Choice of Demand Mode for Subsea Safety Systems

Xiuyu He

Reliability, Availability, Maintainability and Safety (RAMS)
Submission date: July 2013
Supervisor: Jørn Vatn, IPK

Norwegian University of Science and Technology
Department of Production and Quality Engineering
Choice of Demand Mode for Subsea Safety Systems

Master's Thesis
He Xiuyu
Trondheim, June 2013
MASTER THESIS
2013
for
stud. techn. Xiuyu He

Choice of demand mode for subsea safety systems
(Valg av demand mode for undervanns sikkerhetssystemer)

The demand mode of operation for safety instrumented systems (SIS) is often classified into low demand, high demand and continuous demand of operation. It is not straightforward to discriminate between high and low demand although some standards propose ways to discriminate between these two modes of operation. For most SIS system low demand has been assumed, and research has put main emphasis on low demand systems. In recent years more attention has been paid to high demand systems, and several problems are encountered. In this master thesis the candidate shall especially:

1. Perform a literature review, and pay special attention to differences between high and low demand mode of operation.
2. Search for related work in other industries like the railway, nuclear and aviation industry.
3. Present, and compare the main frameworks for reliability assessment and architecture constraints for both high demand, and low demand mode of operation respectively.
4. Perform a case study (on a subsea related “grey area” system) where both the high demand, and low demand mode of operation is used as basis for the approaches, and discuss the results (including a quantitative / qualitative gap analysis)
5. Conclude on the approach both with respect to implications for standardization work, and for the company. The discussion should cover both the issue of SIL allocation, and reliability assessment

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

- An analysis of the work task’s content with specific emphasis of the areas where new knowledge has to be gained.
- A description of the work packages that shall be performed. This description shall lead to a clear definition of the scope and extent of the total task to be performed.
- A time schedule for the project. The plan shall comprise a Gantt diagram with specification of the individual work packages, their scheduled start and end dates and a specification of project milestones.
The pre-study report is a part of the total task reporting. It shall be included in the final report. Progress reports made during the project period shall also be included in the final report.

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

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

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

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

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

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

Deadline: 1st August 2013.

Two bound copies of the final report and one electronic (pdf-format) version are required.
Responsible supervisor: Professor Jørn Vatn
E-mail: jorn.vatn@ntnu.no
Phone: 73 59 71 09

Company Supervisor: Christopher A. Lassen
Senior Engineer (Msc)
Aker Solutions
E-mail: Christopher.lassen@akersolutions.com
Phone: 93 42 73 62

DEPARTMENT OF PRODUCTION
AND QUALITY ENGINEERING

Per Schjølberg
Associate Professor/Head of Department

Jørn Vatn
Responsible Supervisor
Choice of Demand Mode for Subsea Safety Systems

He Xiuyu

June 2013

Master's Thesis

Department of Production and Quality Engineering

Norwegian University of Science and Technology

Supervisor: Professor Jørn Vatn
Preface

This is the final year Reliability Availability Maintainability and Safety (RAMS) master’s thesis. It is conducted at the Norwegian University of Science and Technology in the spring semester of 2013. The thesis work was carried out in co-operation with NTNU and Aker solutions in the 4th semester in Trondheim and Fornebu, Oslo. The title of the thesis is Choice of Demand Mode for Subsea Systems and is written under the guidance of professor Jørn Vatn at the Department of Production and Quality Engineering.

The target group for this report is assumed to have the basic knowledge of the IEC 61508 industrial standard for functional safety of electric/electronic/programmable electronic safety related systems. The reader is assumed to be familiar with the terminology used in Rausand and Hoyland (2004).

Professor Jørn Vatn and Christopher Lassen in Aker Solutions have been my supervisors. I will thank them for supervising me through the process of specifying such topic and for their professional guidance and valuable support.

He Xiuyu
Trondheim, June 2013
Acknowledgment

I wish to express my indebtedness to Professor Jørn Vatn for his valuable and constructive guidance during the thesis work. His willingness to give time so generously has been very much appreciated. I would like to thank my future colleagues John Barry and Christopher Lassen in Aker Solutions, for their great help and support throughout the thesis work. My grateful thanks are also extended to Britt Ewa Lilleler in Aker Solutions for arranging the workplace and access card in Trondheim office.

Special thanks to professor Marvin Rausand and Mary Ann Lundteigen for helpful advises and good suggestions during my master work. Associate professor Yiliu Liu and PHD student Jin hui have always been helpful to answer my questions and provide me with information whenever I need.

Lastly I also wish to express my thanks to my parents, He Hongbin and Li Renqiu for their unflagging support throughout my entire education.

O.N.

(He Xiuyu)
Summary and Conclusions

In the real industry project, which new technology and systems have blossomed and have been codified, many problems and challenges regarding the application of international safety systems standard IEC 61508 in low demand and high demand have been encountered. For instance, automatic train protection system (ATP) is argued to be both low demand system and continuous mode system (Braband (2006)). A low demand blow-out preventer (BOP) system will operate in high demand mode to withstand the well pressure for hours and weeks when it is activated to full closure (Jin (2011)). In the real case, both reliability assessments for low and high demand mode could be requested due to the vague and ambiguous statement of concepts and definitions in the IEC standard. Current existing researches put main emphasis on low demand systems, but addresses on high/continuous demand systems are few.

This master's thesis which is written in co-operation with Aker Solutions aims at discussing those problems confronted in IEC 61508 and summarizing the existing academic work, mathematical models as well as relevant industry guideline. By assuming the system will operate in both low demand and high/continuous demand mode, Subsea High Integrity Pressure Protection System as a case example is used to illustrate the problems in the case study. Both probability of failure on demand (PFD) and probability of dangerous failure per hour (PFH) are calculated by PDS\(^1\) method as the low and high/continuous demand mode reliability assessment. The results from the case study in terms of SIL are found out to be inconsistent. This problem is discussed and traced back to the general quantitative SIL allocation method in IEC 61508-5. The thesis therefore attempts to develop a general consistent SIL range by carrying out SIL calibrations with Matlab. New correction factor is calculated and a new proposed SIL table is given. The decisions on following IEC 61508 SIL table is further argued. Both pros and cons of different solutions are compared.

\(^1\)A calculation method for safety systems developed by Sintef for the Norwegian offshore industry. Full name is "reliability of computer based safety systems"
# Contents

Preface ......................................................... i
Acknowledgment ........................................... ii
Summary and Conclusions ................................. iii

1 Introduction 2

1.1 Background ........................................... 2
1.2 Literature survey .................................... 2
1.3 Objective ............................................. 3
1.4 Approach ............................................. 4
1.5 Limitations .......................................... 4
1.6 Structure of the Thesis ............................... 5

2 Theoretical Framework 7

2.1 Standards and Guidelines ......................... 7
  2.1.1 IEC 61508 ........................................ 7
  2.1.2 IEC 61511 ........................................ 8
  2.1.3 OLF 070 .......................................... 8
2.2 Reliability theory .................................... 9
  2.2.1 Safety Instrumented System ................... 9
  2.2.2 Failure classification .......................... 10
  2.2.3 Test interval .................................... 13
  2.2.4 Safety integrity ................................ 14
  2.2.5 Reliability measures .......................... 15
  2.2.6 Safe failure fraction and architectural constraints .... 16
CONTENTS

2.2.7 Low demand versus high demand .................................. 17
2.3 Relevant research works and industry guidelines ....................... 19

3 Mathematical models for low and high demand calculation ............. 22
  3.1 IEC formula ................................................................. 23
  3.2 Fault tree analysis model ............................................... 24
  3.3 Markov model ............................................................. 25
  3.4 PDS method ............................................................... 26
  3.5 Common approach by HEF .............................................. 29
  3.6 Common approach by MTTH ............................................ 30

4 Case study subsea high integrity pressure protection system ............. 32
  4.1 Description of HIPPS .................................................... 32
  4.2 Assumptions and Failure data of HIPPS .............................. 34
  4.3 Assessment of HIPPS for both low and high demand mode .......... 35
    4.3.1 Fault tree analysis and reliability block diagram ............. 35
    4.3.2 PDS calculation for low demand operation ................. 37
    4.3.3 PDS calculation for high demand operation ............... 39
  4.4 General SIL allocation problem in IEC 61508 ....................... 41
  4.5 SIL calibration .......................................................... 43

5 Summary ............................................................................. 49
  5.1 Conclusions and discussions .......................................... 49
  5.2 Decisions on following IEC 61508 SIL tables ...................... 51
  5.3 Recommendations for further work .................................. 53

A Acronyms ........................................................................... 54

B Matlab Code ...................................................................... 56

C Plotting results .................................................................. 64

Bibliography ......................................................................... 71
Chapter 1

Introduction

1.1 Background

The demand mode of operation for safety instrumented system (SIS) is often classified into low demand and high/continuous\(^1\) demand of operation. It is not straightforward to discriminate between low and high/continuous demand although some standards propose ways to discriminate between these two modes of operation. For most SIS systems, low demand has been assumed, and research has put main emphasis on low demand systems. In recent years, more attention has been paid to high/continuous demand systems, and several problems are encountered.

1.2 Literature survey

A systematic search for literature survey in the scientific databases (ScienceDirect, Compendex, Web of Science, Google Scholar) is conducted in this thesis. The relevant articles are sorted and selected thoroughly among a great amount of literature, more detailed literature survey is given in Chapter 2.3 and Chapter 3.

The literature reviews aimed at conclude on the following main areas:

---
\(^1\)When later stating high demand mode of operation in the thesis, continuous demand operation belongs to this mode.
• Existing scientific research works on high demand study and confronted challenges. (Chapter 2.3)

• Relevant industrial works and guidelines. (Table 2.2)

• Existing mathematical models for low demand and high/continuous demand reliability calculations. (Chapter 3)

1.3 Objective

The main objective of this Master's thesis is to gain indepth insight into the relation between high and low demand mode of operation.

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

• Perform a literature review, and pay special attention to differences between high and low demand mode of operation. Give a brief introduction to IEC 61508, IEC 61511, and the OLF guideline OLF 070.

• Search for related work in other industries like the railway, nuclear and aviation industry.

• Present, and compare the main frameworks for reliability assessment and architectural constraints for both high demand, and low demand mode of operation respectively.

• Perform a case study where both the high demand and low demand mode of operation is used as basis for the approaches and discuss the results.

• Conclude on the approach both with respect to implications for standardization work, and for the company. The discussion should cover both the issue of SIL allocation, and reliability assessment.
1.4 Approach

Theoretical framework and literature review are summarized to structure the knowledge background for the thesis. The PDS method provides the probability of failure on demand (PFD) and probability of dangerous failure per hour (PFH) formulas for different voting configurations (PDS (2013)). In case study in Chapter 4, the PDS method developed by SINTEF for the Norwegian offshore industry is utilized as a calculation method. Based on the results and findings from the case study, this SIL inconsistency is investigated. SIL calibration is carried out with Matlab. The correction factor for IEC 61508 SIL table is calculated. The new SIL table consistency is later tested and discussed.

1.5 Limitations

- High Integrity Pressure Protection System is a typical low demand system. In order to compare results of different operation mode in the case study, HIPPS is assumed to be able to operate in both low and high demand state.

- Adopting $\beta$ factor model for the common cause failure has limitations, as it gives credit to the degree of redundancy and the model assumes the same rate of common cause failures no matter what the configurations are.

- Human factor is not considered in this analysis.

- Limitations in PDS method for HIPPS case study, since it cannot include the effect of process demands and duration of demand-states.

- The failure probability contribution from other systematic failures and the contribution from alternative testing mechanisms are not considered.

- Limited access/information to other relevant industry works.

- The pre study and status report is not included as part of this thesis in agreement with the supervisor.

- Due to limited space, PDS method is used as the only mathematical model for case study.
1.6 Structure of the Thesis

The master's thesis is structured as follows (Figure 1.1):

- Chapter 1: Gives an introduction to the problem at hand and the objectives of the master work.

- Chapter 2: Theoretical framework, which provides the necessary background information to support the master work and for the reader. Literature review is included in this chapter as well.

- Chapter 3: Mathematical models for low and high demand. This chapter identifies and discusses the existing calculation models in literatures used in low and high demand calculation.

- Chapter 4: Case study. Presents the case study of Subsea HIPPS system. PFD and PFH calculation and comparison for low and high/continuous demand system are performed. SIL calibration are carried out with Matlab.

- Chapter 5: Recommendations and conclusions for master's thesis.
CHAPTER 1. INTRODUCTION

Figure 1.1: Structure of the Master's Thesis
Chapter 2

Theoretical Framework

2.1 Standards and Guidelines

2.1.1 IEC 61508

When systems become complex, the safety and software in safety-related applications must be
proved and justified. An IEC (International Eletrotechnical Commission) standard is therefore
made to guide system designers and developers to achieve the safety requirements of the system
for the intended uses.

The international standard IEC 61508 is widely used for handling functional safety for safety
instrumented system. The standard consists of seven parts, previous four parts give the require-
ment of the standards and could be summarized as normative category. Part five to seven give
the example and guidelines and therefore is put into informative category.

Normative part:

• IEC 61508-1: General requirements, provides the global framework permitting functional
  safety, covers general instructions, deals with all the life cycle phases.

• IEC 61508-2: Covers instructions relating to E/E/PE (Electrical/ Electronic/ Programmable
  electronic) safety-related systems, particularly deals with the phase of producing these
  systems.

• IEC 61508-3: Software requirements, dedicated to instructions relating to the software.
• IEC 61508-4: Definitions and abbreviations, group together the main definitions and abbreviations used in the 7 volumes of the standard.

Informative part:

• IEC 61508-5: Examples of methods for determining levels of safety integrity, centered on risk reduction.

• IEC 61508-6: Reference document for our research, provides the directive lines permitting us to apply standard IEC 61508-2 and IEC 61508-3.

• IEC 61508-7: Presents the techniques and measures which are likely to be used.

2.1.2 IEC 61511

The international standard IEC 61511 is a functional safety standard used for the process industry sector. It is developed by the same IEC 61508 committee and is entitled as "Functional Safety: Safety Instrumented Systems for the Process Industry Sector". Safety instrumented systems are defined by IEC 61511 as including sensors, logic solvers and final elements. The standard also focuses on probabilistic evaluation of process risk, required risk reduction, safety life cycle concept and a structured engineering process which ensures functional safety is achieved in a plant. IEC 61511 is used by those who are managing, designing, implementing or operating a safety instrumented system (SIS) application in a process or similar plant.

2.1.3 OLF 070

The guideline OLF(The Norwegian Oil Industry Association) 070 has been developed to support the use of IEC 61508 and IEC 61511. This OLF070 (2004) standard is a simplified application of international standards IEC 61508 and IEC 61511 for the Norwegian petroleum industry and provide. The guideline presents conservative minimum SIL requirements which takes the uncertainty into consideration. The user therefore do not need to derive the SIL requirements, since it has proven difficult to do that.
2.2 Reliability theory

2.2.1 Safety Instrumented System

The SIS is the abbreviation of Safety Instrumented System. The safety instrumented systems are designed to be responsible for the operating safety and ensuring the emergency shutdown and widely used to prevent hazardous events. The safety instrumented system has two main functions (Rausand and Høyland (2004)):

- The deviation is detected by sensors in SIS and the required actuating items are activated and meet the intended functions when a predefined process demand occurs in the EUC (Equipment under control). If this system function fails, it is called fail to function (FTF).

- Without the presence of predefined process demand occurs in the EUC (Equipment under control), the SIS is not activated spuriously. A failure of this function is called a spurious trip (ST).

![Illustration of a Safety Instrumented System](image)

Figure 2.1: Illustration of a Safety Instrumented System

The Safety Instrumented System can be used in proactive or reactive way as a safety barrier. As a proactive barrier, it is used in continuously or rather frequently high demand systems or certain infrequent process low demand systems to prevent and reduce the likelihood of the event. The reactive barriers are mostly low demand systems which aim at stopping or mitigating
the consequences of the event chain following a hazardous event (Liu (2011)). A typical constitution of a safety instrumented system is composed of three subsystems (Figure 2.1):

- **Subsystem S** - One or more Sensors (Input elements) (e.g., Sensor transmitters)
- **LS subsystem** - One or more Logic Solvers (e.g., Relay logic systems and programmable logic controllers)
- **FE subsystem** - One or more Final Elements (e.g., Safety valves and circuit breakers)

The process performance is detected by the sensor. The logic solver reads physical variables (e.g., Temp, Pressure and Level etc.). If they exceed and remain at the set level, the logic solver could activate the Final Element subsystem by carrying out decision making process. The FE subsystem will keep the system in a safe state by acting directly (Emergency stop valves) or indirectly (Solenoid valves) to stop the process.

### 2.2.2 Failure classification

![Classification of failures](image)

Figure 2.2: Classification of failures

The international standard IEC61508 (2010) covers four types of failures based on physical and nonphysical aspects:
• Random hardware failures: Failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware (Figure 2.2).

  – Aging failures
    Failures occur under conditions within the design envelope of the item.
  – Stress failures
    Failures occur due to excessive stresses on the item.

• Systematic failures: Failure, related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors (Figure 2.2).

  – Design failures
    Failures are initiated during engineering, manufacturing, or installation.
  – Interaction failures
    Failures are initiated by human errors during operation, maintenance or testing.

• Dependent failure: Failure whose probability cannot be expressed as the simple product of the unconditional probabilities of the individual events that caused it.

• Common causes failures: A dependent failure in which two or more component fault states exist simultaneously, or within a short time interval, and are a direct result of a shared cause is defined as the common cause failure (Rausand and Høyland (2004)).

  – CCF where the components fail simultaneously, commonly caused by external shocks
  – CCF where the components fail within a larger interval of time, typical examples are CCF due to humidity and vibration

Common cause failure causes the failure of more than one component in a multi-component system and plays a significant role in the safety integrity. Typical root causes for CCF could be shared environmental dust, humidity, fire, vibration, electromagnetic interference (EMI) (Stavri-anidis (1992)). The common cause failures are assumed from random hardware failures and
systematic failures in the systems. The random failures (hardware failures) and systematic failures are classified into dangerous failures and safe failures in IEC 61508. Dangerous failure and Safe failure could further be classified into detected and undetected failures.

- Detected failure
  In relation with hardware, detected by the diagnostic tests, proof tests, operator intervention or through normal operation.

- Undetected failure
  In relation with hardware, undetected by the diagnostic tests, proof tests, operator intervention or through normal operation.

- Dangerous failure
  Failure which has the potential to put the safety related system in a dangerous state or a state where it cannot fulfil its function.
    - Dangerous Detected (DD)
      Dangerous failures that are detected immediately when they occur.
    - Dangerous Undetected (DU)
      Dangerous failures are preventing activation on demand and are revealed only by testing or when a demand occurs.

- Safe failure
  Failure which does not have the potential to put the safety-related system in a dangerous state or a state where it cannot fulfil its function.
    - Safe Detected (SD)
      Non-dangerous failures that are detected by automatic self testing.
    - Safe Undetected (SU)
      Non-dangerous failures that are not detected by automatic self testing.
    - No part failure
      Failure of a component that plays no part in implementing the safety function.
– No effect failure
   Failure of an element that plays a part in implementing the safety function but has no direct effect on the safety function.

### 2.2.3 Test interval

The definitions of diagnostic test interval and proof test interval are shown below:

- **Diagnostic test interval**: Interval between on-line test to detect faults in a safety-related system that has a specified diagnostic coverage.

- **Proof test interval**: Periodic test performed to detect failures in a safety-related system so that, if necessary, the system can be restored to an "as new" condition or as close as practical to this condition.

Functional tests are performed to reveal DU failures at regular intervals before a demand occurs. Diagnostic test is used to reveal certain types of failures by avoiding to fully operate the main functions of the component. Functional test is important for low demand system to detect and prevent hidden dangerous undetected failures. However, functional testing may not be evident to high demand system. The interval in diagnostic test is very short (e.g. few seconds, minutes or hours) compared with functional test in most high demand systems. In low demand system, there will usually be enough time to repair and restore the function before the next occurrence of demand. It is assumed that EUC will be brought to the safe state immediately by SIF when DD failure occurs. The contribution to PFH from dangerous detected failures in diagnostic testing is therefore negligible (Mewcha (2009)).

**Remark**: However, Jin (2013) argues that contributions from dangerous detected failures should be taken into consideration. Because DD failure may not be detected immediately, diagnostic test interval isn't always negligible. After DD failure being detected, it may not be realistic and practicable to switch into the safe state immediately.
2.2.4 Safety integrity

A SIS may perform one or more safety instrumented functions (SIFs) to achieve or maintain a safe state for the system the SIS is protecting, with respect to a specific process demand (Rausand and Høyland (2004)). In IEC 61508 safety integrity is defined as the "Probability of a safety related system satisfactorily performing the required functions under all stated conditions within a stated period of time." The safety integrity is used to measure the performance of the safety function and can also be interpreted as reliability.

Three categories of safety integrity are distinguished in IEC61508 (2010):

- Hardware safety integrity
  - Quantitative requirements
    Probability of failure on demand for low demand system.
    Probability of dangerous failure per hour for high and continuous demand system.
  - Architectural constraints

- Software safety integrity (Qualitative requirements)

- Systematic safety integrity (Qualitative requirements)

The safety integrity level is a measure of the reliability of the safety function performing to specification. It is defined as a relative level of the risk-reduction provided by a safety function, or to specify a target level of risk reduction (AN9025 (2002)). The main principle in IEC 61508 is to provide the basic process control system without any particular safety measures. After the calculation for risk without safety systems is performed. If the risk is higher than the accepted criteria, SIL requirement is used to measure how much risk reduction is required. Four target ranges of safety performance for the safety function have been specified in IEC 61508 for both low demand and high demand. These levels of safety performance are Safety Integrity Levels (SILs). The level of safety integrity increases from SIL 1 (Least reliable) to SIL 4 (Most reliable). The higher the safety integrity level is, the more stringent the requirements become. Those three categories of safety integrity described above must fit the specified safety integrity level altogether to claim the safety instrumented function (SIF) meet the required SIL.
2.2.5 Reliability measures

Two reliability measures for safety instrumented system for low demand and high demand mode of operation are defined in IEC 61508. The average probability of failure on demand (PFD) is used for quantification of the reliability of SISs operating in low demand mode. And the probability of dangerous failure per hour (PFH) is used as the reliability measure for high demand and continuous SISs. Formulas for quantifying the PFD and PFH is given both in the PDS method handbook, and in IEC 61508-6. Mathematical models (eg. Fault Tree Model, Markov Model, Petri Net Model) used in calculating those measures are described in Chapter 3.

For low demand system. Safety integrity levels target at failure measures for a safety function operating in low demand mode of operation. This measure quantifies the safety unavailability caused by random hardware failures. The probability that a SIF will fail to respond adequately upon a demand is also denoted by the probability of failure on demand.

\[ R(t) \] is the reliability function of the safety instrumented system. The formula for probability of failure on demand is:

\[ PFD = 1 - \frac{1}{T} \int_0^T R(t) dt \]  \hspace{1cm} (2.1)

The average probability of failure to perform its design function on demand for low demand mode is presented in the column. Four safety integrity levels for low demand mode are shown in Figure 2.3.

For high demand system. Safety integrity levels target at failure measures for a safety function operating in high demand mode of operation or continuous mode of operation.

The \( w(t) \) is defined as the failure intensity. \( T \) is the time duration. Probability of dangerous
failure per hour is calculated as below:

\[ PFH(T) = \frac{1}{T} \int_0^T w(t) dt \]  (2.2)

The values of probability of dangerous failure per hour are stated in the column. Four safety integrity levels for high or continuous demand mode are shown in Figure 2.4.

### 2.2.6 Safe failure fraction and architectural constraints

Additional requirement for hardware verification, besides PFD, PFH requirements, is called the architectural constraints, which is a semi-quantitative requirement expressed in terms of the safe failure fraction, system type (A or B) and hardware fault tolerance (HWFT). Safe failure fraction (SFF) is defined as the ratio of the average rate of safe failures plus dangerous detected failures of the subsystem to the total average failure rate of the subsystem(Innal. (2008)). The definition of the total failure rate has differences in IEC 61508 and PDS handbook. The total failure rate in IEC 61508 is the sum of all failures, while PDS method limits the total failure rate to the failures that will be critical for the system. Safe Failure Fraction can be calculated in IEC61508 (2010) using the following equation:

\[ SFF = \frac{\sum \lambda_{SD} + \sum \lambda_{SU} + \sum \lambda_{DD}}{\sum \lambda_{SD} + \sum \lambda_{SU} + \sum \lambda_{DD} + \sum \lambda_{DU}} \]  (2.3)

Hardware fault tolerance is the number of failures that are tolerated before the loss of safety function. Index \( N \) in hardware fault tolerance means that \( (N + 1) \) faults could cause a loss of the
CHAPTER 2. THEORETICAL FRAMEWORK

17

safety function (Table 2.1).

<table>
<thead>
<tr>
<th>SFF /HFT</th>
<th>IEC61508</th>
<th>IEC 61511</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Type A</td>
<td>Type B</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>&lt;60%</td>
<td>SIL1</td>
<td>SIL2</td>
</tr>
<tr>
<td>60-90%</td>
<td>SIL2</td>
<td>SIL3</td>
</tr>
<tr>
<td>90-99%</td>
<td>SIL3</td>
<td>SIL4</td>
</tr>
<tr>
<td>&gt;99%</td>
<td>SIL3</td>
<td>SIL4</td>
</tr>
</tbody>
</table>

Table 2.1: Architectural constraints of SIS in IEC 61508 and IEC 61511.

Two types of systems and safe failure fraction (SFF) are used in architectural constraints to determine the safety integrity level. Type A systems are systems with low complexity. Type B systems are complex systems, typically programmable units. A safety instrumented system can be considered to be the type A (Table 2.1) if three requirements below are met (Innal. (2008)):

- The behaviour in the presence of faults is well determined
- The failure modes of its constituent parts are well defined
- The data on their failures from feedback is known with good reliability

Otherwise, safety instrumented system is considered to be type B.

Remark: The differences in architectural constraints for low and high demand mode are caused mainly by SFF. As being discussed in Chapter 2.2.3 and Chapter 4.2, the dangerous detected (DD) failure rate will in most cases not contribute to an increased SFF if there is no automatic transition of the system to a safe state upon a DD failure. It is slightly different restrictions how the SFF is calculated for high demand systems depending on the level of redundancy.

2.2.7 Low demand versus high demand

Demand state is defined as "State of the EUC when the safety-related system is being required to implement a particular safety function(s)" (Y Misumi (1999)). IEC 61508 and IEC 61511 give different definitions for low demand, high demand and continuous demand. If the demand rate is
greater than once per year or twice the frequency of functional test, according to IEC 61508, high demand operation mode is used for safety instrumented system. In this mode, the dangerous conditions are not always present as continuous mode, but happen frequently. The continuous operation mode is used if the demand occur continuously and effectively always present. In this mode, a dangerous situation will normally occur anytime the system fails dangerously (both DU and DD). Otherwise, SIS is operating in low demand mode. Both definitions in the IEC standards are listed below:

Current IEC61508 (2010) standard:

- Low demand mode is where the frequency of demands for operation made on a safety-related system is no greater than one per year and no greater than twice the proof-tests frequency;

- High or continuous demand mode is where the frequency of demands for operation made on a safety-related system is greater than one per year or greater than twice the proof-tests frequency.

Current IEC61511 (2010) standard:

- Demand mode is where a specified action (eg, closing a valve) is taken in response to process conditions or other demands; In the event of a dangerous failure of the safety instrumented function a potential hazard only occurs when there is a failure in the process or the basic process control system (BPCS);

- Continuous mode is where in the event of a dangerous failure of the safety instrumented function a potential hazard will occur without further failure unless action is taken to prevent it.

Three modes of operation (low demand, high demand and continuous demand) can be defined and categorized by three time intervals (Demand Interval, Automatic Diagnostic Interval and Manual Proof Test Interval). The relationships are shown in Figure 2.5.

Below are some of the typical low and high demand systems examples:

- Typical low demand systems are:
2.3 Relevant research works and industry guidelines

For most SIS system low demand has been assumed, and lots of researches have put main emphasis on low demand systems. The probability of failure on demand has already been discussed by several authors, extensive research has been carried out related to modeling and calculation of the PFD in low demand mode (B. Knegtering (1999), Sato (2003) and Bukowski J V (2002)). Comparison of different techniques was found in J.L Rouvroye (2002). In recent years more attention has been paid to high demand systems, however, little information accept the method presented in IEC 61508-6 has been found, lots of challenges and problems are confronted in the high demand systems and PFH calculations. The PFD has been widely recognized as its average unavailability. But the nature of the probability of failure per hour PFH is not defined clearly in the IEC 61508 or in the general literature. Also its applicability confronts significant disadvantages because the character of the statement of certain concepts and major definitions in the IEC 61508 is sometimes vague and ambiguous (Signoret (2010)).
No argument is found for using PFH calculation instead of PFD calculation if the number of demands is above once per year. The demand of once per year or twice the frequency of functional tests as the borderline is not well explained in IEC 61508 or anywhere else (Jin (2011)). There is no further discussion on the distinction between low and high demand systems and no exploits in the differences in reliability between the two categories (Liu (2011)). Serveral problems related to PFH have also been discussed in PDS (2013). It is concluded that $PFH_0$ is a sensible measure for system operated in continuous mode. However, PFH is constant, independent of the demand rate, and so does not reveal how the risk depends on the demand rate, therefore $PFH_0$ alone is not suited as a measure for loss of safety for on demand systems (neither in low demand nor high demand irrespective of $\tau$ and $\delta$). The main contributor to $PFH_0$ does not depend on the length of the test interval, $\tau$. So the decrease in safety experienced by increasing $\tau$ is essentially not captured by $PFH_0$.

The necessities to use low and high demand system have been discussed by Jin (2011). The disadvantages are such as unable to capture the combined effects of functional testing, spurious activations and successful responses to demands. A common approach by Markov model to calculate HEF (Hazardous event frequency) for general demand modes covering both low demand and high demand is forwarded. Liu (2011) explores the classification by studying the SIS reliability for varying demand rates, demand durations, and test intervals. The approach is based on Markov models and is exemplified by two simple system configurations. The PFD is an adequate measure for the SIS reliability for low demand systems, but may be confusing and difficult to interpret for high demand systems. Jin (2013) presents new PFH formulas for general k-out-of-n-systems, that take into account both dangerous detected and dangerous undetected failures, also allow for non-perfect proof-testing. Mathematical models are summarized into two categories (Formula approximation and State transition) in Chapter 3. Related industry guideline\textsuperscript{2} are listed in Table 2.2.

\textsuperscript{1}$PFH_0$ is defined as the average rate of SIS failures. $\tau$ is the length of interval of functional testing. Demand rate is defined as $\delta$.
\textsuperscript{2}Few relevant industry works are found out, partly due to limited access to other industries. However, relevant industry works on similar topic in this dissertation are as few as scientific research papers on high demand systems.
<table>
<thead>
<tr>
<th><strong>Related guidelines in industry</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Nuclear Industry</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Railway industry</strong></td>
<td></td>
</tr>
<tr>
<td>EN50126 (1999)</td>
<td>The overall approach to SIS specification design, construction, and operation, and describes the railway sector version of the overall SIS life cycle requirements by European Norms (EN).</td>
</tr>
<tr>
<td>EN50128 (2001)(IEC 62279)</td>
<td>Give the requirement for software and hardware design and construction, and have similar scope as IEC61508.</td>
</tr>
<tr>
<td>EN50129 (2003)(IEC 62425)</td>
<td>Give the requirement for software and hardware design and construction, have similar scope as IEC61508.</td>
</tr>
<tr>
<td><strong>Civil aviation</strong></td>
<td></td>
</tr>
<tr>
<td>Civil Aviation Authority</td>
<td>Give reference to international regulations, standards, and guidelines.</td>
</tr>
<tr>
<td>European Aviation Safety Agency (EASA)</td>
<td>Give references include standards and guidelines for aircrafts and air traffic management in Europe.</td>
</tr>
<tr>
<td>Joint Aviation Authority (JAA)</td>
<td>Give references include standards and guidelines for aircrafts and air traffic management in Europe.</td>
</tr>
<tr>
<td>The international Civil Aviation Organization (ICAO)</td>
<td>Global forum for civil aviation and works to achieve harmonized regulations, standards, and guidelines.</td>
</tr>
<tr>
<td><strong>Aerospace</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Offshore</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Automobile industry</strong></td>
<td></td>
</tr>
<tr>
<td>Development guidelines for vehicle-based software MISRA (1994)</td>
<td>Published by Motor Industry Reliability Research Association. MISRA guideline defines five integrity levels. No assigned quantitative reliability targets or ranges for these levels.</td>
</tr>
<tr>
<td>ISO26262 (2006)</td>
<td>Apply to SIS installed in road vehicles of class M, N and O. Provides automotive-specific analysis methods to identify SIL requirements. Introduced ASIL to indicate a slightly different SIL concept, also no assigned probabilistic target value.</td>
</tr>
</tbody>
</table>
Chapter 3

Mathematical models for low and high demand calculation

In this chapter, mathematical models for low and high demand reliability calculation are summarized as part of the literature review. The mathematical models for PFD and PFH calculation can be concluded in three categories in general:

- By formula approximation:

- By state transition model:

3.1 IEC formula

The formulas in IEC 61508 are introduced in this section. The limitation is that the IEC-formulas can only be applied to SIS subsystems with at most three elements. The channel equivalent means down time is $t_{CE}$. MRT and MTTR is the abbreviation for mean repair time and mean time to restoration. More detailed explanations of each terms can be found in IEC61508 (2010).

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \left( \frac{\tau}{2} + MRT \right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR \quad (3.1)$$

System equivalent down time $t_{GE}$ is expressed as:

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left( \frac{\tau}{3} + MRT \right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR \quad (3.2)$$

The PFD formula for a single system presented in IEC 61508 is:

$$PFD = (\lambda_{DU} + \lambda_{DD}) \cdot t_{CE} = \lambda_{DU} \left( \frac{\tau}{2} + MRT \right) + \lambda_{DD} \cdot MTTR \quad (3.3)$$

For 1oo2 system, the formula is shown below:

$$PFD_{1oo2} = 2((1 - \beta_D)\lambda_{DD} + (1 - \beta)\lambda_{DU})^2 t_{CE} + \beta_D^2 \lambda_{DD} \cdot MTTR + \beta\lambda_{DU} \left( \frac{\tau}{2} + MRT \right) \quad (3.4)$$

The PFH formula for a single system presented in IEC 61508 is:

$$PFH(T) = \frac{1}{T} \int_0^T w(t) \, dt = \frac{1 - \exp[-\int_0^T \Lambda(t) \, dt]}{T} = \frac{F(T)}{T} \quad (3.5)$$

For a 1oo1 system the PFH is equal to the frequency of dangerous SIS failures:

$$PFH = \lambda_{DU} \quad (3.6)$$

For 1oo2 system, the formula is shown below:

$$PFH_{1oo2} = 2((1 - \beta_D)\lambda_{DD} + (1 - \beta)\lambda_{DU})^2 t_{CE} + \beta_D^2 \lambda_{DD} + \beta\lambda_{DU} \quad (3.7)$$
3.2 Fault tree analysis model

A fault tree method is used to model the failure of a certain TOP event which depends on other basic physical components by AND- or OR- gate in a tree structure. In low demand mode, FTA provides acceptable approximations of the PFD for SIS. For each basic event $i$, the $PFD_{avg}$ is calculated in CARA Fault Tree by the approximation (Equation 3.10):

$$q_i(t) \approx \frac{\lambda_{DU,i} \tau_i}{2}$$  \hspace{1cm} (3.8)

A fault tree with $m$ minimal cut sets can be modelled as a series structure of the $m$ minimal cut parallel structures. The probability of failure on demand for a minimal cut set $j$ with independent components can be expressed as$^1$:

$$Q_{MC_j}(t) \approx \prod_{i=1}^{m_j} q_i(t)$$  \hspace{1cm} (3.9)

The probability of failure on demand for low demand system can be approximated with a conservative upper bound approximation:

$$Q_0(t) \approx 1 - \prod_{j=1}^{m} (1 - Q_{MC_j}(t))$$  \hspace{1cm} (3.10)

The average probability of dangerous failures per hour $PFH(t)$ is defined as the unconditional failure intensity of the system which is also called the failure frequency or the failure density. $PFH$ is obtained from fault tree by considering the components which are in working state.

This failure intensity is defined by:

$$w_i(t) = \lim_{dt \to 0} \frac{Pr(t < T \leq t + dt)}{dt}$$  \hspace{1cm} (3.11)

$$Pr(t < T \leq t + dt) \approx w_i(t) \cdot dt$$  \hspace{1cm} (3.12)

For each component $C_i$, the unconditional failure intensity $w_i(t)$ can be calculated from Equation 3.11. The conditional probabilities are $p(S/c_i)$ and $p(S/\bar{c}_i)$ when we know that com-

$^1$Formula 3.9 is non-conservative for simultaneous testing.
ponent \( c_i \) is failed or not failed respectively. The hazard rate of component \( c_i \) is \( \lambda_i \). \( A_i(t) \) is the instantaneous availability of component of \( c_i \) which can be approximated as the reliability of each component. For each of its components \( c_i \), unconditional failure intensity \( w_s(t) \) and birnbaum importance factor \( I_B(S, c_i) \) are calculated. Their respective products are then added together. The average probability of dangerous failures per hour can be obtained from the sum of the product of the Birnbaum’s measure of importance factor and the unconditional failure intensity of each component (Signoret (2010)):

\[
\omega_s(t) = \sum_i I_B(S, c_i) \omega_i(t) \tag{3.13}
\]

\[
w_s(t) = \sum_i (p(S|c_i) - p(S|\bar{c}_i)) \cdot \lambda_i A_i(t) \tag{3.14}
\]

The PFH is then calculated by formula below:

\[
PFH(T) = \frac{1}{T} \int_0^T w_s(t) dt \tag{3.15}
\]

### 3.3 Markov model

The markov model can be used to analyze and describe dynamic systems with the system states. The system states in markov model can be categorized as:

- Functioning state,
- Non-functioning state
- System is operating in a degraded mode

Lots of researchers prefer not to distinguish the SIS modes and use a common reliability measure with basis in markov modelling (Bukowski (2006) Innal (2008) Signoret (2010) Jin (2011) Liu (2011) Y Misumi (1999) I. Yoshiamura (2009) Jin (2011)). It has been concluded that the techniques that hold the greatest modeling poweer is the Markov analysis compare with the different quantitative techniques (J.L Rouvroye (2002)). State transition diagram and transition rate matrix \( A \) for the calculation of steady state, can be expressed by:
\[
A = \begin{bmatrix}
  a_{00} & a_{01} & a_{02} & \cdots & a_{0r} \\
  a_{10} & a_{11} & a_{12} & \cdots & a_{1r} \\
  \vdots & \vdots & \vdots & \ddots & \vdots \\
  a_{r0} & a_{r1} & a_{r2} & \cdots & a_{rr}
\end{bmatrix}
\] (3.16)

PFD can be acquainted by solving the following set of equations:

\[
\sum_{j=0}^{r} \prod_{j} = 1 \quad \prod A = 0 \quad (3.17)
\]

The set of the critical working states is \( M_C \). \( \Lambda_i \) is the sum of the failure rates removing the critical working state \( i \) and finishing in a failed state. The expression for the \( PFH(t) \) is:

\[
PFH(t) = \omega_s(t) = \sum_{i \in M_c} \Lambda_i p_i(t) \quad (3.18)
\]

The average \( PFH(t) \) over the period of \( T \) is directly deduced from Equation 3.18. \( CST_i[0, T] \) and \( APS_i[0, T] \) denote respectively the cumulative sojourn time in the critical working state \( i \) over the period \( T \), and the average probability of sojourn in this state over the same period. It is expressed as (Signoret (2010)):

\[
PFH = \frac{1}{T} \int_0^T \left( \sum_{i \in M_c} \Lambda_i p_i(t) \right) dt = \frac{1}{T} \sum_{i \in M_c} [\Lambda_i \int_0^T p_i(t) dt] = \frac{1}{T} \sum_{i \in M_c} \Lambda_i CST_i[0, T] = \sum_{i \in M_c} \Lambda_i APS_i[0, T] \quad (3.19)
\]

### 3.4 PDS method

The PDS is a calculation method for safety systems developed by Sintef for the Norwegian off-shore industry. The full name for PDS is Reliability of computer based safety systems. It is assumed as a general rule that random hardware failures are denoted as independent failures while systematic failures may lead to CCFs. The PDS method provides the simplified PFD and PFH formulas for different voting configurations (PDS (2013)). It gives more conservative reliability assessment results and is easy to be used in reliability assessment of safety instrumented
systems. The disadvantages of PDS have also been argued, since it cannot include the effect of process demands and duration of demand-states, the failure probability contribution from application software failures, other systematic failures and the contribution from alternative testing mechanisms are not considered in the modeling approach as well. The $\beta$ factor modeling also exists weaknesses for the common cause failures, as it gives credit to the degree of redundancy and the model assumes the same rate of common cause failures no matter what the configurations are (Per Hokstad (2009)). $C_{MooN}$ factors for different voting logics are listed in Figure 3.1.

The $\tau$ is the period between functional testing. $\lambda_{DU}$ is the dangerous undetected failure. For low demand mode calculation, probability of failure on demand for 1oo1 system can be expressed below:

$$PFD_{1oo1} \approx \lambda_{DU} \cdot \tau/2 \tag{3.20}$$

For a duplicated module 1oo2 system, contribution of common cause failure for PFD is calculated from the formula:

$$PFD_{1oo2}^{CCF} \approx \beta \cdot (\lambda_{DU} \cdot \tau/2) \tag{3.21}$$

PFD contribution from independent failure of 1oo2 system can be approximated by:

$$PFD_{1oo2}^{ind.} \approx (\lambda_{DU} \cdot \tau)^2/3 \tag{3.22}$$

Probability of failure on demand for a 1oo2 voted system is:

$$PFD_{1oo2} \approx \beta \cdot (\lambda_{DU} \cdot \tau/2) + (\lambda_{DU} \cdot \tau)^2/3 \tag{3.23}$$

In general, for components voted MooN system, contribution of CCF and independent failure for PFD is calculated from

$$PFD_{MooN}^{CCF} \approx C_{MooN} \cdot \beta \cdot (\lambda_{DU} \cdot \tau/2); (M < N) \tag{3.24}$$
\[ PFD_{\text{MooN}}^{\text{ind.}} \approx \frac{N!}{(N-M+2)! \cdot (M-1)!} \cdot (\lambda_{DU} \cdot \tau)^{N-M+1}; (M < N) \] (3.25)

In high demand mode calculation, for 1oo1 system, the probability of dangerous failure per hour is equal to dangerous undetected failure rate:

\[ PFH_{\text{1oo1}} = \lambda_{DU} \] (3.26)

For a duplicated module 1oo2 system, the PFH considering common cause failure is:

\[ PFH_{\text{1oo2}}^{\text{CCF}} = \beta \lambda_{DU} \] (3.27)

Contribution from 1oo2 system, independent failures can be approximated by:

\[ PFH_{\text{1oo2}}^{\text{individual}} = (\lambda_{DU} \tau)^2 / \tau = \lambda_{DU}^2 \tau \] (3.28)

Probability of dangerous failure per hour for 1oo2 system is

\[ PFH_{\text{1oo2}} = \beta \lambda_{DU} + (\lambda_{DU} \tau)^2 / \tau \] (3.29)

For components voted MooN system, contribution of CCF and independent failure for PFD is calculated from

\[ PFH_{\text{MooN}}^{\text{CCF}} \approx C_{\text{MooN}} \cdot \beta \cdot \lambda_{DU}; (M < N) \] (3.30)

\[ PFH_{\text{MooN}}^2 \approx C_{\text{MooN}} \cdot \beta \cdot \lambda_{DU} + \frac{N!}{(N-M+1)! \cdot (M-1)!} \cdot \frac{[(\lambda_{DU} \tau)^{N-M+1}]}{\tau} \] (3.31)

**Remark:** It is assumed that the diagnostic test is done with the intervals of length \( \tau_1 \). If DD failure and Proof Test Coverage (PTC) are taken into consideration in PFH calculation. The new PFH formula given by Jin (2013) is shown in the footnote.
3.5 Common approach by HEF

The common approach by calculating hazardous event frequency (HEF) is introduced in Jin (2011). This common approach is based on the Markov model in Figure 3.2.

Kolmogorov forward equations can be expressed below (Rausand and Høyland (2004)):

$$ P(t) \cdot A = \dot{P}(t) $$ (3.32)

The state transition matrix $A = a_{ij}$ is based on the non-zero entries, which means:
### Table 3.1: System states for HEF common approach

<table>
<thead>
<tr>
<th>State 5: Available (non-demand)</th>
<th>State 4: Safe state (N/A)</th>
</tr>
</thead>
<tbody>
<tr>
<td>State 3: Functioning (on-demand)</td>
<td>State 2: DD failure (non-demand)</td>
</tr>
<tr>
<td>State 1: DU-failure (non-demand)</td>
<td>State 0: Dangerous failure (on demand)</td>
</tr>
</tbody>
</table>

\[
a_{ii} = -\sum_{j=0}^{5} a_{ij}, \quad j \neq i \text{ for } i = 0, 1, \cdots, 5. \tag{3.33}
\]

The irreducible Markov process is shown as:

\[
\lim_{t \to \infty} P_i(t) = P_i = \text{constant for } i = 0, 1, ..., 5 \tag{3.34}
\]

\[
\lim_{t \to \infty} \dot{P}_i(t) = 0 \text{ for } i = 0, 1, ..., 5 \tag{3.35}
\]

Sum of the steady state probability equals to 1. Each state probability can be calculated in Equation 3.32 Equation 3.34 and Equation 3.35.

\[
\sum_{i=0}^{5} P_i = 1 \tag{3.36}
\]

HEF at time \( t \) is equal to the visit frequency to state 0 from any other state at time \( t \):

\[
HEF(t) = \sum_{i=1}^{5} P_i(t) \cdot A_{i0} \tag{3.37}
\]

The calculation HEF formula is equal to

\[
HEF(t) = P_1(t) \cdot \lambda_{de} + P_2(t) \cdot \lambda_{de} + P_3(t) \cdot \lambda_D \tag{3.38}
\]

#### 3.6 Common approach by MTTH

Another common approach is to calculate Mean time to failure (MTTH) based on Markov diagram (Figure 3.3). This common approach as "Integrated SIL allocation" is presented by SIEMENS in Safecomp 2006 (Braband (2006)). A proposal for a harmonised SIL Table as an unambiguous
SIL determination method is mentioned as well (See Table 3.2).

Table 3.2: Proposal for a Harmonised SIL Table based on MTTH (Adapted from Braband (2006))

<table>
<thead>
<tr>
<th>Safety integrity level</th>
<th>Mean Time to Hazard (MTTH)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>$\geq 10^4 \text{ years to } &lt; 10^5 \text{ years}$</td>
</tr>
<tr>
<td>3</td>
<td>$\geq 10^3 \text{ years to } &lt; 10^4 \text{ years}$</td>
</tr>
<tr>
<td>2</td>
<td>$\geq 10^2 \text{ years to } &lt; 10^3 \text{ years}$</td>
</tr>
<tr>
<td>1</td>
<td>$\geq 10 \text{ years to } &lt; 10^2 \text{ years}$</td>
</tr>
</tbody>
</table>

Index denotes the initial state\(^3\). Based on the Markov Diagram in Figure 3.3. Mean time to hazard (MTTH) is calculated below:

\[
MTTH_{00} = \frac{1}{\lambda + \lambda_S} + \frac{\lambda}{\lambda + \lambda_S} MTTH_{01} + \frac{\lambda}{\lambda + \lambda_S} MTTH_{10} \quad (3.39)
\]

For initial state $MTTH_{01}$

\[
MTTH_{01} = \frac{1}{\mu + \lambda_S} + \frac{\mu}{\mu + \lambda_S} MTTH_{00} \quad (3.40)
\]

For initial state $MTTH_{10}$

\[
MTTH_{10} = \frac{1}{\lambda + \frac{2}{T}} + \frac{2}{\lambda + \frac{2}{T}} MTTH_{00} \quad (3.41)
\]

\(^3\)Detailed description of each state in Markov Diagram in Figure 3.3 hasn't been given in Braband (2006)
Chapter 4

Case study subsea high integrity pressure protection system

This assessment of the case study is based on the example of High Integrity Pressure Protection System (HIPPS) described and presented in the ISO13628-14 (2011). The PDS method is used as the calculation method in this case study. Typically, HIPPS is a low demand system. Typical high demand systems in subsea are rare, in this case, in order to compare the choice between low and high demand mode, it is assumed that HIPPS can also operate in high/continuous demand mode. Both PFD in low demand and PFH in high demand operational mode are calculated and compared.

4.1 Description of HIPPS

Figure 4.1: Subsea high integrity pressure protection system
HIPPS is called High Integrity Pressure Protection System. It protects against overpressure in pipelines or vessels by quickly isolating the source causing the overpressure. As shown in Figure 4.1, the overpressure source appears in section one which include but not limited to: high reservoir pressures, subsea pumps, and connection to higher pressure pipeline. The source could be gas, liquid or multiphase fluid (ISO13628-14 (2011)). Common demand scenarios could be closed valve, hydral plug leads HIPPS to function. HIPPS is a typical safety instrumented system and a custom-built product which the main functionality is specified by the customer. The location of HIPPS is installed topside or subsea on an X-mas tree, manifold or pipeline end terminal (Figure 4.1). Typically, a SIL 3 requirement is placed on the HIPPS safety function (i.e., shut off to isolate over pressurization in the flow line).

Figure 4.2: A simple HIPPS architecture (Adapted from Signoret (2008), Fiorentini (2010))

As shown in Figure 4.2, a standard High Integrity Pressure Protection System comprises of:

- Pressure transmitters
- Logic solver(s)
- Solenoid-operated hydraulic control valves
- Fastclosing shutdown valves
4.2 Assumptions and Failure data of HIPPS

Assumptions of reliability assessment of High Integrity Pressure Protection System are described below (PDS (2013)):

- All failure rates are assumed to be constant with respect to time, i.e., the time to failure is exponentially distributed.
- The elements considered are identical and have the same constant failure rates.
- It is assumed that the component is as good as new after the repair and functional test.
- The demand rate is assumed to be constant, i.e., the time between demands is exponentially distributed.
- Failures occur independently and their severities are constant over time.
- PFD and PFH are calculated as average values.
- Standard $\beta$ factor model is used to model common cause failures.
- In low demand mode, the time between diagnostic self-tests is assumed significantly lower than the time between demands.
- When giving the "simple" formulas for PFH, the contribution from unavailability due to repair and testing of components is not included; i.e., short MTTRs are assumed.
- For single (1oo1) component systems, the system is immediately put in a safe state upon detection and repair of a dangerous detected failure. DD failure affecting all N redundant components of a system will upon detection immediately result in the system going to a safe-state. In these simplified formulas, DD failures are ignored and PFH equals the rate of the DU failures.
- The term $\lambda_{DU} \cdot \tau$ should be small enough to allow $e^{-\lambda_{DU} \cdot \tau} \approx 1 - \lambda_{DU} \cdot \tau$, i.e., $\lambda_{DU} \cdot \tau \leq 0.2$
- The rate of independent DU failures is throughout approximated with $\lambda_{DU}$ (Rather than e.g., using $(1 - \beta)\lambda_{DU}$ for 1oo2)
• For $N \geq 3$, we ignore the contribution of a combination of single and double failures.

• The self test period is "small" compared to the interval between functional testing, i.e., at least a factor 100 lower.

• The formulas given here do not account for demands as a means of testing to detect dangerous failures.

• It is assumed that $PFH_A$ and $PFH_B$ are small enough: $1 - (1 - PFH_A)(1 - PFH_B) \approx PFH_A + PFH_B$

<table>
<thead>
<tr>
<th>Component</th>
<th>Failure rate per $10^6$ hours</th>
<th>$\beta$</th>
<th>$\tau$ (hours)</th>
</tr>
</thead>
<tbody>
<tr>
<td>PT, Pressure Transmitter</td>
<td>$1.5$</td>
<td>$0.5$</td>
<td>$0.4$</td>
</tr>
<tr>
<td>Trip Amplifier / Analogue Input</td>
<td>$0.04$</td>
<td>$0.4$</td>
<td>$0.4$</td>
</tr>
<tr>
<td>Logic Solver</td>
<td>$0.03$</td>
<td>$0.3$</td>
<td>$0.3$</td>
</tr>
<tr>
<td>Digital Output</td>
<td>$0.04$</td>
<td>$0.4$</td>
<td>$0.4$</td>
</tr>
<tr>
<td>HIPPS Valve</td>
<td>$2.7$</td>
<td>$3.3$</td>
<td>$1.9$</td>
</tr>
</tbody>
</table>

Table 4.1: Generic reliability data for the HIPPS components (Adapted from PDS (2013))

Relevant failure data of reliability assessment of High Integrity Pressure Protection System are from PDS handbook and are shown in Table 4.1, the appropriate test interval $\tau$ is assumed to be one year (8760 hours).

### 4.3 Assessment of HIPPS for both low and high demand mode

#### 4.3.1 Fault tree analysis and reliability block diagram

The purpose of fault tree analysis and reliability block diagram in this chapter is to visualize the logic structure of the system in the analysis. CARA Fault Tree version 4.0 (c) SINTEF 1996 is utilized for fault tree analysis. The fault tree relating to the HIPPS appears in Figure 4.3. The safety function “Failure to isolate over-pressurization in flowline” can be represented by a reliability block diagram as shown in Figure 4.4.
CHAPTER 4. CASE STUDY SUBSEA HIGH INTEGRITY PRESSURE PROTECTION SYSTEM

Figure 4.3: Fault tree for subsea high integrity pressure protection systems

Figure 4.4: Reliability block diagram for subsea high integrity pressure protection systems
4.3.2 PDS calculation for low demand operation

In this reliability assessment, Probability of failure on demand (PFD) is calculated by PDS method which is introduced in Chapter 3.4. Contributions from the common cause failures of Pressure Transmitter, Logic Solver and Valves are calculated below:

\[
PFD^{CCF}_{PT(2oo3)} = C_{2oo3} \cdot \beta \cdot \lambda_{DU} \cdot \tau / 2 = 2 \cdot 0.06 \cdot 0.5 \cdot 10^{-6} \cdot 8760 / 2 = 2.63 \times 10^{-4} \quad (4.1)
\]

\[
PFD^{CCF}_{Logic(1oo2)} = \beta \cdot \lambda_{DU} \cdot \tau / 2 = 0.03 \cdot (0.04 \cdot 10^{-6} + 0.03 \cdot 10^{-6} + 0.04 \cdot 10^{-6}) \cdot 8760 / 2 = 1.4 \times 10^{-5} \quad (4.2)
\]

\[
PFD^{CCF}_{Valve(1oo2)} = \beta \cdot \lambda_{DU} \cdot \tau / 2 = 0.05 \cdot 1.9 \cdot 10^{-6} \cdot 8760 / 2 = 4.16 \times 10^{-4} \quad (4.3)
\]

Individual contributions in HIPPS can be expressed as:

\[
PFD^{ind.}_{PT(2oo3)} = (\lambda_{DU} \cdot \tau)^2 = (0.5 \cdot 10^{-6} \cdot 8760)^2 = 1.92 \times 10^{-5} \quad (4.4)
\]

\[
PFD^{ind.}_{Logic(1oo2)} = (\lambda_{DU} \cdot \tau)^2 / 3 = [(0.04 \cdot 10^{-6} + 0.03 \cdot 10^{-6} + 0.04 \cdot 10^{-6}) \cdot 8760]^2 / 3 = 3.1 \times 10^{-7} \quad (4.5)
\]

\[
PFD^{ind.}_{Valve(1oo2)} = (\lambda_{DU} \cdot \tau)^2 / 3 = (1.9 \cdot 10^{-6} \cdot 8760)^2 / 3 = 9.23 \times 10^{-5} \quad (4.6)
\]

The total probability of failure on demand is calculated below:

\[
PFD_{total} = PFD_{Sensors} + PFD_{Logic Solvers} + PFD_{Final Elements} = 8.05 \times 10^{-4} \quad (4.7)
\]

The probability of failure on demand of High Integrity Pressure Protection System calculated by PDS method is \(8.05 \times 10^{-4}\). Comparing the PFD figure with the SIL table presented in Figure 2.3, the system is classified as a SIL 3 system (Figure 4.5), as the calculated PFD is less than \(10^{-3}\) and greater than \(10^{-4}\).
Figure 4.5: Components/Subunits SIL Capability in low demand mode
4.3.3 PDS calculation for high demand operation

Probability of dangerous failure per hour (PFH) is calculated by PDS method, which is introduced in Chapter 3.4. Contributions from common cause failures of Pressure Transmitter, Logic Solver and Valves are calculated below:

\[
P_{FH}^{CCF}_{PT(2oo3)} \approx C_{2oo3} \cdot \beta \cdot \lambda_{DU} \approx 2 \times 0.06 \times 0.5 \times 10^{-6} \approx 6 \times 10^{-8} \tag{4.8}
\]

\[
P_{FH}^{CCF}_{Logic(1oo2)} \approx C_{1oo2} \cdot \beta \cdot \lambda_{DU} \approx 0.03 \times (0.04 + 0.03 + 0.04) \times 10^{-6} \approx 3.3 \times 10^{-9} \tag{4.9}
\]

\[
P_{FH}^{CCF}_{Value(1oo2)} \approx C_{1oo2} \cdot \beta \cdot \lambda_{DU} \approx 0.05 \times 1.9 \times 10^{-6} \approx 9.5 \times 10^{-8} \tag{4.10}
\]

Individual contributions in HIPPS can be expressed as:

\[
P_{FH}^{ind.}_{PT(2oo3)} \approx 3 \cdot (\lambda_{DU} \cdot \tau)^2 / \tau = 3 \cdot \lambda_{DU}^2 \cdot \tau = 3 \times (0.5 \times 10^{-6})^2 \times 8760 \approx 6.57 \times 10^{-9} \tag{4.11}
\]

\[
P_{FH}^{ind.}_{Logic(1oo2)} \approx (\lambda_{DU} \cdot \tau)^2 / \tau = \lambda_{DU}^2 \cdot \tau = (0.11 \times 10^{-6})^2 \times 8760 \approx 1.06 \times 10^{-10} \tag{4.12}
\]

\[
P_{FH}^{ind.}_{Value(1oo2)} \approx (\lambda_{DU} \cdot \tau)^2 / \tau = \lambda_{DU}^2 \cdot \tau = (1.9 \times 10^{-6})^2 \times 8760 \approx 3.16 \times 10^{-8} \tag{4.13}
\]

The total probability of dangerous failure per hour is calculated below:

\[
P_{FH}^{total} = P_{FH}^{Sensors} + P_{FH}^{LogicSolvers} + P_{FH}^{FinalElements} = 1.97 \times 10^{-7} \tag{4.14}
\]

The probability of dangerous failure per hour of High Integrity Pressure Protection System calculated by PDS method is \(1.97 \times 10^{-7}\). Comparing the PFH figure with the SIL table presented in Figure 2.4, the system is classified as a SIL 2 system, as the calculated PFH is less than \(10^{-6}\)
and greater than $10^{-7}$. The common cause contribution $PFH_{CCF}$ is an essential contributor to the $PFH_{Total}$, as $PFH_{CCF}$ has already reached SIL 2. Common cause failures should therefore be paid particular attention (Figure 4.6).

**Remark:** Requirements in the IEC 61508 and IEC 61511 related to qualitative aspects (management of functional safety/avoidance and control of systematic failures) and architectural constraints requirements have not been considered as part of the thesis work.

### 4.4 General SIL allocation problem in IEC 61508

In IEC61508 (2010) and IEC61511 (2010). Three types of methods of determine SIL requirements are introduced:

- General quantitative method
- Semi-Quantitative (Risk Graph, Layer of Protection Analysis)
- Qualitative (Hazardous event severity matrix)

In SIL allocation, safety integrity levels for both demand modes can be decided directly in Risk graph, LOPA and Hazardous event severity. However, resulting contradictions in safety integrity level appear by different PFD and PFH calculations. This problem can be traced back and discussed in general quantitative method in IEC 61508-5.

![Safety integrity allocation - Example for safety-related production system](image)

Figure 4.7: Safety integrity allocation - Example for safety-related production system.(Adapted from IEC61508 (2010))
The general quantitative method uses $PFD_{avg}$ as the only calculation example in IEC 61508-5 Page 28 to demonstrate SIL allocation. The $F_t$ is the tolerable hazard frequency and $F_{np}$ is the demand rate on the safety-related protection system. Basic steps are described below:

1. Determine the tolerable risk (e.g., from ALARP)
2. Determine the EUC risk.
3. Determine the necessary risk reduction to meet the tolerable risk.
4. Allocate the necessary risk reduction to the E/E/PE safety-related systems, other technology safety-related systems and other risk reduction measures (IEC 61508-1 7.6).
5. Determine the probability of failure on demand for the safety-related protection system ($PFD_{avg}$) to meet the necessary risk reduction ($\Delta R$). For a constant consequence in the specific situation described, $PFD_{avg} = (F_p/F_{np}) = \Delta R$. ($F_p$ is the risk frequency with the protective features in place.)
6. For $PFD_{avg} = (F_p/F_{np})$, the safety integrity level can be obtained from Table 4.2 of IEC 61508-1

<table>
<thead>
<tr>
<th>Safety integrity level (SIL)</th>
<th>Average probability of a dangerous failure on demand of the safety function ($PFD_{avg}$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>$\geq 10^{-5}$ to $&lt; 10^{-4}$</td>
</tr>
<tr>
<td>3</td>
<td>$\geq 10^{-4}$ to $&lt; 10^{-3}$</td>
</tr>
<tr>
<td>2</td>
<td>$\geq 10^{-3}$ to $&lt; 10^{-2}$</td>
</tr>
<tr>
<td>1</td>
<td>$\geq 10^{-2}$ to $&lt; 10^{-1}$</td>
</tr>
</tbody>
</table>

Table 4.2: SIL allocation problems in IEC 61508

The SIL requirements is determined by the risk reduction factor which is independent of low and high/continuous demand mode. In general SIL allocation method step five, $PFD_{avg}$ is calculated first by formula $PFD_{avg} = (F_p/F_{np}) = \Delta R$. The average of probability of failure on demand ($PFD_{avg}$) is used to allocate the low demand SIL range in the left part1 of Table 4.2. If it is needed to find out the high/continuous demand mode SIL range, then the SIL table is switch

---

1Only the left hand table has a unit-less column ($PFD_{avg}$)
to the right part which seems to be a rather arbitrary calibration. Probability of dangerous failure per hour \( (PFH) \) in high demand is decided based on SIL allocated by \( PFD_{avg} \) (Figure 4.2). By definition and calculation in Chapter 2.2.7, there are many differences between low demand and high demand operation. It is inappropriate to determine SIL for high demand based on \( PFD_{avg} \) which is a measurement for low demand system. Safety integrity levels could result in contradictions.

### 4.5 SIL calibration

The SIL range in right hand part in Table 4.2 for high/continuous demand mode of operation is arbitrarily calibrated, making it inappropriate for use. The results from case study have demonstrated the inconsistent safety integrity level result. In this section, Matlab is used to carry out SIL calibration and find out the general correction factor to propose a better calibration of the SIL table. Ideally, the general correction factor is hoped to provide a consistent calibration regime and this will be further tested in Matlab in Chapter 5.2. \( \alpha_n \) and \( \beta_n \) is defined as the equivalent upper limit of low demand and high demand safety integrity level in Table 2.3 and Table 2.4:

\[
\alpha_n = 10^{-n} \quad \beta_n = 10^{-(n+4)} \quad (4.15)
\]

When the total probability of failure of demand is calculated. \( \theta \) is used to express the ratio between the upper limit of low demand system and PFD:

\[
\theta = \frac{\alpha_n}{PFD_{hipps}} \quad (4.16)
\]

Adjustment ratio is the \( \theta \) multiply with PFH then divide high demand SIL upper limit:

\[
\varepsilon = \theta \cdot \frac{PFH_{hipps}}{\beta_n} = \frac{\alpha_n \cdot PFH_{hipps}}{PFD_{hipps} \cdot \beta_n} \quad (4.17)
\]

In Figure 4.8, it is assumed the \( \varepsilon \) equals to one if the safety integrity levels are consistent. If the safety integrity levels are inconsistent, corrected range for high demand is expressed below:
\[ \frac{\alpha_{n+1}}{PFD_{hipps}} \times PFH_{hipps} \leq SIL_1^{PFH_{corrected}} \leq \frac{\alpha_{n}}{PFD_{hipps}} \times PFH_{hipps} \] 

(4.18)

Final average correction factor $\Delta$ is

\[ \Delta = \frac{\sum_{1}^{n} \varepsilon_n}{n} \] 

(4.19)

The complete simulation calculation process is shown in Figure ???. Detailed explanation are given as comments behind the Matlab code in Appendix B. SIL calibrations are carried out by varying both failure rate and CCF. The original failure rate in Figure 4.1 is expanded by 10 from $10^{-8}$ to $10^{-6}$. As shown in Figure 4.3 the range between maximum and minimum is $10^{2}$. The beta factor range for common cause failure is from 1 percent to 15 percent. Therefore beta factor has been expanded by $10^{0.477} = 3$, the range between maximum and minimum is $10^{0.954} = 9$ in Figure 4.4. Both variables follow logarithmic scale in the plotting graphic. This makes it easy to compare those values which cover a large range. The suitable test interval for low and high demand system in the simulation is assumed from one month to one year.

<table>
<thead>
<tr>
<th>Component</th>
<th>Failure rate</th>
<th>$\beta$</th>
<th>$\tau$ (hours)</th>
</tr>
</thead>
<tbody>
<tr>
<td>PT, Pressure Transmitter</td>
<td>$5 \times 10^{-8}$</td>
<td>6%</td>
<td>730hr ~ 8760hr</td>
</tr>
<tr>
<td>Trip Amplifier / Analogue Input</td>
<td>$4 \times 10^{-9}$</td>
<td>3%</td>
<td>730hr ~ 8760hr</td>
</tr>
<tr>
<td>Logic Solver</td>
<td>$3 \times 10^{-9}$</td>
<td>3%</td>
<td>730hr ~ 8760hr</td>
</tr>
<tr>
<td>Digital Output</td>
<td>$4 \times 10^{-9}$</td>
<td>4%</td>
<td>730hr ~ 8760hr</td>
</tr>
<tr>
<td>HIPPS Valve</td>
<td>$1.9 \times 10^{-7}$</td>
<td>5%</td>
<td>730hr ~ 8760hr</td>
</tr>
</tbody>
</table>

Table 4.3: Reliability data for SIL calibration by varying failure rates

<table>
<thead>
<tr>
<th>Component</th>
<th>$\lambda_{PU}$</th>
<th>$\beta_{Min}$</th>
<th>$\beta_{Base}$</th>
<th>$\beta_{Max}$</th>
<th>$\tau$ (hours)</th>
</tr>
</thead>
<tbody>
<tr>
<td>PT, Pressure Transmitter</td>
<td>$5 \times 10^{-7}$</td>
<td>2%</td>
<td>6%</td>
<td>18%</td>
<td>730hr ~ 8760hr</td>
</tr>
<tr>
<td>Trip Amplifier / Analogue Input</td>
<td>$4 \times 10^{-8}$</td>
<td>1%</td>
<td>3%</td>
<td>9%</td>
<td>730hr ~ 8760hr</td>
</tr>
<tr>
<td>Logic Solver</td>
<td>$3 \times 10^{-8}$</td>
<td>1%</td>
<td>3%</td>
<td>9%</td>
<td>730hr ~ 8760hr</td>
</tr>
<tr>
<td>Digital Output</td>
<td>$4 \times 10^{-8}$</td>
<td>1.7%</td>
<td>5%</td>
<td>15%</td>
<td>730hr ~ 8760hr</td>
</tr>
<tr>
<td>HIPPS Valve</td>
<td>$1.9 \times 10^{-6}$</td>
<td>1.7%</td>
<td>5%</td>
<td>15%</td>
<td>730hr ~ 8760hr</td>
</tr>
</tbody>
</table>

Table 4.4: Reliability data for SIL calibration by varying beta factors

Matlab calculates the average correction factor by carrying out 4016000 times calculation.
Figure 4.8: Flow chart for the proposed simulation method for SIL calibration
The SIL calibration results are listed in Table 4.5.

<table>
<thead>
<tr>
<th></th>
<th>Total calculation times</th>
<th>Average correction rate:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Varying the failure rates</td>
<td>( nnr_1 = 4016000 )</td>
<td>( \Delta_1 = 5.7059 )</td>
</tr>
<tr>
<td>Varying the beta factors</td>
<td>( nnr_2 = 4016000 )</td>
<td>( \Delta_2 = 5.6953 )</td>
</tr>
</tbody>
</table>

Table 4.5: SIL calibration results

Plotting graphics are generated and given below. The test interval \( \tau \) has critical influences on the correction rate compared with the failure rates and beta factors. When the safety integrity levels are consistent, the correction rate is assumed to be 1. If SIL is inconsistent, the correction range will gradually close to the range from IEC 61508 when test interval increases. However, test interval less than 8760h (1 year) would be meaningful for high demand system. All the adjustment will be significant since the correction rate will not be less than 2 when test interval is equal to one year. There is almost one level adjustment (correction factor is around 10) for SIL when test interval is around 2 to 3 months.

Figure 4.9: Correction factor \( \varepsilon \) plotting by varying failure rates

New safety integrity level table with correction ranges\(^2\) is given in Table 4.6:

---
\(^2\)The correction factor \( \Delta \) is used as 5.7, since two correction rates calculated above in the simulations are quite close with this value. The SIL consistency of this range is further discussed and tested in Chapter 5.2.
Figure 4.10: Correction factor $\varepsilon$ plotting by varying beta factors

Figure 4.11: Ratio between upper limit and PFD $\theta$ by varying failure rates
Figure 4.12: Ratio between upper limit and PFD $\theta$ by varying beta factors

Table 4.6: New safety integrity level correction ranges

<table>
<thead>
<tr>
<th>Safety integrity level (SIL)</th>
<th>Average probability of a dangerous failure on demand of the safety function ($PFD_{avg}$)</th>
<th>Average frequency of a dangerous failure of the safety function [h$^{-1}$] ($PFH$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>$\geq 10^{-5}$ to $&lt; 10^{-4}$</td>
<td>$\geq 5.7 \times 10^{-6}$ to $&lt; 5.7 \times 10^{-7}$</td>
</tr>
<tr>
<td>3</td>
<td>$\geq 10^{-4}$ to $&lt; 10^{-3}$</td>
<td>$\geq 5.7 \times 10^{-7}$ to $&lt; 5.7 \times 10^{-6}$</td>
</tr>
<tr>
<td>2</td>
<td>$\geq 10^{-3}$ to $&lt; 10^{-2}$</td>
<td>$\geq 5.7 \times 10^{-8}$ to $&lt; 5.7 \times 10^{-5}$</td>
</tr>
<tr>
<td>1</td>
<td>$\geq 10^{-2}$ to $&lt; 10^{-1}$</td>
<td>$\geq 5.7 \times 10^{-5}$ to $&lt; 5.7 \times 10^{-4}$</td>
</tr>
</tbody>
</table>
Chapter 5

Summary and Recommendations for Further Work

5.1 Conclusions and discussions

All the objectives in the master's thesis set in Chapter 1.3 are aimed to be met with the utmost possible effort. The literature review has been performed in Chapter 2.3. IEC 61508, IEC 61511, and the OLF guideline OLF 070 are introduced. The existing mathematical models for low and high demand reliability calculation are summarized in Chapter 3. In the literature review, mathematical model and theoretical framework section, special attention has been paid on the differences between high and low demand mode of operation. Relevant industry standard and guidelines are summarized in Table 2.2. Related works in other industries are found out to be few, this is also partly due to limited access to other industries. The main frameworks for reliability assessment for both high demand, and low demand mode of operation have been illustrated and compared through subsea HIPPS case study in Chapter 4.3 and mathematical models for reliability calculation in Chapter 3. The differences in architectural constraints are presented and compared in Chapter 2.2.6. The case study is performed and is used as basis for the SIL calibration approaches in Chapter 4. The approach both with respect to implications for standardization work, and for the company have been concluded. The discussions on both the issue of SIL allocation, and reliability assessment have been covered.

PDS method introduced in Chapter 3 has been used as the reliability assessment method in
CHAPTER 5. SUMMARY

the case study. The probability of failure on demand of High Integrity Pressure Protection System calculated by PDS method is $3.7 \times 10^{-4}$. Compared to the values presented in SIL in Figure 2.3, it is concluded that the safety function is within safety integrity level 3, as the calculated PFD is less than $10^{-3}$ and greater than $10^{-4}$.

The probability of dangerous failure per hour of HIPPS calculated by PDS method is $1.77 \times 10^{-7}$. Compared to the values presented in SIL in Figure 2.4, it is concluded that the safety function is within safety integrity level 2, as the calculated PFH is less than $10^{-6}$ and greater than $10^{-7}$. Typically, a SIL 3 requirement has been allocated to the subsea HIPPS by the oil companies in the subsea industry. Therefore in high demand operation, safety integrity target has not been met. The results in case study in terms of SIL are found out to be inconsistent. This problem is discussed and traced back to the general quantitative SIL allocation method in IEC 61508-5. The thesis therefore attempts to develop a general consistent SIL range by carrying out SIL calibrations with Matlab. New correction factor is calculated to be 5.7. A new SIL table is given in Table 4.6.

The differences in safety integrity levels are mostly caused by inconsistency in SIL ranges for low and high demand mode in Table 4.2. Although this could be due to safety considerations when the system is operating in high demand mode, but no explanations are found to support this either in IEC 61508 or other literatures. Another reason is that PFH and PFD are calculated in different formulas. The relationship between the PFD and PFH in PDS handbook is shown in Equation 5.1.

$$PFD_{MooN} \approx PFH_{MooN}^{ind} \cdot \tau / (N - M + 2) + PFH_{MooN}^{CCF} \cdot \tau / 2 (M < N)$$  \hspace{1cm} (5.1)

The distinguishing frequency once per year in IEC 61508 is not reasoned and arbitrary(PDS (2013), Jin (2011)). Also the ranges in SIL Table 4.2 for both low demand and high demand lack consistency and may lead to contradictions. Therefore choosing different demand mode will lead to different results. Example could be Automatic train protection system (ATP). The demand rate often depends on the reliability of the human operator (acting as a control system) and the operation profile, so it may be argued that the ATP system is both a low demand system and a continuous mode system (Braband (2006)).

Another problem is that various elements have different demand rates for different SIFs.
This will make it hard to define the mode of operation. Example could be logic solver may operate more than the input and final elements. Lastly, the classification in IEC 61508 disregards the aspect of the demand duration. Example could be blow-out preventer (BOP) which is used to stop uncontrolled flow from oil wells during drilling. BOP as a safety instrumented system is in low demand mode between demands. But when it is rarely activated to full closure, BOP will withstand the well pressure for hours and weeks in high demand operation mode. No reliability measures are able to deal with this situation (Jin (2011)).

5.2 Decisions on following IEC 61508 SIL tables

There are two directions for High Integrity Pressure Protection System to achieve safety integrity level 3 both in low and high demand mode based on whether follow IEC 61508 SIL table or not. Choosing to follow IEC 61508 SIL table means the reliability of HIPPS operating in high demand mode needs to be improved to meet SIL 3. More costs will get involved. However, there are also disadvantages to adopt the common approach or new SIL correction ranges. The average mean value used as the general correction factor for the new SIL table could be questionable. The failure rates and beta factors don't have much influences on this value. However, the average correction rate depends greatly on the test interval range chosen to be used in the simulations. In Figure 5.1, the consistency of safety integrity level has been tested. By expanding the SIL range for high demand system, the safety integrity levels become more consistent as shown in the figure. However the approaches to correct the SIL table for IEC 61508 and give the general correction rate confront challenges. Choosing to use PFD calculation for low demand and close to high demand system would be one of the recommended solutions. For the common approach, HEF would be hard to link with safety integrity level and the proposed MTTH SIL ranges have not been tested or supported.

---

1. The SIL calibration uses non-conservative test interval range from 1 month to 1 year, possible test interval range could be, for example, 3 month to 4 month.
2. In Matlab, if SIL is consistent the value in plotting is set to be 1, else is 0.
CHAPTER 5. SUMMARY

Figure 5.1: Safety integrity level consistency testing

Figure 5.2: Decisions on following IEC 61508 SIL tables or not
• Keep following IEC 61508 SIL tables, the decisions could be:
  – Reduce the common cause failures (Main contributions)
  – Increase redundancy (More spurious trips)
  – Add protection layers
  – Reduce test interval
  – Improve reliability of the components

• Not to follow IEC 61508 SIL tables:
  – Use new safety integrity level correction ranges in Table 4.6.
  – Use PFD calculation for low demand and close to high demand systems.
  – HEF method as common approach (Hard to link with SIL)
  – Mean Time to Hazard (MTTH) (No literatures are found to support the new proposed MTTH SIL ranges)

### 5.3 Recommendations for further work

Future works could be performed in several directions:

• Investigating in the cost caused by lack of consistency in IEC 61508 SIL ranges.

• Link the HEF method with safety integrity level.

• Study on the applicability of proposed MTTH SIL ranges.
Appendix A

Acronyms

CCF  Common Cause Failure
DD  Dangerous Detected
DU  Dangerous Undetected
ESD  Emergency Shutdown
EUC  Equipment under control
FTA  Fault tree analysis
FTF  Fail to function
HWFT  Hardware Fault Tolerance
IEC  International Eletrotechnical Commission
KooN  K out of N system
OREDA  Offshore reliability data
OLF  The Norwegian Oil Industry Association
PFH  Probability of failure per hour
PFD  Probability of failure on demand
APPENDIX A. ACRONYMS

PDS  Norwegian for "Reliability of Computer-based Safety Systems"

PT  Pressure Transmitter

RAMS  Reliability, availability, maintainability, and safety

RFF  Risk reduction factor

RBD  Reliability block diagram

SIS  Safety-instrumented systems

SFF  Safe failure fraction

SIF  Safety Instrumented Function

SOV  Solenoid Valve

SRS  Subsea Requirements Specification

SIL  The Safety integrity level

ST  Spurious trip

MTTF  Mean time to failure

MTTR  Mean time to repair
%This is the Matlab code for the Master thesis: Choice of demand mode for subsea systems

clear all;
close all;

%Definitions for the fixed value and variables for calculations

%Beta factors for the common cause failures
beta1 = 0.06;
beta2 = 0.03;
beta3 = 0.05;

%CCF configuration factors – Cmoon
C1oo2 = 1;
C2oo3 = 2;

nr = 1000; %This defines the intervals for lambda_dt
%DU failure rates are defined as variables which follow Logarithmic scale.
This makes it easy to compare values which cover a large range

%All the DU failures are separated nr times. All DU failures follow the 
  same pace with nr%

\[
\text{lamda}_{\text{du1}} = \logspace(-7.301, -5.301, \text{nr})
\]
\[
\text{lamda}_{\text{du2}} = \logspace(-8.3979, -6.3979, \text{nr})
\]
\[
\text{lamda}_{\text{du3}} = \logspace(-8.5223, -6.5229, \text{nr})
\]
\[
\text{lamda}_{\text{du4}} = \text{lamda}_{\text{du2}}
\]
\[
\text{lamda}_{\text{du5}} = \logspace(-6.7212, -4.7212, \text{nr})
\]

%Test intervals for high demand system are from 730hrs (1 month) to 8760hrs 
(12 months)%

\[
\tau = 730:2:8760;
\]

%Calculations%

\[
\text{for } i = 1 : \text{length(}\tau\text{)}
\]
\[
\text{for } j = 1 : \text{length(}\text{lamda}_{\text{du1}}\text{)}
\]

%Low demand operation mode%

\[
\text{PFD1} = C200*\beta_1*\text{lamda}_{\text{du1}}(j).*\tau(i)./2; \ %\text{CCF Pressure transmitters%}
\]
\[
\text{PFD2} = \beta_2.*(\text{lamda}_{\text{du2}}(j)+\text{lamda}_{\text{du3}}(j)+\text{lamda}_{\text{du4}}(j)).*\tau(i)./2; \ %\text{CCF Logic Solvers%}
\]
\[
\text{PFD3} = \beta_3*\text{lamda}_{\text{du5}}(j).*\tau(i)./2; \ %\text{CCF Final Elements%}
\]
\[
\text{PFD4} = (\text{lamda}_{\text{du1}}(j).*\tau(i)).^2; \ %\text{PFDind for Pressure transmitters%}
\]
\[
\text{PFD5} = (((\text{lamda}_{\text{du2}}(j)+\text{lamda}_{\text{du3}}(j)+\text{lamda}_{\text{du4}}(j)).*\tau(i)).^2)/3; \ %\text{PFDind for Logic Solvers%}
\]
\[
\text{PFD6} = (((\text{lamda}_{\text{du5}}(j).*\tau(i)).^2)/3; \ %\text{PFDind for Final Elements%}
\]
APPENDIX B. MATLAB CODE

PFD=PFD1+PFD2+PFD3+PFD4+PFD5+PFD6; %Total probability of failure on demand
%
SIL_ZE=-log10(PFD); %SIL equivalent value for total PFD%
SIL=floor(SIL_ZE); %Safety integrity level for the system%
EUB=10.^(-SIL); %Equivalent upper limit%
RATE(i,j)=EUB./PFD; %Ratio Upper/PFD%
%
%High demand operation mode%
PFH1=C2oo3*beta1*lamda_du1(j); %CCF Pressure transmitters%
PFH2=C1oo2*beta2*(lamda_du2(j)+lamda_du3(j)+lamda_du4(j)); %CCF Logic Solvers%
PFH3=C1oo2*beta3*lamda_du5(j); %CCF Final Elements%

PFH4=(3*(lamda_du1(j)*tau(i)).^2)./tau(i); %PFHind for Pressure transmitters%
PFH5=((lamda_du2(j)+lamda_du3(j)+lamda_du4(j)).*tau(i)).^2)./tau(i); %PFHind for Logic Solvers%
PFH6=((lamda_du5(j)*tau(i)).^2)./tau(i); %PFDind for Final Elements%

PFH=PFH1+PFH2+PFH3+PFH4+PFH5+PFH6; %Total probability of dangerous failure per hour%

EUBL=10.^(-SIL-4); %Equivalent high demand SIL upper limit in IEC 61508%

if (PFH>=EUBL/10 & PFH<=EUBL)
    DELTA(i,j)=1;
else
    DELTA(i,j)=0;
end
% Used to test the consistency of safety integrity level in both low and high demand modes

if (PFH>=EUBL/10 & PFH<=EUBL)
    EUL=EUBL;
else EUL=PFH.*RATE(i,j);
end

% Test the consistency of SIL, if not give a new high demand SIL upper limit based on RATE(i,j)%

RATE2(i,j)=EUL./EUBL; % SIL correction rate%
TAU(i,j)=tau(i);
NR(i,j)=j;

end

nnr=i*j % Total calculation times%
sum(sum(RATE2))/nnr % Average SIL correction rate%

mintau=min(min(TAU));
maxtau=max(max(TAU));
minnr=min(min(NR));
maxnr=max(max(NR));
totallr=i*j;
meanrate=sum(sum(RATE))/totallr;
meanrate2=sum(sum(RATE2))/totallr;
mx=[minnr minnr maxnr maxnr];
my=[mintau mintau maxtau maxtau];
[MY,MX]=meshgrid(mx,my);
MR=ones(4)*meanrate;
MR2=ones(4)*meanrate2;
surf(MX,MY,MR2)
shading interp
alpha(0.5);
hold on
surf(TAU,NR,RATE2)
shading interp

% Plot the SIL correction rate and the average SIL correction value%

mesh(TAU,NR,RATE)
shading interp
%Plot the Rate(i,j)%

mesh(TAU,NR,DELTA)
shading interp

% Used to test the consistency of SIL in both operation modes%
%Matlab code for common cause failure sensitivity case study

clear all;
close all;

%Definitions for the fixed value and variables for calculations%

% CCF configuration factors – Cmoon%
Cloo2=1;
C2oo3=2;

% Dangerous undetected failure rates%
lamda_du1=0.5/1e6;
lamda_du2=0.04/1e6;
lamda_du3=0.03/1e6;
lamda_du4=lamda_du2;
lamda_du5=1.9/1e6;

nr=1000; %This defines the intervals for beta factors%

% Beta factors are defined as variables which follow Logarithmic scale. This makes it easy to compare values which cover a large range%
% All the beta factors are separated nr times. All values follow the same pace with nr%

beta1=logspace(-2.222,0.222,nr);
beta2=logspace(-2.523,0.523,nr);
beta3=logspace(-2.301,0.301,nr);

% Test intervals for high demand system are from 730hrs (1 month) to 8760hrs (12 months)%
tau = 730:2:8760;

% Calculation for the results
for i = 1:length(tau)
    for j = 1:length(beta1)
        % Low demand operation mode
        PFD1 = C2003 * beta1(j) * lamda_du1 * tau(i) / 2; % CCF Pressure transmitters
        PFD2 = beta2(j) * (lamda_du2 + lamda_du3 + lamda_du4) * tau(i) / 2; % CCF Logic Solvers
        PFD3 = beta3(j) * lamda_du5 * tau(i) / 2; % CCF Final Elements
        PFD4 = (lamda_du1 * tau(i))^2; % PFDind for Pressure transmitters
        PFD5 = (((lamda_du2 + lamda_du3 + lamda_du4) * tau(i))^2) / 3; % PFDind for Logic Solvers
        PFD6 = ((lamda_du5 * tau(i))^2) / 3; % PFDind for Final Elements
        PFD = PFD1 + PFD2 + PFD3 + PFD4 + PFD5 + PFD6; % Total probability of failure on demand

        SIL_ZE = -log10(PFD); % SIL equivalent value for total PFD
        SIL = floor(SIL_ZE); % Safety integrity level for the system
        EUB = 10.^(−SIL); % Equivalent upper limit
        RATE(i,j) = EUB ./ PFD; % Ratio Upper/PFD

        % High demand operation mode
        PFH1 = C2003 * beta1(j) * lamda_du1; % CCF Pressure transmitters
        PFH2 = C1002 * beta2(j) * (lamda_du2 + lamda_du3 + lamda_du4); % CCF Logic Solvers
        PFH3 = C1002 * beta3(j) * lamda_du5; % CCF Final Elements
APPENDIX B. MATLAB CODE

55 PFH4 = (3 * (lambda_du1 * tau(i)).^2) ./ tau(i); % PFHind for Pressure transmitters%
56 PFH5 = (((lambda_du2 + lambda_du3 + lambda_du4) .* tau(i)).^2) ./ tau(i); % PFHind for Logic Solvers%
57 PFH6 = ((lambda_du5 * tau(i)).^2) ./ tau(i); % PFDind for Final Elements%
58
59 PFH = PFH1 + PFH2 + PFH3 + PFH4 + PFH5 + PFH6; % Total probability of dangerous failure per hour%
60
61 EUBL = 10.^(-SIL - 4); % Equivalent high demand SIL upper limit in IEC 61508%
62
63 if (PFH >= EUBL/10 & PFH <= EUBL)
64    EUL = EUBL;
65 else
66    EUL = PFH .* RATE(i, j);
67 end
68
69 RATE2(i, j) = EUL ./ EUBL;
70 TAU(i, j) = tau(i);
71 NR(i, j) = j;
72
73 end
74 end
75
76 mesh(TAU, NR, RATE)
77 shading interp
78 % Plot the Rate(i, j)%
79
80 mesh(TAU, NR, RATE2)
81 shading interp
82 % Plot the SIL correction rate%
Appendix C

Plotting results
APPENDIX C. PLOTTING RESULTS

Figure C.1: Correction rate $\epsilon$ plotting by varying failure rates

Figure C.2: Correction rate $\epsilon$ plotting by varying failure rates
Figure C.3: Correction rate $\epsilon$ plotting by varying failure rates

Figure C.4: Correction rate $\epsilon$ plotting by varying failure rates
Figure C.5: Ratio between upper limit and PFD $\theta$ by varying failure rates

Figure C.6: Ratio between upper limit and PFD $\theta$ by varying failure rates
Figure C.7: Correction rate $\epsilon$ plotting by varying beta factors

Figure C.8: Correction rate $\epsilon$ plotting by varying beta factors
Figure C.9: Correction rate $\epsilon$ plotting by varying beta factors

Figure C.10: Correction rate $\epsilon$ plotting by varying beta factors
Figure C.11: Ratio between upper limit and PFD $\theta$ by varying beta factors

Figure C.12: Ratio between upper limit and PFD $\theta$ by varying beta factors
Bibliography


Fiorentini, P. (2010). *HIPPS High integrity Pressure Protection Systems*.


MISRA (1994). *Development guidelines for vehicle-based software*. Themotorindustry The motor industry reliability association, Watling St UK.


Curriculum Vitae

PERSONAL INFORMATION

Xiuyu He

Grenseveien 9E, 0571 Oslo (Norway)
+47 94988899  +47 22947128
hexiuyu@live.cn
www.facebook.com/hexiuyu
Skype: he.xiuyu

Sex: Male  Date of birth: 02 November 1989  Nationality: Chinese

JOB APPLIED FOR

WORK EXPERIENCE

01 June 2012 – 01 August 2012
Summer internship
Aker solutions, Oslo (Norway)
Skuld and Vilje Sor Project RAM Analysis

01 October 2010 – 01 December 2010
Internship
Guangzhou Railway (Group) Company, Guangzhou (China)

EDUCATION AND TRAINING

01 August 2011 – 01 July 2013
Msc in Reliability Availability Maintainability and Safety
Norwegian University of Science and Technology, Trondheim (Norway)

01 August 2009 – 01 July 2010
Exchange study
Norwegian University of Science and Technology, Trondheim (Norway)

01 September 2007 – 01 November 2011
Bachelor in Traffic and Transportation Engineering
Central South University, Changsha (China)

01 September 2004 – 01 July 2007
Senior Secondary Education
Kunming No.10 Middle School, Kunming (China)

PERSONAL SKILLS

Mother tongue(s)
Chinese

Other language(s)

<table>
<thead>
<tr>
<th>UNDERSTANDING</th>
<th>SPEAKING</th>
<th>WRITING</th>
</tr>
</thead>
<tbody>
<tr>
<td>Listening</td>
<td>Reading</td>
<td>Spoken interaction</td>
</tr>
<tr>
<td>English</td>
<td>C2</td>
<td>C1</td>
</tr>
</tbody>
</table>

Curriculum Vitae

Xiuyu He

Common European Framework of Reference for Languages

Communication skills
Effective communication skills gained in team work.

Organisational / managerial skills
Good experience in project or team work.

Job-related skills
Using Miriam Regina to carry out RAM analysis

Computer skills
Program experiments and function using C and SPSS.
Using AUTOCAD to design and to build components and systems.
Using Minitab, R-project and Microsoft office adroitly.

ADDITIONAL INFORMATION

Projects
Reliability assessment of subsea shutdown system.
   Master project Autumn 2012
Projects
Maintenance optimization of windfarm Expert in Teamwork project.
   Technoport RAMS challenges in ocean energy utilization
Projects
Risk analysis of the collision between Gudermes and Saint Jacques II in Dover Strait, Norwegian University of Science and Technology.
   Risk Analysis and Safety Management in Maritime Transportation Semester Project
Projects
Reliability and safety analysis of the separator protection system, Norwegian University of Science and Technology
   Safety and Reliability Analysis Semester Project
Projects
Quality and Performance Oriented Management in Nokia, Norwegian University of Science and Technology
   Quality and Performance Oriented Management Semester Project
Projects
Purchasing Strategy in Trondheim E6 Project 2010, Norwegian University of Science and Technology
   Purchasing and Logistics Management Semester Project
Projects
Review of the ICE train disaster, Norwegian University of Science and Technology
   Risk Analysis Semester Project

Honours and awards
President of Chinese Students and Scholars Association, NTNU 2011
   Photographer in BeiXing magazine 2011
   Central South University Excellent Graduate Student 2011
   Central South University Excellent Student Honor 2008, 2009
   Scholarships for Excellent Students, Central South University 2008, 2009
   First Prize Honor in Innovation and Entrepreneurship essay competition CSU Jun.2008
   Awarded 6th Keub Green Belt by The World Taekwondo Federation(WTF), 2009
   Awarded 8th Keub Yellow Belt by The World Taekwondo Federation(WTF), 2008
   Third Prize Honor in China Network Television cup english speech contest CSU May.2009
   Third Prize in Olympic Physics competition, China Oct.2006