affect the SIL rating.

5.2.2.2 Framework

To consider the impact of physical aspects on the achieved SIL in a practically feasible, all physical factors, which may influence SIL of SIS, are screened and assessed. These physical factors are called uncertainty influencing factors. Next, a model is proposed to quantify the relationship between physical factors and the achieved SIL. Thus, influencing factors are linked directly to the safety integrity level.

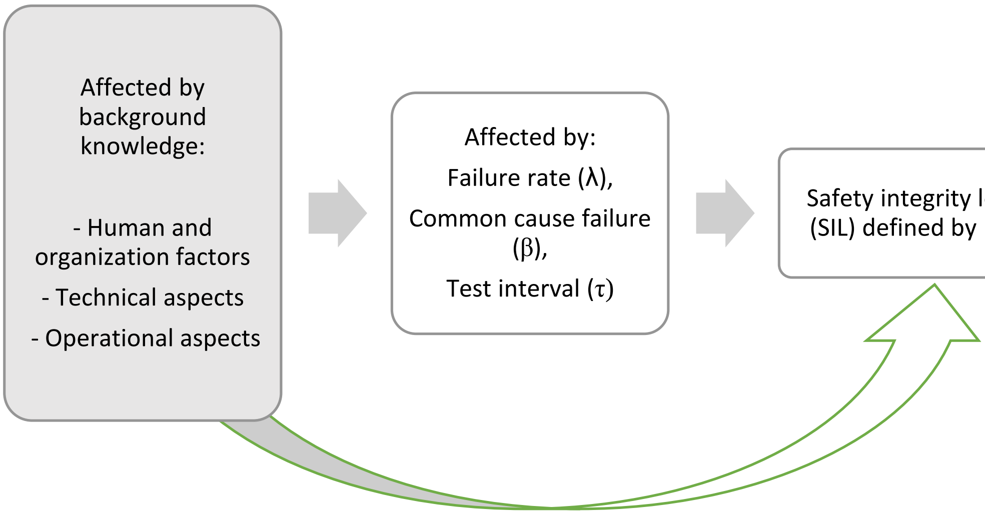

Affected by background knowledge:
- Human and organization factors
- Technical aspects
- Operational aspects
Affected by:
Failure rate (λ),
Common cause failure (β),
Test interval (τ)
Safety integrity level (SIL) defined by PFD

Figure 11: Linking background knowledge directly to PFD

Examples of such safety influencing factors are presented below:

Table 5: Example of uncertainty influencing factors

Main categories	Sub-categories	Evaluation with details	Impact on the system as a measure of uncertainty
Human aspects	--	--	High/medium/low
Technical aspects	--	--	High/medium/low
Operational aspects	--	--	High/medium/low

Basic steps of this framework is as bellows:

1. For simplicity, it is assumed that the predicted SIL calculated by the deterministic model (the PDS model in this thesis) is based on an ideal situation where all the physical factors function optimally. But in practice, the calculation of the SIL is based on field data, so a certain influence of these factors is already included in the predicted SIL.

2. The first step is to identify the qualitative factors which may affect the SIL of SIS. Focus is given on the details of technical, operational aspects and human aspects. Here human aspects include organizational factors also.

3. The second step is the assessment of the impact of influencing factors. A weight is given to each factor depending on their contribution on system behavior. This weight should be given following a comparative study, whether any factor has more or less contribution to system behavior than other or not. The highest weight ratings factors contribute most to SIL uncertainty, and are therefore needs to be improved priory. After completing weight assignment to each factor, these weights have to be normalized. The weight factor Wi for qualitative factor i is calculated in such a way that $\sum_{i=1}^{n} W_i = 1$:

$$W_i = \frac{\widetilde{W\iota}}{\sum_{i=1}^{n} \widetilde{W_\iota}}$$

4. In the next step the state of each influencing factors is assessed. The influencing factors are rated as a contributor to uncertainty which may influence the calculated SIL and try to classify their uncertainty severity as low, medium, high. To quantify this severity a scale is assigned to quantify this uncertainty severity, where R_i=1/3 expresses low uncertainty, R_i=2/3 indicates medium uncertainty and R_i=3/3=1 indicates high uncertainty. These severity of uncertainty should be established using expert judgment for the specific system under consideration. If these severity are established from accident statistics, they may induce further uncertainty in the estimation. A rate is given to each factor depending on the severity of uncertainty.

5. This step is to determine the strength of knowledge, ξ. ξ can be from 0 to 1 where ξ = 1 indicates high strength of knowledge and ξ = 0 indicates poor strength of knowledge. To determine the value of ξ, following strategy can be considered:

Strength of knowledge will be poor:

   a. If the system under study is new (e.g. a new system installed in a new built platform),
   b. The system under study have never assessed before for SIL calculation and verification
   c. Analyst is unknown with the system performance and other criteria that can affect the SIL
   d. Some safety instrumented systems can be more prone/vulnerable comparative to the other system depending on the system configuration and operating conditions. If the analyst is well aware of this, he can put the knowledge dimension as poor as these systems cannot be predicted properly with this type of analysis

In case of known system and/or for which SIL analysis has been done before, strength of knowledge will be considered as high.

6. The actual SIL rating after taking into consideration of the uncertainties can be calculated as follows:

$$SIL_{uncertain} = \left[1 - \left\{(1-\xi).\left(\sum_{i=1}^{n} RiWi\right)\right\}\right].\ \mathrm{SIL}_{Calculated}$$

Where, ξ is strength of knowledge of the analyst (0 ≤ ξ ≤ 1);
R_i the uncertainty rating for factor i (0 ≤ R ≤ 1for all i),
W_i the weight factor for factor i (0 ≤ Wi ≤ 1 for all i),
$\mathrm{SIL}_{\mathrm{Calculated}}$ is previously determined SIL calculated by deterministic method.

A similar equation is proposed by Schönbeck, Rausand, and Rouvroye (2010). Instead of ξ factor they introduced a factor θ, where θ expresses a measure of the uncertainty level of the system toward the human and organizational factors.

5.3 Selection of uncertainty assessment method

Required Level of uncertainty analysis may be different for different decision context. Depending on the problem addressed, framework conditions, organizations involved and motivations, different methods may be advisable in practical decision-making context[5].

The question may arise how to determine the requirements of uncertainty analysis, based on the situation under consideration.
This depends on:

- Scope and motivation of the analysis
- Complexity of the system under consideration
- Available resources and skills for the analysis
- Availability of tools
- Limitation of various tool for practical application

5.3.1 In Design phase or early phase of a new installation

In design phase of new installations, following methods should be followed for detailed analysis:

- Sensitivity analysis
- Qualitative or semi-quantitative uncertainty analysis
- Quantitative analysis
- Expert review
- Consideration of other risk reduction measure

In design phase of the new installation, sensitivity analysis and importance measure should be given most weight. The uncertainty is at the highest level in early life-cycle phase. At this stage most compliance studies are executed. During decision phase, it is important to predict the performance of several (perhaps many) design alternatives.

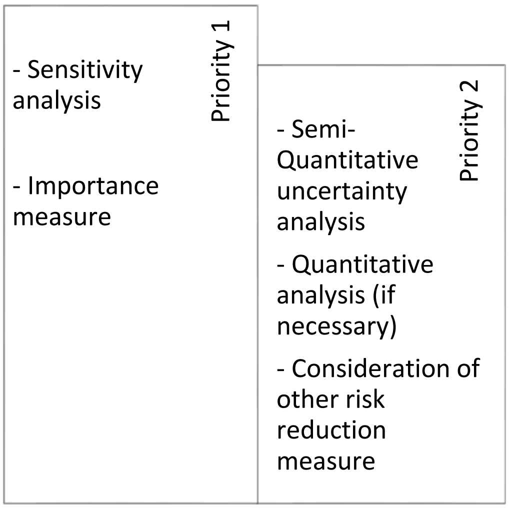

Priority 1
- Sensitivity analysis
- Importance measure
Priority 2
- Semi-Quantitative uncertainty analysis
- Quantitative analysis (if necessary)
- Consideration of other risk reduction measure

Figure 12: Priority chart for use of method in design phase

[5] The decision context involves defining what decision is being made and why, as well as its relationship to other decisions previously made or anticipated (Compass Resource Management 2015)

Statistical quantities may be difficult to interpret. The qualitative framework facilitates a whole view for the decision maker of all involved fields. It provides a more rational scenario for making a choice. A semi-quantitative or qualitative uncertainty assessment will be helpful in this regard. An overall evaluation of the uncertainty should be discussed based on subjective judgements of analysts and experts.

In design phase, one can increase the SIL by using more reliable equipment or by reducing the test interval, or by improving the diagnostic test coverage. The System can be less sensitive to one specific factor which leads to a lower value of SIL (Schönbeck, Rausand, and Rouvroye 2010). Alternative option may be to increase the redundancy of a system by adding a similar component in a parallel setting. However, decision maker has to select a suitable one.

5.3.2 At modification phase of the existing installation

In modification phase of existing installations following workflow can be followed:

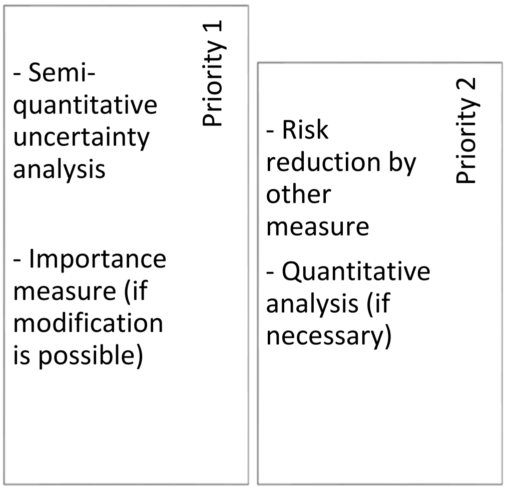

Priority 1
- Semi-quantitative uncertainty analysis
- Importance measure (if modification is possible)
Priority 2
- Risk reduction by other measure
- Quantitative analysis (if necessary)

Figure 13: Priority chart for use of method in modification phase

In the modification phase of existing installations which was installed a long time ago, semi quantitative uncertainty analysis will help the decision maker about the possible improvement in the specific sector (e.g., if any technical aspect is the reason for the reduction of SIL rating, it can be easily visible by a semi-quantitative assessment. If the modification of the system configuration is possible, then importance measure can be used to check the effect of the possible alternative configuration in SIL rating, otherwise it will be of no use. Alternative risk reducing measures should be assessed for their applicability, costs and other benefit/dis-benefit. Quantitative uncertainty analysis can be a supplement of semi-quantitative analysis if the analysis is not confident about the parameters and result of the semi assessment.

6 COMPARATIVE STUDY WITH EXISTING MODELS

In the previous section, two different approaches are presented to assess uncertainty. One is probabilistic based quantitative uncertainty analysis and another is semi-quantitative approach.

6.1 QUANTITATIVE ANALYSIS

In quantitative uncertainty analysis, MC sampling approach based on the purely probabilistic approach is used. Motivation is that, MC can well handle precise or interval variables in input parameters, and their effects on the output value can be observed simultaneously. Probability can perfectly describe aleatory or epistemic uncertainty. As an alternative to 'precise' subjective probabilities, Interval or imprecise probabilities are proposed when the analyst has less confidence about the value any parameter due to the existence of less amount of data.

The advantage of this tool is that it is a highly innovative, high-tech and high-performance tool. Concepts used are well established and accepted in science and business and results are generally understood by proficient users. Numerical results turned out to be stable, precise and reliable. Commercial software is also available. But it requires a huge amount of work for a new system and interpretation of the results in a theoretical correct way is a critical task.

Objective reliability assessments are based on the belief that reliability can be estimated and has valuable meaning for decision makers. However, such assessments are based on various assumptions. When the complexity of the system increases, the uncertainty in the obtained result also increases (Lundteigen and Rausand 2006). In the standard MC setting, epistemic and aleatory uncertainty can be propagated simultaneously. However, scientists are on behalf of the opinion that different types of uncertainties should be treated separately. This will reduce the total uncertainty of the model by understanding what steps can be taken and what potential change to the system one can make.

Researcher previously adopted MC approach for uncertainty analysis in SIL verification, but there were lacking in the following factors:

- Did not take into account background knowledge
- Did not take into account of human and operational factors
- Uncertainty was not given much attention with broader perspective, only stochastic uncertainty was treated

MC is able to propagate uncertainty evolved from randomness of the system, but background knowledge hidden in the uncertainty was out of focus. The information about the system discrepancy of system behavior is hidden. The deviated result after the simulation may not be meaningful without the evolution of physical parameter which influence and characterize the system behavior. In the complex system, there is a need to take into account of Man-technology-organization aspects. Human interaction is important for a manually activated instrumented system, whereas for subsea instrumented system, operational factors are more important than human involvement.

One should keep in mind that, this quantitative uncertainty analysis just provides an estimate of the uncertainty (variation) of the output quantity. This estimate may be subjected to an error that depends on the number of MC sampling of the aleatory quantities.

6.2 Semi-quantitative analysis

Semi-quantitative uncertainty analysis proposed in the thesis follows the previous work presented by Abrahamsen and Røed (2011). In Abrahamsen and Røed (2011), human and operational aspects are covered in a systematic way to consider the uncertainty of background knowledge in SIL verification. The uncertainty influencing factors are evaluated in a qualitative way and categorized into three level of uncertainties such as high, low or medium. This thesis adopts the same evaluation process with slight modification.

The method, proposed in this thesis, tries to quantify the effect of these qualitative factors on SIL rating and a formula is proposed to calculate deviated SIL due to the effects of these uncertainty factors. For quantification, the concept of Schönbeck, Rausand, and Rouvroye (2010) is adopted (details are described in section 5.2.2). The logic behind this is that only semi-quantitative evaluation of these factors may create confusion to the technical staff about their overall effects on system SIL. This quantification method is proposed to become aware of the overall effect on system SIL. Therefore, the technical staff may show the effects of a specific criterion to the decision maker in a numerical way.

The pros of the method is as below:

- Final output is fully understandable so the decision maker may take a decision based on the provided/available data.
- The method itself is easy to use and follows a very straightforward and structured workflow. The complexity lies at the starting point, in the process of screening and defining the uncertainty influencing factors and effects. Expert involvement in therefore recommended in this step.

However, following cons can be faced:

- This method is quite new, technical staffs may be unfamiliar with this work process and relevant required information
- The effort of weighting can be high as understanding of the complex environment is critical. The feasibility of each weight assignment should be evaluated.
- Can be quite time consuming depending on the dimension and complexity of the system.
- Overlapping, inter-dependencies was not taken into account, it may influence the correctness of evaluations.
- One may raise the question that this approach is subjected to analysts' point of view. Expert judgments may vary due to different background knowledge and experience. This may lead to two different results for the same analysed system if studied by two independent reliability experts. If the technical expert have an overconfidence about the system they are working daily, the result of uncertainty analysis may result into low uncertainty instead of high uncertainty. The analysis may lose its importance due to this type of subjective judgement. As a conclusion, it can be said that, analytically correct evaluations require the mutual independence

and minimum overlap between each criteria. A correct result thus requires a detailed understanding and analysis of the criteria in the specific context of the use case. Treatment of interdependencies and overlaps is not implemented in the tool but requires further analysis and treatment in the selection and weighting process. Sophisticated scientific investigations are thus necessary.

7 A CASE STUDY WITH PROPOSED MODEL

In section 5.1, it is discussed that the SIL verification process should consist the following steps:

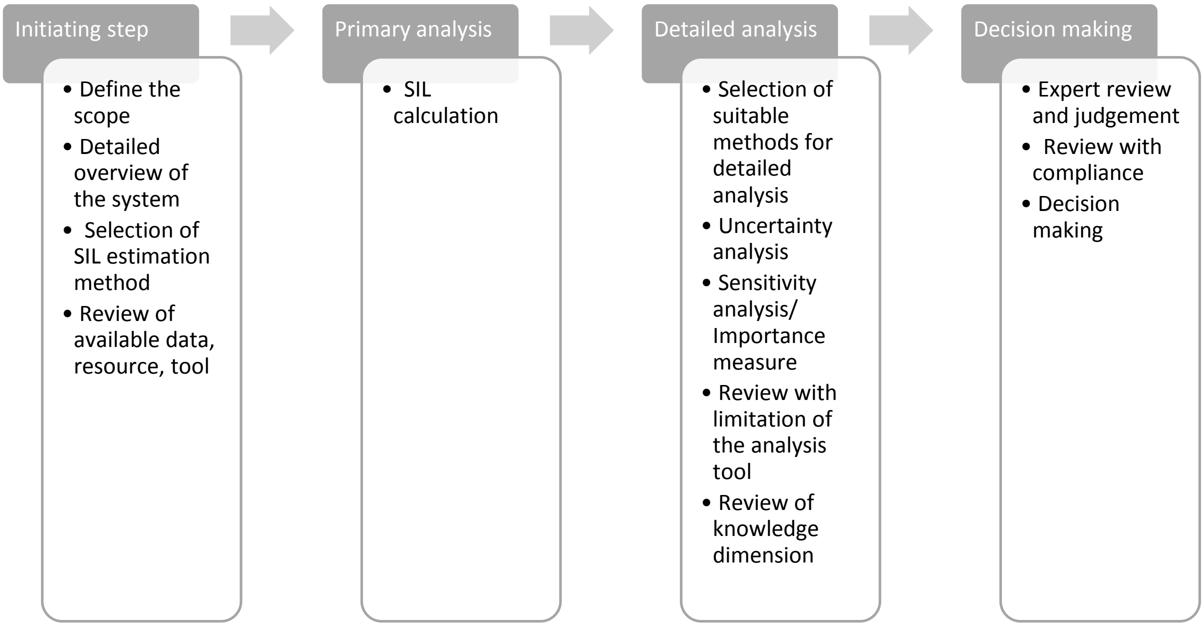

Initiating step
• Define the scope
• Detailed overview of the system
• Selection of SIL estimation method
• Review of available data, resource, tool
Primary analysis
• SIL calculation
Detailed analysis
• Selection of suitable methods for detailed analysis
• Uncertainty analysis
• Sensitivity analysis/ Importance measure
• Review with limitation of the analysis tool
• Review of knowledge dimension
Decision making
• Expert review and judgement
• Review with compliance
• Decision making

Figure 8: Proposed steps for SIL verification and decision making

How this model can be implemented in reality is shown in this section with a case example.

7.1 INITIATING STEP

7.1.1 Scope

The system taken for case study in this thesis is the subsea well isolation system or subsea ESD system. This case is in the modification phase for an existing platform which was installed a long time ago. The safety instrumented system is analyzed to check compliance with safety integrity level (SIL) requirement.

7.1.2 Overview of the safety instrumented system

The function of the subsea ESD system is to Isolate well from manifold/flow line by activation through topside ESD logic solver and closure of well valves (relevant XT-valves, including DHSV). In case of an emergency situation, activation of the subsea Emergency Shutdown (ESD) system shall isolate one well from the manifold flow line and service lines. In the case study, SIS is composed of the following systems:

- ESD node
- Electrical power control unit
- Subsea control module
- X-mas tree valves
- Downhole safety valves

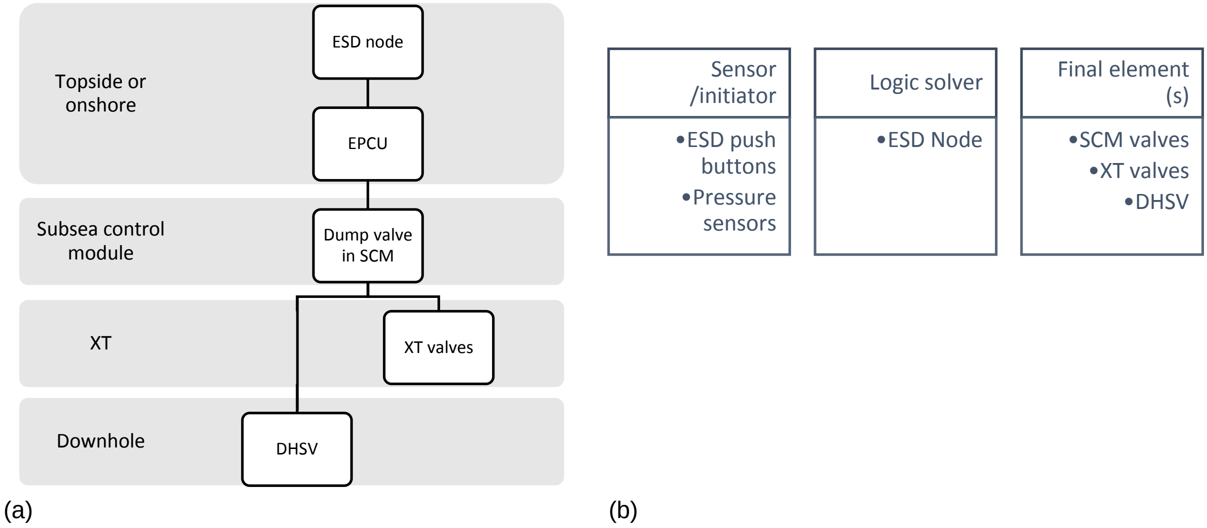


Figure 14: a) An overview of the functional blocks and components that comprises the SIS; b) SIF components

Table 6: SIS functionality and related information

	Subsystem	**Location**	**SIS functionality**	**SIS related info**
1	ESD node	Onshore	Carries ESD signals	SIS logic solver common to all SIF's
2	EPCU (safety relay and main contactor)	Onshore	Isolates electric power from subsea EPCU channels	Part of SIF final element; equipped with ESD relays/contractors necessary for isolating power to subsea control systems during certain shutdowns.
3	Subsea control module	Subsea	Depressurize function lines by venting hydraulic fluid to sea	Part of SIF final element; Equipped with fail safe quick dump solenoid valves to vent hydraulics subsea.
4	Xmas tree (valves with hydraulic actuators	Subsea	Isolate the well using XMT valve (e.g. PMV, PWV)	Part of SIF final element; Equipped with main well isolation valves, forms the secondary well barrier.
5	Downhole safety valve	Subsea (downhole)	Isolation of the production bore	Part of SIF final element; Downhole safety valve forms the primary well control barrier.

7.1.3 Detailed study of the system and operating condition

7.1.3.1 ESD signal

The SIS shall receive a continuous ESD signal directly from the ESD Node. Removal of the ESD signal shall trip the safety relays.

7.1.3.2 EPCU Safety relays

The ESD function is hardwired into the EPCU as a discrete signal. The safety relay is held by, and will trip upon a loss of the ESD signal.

7.1.3.3 EPCU Main contactors

Tripping the safety relays will, in turn, causes the two EPCU main contactors to go open circuit resulting in removal of power from EPCU channel.

7.1.3.4 Subsea Control Module (SCM)

Removal of subsea electric power de-energizes the solenoid of the dump DCV valve in the SCM. This action disconnects the hydraulic supply and vents the SCM hydraulic pressure to sea. A chain of events crucial for the shut in of the tree is then triggered within the SCM. All DCV control valves controlling the individual functions (i.e. XT valves) closes due to loss of pilot pressure, in turn depressurizing its external output line.

7.1.3.5 Directional Control Valves (located inside SCM)

The DCV"s are two positions, control valves mounted in the protective dielectric oil environment inside the SCM. Each of the external hydraulic functions (i.e. tree valve actuators, DHSV) are controlled by directional control valves. The two positions noted are:
Open: The position in which the DCV connects the hydraulic function to its supply line
Closed: Default, de-energized and the position in which the DCV disconnects from the supply and connects the hydraulic function to its return line (safe state).
The continuously energized (CE) DCV is a solenoid operated hydraulic piloted valve. It requires a continuous electrical power to its solenoid, and hydraulic pressure to its pilot stage, in order to remain in the open position. In an ESD event, loss of this electrical signal to the solenoid will cause the valve to return to its default closed position venting pressure downstream in the SCM.

7.1.3.6 Other components

The safety loop contains other components such as pipe work. The pressure accumulators are omitted in calculation of the PFD since all failure modes are believed to lead to a safe state with regards to the safety function.

7.1.3.7 Operation Environment

The ESD SIS is to operate subsea at 350 m with a seawater temperature of +4 °C. Any other specific extremes of environmental conditions are not considered to be likely in the study. It is understood that components are suitable for the environment where they operate both in the term of pressure, temperature, vibrations, corrosion. It is assumed that the SIF will be initiated manually by the ESD push button detection of the hazardous situation within the topside system or automatically via the ESD node.

7.1.3.8 Diagnostic function and HMI

The SIF operates on an on-demand basis, it is evident that the ESD function shares final elements (DCV and Xmas tree gate valves) with general process control functions. This opens for incidental detection of faulty control valves and/or gate valves. Detection of a dangerous fault (by diagnostic testing, proof testing, during process control or by other means) related to components that is part of the safety critical function shall immediately result in specified action to achieve a safe state. The reason is that the safety system is degraded. After a safe state has been achieved, repairs shall be completed prior to restart.

7.1.3.9 Safe state

The safe state of SIF corresponds to complete isolation of one well from the manifold flow line and the utility/service lines (i.e. valves closed and leakage free). Well stream isolation is here understood as closure of both the main production bore and the annulus. All the logics are hardwired, de-energized and de-pressurized to the safe state. Hence, the functional components and software used during the normal operation (not safety critical) cannot force the SIS to a dangerous state nor prevent execution of the SIF.

7.1.3.10Degraded operation

Operation shall not be carried on with degraded safety function. On detection of faults on any components related to the SIS, the system shall immediately be taken to a safe state, or alternative risk reducing measures be put in place, which is assessed to reduce the risk by the same factor as the SIS.

7.1.3.11Safety requirements

Some general requirements for the subsea ESD function are listed below:

- ESD valves shall isolate and sectionalize process segments in a fast and reliable manner according to dimensioning fire and explosion scenarios on the loss of ESD signal, or power, or hydraulic pressure.
- The ESD function of well stream isolation should, for subsea installations, apply a fail-to safe principle, ensuring immediate closure of the wing valve and Master Valve, e.g. utilization of energized electrical circuits to keep the valves in open position"

7.1.4 Selection of SIL assessment method

ESD safety function is defined as a "low demand mode function" because the frequency of demands for operation is no greater than one per year or twice the proof test frequency (IEC 2000). So SIL classes will be defined as average probability of failure (PFD_{avg}) to perform its design function. PDS method will be adopted here for PFD calculation.

7.2 Primary analysis: SIL estimation by PDS method

7.2.1 Assumptions

7.2.1.1 Calculation approach

- When calculating PFD, the contribution from unavailability due to repair and testing of components is not included.
- The PFD of the function (safety system) is obtained by summing the PFD of each set of redundant modules.
- The term $\lambda_{DU}.\tau,$ is assumed as small enough to allow $e^{-\lambda_{DU}.\tau} \approx 1 - \lambda_{DU}.\tau.$
- The self-test period is small compared to the interval between functional testing.
- Classification of all failures is made on the basis of an assessment from safety function's point of view. The impacts on other function or systems are not evaluated.
- All failure rates are considered constant with respect to time, an exponential failure model is assumed. Although it is acknowledged that failures may be more prone to occur a short time after commissioning and in the end of the life cycle due to aging, wear and tear
- PFD is calculated as average values and are used as unavailability measures.
- When calculating PFD, it is assumed that the component can be considered as good as new after a repair or a functional test
- There exist no dependency between elements
- Only random hardware failures are included in the calculations without taking into consideration of the systematic failure (H. Jin, Lundteigen, and Rausand 2012)
- Human and organizational errors are disregarded (H. Jin, Lundteigen, and Rausand 2012)
- Maintenance errors are not considered (H. Jin, Lundteigen, and Rausand 2012)
- The SIS is not influenced by any factors outside the physical boundaries of the SIS (H. Jin, Lundteigen, and Rausand 2012)
- The test and repair times are negligible compared to the length of the functional test interval
- On detection of safe and DD failures, the system is restored immediately within a short time compared to functional test interval
- All elements are proof tested at the regular time interval, t (H. Jin, Lundteigen, and Rausand 2012)

7.2.1.2 Reliability data

1. The components are operated in an environment comparable to other subsea systems where reliability data origins from.
2. Hydraulic lines and connectors are most often regarded as passive components and hence disregarded in computation of the PFD: generally, failure of pipes,

hoses ore connectors will result in the system to fail to a safe state. The most prominent exception is the blockage.

3. The analysis is based on data for dangerous undetected failures. Generic failure data is used for PFD calculation.

7.2.1.3 Systematic and common cause failure

Systematic failure and Common Cause Failures (CCF), both largely contribute to the unreliability of a system. Since one single failure or condition affects the operation of multiple components that would otherwise be considered independent, these failures by definition defeat the randomness of failures.

The potential for dangerous CCF exists between similar redundant XT-valves and their actuators, DCVs inside the SCM, hydraulic lines and couplings, and between the redundant hydraulic dump valves. There are numerous methods that can be employed to estimate the probabilistic contribution of CCF to redundant systems. The PDS method assumes that a certain fraction of the failures (β) are common cause (PDS method 2013). Such failures will cause all the redundant components to fail simultaneously or within a short time period.

7.2.1.4 Diagnostic

1. The SCM contains numerous pressure, temperature and flow sensors which could in theory provide information about the status of some components (e.g. valve profiling). No online diagnostic has been defined to support the Safety Instrumented System.
2. A consequence of ESD activation is necessarily loss of subsea power, including the instrumentation power. The operators are thus unable to monitor the execution of the ESD function.

7.2.1.5 Maintenance interface

1. The equipment is designed to be maintenance free for the design life when installed subsea, with the exception of periodic proof testing.

7.2.1.6 Proof testing

1. A full proof test is performed periodically with one (1) year intervals.
2. 100 % proof test coverage is assumed, meaning that proof test is carried out such that all faults critical to the safety function are detected, and thereafter corrected.
3. Operation shall not be resumed until full functionality of the safety system is restored.

7.2.1.7 Mean-time to repair

For the purpose of this safety *analysis* it is assumed that in the event of detecting dangerous – which is anticipated to happen only during proof test –the system is brought to a safe state and repairs are made before production is restarted. This corresponds, calculation wise, to an MTTR of 0. On this basis, the MTTR has not been taken into account in the quantitative functional safety analysis since it is not considered to be appropriate in this implementation.

7.2.2 Reliability block diagram

The RBD is roughly arranged by the timeline of events, starting from the initial activation of the ESD signal and ending with closure of the valves representing the final element. Closure of the well can be achieved in three different ways which split the RBD into three parallel branches for the final elements. The DCV (control valves) are placed adjacent to their respective valve in the RBD, even though they are physically located inside the SCM. The calculated PFD for each subsystem of the analyzed function performing its SIF is detailed in

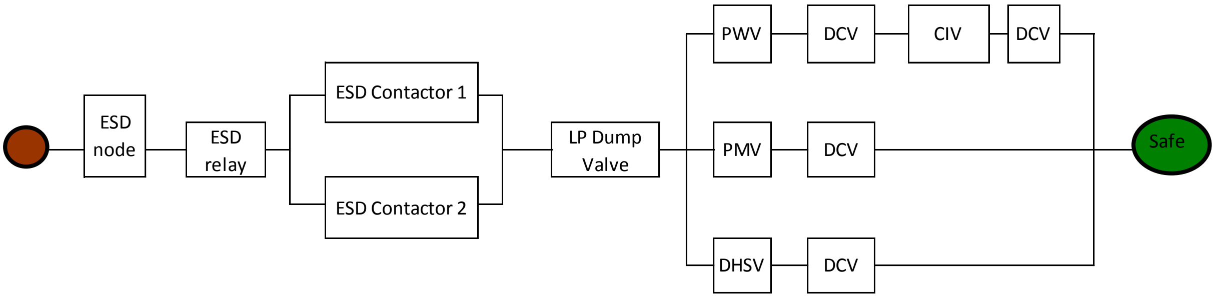


Figure 15: Reliability block diagram of subsea ESD system

7.2.3 PFD calculation

The PFD calculations are based on the formulas stated in the PDS Method Handbook. PFD calculation is carried out on the spreadsheet (MS-Excel) and results are listed in the table. One can see the theoretical framework section for calculation details. Failure rate and beta factor data are collected from PDS data handbook (PDS Data Handbook 2013).

Table 7: Characteristics data for each SIS component

Group	Sub-system	Component typical	λ_{DU} (1/hrs.)	Test interval (hrs.)	Beta-factor
1	**ESD node**	ESD node	8.00E-07	2190	0.05
2	**EPCU and Dump valve**	ESD relay	2.00E-07	8760	0.05
		ESD contactor 1	3.00E-07	8760	0.05
		ESD contactor 2	3.00E-07	8760	0.05
		Dump valve	1.60E-07	8760	0.05
3	**XT valves**	PWV (Production wing valve)	1.80E-07	8760	0.05
		DCV (Directional control valve)	6.00E-07	8760	0.05
		CIV (Chemical injection valve)	2.20E-07	8760	0.05
		DCV (Directional control valve)	6.00E-07	8760	0.05
		PMV (Production master valve	1.80E-07	8760	0.05
		DCV (Directional control valve)	6.00E-07	8760	0.05
4	**DHSV**	DSHV	3.20E-06	8760	0.05
		DCV (Directional control valve)	6.00E-07	8760	0.05

Table 8: PFD calculation for each component and subsystem

Group	Sub-system	Component typical	Voting level 1	Voting level 2	PFD level 1	PFD level 2
1	**ESD node**	ESD node	1oo1		8.76E-04	
2	**EPCU and Dump valve**	ESD relay	1oo1		8.76E-04	
		ESD contactor 1	1oo1	1oo2	1.31E-03	6.80E-05
		ESD contactor 2	1oo1		1.31E-03	
		Dump valve	1oo1		7.01E-04	
3	**XT valves**	PWV	4oo4	1oo3	7.01E-03	1.85E-04
		DCV				
		CIV				
		DCV				
		PMV	2oo2		3.42E-03	
		DCV				
4	**DHSV**	DSHV	2oo2		1.66E-02	
		DCV				

Table 9: Calculated PFD for each subsystem and overall SIS

Subsystem	**PFD**	**Relative contribution to PFD**	**SIL3 compliant**	**SIL2 compliant**
ESD Node	8.76E-04	34.75 %	Yes	
EPCU (Electrical)	9.44E-04	37.45 %	Yes	
SCM (Dump) valve	7.01E-04	27.80 %	Yes	
XT valves, DHSV valves	1.85E-04	6.83 %	Yes	
Total PFD	2.71E-03	100.00 %	No	Yes

The overall conclusion is that above mentioned SIS does not fulfil the SIL3 requirements. The reason of un-fulfilment of the SIL3 requirement of the SIS is beyond the scope of the thesis.

7.3 DETAILED ANALYSIS

7.3.1 Selection of tool for analysis

This the case study is for the modification phase of an existing installation, where the modification of SIS configuration is not possible. So, sensitivity study or importance measure will be of no use. Semi-quantitative uncertainty assessment should be given more weight. However, a quantitative uncertainty assessment is also presented here to show the work procedure for practical case example.

7.3.2 Semi-quantitative uncertainty assessment

When selecting a framework for semi-quantitative analysis, one should keep in mind that, capturing the entire complexity of the system and all the physical influencing factors in a model is not possible. But one can try to identify the most dominant factors that significantly influence safety (Schönbeck, Rausand, and Rouvroye 2010). Safety influencing factors which are considered for current case study are presented below along with the detailed evaluation and impact on the system.

Table 10: Example of uncertainty influencing factors (Abrahamsen and Røed 2011)

Main categories	Sub-categories	Evaluation with details	Impact on system as a measure of the uncertainty
Human aspects	Competence and training	Lack of experience among the crew about dealing with the same operation	High
	Training for operating personnel	Will be trained in advance before starting the operation	Medium
Technical aspects	Environmental aspects	Harsh environment at offshore	Medium
	Internal: fluid composition	High uncertainties on fluid Composition. May result in corrosion and other challenges	High
	New or well-known technology	New equipment: Limited experience with the equipment to be installed subsea	High
	Well characteristics	Challenging condition: High pressures and unknown reservoir characteristics	High
Operational aspects	Experience with subcontractors	New subcontractor (first Operation). Limited experience from Norwegian Continental Shelf	High
	Planning, coordination, control	Have the necessary preparation for the execution of operational and maintenance tasks	Low
	Maintenance	No specific challenges	Low
	Documentation	Have adequate written and oral information about performing the operational and maintenance tasks in a correct and safe manner	Low

At first, as described in section 5.2.2.2, a weight is given to each factor depending on their contribution to the system behavior. These weights have to be normalized then. The weight factor, Wi for qualitative factor, i is calculated in such a way that $\sum_{i=1}^{n} W_i = 1$:

$$W_i = \frac{\widetilde{W\imath}}{\sum_{i=1}^{n} \widetilde{W_\imath}}$$

In our case study, it is assumed that each factor has equal contribution to SIS performance. Weight factor (W_i) is calculated according to that.

In the next step, (described in section 0), to quantify the uncertainty severity of these uncertainty influencing factors (i), a scale is assigned, where R_i=1/3 expresses low uncertainty, R_i=2/3 indicates medium uncertainty and R_i=3/3=1 indicates high uncertainty. Uncertainty weighted rating (R_iW_i) is calculated by multiplying R_i and W_i. Details calculations are shown in the next table.

Table 11: Calculation of weight factor, uncertainty rating and uncertainty weighted rating

Uncertainty influencing factor, i	Weight	Weight factor W_i	Uncertainty Rating R_i	Uncertainty weighted rating R_iW_i
1	1	0.10	1.000	0.111
2	1	0.10	0.667	0.074
3	1	0.10	0.667	0.074
4	1	0.10	1.000	0.111
5	1	0.10	1.000	0.111
6	1	0.10	1.000	0.111
7	1	0.10	1.000	0.111
8	1	0.10	0.333	0.037
9	1	0.10	0.333	0.037
10	1	0.10	0.333	0.037

The actual SIL rating after taking into consideration of the uncertainties can be calculated as follows (shown in section 0):

$$SIL_{uncertain} = \left[1 - \left\{(1-\xi).\left(\sum_{i=1}^{n} R_i W_i\right)\right\}\right].\ \mathrm{SIL}_{Calculated}$$

Where, ξ is the strength of knowledge.

$\mathrm{SIL}_{\mathrm{Calculated}}$ is previously determined SIL calculated by deterministic method. Obtained SIL value is 2, calculated by PDS method.

Taking different ξ values, following $\mathrm{SIL}_{\mathrm{uncertain}}$ values can be obtained:

Table 12: SIL value after the semi-quantitative uncertainty assessment

Value of ξ	SIL value after the uncertainty analysis	Value of ξ	SIL value after the uncertainty analysis
0.1	0,680	0.6	1,413
0.2	0,827	0.7	1,560
0.3	0,973	0.8	1,707
0.4	1,120	0.9	1,853
0.5	1,267	1	2,000

As the weight factor and the uncertainty rating is assigned arbitrarily in the first case, to check the consistency of the analysis result, some additional calculations is performed (case 2 and case 3).

Case 2

For this case, the same weight factor is assigned and it is assumed that each uncertainty influencing factor affects the system highly. So in this case uncertainty contribution of these factors will be high. Therefore, the overall system is highly uncertain. The uncertainty rating (Ri) will be equal to 1 for each factor i. SIL value after implementing the uncertainty model is shown here:

Table 13: Semi-quantitative uncertainty assessment and obtained SIL value for case 2

Uncertainty influencing factor, i	Weight Wi	Weight factor Wi	Uncertainty Rating Ri	Uncertainty weighted rating RiWi	Value of ξ	SIL value after uncertainty analysis
1	1	0.10	1.000	0.111	0.1	0.20
2	1	0.10	0.667	0.074	0.2	0.40
3	1	0.10	0.667	0.074	0.3	0.60
4	1	0.10	1.000	0.111	0.4	0.80
5	1	0.10	1.000	0.111	0.5	1.00
6	1	0.10	1.000	0.111	0.6	1.20
7	1	0.10	1.000	0.111	0.7	1.40
8	1	0.10	0.333	0.037	0.8	1.60
9	1	0.10	0.333	0.037	0.9	1.80
10	1	0.10	0.333	0.037	1	2

Case 3

For this case, the same weight factor is assigned and it is assumed that the contribution of each uncertainty influencing factor of the system is low. In this case the uncertainty rating will be equal to 1/3. SIL value after implementing the uncertainty model is shown below:

Table 14: Semi-quantitative uncertainty assessment and obtained SIL value for case 3

Uncertainty influencing factor, i	Weight Wi	Weight factor Wi	Uncertainty Rating Ri	Uncertainty weighted rating RiWi	Value of ξ	SIL value after uncertainty analysis
1	1	0.10	0.333	0.033	0.1	1,406
2	1	0.10	0.333	0.033	0.2	1,472
3	1	0.10	0.333	0.033	0.3	1,538
4	1	0.10	0.333	0.033	0.4	1,604
5	1	0.10	0.333	0.033	0.5	1,67
6	1	0.10	0.333	0.033	0.6	1,736
7	1	0.10	0.333	0.033	0.7	1,802
8	1	0.10	0.333	0.033	0.8	1,868
9	1	0.10	0.333	0.033	0.9	1,934
10	1	0.10	0.333	0.033	1	2

Results are plotted in a chart for a better review.

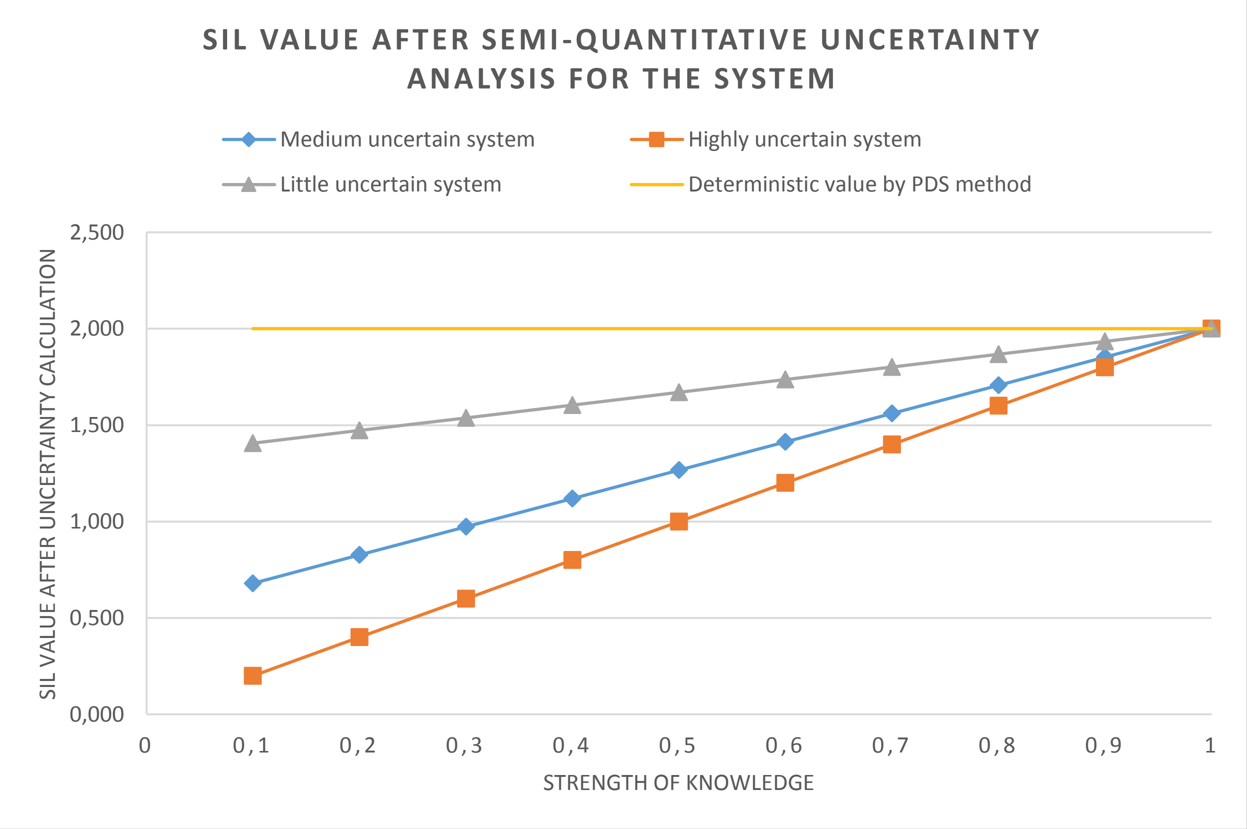


Figure 16: SIL value after semi-quantitative Uncertainty analysis for the system

From the chart it can be seen that for the highly uncertain system if strength of knowledge is poor, then SIL value after uncertainty analysis deviates much from the SIL value calculated by deterministic method. For the little uncertain system this difference is very low. The difference between uncertain SIL value and the deterministic SIL value reduces with the increase of strength of knowledge. For ξ=1, which means the analyst is 100% sure about the system and analysis, the uncertain SIL value will be equal to the deterministic SIL value, which can be very rare in the practical situation. However, the overall trend shows the consistency of the proposed formula. In this framework, system uncertainty factors and strength of knowledge dimension are considered simultaneously. The necessity to take into consideration of both the uncertainty factors and strength of knowledge is described in section 5.1.1 in details. One may raise the question that as in the semi-quantitative analysis we are analyzing the uncertainty factors concealed in the background knowledge, why do we need to consider the strength of knowledge assignment again. It is tried to give the answer to this question is that section.

7.3.3 Quantitative uncertainty analysis: MC simulation

7.3.3.1 Procedure

Here, uncertainty analysis in SIL estimation is performed by MC simulation where PFD is calculated by the PDS method of approximated formula.

Following the proposed framework presented in section 5.2.1.3, sampling is done for failure rate data, common cause failure and test interval. To treat uncertainty in the failure rate of various components in the system, exponential distribution is assigned to failure rate with a median. The median value, collected from the database, is frequentist probability (failure rate data obtained from similar installation). For β factor, interval probabilities are assigned with a range of 1% to 10%. This interval is assigned on the basis of database value, from which it is seen that for various components like topside/subsea equipment, β factor value lies in the interval. Constant value is assigned for the test interval, as this value is known exactly.

The present SIS has 13 components. For each component, $PFD_{1...}PFD_{13}$ are calculated using each uncertain input variables. The number of iterations in this step is 50000 to increase accuracy of the result. Overall PFD is calculated simultaneously for each varying PFD. Several test cases for variable input parameters are simulated and resulted are summarized in the Table 16. 95 percentile value is taken as the final outcome which means that we are 95% sure that the value lies at or below the value.

To specify the obtained results more precisely, SIL level is defined in details according to the PFD value in the similar way as shown in table 15.

Where, SIL level follows the following interval of PFD:
SIL 3 region: 0.0001 to 0.001
SIL 2 region: 0.001 to 0.01
SIL 1 region: 0.01 to 0.1

Table 15: PFD value and corresponding SIL level

PFD value	0.0001	0.0002	0.0003	0.0004	0.0005	0.0006	0.0007	0.0008	0.0009	0.001
SIL Approximated value	3.9	3.8	3.7	3.6	3.5	3.4	3.3	3.2	3.1	3
PFD value	0.001	0.002	0.003	0.004	0.005	0.006	0.007	0.008	0.009	0.01
SIL Approximated value	2.9	2.8	2.7	2.6	2.5	2.4	2.3	2.2	2.1	2
PFD value	0.01	0.02	0.03	0.04	0.05	0.06	0.07	0.08	0.09	0.1
SIL Approximated value	1.9	1.8	1.7	1.6	1.5	1.4	1.3	1.2	1.1	1

7.3.3.2 Result

Table 16: Results of various case studies of MC simulation (using @risk software)

case	**Input parameters**	**PFD (50 percentile)**	**PFD (95 percentile)**	**SIL level**
1	λ is exponentially distributed with mean value taken from database (PDS Data Handbook 2013) Test interval – constant β –constant (0.05, (PDS Data Handbook 2013))	2.68E-3	5.39E-3	2.5
2	λ is exponentially distributed with mean value taken from database Test interval – constant β –uniformly distributed (1% to 10%)	2.73E-3	5.44E-3	2.5
3	λ is exponentially distributed (mean=0.00001) Test interval – constant β –uniformly distributed (1% to 10%)	1.11E-01	2.36E-01	0
4	λ is exponentially distributed with mean value taken from database Test interval – constant β –beta distribution (2,2)	4.65E-3	8.21E-3	2.2
5	λ is uniformly distributed taking 90% interval of mean value taken from database Test interval – constant β –interval value (0.045,0.0552)	2.71E-3	2.84E-3	2.8
6	λ is Weibull distributed (α=2,β=0.00001) Test interval – constant β –uniformly distributed (1% to 10%)	9.65E-2	1.49E-1	1
7	λ is lognormal distribution (μ=0.00001,σ=0.00001) Test interval – constant β –uniformly distributed (1% to 10%)	1.12E-1	2.32E-1	0
8	λ is uniformly distributed (0.00001,0.00001) Test interval – constant β –uniformly distributed (1% to 10%)	5.3E-2	8.34E-2	1.2
9	λ is triangular distribution (0.000001,mean value, 0.00001) Test interval – constant β –constant	3.88E-02	6.45E-2	1.4
10	λ is uniformly distributed (0.000001,0.00001) Test interval – constant β –constant	5.84E-2	8.56E-2	1.2

The simulation case was also checked with a programming language (Scilab) to check the consistency of the result of @risk. The result shows the similar tendency. Two test cases are performed by Scilab. The first case is for variable failure rate. The number of trial was 50000 in this case. The second case is for variable failure rate and beta factor. The number of trial is 500 for lambda value and 50 for beta factor value. For each variable input parameter output PFD is calculated and results are obtained both numerically and graphically. The test case 2 shows a little unexpected result (less uncertainty compared to case 1). The increasing number of trial will give more sophisticated result. One can see the code lines and plots in appendix C.

Table 17: Obtained PFD result for case 1, simulation carried by Scilab programming language

Subsection	Min	Max	St.Dev	50 percentile	95 percentile	SIL
ESD node	1.38E-04	1.38E-04	2.06E-04	3.46E-04	7.93E-04	3.3
EPCU	5.79E-04	3.67E-03	8.68E-04	1.46E-03	3.35E-03	2.7
LPDV	5.51E-04	3.48E-03	8.23E-04	1.39E-03	3.17E-03	2,9
XTV	6.13E-05	3.94E-04	9.32E-05	1.55E-04	3.59E-04	3.9
Overall	1.33E-03	8.41E-03	1.99E-03	3.34E-03	7.67E-03	2.3

Table 18: Obtained PFD result for case 2, simulation carried by Scilab programming language

Subsection	Min	Max	St. Dev	50 percentile	95 percentile	SIL
ESD node	1.38E-04	8.70E-04	2.06E-04	3.46E-04	7.96E-04	3.3
EPCU	5.57E-04	3.84E-03	8.63E-04	1.44E-03	3.32E-03	2.7
LPDV	5.51E-04	3.48E-03	8.25E-04	1.39E-03	3.18E-03	2.7
XTV	1.23E-05	7.81E-04	1.26E-04	9.87E-05	4.14E-04	3.6
total	1.26E-03	8.97E-03	1.97E-03	3.29E-03	7.57E-03	2.3

7.3.3.3 Discussion

After the MC simulation, Output distribution is obtained for each input distribution from which statistical data is extracted. 95 percentile of PFD value is used to determine SIL rating after the uncertainty assessment, which will give higher confidence in decision making.

Various cases are simulated to make a comparison. For the first case, exponentially distributed failure rate with mean value, constant β factor and constant functional test interval is used. Mean failure rate value, is taken from PDS handbook. The result of PFD distribution deviates much from the deterministic result obtained by PDS method. The overall PFD is more than 2 times when 95 percentile of the distribution is considered, but the SIL rating still belongs to the SIL2 zone.

After analyzing the other case study it is seen that, SIL rating may vary from SIL2 to SIL0 for various case study. Functional test interval time is assumed constant for all cases as this is normally fixed by the operation team before carrying out the activity. SIL0 rating is not so expectable, because these are the cases where failure rate is assumed to be

Weibull or lognormal distributed. However, it is a questionable topic to scientists whether failure rate should be assumed as exponentially distributed or Weibull distributed.

The same question remains for the other input parameter e.g., whether β factor should be assumed as constant or uniform distributed or beta distributed. In PDS data handbook, β factor ranges are observed as maximum 10 % and minimum 2% for various safety instrumented components including topside equipment. So in the present cases β factor interval (1% to 10%) are used as input distribution and changes in the output result is observed, which indicates that for this small variation for β factor values does not impact much the output distribution. SIL0 rating is obtained for one additional case, where a very high failure rate is assumed for each component of the system which may not be true for today's modern, highly reliable instrumented system.

Overall analysis gives the indication to the decision maker that in certain situations, the overall SIL of the SIS may reduce to SIL1 or lower SIL 2 value. MC simulation just provides an estimate of the uncertainty of the output quantity. The accuracy of the result depends on the number of MC sampling of input parameters. Higher values of sampling yields a higher accuracy of the output uncertainty distribution estimate, but increases computational time. In present case, simulation is performed by using 50000 random trial by checking that this number of trial will give a stable result. This estimate may be subjected to an error that depends on the number of MC sampling of the aleatory quantities. Higher values of sampling yields a higher accuracy of the output uncertainty distribution estimate.

7.3.4 Review of result and limitation of analysis

As a part of detailed analysis of the SIL verification process, semi-quantitative uncertainty analysis is proposed as starting analysis method. As the case study is for a system of an existing platform where the modification of the system configuration is not possible, sensitivity analysis and importance measure were not performed. As a supplement of this semi-quantitative uncertainty analysis, quantitative uncertainty analysis is also performed. The results of two analyses are shown below:

Table 19: SIL value after quantitative and semi-quantitative uncertainty analysis:

	Determined by PDS method	After semi-quantitative uncertainty analysis (for a medium uncertain system, assuming ξ=0.5)	After quantitative uncertainty analysis (MC simulation)
SIL value	2	1.2	1.2
%Factor subjected to uncertainty		57.1%	57.1%

From overall analysis, it can be seen that SIL value may range from lower value of SIL2 to SIL1 after implementing the uncertainty model. The quantitative uncertainty analysis result shows a quite higher percentage of uncertainty comparative to semi-quantitative uncertainty analysis. In semi-quantitative uncertainty analysis, strength of knowledge of the analyst may affect the SIL value in a large amount (Figure 16). So the results shown in the table cannot be taken as absolute value.

The developed semi-quantitative uncertainty model is quite straight-forward to follow and contains a simple calculation method. This model needs to be further tested for different SIS for different applications. Moreover, the dimension of strength of knowledge is difficult to predict in practical situation. Uncertain factors are considered independent. Overlaps and interdependencies are not taken into account. More details are discussed in section 6.2.

On the other hand, quantitative uncertainty analysis performed by MC simulation is a well-established method in literature and industry. However, MC simulation just provides an estimate of the uncertainty (variation) of the output quantity. This estimate may be subjected to an error that depends on the number of MC sampling of the aleatory quantities. 50000 random trial is performed for the present case. Higher values of sampling yields a higher accuracy of the output uncertainty distribution estimate.

The scope of the thesis is not to assess which method is better. This thesis proposes semi-quantitative uncertainty analysis as a starting point in detailed analysis of SIL verification. In the case of further investigation of the system or the analyst is not confident about semi-quantitate uncertainty analysis, quantitative analysis can be carried out as a supplement to semi-quantitative analysis.

7.4 Decision making

7.4.1 Risk mitigation

Overall analysis gives the indication to the decision maker that in certain situations, the overall SIL of the SIS may reduce to SIL1 or lower SIL 2 value. So enough risk mitigation measures should be proposed for current SIS.

Depending on the SIL decision, the decision maker may choose analysis based approach or cautionary or precaution based approach for risk mitigation. Decision analysis should reveal the potential costs associated with an alternative. The analysis-based approach gives weight to the traditional assessment method like statistical analysis, risk assessment, cost benefit analyses. Stakeholder may become involved also in this process which is called discourse based approach. Different prevention measures may be appropriate for various situations. In times, decision makers have to choose one specific option from a set of possible options.

How to select the best suitable measure for specific situation or organization needs detailed analysis, which is not focus of this thesis and not discussed here. The result of current cases (subsea SIS, which was installed a long time ago and no equipment modification is possible) advises the decision maker that potential risk reduction measures should be implemented. The cautionary or precautionary principle may be given weight to reduce risks and uncertainties. However, the level of caution should to be balanced with other concerns like costs, operating constraint. All industries are advised to follow some minimum requirements to protect people and the environment as a priori requirement.

As a summary, the following work process is followed for present case study:

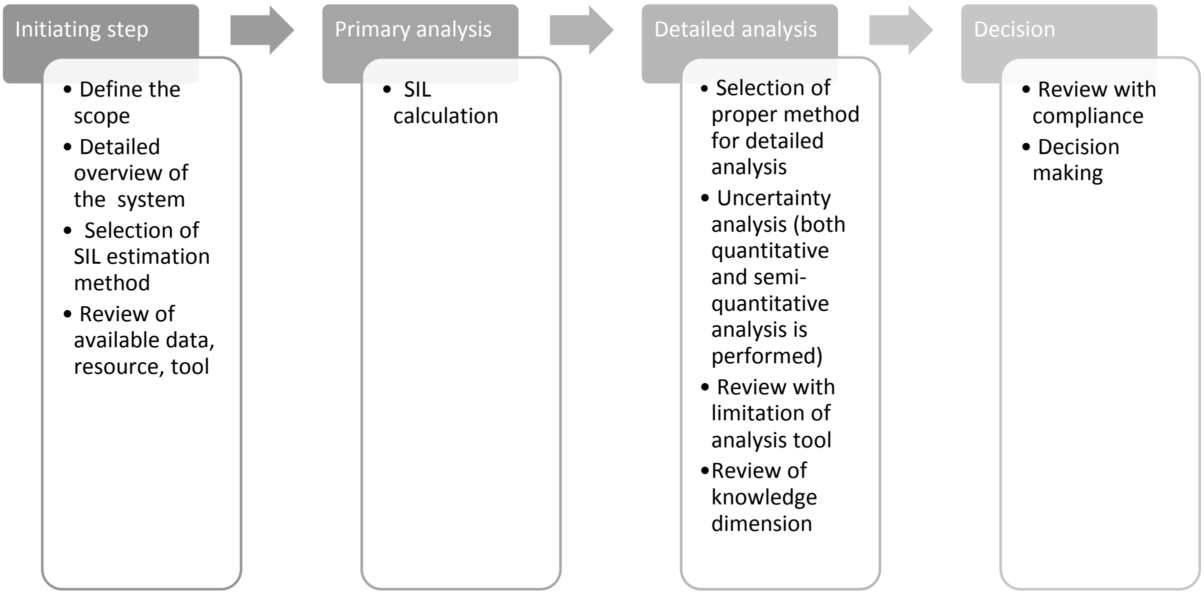

Initiating step
• Define the scope
• Detailed overview of the system
• Selection of SIL estimation method
• Review of available data, resource, tool
Primary analysis
• SIL calculation
Detailed analysis
• Selection of proper method for detailed analysis
• Uncertainty analysis (both quantitative and semi-quantitative analysis is performed)
• Review with limitation of analysis tool
•Review of knowledge dimension
Decision
• Review with compliance
• Decision making

Figure 17: Performed steps for SIL verification for the presented case study

8 CONCLUSION AND FUTURE WORK

This thesis proposes a systematic work flow of the SIL verification process. A framework is proposed for the treatment of uncertainty in various decision context. The overall idea is to present a systematic approach to merge the proposed approaches to support decision making. Two methods are presented for uncertainty treatment, between them one is the quantitative method based on MC simulation and another is the semi-quantitative method which takes into account uncertainty factors concealed in the background knowledge. The motivation of the development of the framework of semi-quantitative method is based on the logic that the uncertainty analysis should not be carried out only in the mathematical or quantitative framework. One should look beyond this objective evaluation. One should look ahead of the background knowledge which affects the safety integrity level of safety instrumented system. Qualitative or semi-quantitative uncertainty analysis should be a starting point of detailed analysis of SIL verification in practical application.

The proposed methods are executed with a case study. Case study was the subsea well isolation system for an existing installation. Quantitative uncertainty analysis based on MC simulation, proposed in the thesis, is already established in literature. However, for most of the simulation cases, SIL was determined by the method proposed by IEC standard. For this thesis, SIL is determined by PDS method and MC simulation is carried out based on PDS method.

The semi-quantitative method proposed in the thesis, takes into consideration of MTO perspectives for uncertainty treatment. This work is motivation of the previous two works presented by Abrahamsen and Røed (2011) and Schönbeck, Rausand, and Rouvroye (2010). The present approach combines the above mentioned two ideas into one framework. The whole framework is described in the view of risk management perspective. The framework is executed with the same case study and model is checked for consistency by varying various parameters.

This semi-quantitative model is verified in the sense that obtained results by this model have been compared with the results obtained from MC simulation applied in the practical case example. However, overlapping, inter-dependencies was not taken into account which may influence the correctness of evaluations. Correct evaluations require the mutual independence and the minimum overlap between every criteria. Treatment of interdependencies and overlaps is not implemented in the tool and requires further analysis and treatment in the selection and weighting process. Further scientific investigations and a number of case studies can be performed in the future with this semi-quantitative model which may direct the researchers toward the more developed and sophisticated approach of the model.

Overall analysis can be a guide work for the SIL analysts how the uncertainty analysis can be done in a practical case example and how the decision should be made. Further, the presentation of this semi-quantitative approach will provide a robust and simplified new model toward the uncertainty treatment of SIL verification.

BIBLIOGRAPHY

Abrahamsen, E. B., and W. Røed. 2011. “A NEW APPROACH FOR VERIFICATION OF SAFETY INTEGRITY LEVELS.” *LIA*, 20.

Abrahamsson, Marcus. 2002. “Uncertainty in Quantitative Risk Analysis-Characterisation and Methods of Treatment.” PhD, Department of Fire Safety Engineering, Lund University.

Aven, T. 2011. “Interpretations of Alternative Uncertainty Representations in a Reliability and Risk Analysis Context.” *Reliability Engineering & System Safety* 96 (3): 353–60.

Aven, Terje. 2010. Misconceptions of Risk. Chichester, West Sussex, U.K: Wiley.

Aven, Terje. 2010 "On how to define, understand and describe risk." Reliability Engineering & System Safety 95.6 (2010): 623-631.

Aven, Terje. "On how to conceptualise and describe risk." (2011).

Aven, Terje. "Practical implications of the new risk perspectives." Reliability Engineering & System Safety 115 (2013): 136-145.

Aven, Baraldi, Flage, and Zio. 2014. *Uncertainty in Risk Assessment: The Representation and Treatment of Uncertainties by Probabilistic and Non-Probabilistic Methods*. March. Somerset, NJ, USA: John Wiley & Sons.

Aven, Terje, and Enrico Zio. 2011. “Some Considerations on the Treatment of Uncertainties in Risk Assessment for Practical Decision Making.” *Reliability Engineering & System Safety* 96 (1): 64–74.

Aven, Terje, and Bodil S. Krohn. 2014. “A New Perspective on How to Understand, Assess and Manage Risk and the Unforeseen.” *Reliability Engineering & System Safety* 121 (January): 1–10.

Aven, T., and T.E. Nøkland. 2010. “On the Use of Uncertainty Importance Measures in Reliability and Risk Analysis.” *Reliability Engineering & System Safety* 95 (2): 127–33.

Baudrit, Cédric, and Didier Dubois. 2006. “Practical Representations of Incomplete Probabilistic Knowledge.” *Computational Statistics & Data Analysis* 51 (1): 86–108.

Charlwood, Mark, Shane Turner, and Nicola Worsell. 2004. *A Methodology for the Assignment of Safety Integrity Levels (SILs) to Safety-Related Control Functions Implemented by Safety-Related Electrical, Electronic and Programmable Electronic Control Systems of Machines*. HSE Books.

Compass Resource Management. 2015. “Structured Decision Making.” Accessed May 27. http://www.structureddecisionmaking.org/steps/decisioncontext/.

Ferson, S, and R Kuhn. 1992. “Propagating Uncertainty in Ecological Risk Analysis Using Interval and Fuzzy Arithmetic.” *IN: Computer Techniques in Environmental Studies IV. Computational Mechanics Publications, Boston. 1992. P 387-401, 4 Fig, 14 Ref.*

Hauge, Stein, Mary Ann Lundteigen, Per Hokstad, and Solfrid H\a abrekke. 2010. “Reliability Prediction Method for Safety Instrumented Systems–pds Method Handbook, 2010 Edition.” *SINTEF Report STF50 A* 6031.

Helton, Jon C, Jay Dean Johnson, Cedric J Sallaberry, and Curt B Storlie. 2006. “Survey of Sampling-Based Methods for Uncertainty and Sensitivity Analysis.” *Reliability Engineering & System Safety* 91 (10): 1175–1209.

Helton, Jon C., Jay D. Johnson, William L. Oberkampf, and Cedric J. Sallaberry. 2008. “Representation of Analysis Results Involving Aleatory and Epistemic Uncertainty.” SAND2008-4379. California: Sandia National Laboratories.

IEC. 2000. “Functional Safety of Electrical/electronic/programmable Electronic Safety Related Systems.” International Electrotechnical Commision.

Innal, Fares. 2008. “Contribution to Modelling Safety Instrumented Systems and to Assessing Their Performance Critical Analysis of IEC 61508 Standard.” University of Bordeaux.

Innal, Fares, Yves Dutuit, and Mourad Chebila. 2013. “Monte Carlo Analysis and Fuzzy Sets for Uncertainty Propagation in SIS Performance Assessment.” *International Journal of Mathematical, Computational, Physical and Quantum Engineering* 7 (11).

Jin, H., M. A. Lundteigen, and M. Rausand. 2012. “Uncertainty Assessment of Reliability Estimates for Safety-Instrumented Systems.” *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability* 226 (6): 646–55. doi:10.1177/1748006X12462780.

Jin, Hui. 2013. “A Contribution to Reliability Assessment of Safety-Instrumented Systems.” Trondheim, Norway: Norwegian University of Science and Technology.

Jin, Hui, Mary Ann Lundteigen, and Marvin Rausand. 2011. “Reliability Performance of Safety Instrumented Systems: A Common Approach for Both Low- and High-Demand Mode of Operation.” *Reliability Engineering and System Safety* 96 (3). Elsevier: 365–73.

Kima, Sungteak, Kwangpil Changa, Younghun Kima, and Eunhyun Parka. 2014. “Uncertainty Analysis for Target SIL Determination in the Offshore Industry.” In . Honolulu, Hawaii. http://psam12.org/proceedings/paper/paper_388_1.pdf.

Kiureghian, Armen Der, and Ove Ditlevsen. 2009. “Aleatory or Epistemic? Does It Matter?” *Structural Safety* 31 (2). Elsevier Ltd: 105–12. doi:10.1016/j.strusafe.2008.06.020.

Lundteigen, Mary Ann, and Marvin Rausand. 2006. “Assessment of Hardware Safety Integrity Requirements.” In *Proceedings of the 30 Th EDReDA Seminar*. Trondheim, Norway.

Lundteigen, Mary Ann, and Marvin Rausand. 2007. “Common Cause Failures in Safety Instrumented Systems on Oil and Gas Installations: Implementing Defense Measures through Function Testing.” Journal of Loss Prevention in the Process Industries 20 (3): 218–29.

Lundteigen, Mary Ann, and Marvin Rausand. 2009. “Architectural Constraints in IEC 61508: Do They Have the Intended Effect?” Reliability Engineering & System Safety 94 (2): 520–25.

Mechri, W., C. Simon, and K. Ben Othman. 2011. “Uncertainty Analysis of Common Cause Failure in Safety Instrumented Systems.” In *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, 225:450–60.

Nilsen, Thomas, and Terje Aven. 2003. “Models and Model Uncertainty in the Context of Risk Analysis.” *Reliability Engineering & System Safety* 79 (3): 309–17.

Oberkampf, William L., and Christopher J. Roy. 2010. *Verification and Validation in Scientific Computing*. Cambridge University Press.

OLF, Guidline. 2004. “OLF 070:Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry.” *The Norwegian Oil Industry Association* 2.

PDS Data Handbook. 2013. *Reliability Data for Safety Instrumented Systems*. SINTEF Technology and Society.

PDS method, Handbook. 2013. *Reliability Prediction Method for Safety Instrumented Systems*. Vol. 6031. SINTEF Technology and Society.

Rausand, Guro. 2005. “Uncertainty Management in Reliability Analyses.” Master’s thesis. Norwegian University of Science and Technology (NTNU), 2005, Trondheim, Norway.

Rausand, Marvin, and Arnljot Høyland. 2004. *System Reliability Theory: Models, Statistical Methods, and Applications*. Vol. 396. John Wiley & Sons.

Redmill, F. 1999. “Understanding Safety Integrity Levels.” *Measurement and Control* 32: 197–200.

Sallak, M., C. Simon, and J.-F. Aubry. 2008. “A Fuzzy Probabilistic Approach for Determining Safety Integrity Level.” *IEEE Transactions on Fuzzy Systems* 16 (1): 239–48.

Schönbeck, Martin, Marvin Rausand, and Jan Rouvroye. 2010. “Human and Organisational Factors in the Operational Phase of Safety Instrumented Systems: A New Approach.” *Safety Science* 48 (3): 310–18.

Smith., David J. 2001. *Reliability, Maintainability and Risk*. *Butterworth-Heinemann Linacre House, Jordan Hill, Oxford*. 6th ed.

Spellemaeker, M, and L Witrant. 2007. “How to Determine the Safety Integrity Level (SIL) of a Safety System.” *URL: Http://www. Indsci. com/docs/Press/PIN_0907. pdf.(Reached on: 08.03. 2013)*.

Veland, H., and T. Aven. 2013. “Risk Communication in the Light of Different Risk Perspectives.” *Reliability Engineering & System Safety* 110 (February): 34–40.

Wang, Y, HH West, and MS Mannan. 2004. “The Impact of Data Uncertainty in Determining Safety Integrity Level.” *Process Safety and Environmental Protection* 82 (6): 393–97.

Zio, Enrico. 2013. The Monte Carlo Simulation Method for System Reliability and Risk Analysis. Springer Series in Reliability Engineering. London: Springer London.

APPENDIX A: ACRONYMS AND MATHEMATICAL NOTATION

A.1 ACRONYMS

CCF	Common Cause Failure
CIV	Chemical Injection Valve
DC	Diagnostic coverage
DCV	Directional Control Valve
DD	Dangerous Detected
DHSV	Downhole Safety Valve
DU	Dangerous Uundetected
ESD	Emergency Shut Down
EUC	Equipment under control
FMEA	Failure Mode and Effects Analysis
FMECA	Failure Mode Effects and Criticality Analysis
HAZID	Hazard identification
HFT	Hardware Fault Tolerance
IEC	International Electrotechnical Commission
MC	Monte Carlo
MooN	M out of N
MTO	Man-Technology-Organization
MTTR	Mean Time to Repair
NPD	Norwegian Petroleum Directorate
OREDA	Offshore Reliability Data
PDS	Reliability of Safety Instrumented Systems (Norwegian Abbreviation)
PFD/PFD_{avg}	Probability of Failure on Demand
PFH	Probability of Failure per Hour
PMV	Production Master Valve
PWV	Production Wing Valve
SCM	Subsea Control Module
SD	Safe Detected
SFF	Safe Failure Fraction
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SU	Safe Undetected
XT	X-mas Tree

A.2 MATHEMATICAL NOTATION

β the fraction of random hardware failures of a single item that causes both items of a redundant pair to fail simultaneously, or within a short time interval, as a direct result of a shared cause.

λ_S Rate of safe (spurious trip) failures, including both undetected and detected failures
$\lambda_S = \lambda_{SU} + \lambda_{SD}$

λ_{DD} rate of dangerous detected failures

λ_{DU} Rate of dangerous undetected failures

λ_{SD} rate of safe detected failures; detected both by automatic self-test or manual test

λ_{SU} rate of safe undetected failures; undetected both by automatic self-test or manual test

C_{MooN} Modification factor for voting configuration

ξ Strength of knowledge

W_i Weight of uncertainty influencing factors

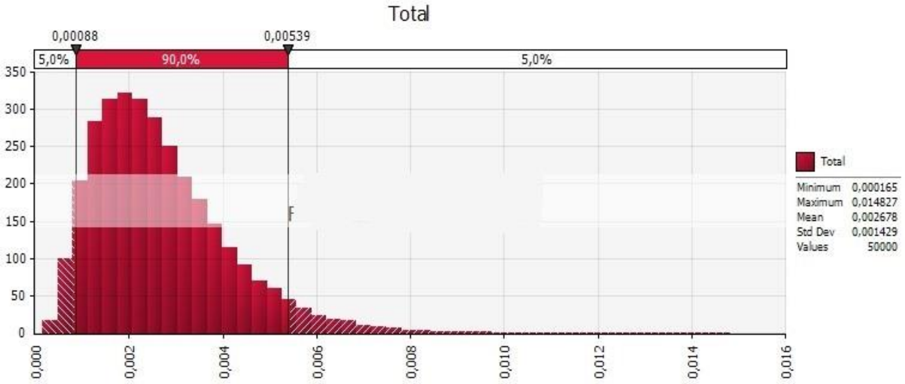
R_i Uncertainty rating

APPENDIX B: @RISK RESULT

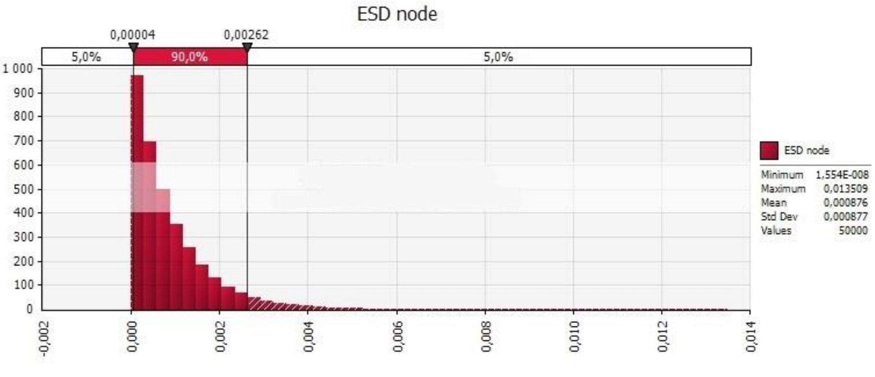
B.1 CALCULATION WITH @RISK

Here it is shown how the calculation was done in MS-excel using @risk add-on software. The first thing necessary is to define the distribution of failure rate (λ). In order to create the exponential distribution with constant failure rate, riskexpon (λ) function is used which creates the distribution automatically. For each failure rate PFD of each component is calculated for each varying failure rate. For the first case, constant beta factor and constant proof test interval are used. The output distribution is given as RiskOutput () + PFD formula. To define variable beta factor value, uniform distribution is given using riskunifor () function. Simulation is carried out using 50000 trial. The risk output can be found in a separate @RISK sheet with graph which are shown here.

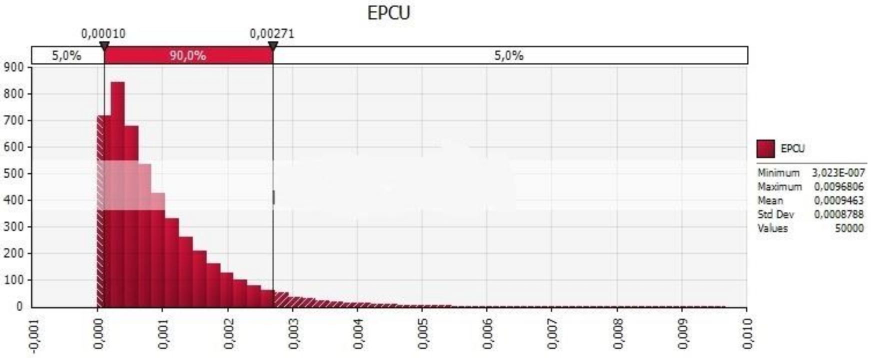
B.2 PLOTTING RESULTS



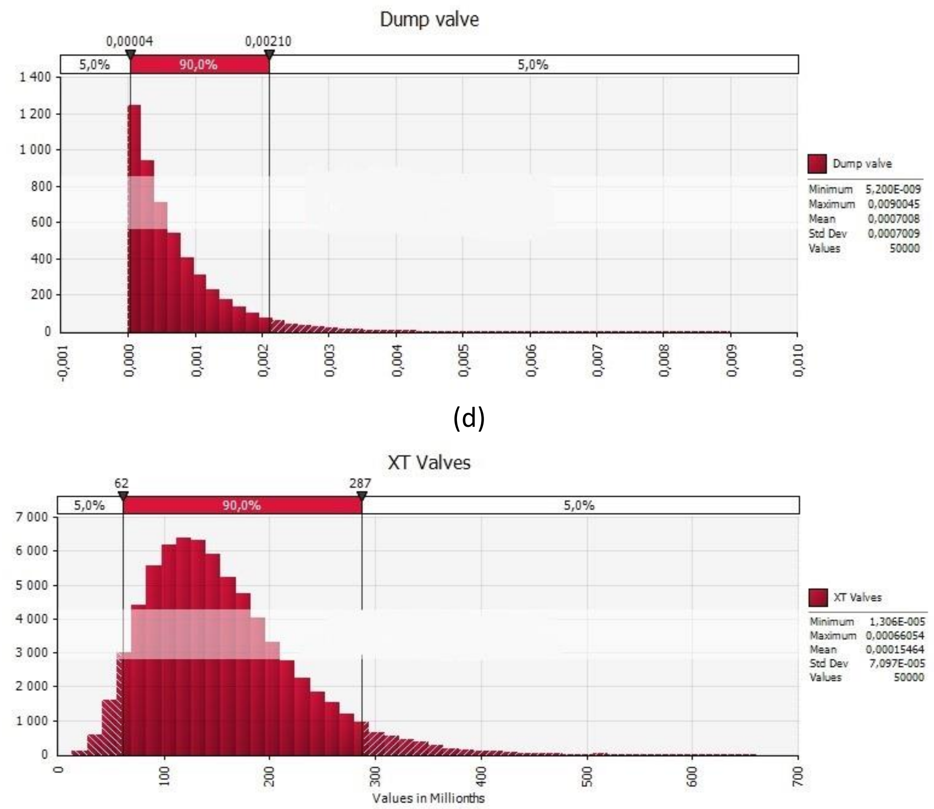
(a)



(b)



(c)



(d)

(e)

Figure 18: Output PFD distribution for a) Overall SIS b) ESD node c) EPCU d) SCM valve e) Xmas valve

APPENDIX C: SIMULATION BY SCILAB PROGRAMMING LANGUAGE

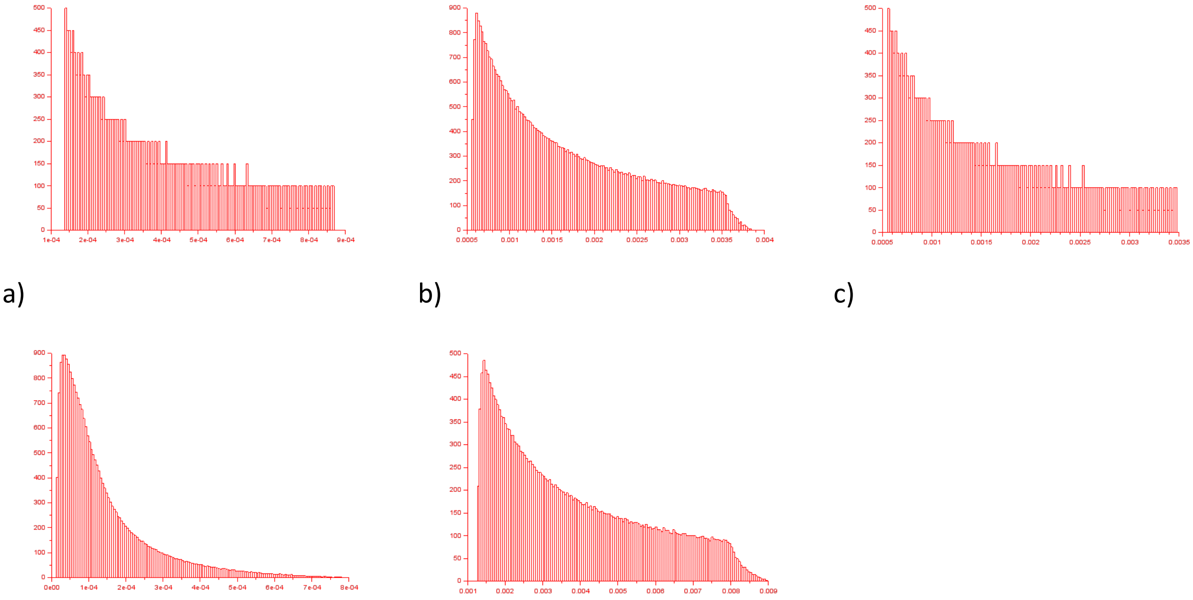
PROGRAMMING CODE

```
#Test case 1
#start the simulation
clear all
#number of trial
nr=50000;
# constant value of proof test interval and beta factor
tau1=2190;
tau2=8760;
beta1=0.05;
# variable failure rate (in the interval of $10^{-5}$ to $10^{-6}$) for each component,
lamda_du1=logspace (-6.1 ,-6.9 ,nr);
lamda_du2=logspace (-6.1 ,-6.9 ,nr );
lamda_du3=logspace (-6.1 ,-6.9 ,nr );
lamda_du5=logspace (-6.1 ,-6.9 ,nr );
lamda_du6=logspace (-6.1 ,-6.9 ,nr );
lamda_du7=logspace (-6.1 ,-6.9 ,nr );
lamda_du8=logspace (-6.1 ,-6.9 ,nr );
lamda_du9=logspace (-6.1 ,-6.9 ,nr );
lamda_du10=logspace (-6.1 ,-6.9 ,nr );
lamda_du11=logspace (-6.1 ,-6.9 ,nr );
lamda_du12=logspace (-5.1 ,-5.9 ,nr );
lamda_du13=logspace (-6.1 ,-6.9 ,nr );
# do the simulation
for i =1:nr
        ESDnode(i)=(lamda_du1(i)*tau1)/2;
        PFD2(i)=(lamda_du2(i)*tau2)/2;
        PFD34_common(i)=beta1*lamda_du3(i)*tau2/2;
        PFD34_ind(i)=((lamda_du3(i)*tau2)^2)/3;
        PFD34(i)= PFD34_common(i)+PFD34_ind(i);
        EPCU(i)=PFD2(i)+PFD34(i);
        LPDV(i)=(lamda_du5(i)*tau2)/2;
        PFD6(i)=tau2*(lamda_du6(i)+lamda_du7(i)+ lamda_du8(i)+ lamda_du9(i))/2;
        PFD10(i)=tau2*(lamda_du10(i)+ lamda_du11(i))/2;
        PFD12(i)=tau2*(lamda_du12(i)+ lamda_du13(i))/2;
        PFD610_ind(i)=2*PFD6(i)*PFD10(i)*PFD12(i);
        PFD610_common(i)=0.5*beta1*((PFD6(i)*PFD10(i)*PFD12(i))^(1/3));
        XTV(i)=PFD610_ind(i)+PFD610_common(i);
        total(i)=ESDnode(i)+EPCU(i)+LPDV(i)+XTV(i);
        save('ESD.sod','ESDnode', 'EPCU', 'LPDV', 'XTV', 'total')
end
# Finding min, max, percentiles value for each subsection
a_esd=min(ESDnode)
b_esd=max(ESDnode)
P50_esd=perctl(ESDnode,50)
P95_esd=perctl(ESDnode,95)
S=stdev(ESDnode)
#result plotting
clf(); histplot(90,total);
#define number of trial for lamda and beta
nr=500;
nrb=50;
#define constant value for proof test interval
tau1=2190;
tau2=8760;
#variable beta factor (from 0.01 to 0.1, taking 50 trial in each case)
beta1= logspace(-1,-2,nrb);
#variable failure rate (interval same as case 1, 500 trial in each case)
lamda_du1=logspace (-6.1 ,-6.9 ,nr);
#run the simulation
for i =1:nr
for j=1:nrb
ESDnode(i,j)=(lamda_du1(i)*tau1)/2;
PFD2(i,j)=(lamda_du2(i)*tau2)/2;
PFD34_common(i,j)=beta1(j)*lamda_du3(i)*tau2/2;
PFD34_ind(i,j)=((lamda_du3(i)*tau2)^2)/3;
PFD34(i,j)= PFD34_common(i,j)+PFD34_ind(i,j);
EPCU(i,j)=PFD2(i,j)+PFD34(i,j);
LPDV(i,j)=(lamda_du5(i)*tau2)/2;
PFD6(i,j)=tau2*(lamda_du6(i)+lamda_du7(i)+ lamda_du8(i)+ lamda_du9(i))/2;
```

```
PFD10(i,j)=tau2*(lamda_du10(i)+ lamda_du11(i))/2;
PFD12(i,j)=tau2*(lamda_du12(i)+ lamda_du13(i))/2;
PFD610_ind(i,j)=2*PFD6(i,j)*PFD10(i,j)*PFD12(i,j);
PFD610_common(i,j)=0.5*beta1(j)*((PFD6(i,j)*PFD10(i,j)*PFD12(i,j))^(1/3));
XTV(i,j)=PFD610_ind(i,j)+PFD610_common(i,j);
total(i,j)=ESDnode(i,j)+EPCU(i,j)+LPDV(i,j)+XTV(i,j)
save('try.sod','ESDnode', 'EPCU', 'LPDV', 'XTV', 'total')
end
end
#finding results similar as case 1
```

PLOT

Only test case 2 results are shown here:



a)

b)

c)

d)

e)

Figure 19: Output PFD distribution of a) ESD node b) EPCU c) SCM valve d) XT valves e) overall