

Hui Jin

**A contribution to reliability
assessment of
safety-instrumented
systems**

Thesis for the degree of Philosophiae Doctor

Trondheim, September 2013

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



NTNU – Trondheim
Norwegian University of
Science and Technology

NTNU

Norwegian University of Science and Technology

Thesis for the degree of Philosophiae Doctor

Faculty of Engineering Science and Technology
Department of Production and Quality Engineering

© Hui Jin

ISBN 978-82-471-4632-3 (printed ver.)
ISBN 978-82-471-4633-0 (electronic ver.)
ISSN 1503-8181

Doctoral theses at NTNU, 2013:254

Printed by NTNU-trykk

Preface

This thesis is prepared in partial fulfillment of the requirements for the degree of Doctor of Philosophy at the Faculty of Engineering Science and Technology, the Norwegian University of Science and Technology (NTNU). The main work of the PhD thesis was carried out at the Department of Production and Quality Engineering (NTNU), but I also spent six months at the Center for Risk and Reliability at University of Maryland College Park as part of my PhD study.

Starting a PhD is an important decision, and I am lucky to finish in three years. PhD is a long journey, and along the way, there are ups and downs, pleasures and frustrations, and rewards and discouragements. But looking back, I have never regretted that I started and held on until the very end. It has been a unique experience in my life, and I am proud that only very few of us can actually have this experience. I do not know how useful my contributions during the past three years will be. But does it really matter that much? Probably not. Going through all the processes and finally reach the end is itself a big achievement.

Trondheim, Norway
June 2013

Hui Jin

Acknowledgements

First and foremost, I would like to thank my main supervisor, Professor Marvin Rausand from the Department of Production and Quality Engineering at NTNU, for his patient guidance and tireless support. Without Marvin's help and encouragement, I would never have come this far.

I am indebted to my co-supervisor, Professor Mary Ann Lundteigen from NTNU and DNV. Mary Ann is a very positive supervisor, her encouragement has been a momentum to push me forward. She is co-author of most of my publications.

Professor Ali Mosleh is very kind and hosted my stay in University of Maryland College Park (UMCP). It was a great experience to stay in Maryland and a pleasure to work with Ali. I got lots of inspirations from our conversations. I also wish to thank Dr. Yuandan Li from UMCP for her help and the great moments she brought in Maryland.

The RAMS group and the administrative staff of the Department of Production and Quality Engineering are acknowledged for providing a dynamic academic environment and excellent working facilities. My thanks go to Professor Stein Haugen and Associate Professor Yiliu Liu for co-authoring articles during my PhD. I am also grateful to NTNU for the financial support.

I would like to thank Per Hokstad and Stein Hauge from SINTEF Safety Research for involving me in their projects and providing a practical perspective of the PhD topic. It was pleasant to work with both of them.

Special thanks go to my friends Xiaoxi Tao, Xue Yang, Yu Wang, and Jianyin He, my roommate Vegard Brøtan, and my office-mate Inger Lise Johansen.

Last but not least, I would like to thank my parents and grandparents for their love and support ever since I was born.

Summary

Safety-instrumented systems (SISs) are among the most important and effective safety barriers in reducing the likelihood of hazardous events and/or mitigate their consequences to assets (humans, environment, and material assets). This PhD thesis focuses on the reliability of SISs.

The overall objective of this PhD thesis has been *to develop new methods and new concepts for reliability assessment of safety-instrumented systems*. With the knowledge generated in this PhD project, the decision-makers are able to make more rational decisions related to SIS reliability in design, technology qualification, implementation, and operation, hence to achieve a better strategy for major risk prevention.

This PhD thesis has been a theoretical exercise with the functional safety standards (IEC 61508, IEC 61511, etc.), probability theory, and system reliability theory as bases. SISs in the process (mainly oil and gas) industry have been extensively used as examples and cases, but the reliability assessment methods and models developed during this PhD are applicable to all industry sectors.

This PhD thesis investigates several important issues in SIS reliability assessment, and significant achievements have been made to obtain better SIS reliability assessment results. The main contributions of this PhD project are documented in the form of ten articles, among which, four articles have been published in relevant international journals, two are currently under review and the other four have been presented in peer reviewed international conferences and published in the conference proceedings. In addition to the articles, the results from this PhD thesis are also partly implemented in the 2013 version of the PDS¹ method handbook.

Simplified formulas are the preferred approach for SIS reliability assessment among practitioners, but the current formulas from IEC 61508 and PDS method

¹ PDS is the Norwegian acronym for “Reliability and availability of computer-based safety systems.” The PDS-method is developed by the Norwegian research institute, SINTEF, for SIS reliability analysis. It is a well accepted method in the oil and gas industry.

fail to account for some important aspects such as dangerous detected (DD) failures, non-perfect proof tests, and partial tests. In this PhD thesis, several extensions are proposed such that the new formulas are able to treat the DD-failures, non-perfect proof tests, and partial tests properly, such that the applicability of the simplified formulas is extended. For complex SISs, advanced methods are needed to study their reliability. This thesis points to the Markov methods and Petri nets as promising candidates. These two methods are investigated in depth in relation to SIS reliability assessment and their advantages are demonstrated.

Common cause failures (CCFs) have significant influences on the SIS reliability. Despite the efforts made in the past decades, there are still inconsistency between different CCF definitions and a commonly accepted definition is missing. In SIS reliability assessment, CCFs are usually modeled by the beta-factor model and the multiple beta-factor (MBF) model without the adequacy of these models being checked. This PhD thesis proposes to define CCF on component and system level separately to harmonize the differences between the current CCF definitions. Based on the new definitions, the adequacy of the beta-factor model and multiple beta-factor (MBF) model are verified with respect to several assumptions, and conservative models are identified for different system configuration.

Human and organizational factors (HOFs) influence SIS reliability, but they have not been systematically studied in the context of SIS. This PhD thesis investigates the HOF influence on the component failure rate by extending the failure rate model in MIL-HDBK-217F such that HOFs are considered. A Bayesian approach is proposed to integrate field data and expert opinion to quantify the HOF influences on failure rate. By using the proposed approach, the company and local influences are considered and better SIS reliability assessment are achieved.

Process demands are threats to the systems safety, at the same time, they also reveal the state of a SIS. Using demands as tests and taking credits from demands in SIS reliability assessment have been controversial topics. The industry wants to use the information about the state of the SIS from an actual demand to support decisions but fears of the possible accidents due to the demand. This PhD thesis systematically investigates this issue, and provides a thorough discussion of the pros and cons of using such a “testing strategy”, and highlights cautions, challenges, and conditions of use. With the material from this PhD thesis, the decision-makers can have a broader and better picture of using demands as tests, and can decide whether and how to use the information from demands in SIS-related decisions without failing to maintain the due safety level.

The functional safety standards classify SISs into low-demand, high-demand, and continuous modes of operation based on the demand frequency, and use different measures to quantify the reliability of SISs working in different modes. The classification and use of reliability measures are, however, lacking of scientific basis, and the practitioners are sometimes confused. This thesis provides

a thorough discussion of this issue, and suggests a common approach to integrate demand frequency into SIS reliability assessment with Markov methods so that the demand frequency is considered in the assessment and no classification is needed. This thesis also proposes a common reliability measure, that is applicable to all demand frequencies, to be used together with the common approach.

The standpoint of this PhD thesis is that all reliability and risk analyses are merely tools to provide inputs for better and more rational decision-making, if there is no decision to make, a reliability or risk analysis should never be initiated. Uncertainty plays an important role in SIS-related decisions. Without knowing the uncertainty level of the reliability assessment results, erroneous decisions may be made and an unacceptable risk level may result. This PhD thesis adopts the uncertainty classification from the quantitative risk analysis in nuclear industry, and provides a thorough discussion of each uncertainty category in relation to SIS. It is concluded that the completeness uncertainty is the most important to address in decisions under uncertainty, followed by model uncertainty and parameter uncertainty. To consider the uncertainties in decision-making, this PhD thesis proposes a simple and practical approach to quantify the uncertainty, and hence help to reach more rational decisions.

Structure of thesis

Structure of the thesis

This PhD thesis has two main parts:

- Part I Main report: This part first presents the background, the challenges and research questions, as well as the objectives and the scope of this PhD thesis, and then proceeds to a discussion of the research methodology and approach. Finally the main results are summarized and the possible areas for future research are indicated.
- Part II Articles: This part includes six journal articles and four conference papers published or prepared during the PhD project. These articles consist of the main work and achievements during the PhD.

Journal articles**Article 1:**

Jin, Hui; Lundteigen, Mary Ann and Rausand, Marvin. New PFH-formulas for k -out-of- n -F-systems. *Reliability Engineering and System Safety*, Volume 111, p. 112-118, 2013

Reference

[53]

Article 2:

Jin, Hui and Rausand, Marvin. Reliability of safety-instrumented systems subject to partial-testing and common-cause failures. *Accepted for publication in Reliability Engineering and System Safety*

[55]

Article 3:

Liu, Yiliu; Hui, Jin; Lundteigen, Mary Ann and Rausand, Marvin. Reliability modeling of safety-instrumented systems by Petri nets. *Submitted to Reliability Engineering and System Safety*

[63]

Article 4:

Jin, Hui; Lundteigen, Mary Ann and Rausand, Marvin. Reliability performance of safety-instrumented systems: A common approach for both low- and high-demand mode of operation. *Reliability Engineering and System Safety*, Volume 96, p. 365-373, 2011

[49]

Article 5:

Jin, Hui; Lundteigen, Mary Ann and Rausand, Marvin. New reliability measure for safety-instrumented systems. *International Journal of Reliability, Quality and Safety Engineering*, Volume 20, 2013

[54]

Article 6:

Jin, Hui; Lundteigen, Mary Ann and Rausand, Marvin. Uncertainty assessment of reliability estimates for safety-instrumented systems. *Journal of Risk and Reliability*, Volume 226, p. 646-655, 2012

[52]

Conference papers**Article 7:**

Jin, Hui; Lundteigen, Mary Ann and Rausand, Marvin. Can functional tests be replaced by inspection after demands? *7th Global Congress on Process Safety*, Chicago, 2011

Reference

[48]

Article 8:

Jin, Hui; Rausand, Marvin; Mosleh, Ali and Haugen, Stein. Quantification of organizational influences on failure rate: A Bayesian approach. *IEEE International Conference on Industrial Engineering and Engineering Management*, Hong kong, 2012

[56]

Article 9:

Jin, Hui; Lundteigen, Mary Ann and Rausand, Marvin. Common cause failures in safety instrumented systems: Concepts and analytical approaches. *11th International Probabilistic Safety Assessment and Management Conference and Annual European Safety and Reliability Conference 2012*, Helsinki, 2012

[51]

Article 10:

Jin, Hui; Lundteigen, Mary Ann and Rausand, Marvin. Uncertainty assessment of reliability estimates for safety instrumented systems. *Annual European Safety and Reliability Conference 2011*, Troyes, 2011

[50]

Contents

| | |
|---|-----|
| Preface | i |
| Acknowledgements | iii |
| Summary | v |
| Structure of thesis | ix |
| Part I Main report | |
| 1 Introduction | 3 |
| 1.1 Background | 3 |
| 1.2 Reliability of safety-instrumented systems | 5 |
| 1.3 Standards and guidelines | 7 |
| 1.4 SIS reliability assessment | 10 |
| 1.4.1 Stakeholders of SIS reliability | 10 |
| 1.4.2 Aspects in SIS reliability | 12 |
| 1.4.3 Quantification of SIS reliability | 13 |
| 1.5 State-of-the-art | 14 |
| 1.5.1 Eindhoven University of Technology | 15 |
| 1.5.2 NTNU/SINTEF | 15 |
| 1.5.3 University of Technology of Troyes | 16 |
| 1.5.4 University of Bordeaux | 16 |
| 1.5.5 Tsinghua University | 16 |
| 1.5.6 Tokyo University of Marine Science and Technology ... | 17 |
| 1.5.7 Villanova University | 17 |
| 1.5.8 SIS-tech | 17 |
| 1.5.9 Exida | 18 |
| 1.5.10 Others | 18 |
| 1.6 What is a reliability measure? | 18 |

| | | |
|----------|--|------------|
| 1.7 | Terms for safety systems | 20 |
| 2 | Research questions and objectives | 21 |
| 2.1 | Research questions | 21 |
| 2.1.1 | Testing strategies | 22 |
| 2.1.2 | Common cause failures | 23 |
| 2.1.3 | Human and organizational factors | 24 |
| 2.1.4 | SIS classification | 25 |
| 2.1.5 | State-based reliability methods | 25 |
| 2.1.6 | Uncertainty and decision-making | 26 |
| 2.2 | Research objectives | 27 |
| 2.2.1 | Reliability method and models | 28 |
| 2.2.2 | Classification and reliability measure | 28 |
| 2.2.3 | Uncertainty and decision-making | 28 |
| 2.3 | Delimitations | 29 |
| 3 | Research methodology and approach | 31 |
| 3.1 | What is research? | 31 |
| 3.2 | Classification of research | 32 |
| 3.3 | Scientific method | 33 |
| 3.4 | Research approach | 35 |
| 3.5 | Whole equals to sum? | 37 |
| 4 | Main results and future research | 39 |
| 4.1 | Main results | 39 |
| 4.1.1 | Contributions to reliability methods and models | 39 |
| 4.1.2 | Contributions to classification and reliability measure | 44 |
| 4.1.3 | Contributions to uncertainty and decision-making | 46 |
| 4.2 | Future research | 47 |
| 5 | Acronyms and abbreviations | 49 |
| | References | 51 |
| | Part II Articles | |
| | Article 1 on reliability of high-demand SIS (journal) | 61 |
| | Article 2 on SISs subject to partial-testing (journal) | 71 |
| | Article 3 on Petri nets in SIS reliability (journal) | 89 |
| | Article 4 on common approach for SIS in different modes (journal) | 111 |
| | Article 5 on new SIS reliability measure (journal) | 123 |

| | |
|---|-----|
| Article 6 on uncertainty of SIS reliability (journal) | 141 |
| Article 7 on using demands as tests in SIS reliability analysis (conference) | 153 |
| Article 8 on quantification of HOF influences on failure rate (conference) | 169 |
| Article 9 on common-cause failures in SIS (conference) | 177 |
| Article 10 on uncertainty of SIS reliability (conference) | 189 |

Part I
Main report

Chapter 1

Introduction

1.1 Background

Major accidents have made frequent headlines in the news around the globe in the past years, from the Fukushima Daiichi nuclear power plant accident in Japan [79] and the high-speed train crash in China [108], to the Deepwater horizon explosion in the Gulf of Mexico [5]. The significant loss of human lives and economic assets, as well as the damage to the environment and ecological systems have clearly shown that: While our society receives greater benefits from technological developments, we are also more vulnerable to the risks posed by these technologies.

Intensive use of computers has brought many changes to the systems we are dealing with today, and also to the way safety is managed. According to Leveson [62], today's systems are characterized by:

- Fast pace of technological change
- Reduced ability to learn from experience
- Changing nature of accidents
- New types of hazards
- Increasing complexity and coupling
- Decreasing tolerance for single accidents
- Difficulty in selecting priorities and making tradeoffs
- More complex relationships between humans and automation
- Changing regulatory and public views on safety

With these system characteristics, accident prevention becomes difficult, if not impossible; and it is more or less expected to have accidents—accident becomes normal phenomena [85]. Yet, we can still strive to reduce the likelihood and mitigate the consequences of accidents. Various measures related to man, organization and technology are sought to reduce accident risk. An effective and often used measure is safety barriers [36]. A safety barrier is a physical and/or

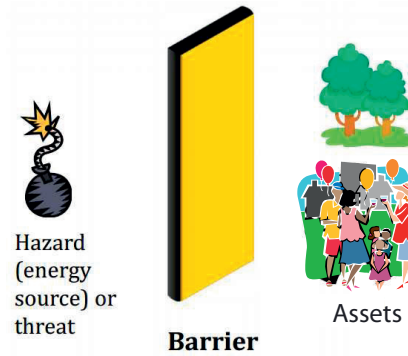


Fig. 1.1 The energy accident model.

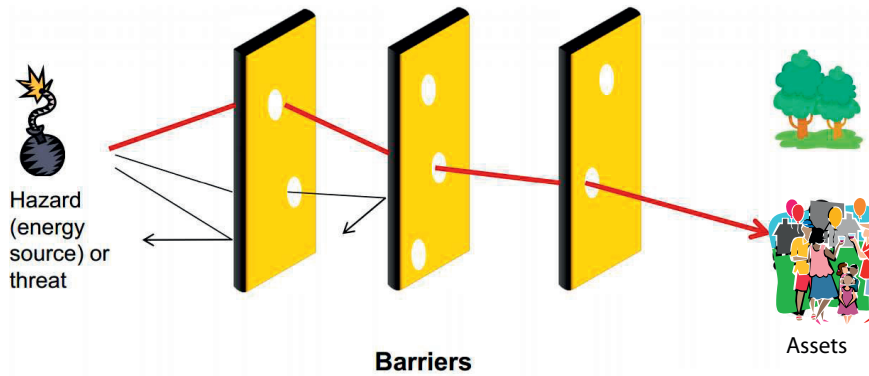


Fig. 1.2 The Swiss cheese model, adopted from [89].

non-physical means planned to prevent, control, or mitigate undesired events or accidents [97, 98]. The concept of safety barrier is illustrated in the energy model [22, 27], see Fig. 1.1. Ideally, no accident would occur when there is a barrier, but since barriers are not perfect—they may fail or not be strong enough—the energy flow may penetrate and result in harm to the assets (human, environment and/or material assets). Reason’s [88, 89] Swiss cheese model depicts how accidents occur despite the use of (often more than one) safety barriers, see Fig. 1.2. As in Swiss cheeses, there are “holes” representing the weakness of safety barriers and likelihood of failure. To strengthen the barriers, it is important to know where and how big the “holes” are. This brings the important issue of reliability (integrity) of safety barriers into the spotlight. To some extent, the reliability of a safety barrier is more important than the barrier itself, because people would be more careful when they are aware of being unprotected than when they believe they are protected but in fact are not.

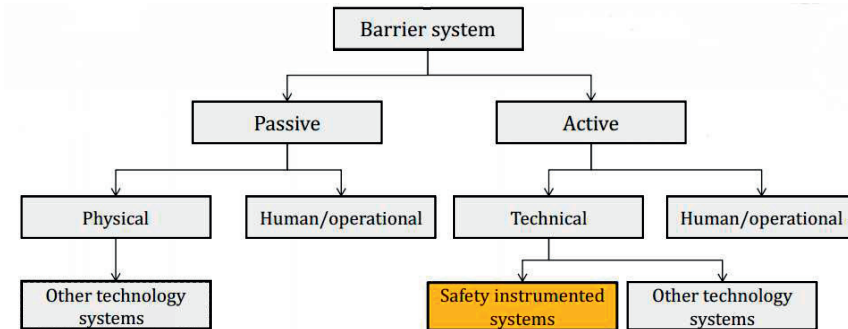


Fig. 1.3 Safety barrier classification, adopted from [97].

Different safety barriers are used to reduce risk, and these barriers may be classified in several dimensions. Sklet [97, 98] distinguishes between passive and active barrier, as well as physical, technical, and human/operational barrier, and proposed a classification as shown in Fig. 1.3. This PhD thesis focuses on one specific type of the technical active safety barriers—safety-instrumented systems (SISs)¹ [40], and more specifically, the reliability of SISs.

1.2 Reliability of safety-instrumented systems

A SIS may be functionally split into three main subsystems: An input subsystem to detect abnormal situations, a logic solver to initiate action based on a predefined logic, and a final element subsystem to respond to the detected abnormal situation, see Fig. 1.4 for a simplified illustration. Redundant designs are often used to improve the reliability of SISs, so each subsystem may consist of one or more (usually but not always) identical channels. It is worth noting that a SIS may perform more than one safety-instrumented function (SIF) [39], but the reliability analysis is always with respect to one specific SIF, because it is the SIF that matters in an accident prevention context. Nevertheless, people are used to say reliability of SIS, and we use this expression in this thesis even though what we actually refer to is one SIF.

Why is it important to study the reliability of SIS? Our safety is more and more taken care of by SISs. The mechanical inter-locking systems and pressure safety valves in the process plants are being replaced or supplemented by computer-based process and emergency shutdown systems. The floating oil installations in ultra-deepwater are no longer kept in position by traditional moor-

¹ SIS is the name mainly used in the process industry, other sectors may use different names. A more detailed discussion can be found in Section 1.7.

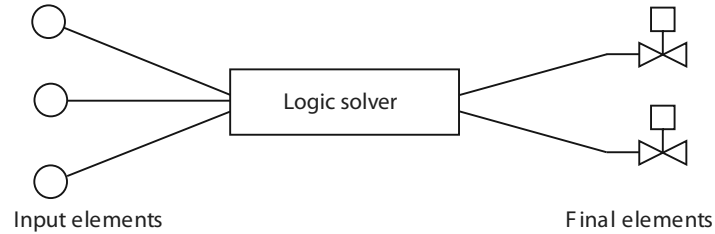


Fig. 1.4 A simplified illustration of a SIS[65].

ing systems, instead dynamic positioning (DP) systems are employed. The DP system [14] uses various sensors to measure the environmental loads and to locate the installation, calculates the amount and direction of forces needed to keep the installation in position, and applies multiple thrusters/propellers to provide the necessary forces from the correct directions. Modern cars are equipped with all sorts of computer-based safety systems, ranging from the anti-lock braking system (ABS) and airbag system to the collision warning and braking system that automatically brakes a car to avoid collision and automatic parking system that gets rid of the trouble of parallel parking. Fire alarm and extinguishing systems are found in most office and residential buildings, they sense fire signal and send out alarm and/or spray water to put out fire. There are many more other SIS applications: railway signaling system, burner management system for power generation, high integrity pressure protection system (HIPPS) used to protect pipelines, to name a few. In fact, a 12% compounded annual growth rate was predicted for SISs market by the ARC Advisory Group [4].

SISs are extensively used to reduce accident risk, but they may also introduce new hazards. A simple example is the airbag system in an automobile. The airbags are installed to protect the passengers from fatal accident in the occasion of collision, but several accidents have occurred where the airbags have accidentally blown up in a normal situation and resulted in fatalities. More serious issues may be found in industrial settings, the use of SIS adds to the overall system complexity, which may lead to more unexpected and unknown interactions in the system and result in new types of accidents. Despite the strict independency requirement between SISs and the rest of the system, dependencies still exist. It may not be so difficult to make SISs physically independent, but the SISs always need to share the environmental conditions as well as human and organizational factors with the rest of the system. It is therefore important to be aware of the side effects of SIS, and take them into account in relevant decisions. In addition to the possible safety hazards, the SIS may also spuriously operate to disturb production and lead to losses and costs. For example, a process shutdown due to the malfunction of an emergency shutdown system in a chemical plant may take several days to restart, and these abnormal system states are major sources of latent errors and accidents. To avoid costs due

to spurious operations, some operators chose to compromise safety, and in the extreme cases, they disconnect SISs. These decisions in turn put the system into a high risk situation. It is therefore important to maintain SIS reliability for both safety and economic purpose—not just perform the required functions, but also avoid the undesired actions.

Increased use of SISs alone does not justify the importance of SIS reliability study. Another and perhaps more important reason to study SIS reliability is that failure of SISs to perform the required function may lead to significant consequences, and unfortunately, SISs do fail. The three major accidents mentioned in Section 1.1 all involve SIS failures. Had the blowout preventer (BOP) functioned properly, the Deepwater Horizon would not explode or sink, and 11 lives would be saved and the biggest oil spill in the history of the United States would be avoided [5, 75]. Had the core cooling system been able to successfully cool down the core in Fukushima [79], we would have avoided a nuclear disaster in Japan, and Germany and Switzerland would not give up nuclear power so quickly (even though we are not sure if it is a good thing). And if the signaling system in the Yongtaiwen railway line did not malfunction, some 40 lives would not be lost in China [108]. These are only a few of the consequences of SIS failures that have made the headlines in the international newspapers, much more can be found in the national and local news. It is therefore of paramount importance to ensure the reliability of our SISs.

1.3 Standards and guidelines

A number of standards and guidelines have been issued to assist in designing, implementing, and maintaining reliable SISs. The most important of these is the international standard IEC 61508 [39], which is a generic standard that outlines key requirements to all phases of the SIS life-cycle. Under the umbrella of IEC 61508 [39], various sector specific standards are developed, such as IEC 61511 [40] for the process industry, IEC 62425 [43] for the railway industry, ISO 26262 [46] for the automobile industry, IEC 61513 [41] for the nuclear power industry, IEC 60601 [37] for medical devices, and IEC 62061 [42] for machinery systems. These standards are commonly known as functional safety standards. The main feature that distinguishes functional safety standards from other safety related standards is that, functional safety standards are performance-based whereas many other standards are prescriptive standards—instead of simply requiring two safety valves to be installed as in the prescriptive standards, the functional safety standards provide work processes, procedures, and tools for the standard user to decide, based on the tolerable risk level, how many safety valves are needed and how should the valves be designed, installed, operated, and maintained. By this,

the functional safety standards can deliver directly to the ultimate goal—tolerable risk.

A general risk reduction framework is presented in IEC 61508 to achieve tolerable risk, see Fig. 1.5. The same framework is followed and adopted in the sector specific standards. Risk is commonly expressed as the combination of the frequency and consequence of the accident. An assessment of frequencies and consequences of hazardous events is first performed to determine the initial risk of the equipment under control (EUC), at the same time the tolerable risk of that EUC is set. SIS and non-SIS safety barriers are designed and implemented to bridge the gap between the initial EUC risk and the tolerable risk. More often than not, we are not able to be so precise to have the safety barriers providing the exact amount of necessary risk reduction. We, in this situation, need to be on the conservative side and have an actual risk reduction greater than the necessary one such the residual risk is under the tolerable level.

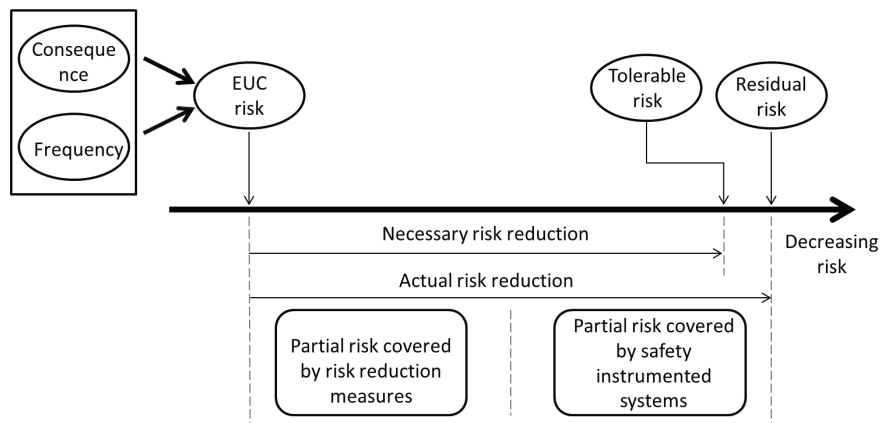


Fig. 1.5 The framework for risk reduction, adopted from [39].

There are several tasks on the way to a system with tolerable risk by applying the functional safety standards. The main tasks include: define system scope; identify requirement; design and realize the system (possibly with several iterations) according to the requirements; install and operate the system; maintain, repair and modify when necessary; and eventually dispose the system. IEC 61508 presents the requirements for each of the main tasks according to a safety life-cycle of 16 phases, see Fig. 1.6. The same life-cycle is more or less followed and adopted in the sector specific standards.

Two types of requirements need to be specified for SIS: the functional requirement stating what the safety function is, e.g., the valve should close and seal upon an upstream pressure over 20 Pa; and the safety integrity requirement stating how well the SIS is required to perform, e.g., the valve should close at

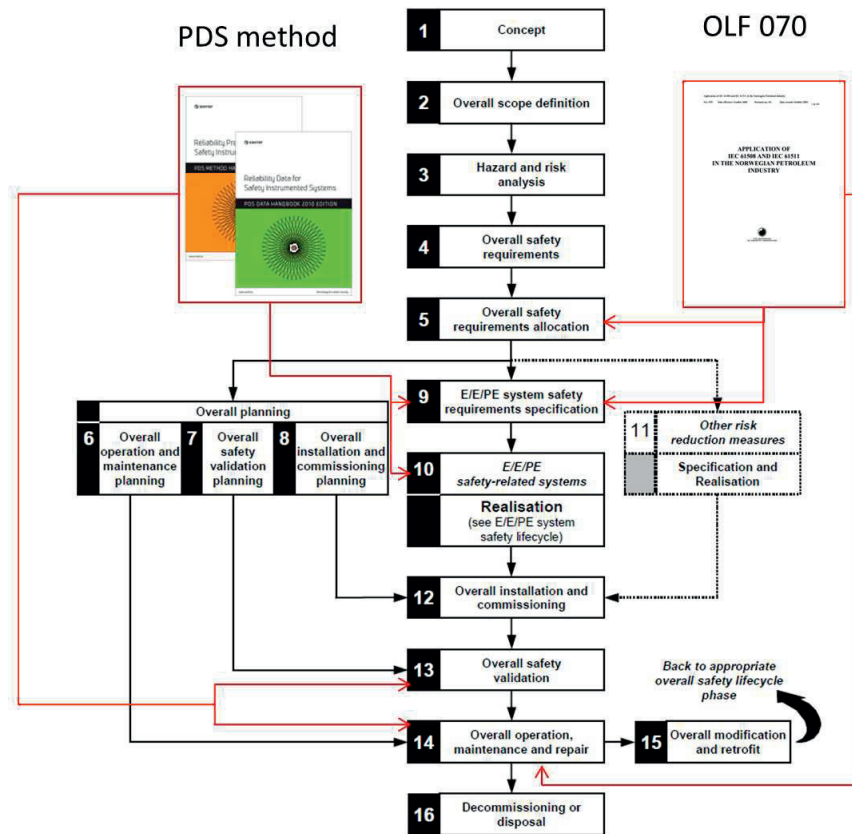


Fig. 1.6 IEC 61508 SIS life-cycle, adopted from [39].

least 99 out of 100 times when it is required to do so. The functional requirement is out of the scope of this thesis and will not be further pursued. We will focus on the integrity requirement.

A central concept of the safety life-cycle in IEC 61508 is the safety integrity level (SIL) [39]. The SIL requirement specifies the collective integrity requirements to each SIF. The standards differentiate four SIL levels with SIL 4 being the most reliable and SIL 1 the least reliable. For a SIF to achieve a required SIL, reliability requirements with respect to hardware safety integrity, software safety integrity and systematic safety integrity need to be fulfilled at the same time. This thesis addresses only the quantitative requirements, which are parts of the hardware safety integrity requirement.

On the Norwegian continental shelf, two SIS related documents must be mentioned. One is the NOG 070 guideline, issued by the Norwegian Oil and Gas Association (former Norwegian Oil Industry Association, OLF) [80], on the

application of IEC 61508 and IEC 61511 in the Norwegian petroleum industry. NOG 070 assists the use of IEC 61508 and IEC 61511 by giving system boundaries and definitions of typical SISs in the offshore petroleum industry as well as the minimum SIL requirements for these SISs. Another document is the PDS method² [31, 33, 30] developed by SINTEF Safety Research. The PDS method presents an alternative way of calculating PFD_{avg} and PFH. The most important features of the PDS method include: use of the multiple beta-factor (MBF) model instead of the beta-factor model for common cause failure (CCF) modeling and inclusion of systematic failures in PFD_{avg} and PFH calculations. The PDS method is of particular importance because it has extracted and documented reliability data of typical SIS components used in the offshore petroleum industry from the offshore reliability data project (OREDA) [84]. These two documents do not cover all the life-cycle phases in IEC 61058. The most relevant phases for NOG 070 and the PDS method are indicated in Fig. 1.6.

1.4 SIS reliability assessment

1.4.1 Stakeholders of SIS reliability

Several stakeholders play important roles in SIS reliability, including the end-user, system integrator, component supplier and functional safety assessment (FSA) assessor as illustrated in Fig. 1.7. These stakeholders work collaboratively under a common environment defined by the standards, regulations, social responsibilities and morality to develop and operate a reliable SIS. In this collaboration, the system integrator takes the central position to coordinate the work and interacts with the other stakeholders.

Most SIS projects are initiated by the end-user who needs to install SISs on the plant to achieve a tolerable risk level. A risk analysis is first performed by the end-user (or consultant hired by the end-user) to determine the risk level of the plant (or EUC), and then a decision is made on whether or not a SIS needs to be installed. When the need is confirmed, the next step is to determine how reliable the SIS and each subsystem should be. Following the terminology of functional safety standards, this process is defined as SIL allocation. SIL allocation is usually a joint task carried out by the end-user, the system integrator and possibly consultants. At the end of SIL allocation, a safety requirement specification (SRS) is prepared. The SRS serves as the governing document in the SIS development, and specifies the detailed requirements for the SIS reliability.

² PDS is the Norwegian acronym for “Reliability and availability of computer-based safety systems.” The PDS-method is developed by the Norwegian research institute, SINTEF, for SIS reliability analysis. It is a well accepted method in the oil and gas industry.

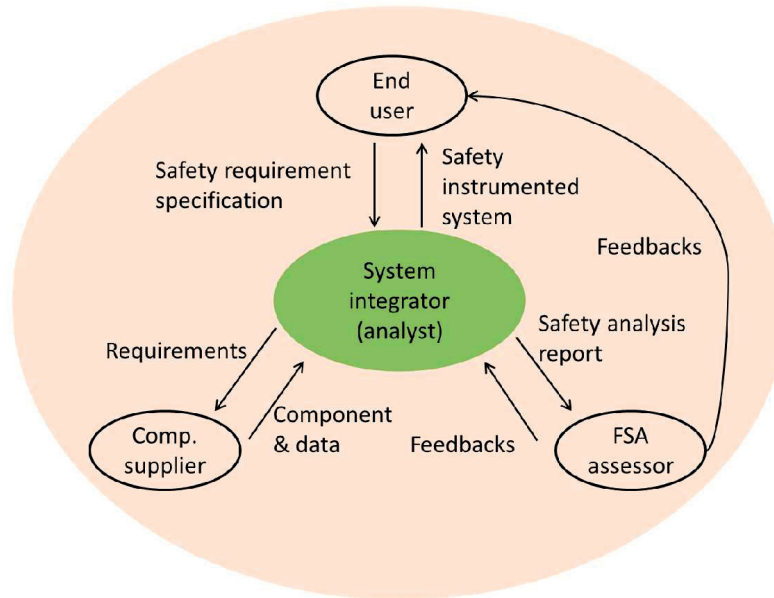


Fig. 1.7 The stake-holders of SIS reliability

Based on the SRS, the system integrator develops a SIS design and assesses the reliability of the design to see whether or not the reliability requirements are achieved. It is not always the case that the first design would meet all the reliability requirements and to become financially feasible, several iterations of SIS design and reliability assessment may be needed until a feasible design is reached. The system integrator may obtain data such as component failure rates from the supplier for reliability analysis, and the system integrator also relies on the supplier to know the available and financially feasible technology, therefore the component supplier is actively involved in the SIS design process. When a SIS design is determined, the system integrator issues contracts to the component suppliers with stated requirements. When the components are ready, the system integrator can proceed to further develop and install the SIS.

To demonstrate that the reliability requirements in the SRS are fulfilled, the system integrator needs to prepare a safety analysis report (SAR) that documents all the evidence and arguments including reliability calculation. The FSA assessor will assess the SAR independently and verify the arguments therein. Based on the assessment, the FSA assessor decides to approve or reject the SAR. When a SAR is rejected, the system integrator needs to revisit and modify the SIS design and reliability analysis to achieve a better system. To provide a better third part opinion, the FSA assessor not only read the SAR but also participates in various phases of the development and provides feedbacks to both the end-user and system integrator.

1.4.2 Aspects in SIS reliability

There are many important topics in SIS reliability ranging from design and analysis, through manufacturing and installation, to operation and maintenance. Figure 1.8 illustrates the most important SIS reliability related topics under the framework of IEC 61508. This thesis is written from an analyst's (system integrator) perspective and focuses on the reliability analysis, so topics such as risk analysis, SIL allocation, SRS, SLS, and FSA are important but not further pursued. Using SIL as the overall measure for SIS reliability (safety integrity), three categories of safety integrity are distinguished, and each of them needs to be assessed:

- Hardware safety integrity
- Software safety integrity
- Systematic safety integrity

In this thesis we discuss only the hardware safety integrity, systematic failures and software failures are not addressed. Attention is given to the red spots in Fig. 1.8: random hardware failure, reliability quantification, human and organizational factor (HOF) and demand modes.

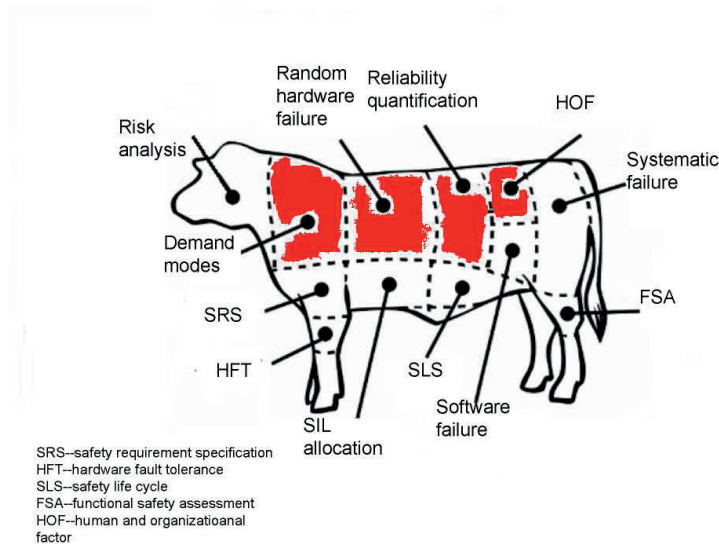


Fig. 1.8 Topics in SIS reliability

1.4.3 Quantification of SIS reliability

Many factors influence the results of SIS reliability quantification. The mode of operation will impact the reliability measure, the assumptions and operational strategy will influence the selection of reliability model and method, and the reliability data and method will determine the quality of the results. Figure 1.9 illustrates the factors that have significant impacts on SIS reliability quantification, and they comprise a large part of the research subjects of this thesis.

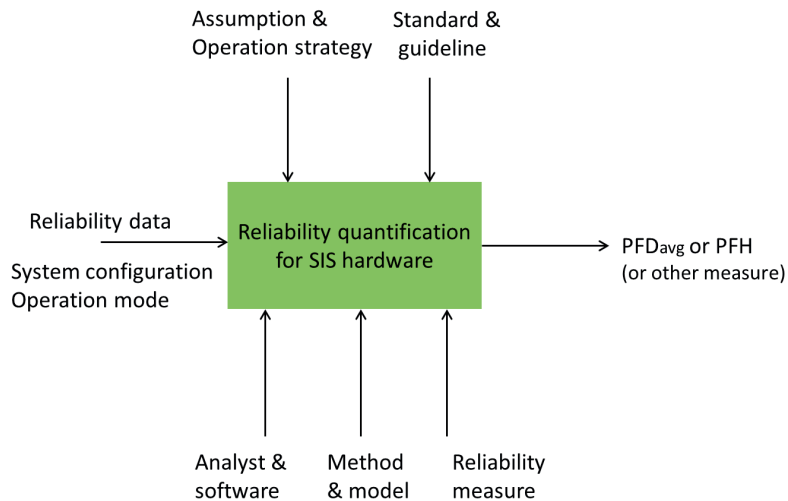


Fig. 1.9 Hardware reliability quantification

IEC 61508 [39] differentiates between on demand and continuous mode of operation. A SIS is working in continuous mode when the safety function retains the EUC in a safe state as part of normal operation [39]. In the oil and gas industry, most SISs are working in the on demand mode, where the SIS is normally in a passive state and will only be activated when a demand occurs. The on demand mode is further classified into low-demand and high-demand mode. When the frequency of demands for a SIS is less than once per year, the SIS is in low-demand model, and the reliability is quantified by the average probability of failure on demand (PFD_{avg}). The PFD_{avg} may be interpreted either as the average probability that the SIS is not able to successfully respond to a demand or the average proportion of time where the SIS is not able to perform its safety function. When the SIS is operated in high-demand mode, which means the demand occurs equal to or greater than once per year, or continuous mode, the frequency of dangerous failures per hour (PFH)³ is used to quantify the

³ Definition changed from probability of failure per hour in the first edition of IEC 61508.

reliability. The SIL range for PFD_{avg} and PFH specified by IEC 61508 [39] are given in Table 1.1.

Table 1.1 SIL requirements [39].

| SIL | PFD_{avg} | PFH |
|-----|---------------------------|----------------------|
| 4 | $[10^{-5}, 10^{-4})$ | $[10^{-9}, 10^{-8})$ |
| 3 | $[10^{-4}, 10^{-3})$ | $[10^{-8}, 10^{-7})$ |
| 2 | $[10^{-3}, 10^{-2})$ | $[10^{-7}, 10^{-6})$ |
| 1 | $[10^{-2}, 10^{-1})$ | $[10^{-6}, 10^{-5})$ |

PFD_{avg} and PFH are reliability measures with respect to dangerous failure–failure that has the potential to put the SIS in hazardous or fail-to-function state. A characteristic of SIS is that the failures are normally hidden, meaning that the failures remain unrevealed unless some efforts are made to detect them. Proof testing and diagnostic testing are the two main techniques applied to detect dangerous failures. The proof tests are usually performed periodically with an interval between several months and several years, and after a proof test the SIS is assumed to be in an “as good as new” condition. The diagnostic tests are performed more often than the proof tests, usually with an interval between seconds and hours. The diagnostic testing can detect dangerous failure more or less immediately after the failure occurred, but the “as good as new” condition cannot be assumed because only a fraction of dangerous failures can be detected. This fraction of dangerous failures is defined as dangerous detected (DD) failure, and the rest failures that are only detected by proof testing are dangerous undetected (DU) failure.

1.5 State-of-the-art

SIS reliability assessment has attracted a lot of research interests. Several groups of researchers have made significant contributions to this topic. For the development of SIS reliability assessment methods and models, we would like to highlight the following groups from universities, research institutes and the industry⁴.

⁴ In spite of the high number of companies contributing to the SIS related issues, only the two companies that are engaged in the research forefront of developing SIS reliability assessment methods and models are presented.

1.5.1 Eindhoven University of Technology

The research group at Eindhoven University of Technology (TU/e) in the Netherlands is one of the pioneers in the field of SIS reliability analysis. They looked at several important aspects of SIS reliability analysis. Shortly after the release of the first edition of IEC 61508 [38], Rouvroye and Van Den Blik [90] and Rouvroye and Brombacher [91] compared different safety and reliability analysis techniques. The results from these studies show that different techniques may lead to different results for SIS reliability analysis, and the enhance Markov method is recommended because of its comprehensive converge. The use of Markov method in SIS reliability analysis is further investigated by Knegtering and Brombacher [59, 58], where a micro Markov method is proposed to combine the benefits of Markov method and reliability block diagram. Goble and Brombacher [24] discuss the role of diagnostic coverage in SIS reliability and develop the failure modes, effects and diagnostic analysis (FMEDA) method.

1.5.2 NTNU/SINTEF

The Norwegian University of Science and Technology (NTNU) and its strategic partner SINTEF have a long history of studying SIS. In the early days, the studies were concentrated on special safety systems in the offshore petroleum industry such as BOP and down-hole safety valve (DHSV). As more experiences and knowledge were accumulated, the studies were extended and applied to more general safety systems. The PDS project was initiated by SINTEF to study the reliability and availability of computer-based safety systems. The products of the PDS project are periodically updated SIS reliability assessment method handbook [31] and reliability data handbook [33]. In addition to the handbooks, efforts are also made to more specific topics. Hokstad and Corneliussen [34] discuss the failure classification in IEC 61508 and suggest relevant clarifications and improvements. In particular, they propose a multiple beta-factor (MBF) [34] model to treat CCFs in SIS reliability analysis, and relevant defense measures against CCFs in the oil and gas industry can be found in [66]. Lundteigen and Rausand [67, 68] study partial stroke testing (PST) and provide a method to estimate the PST coverage. They [69] also provide a thorough discussion on spurious activation to clarify the concepts and suggest ways for calculation. Schönbeck et al. [94] discuss the impact of human and organizational influence on SIS reliability and propose a model to account for human and organizational influence in the operational phase. Janbu [47] provides perspectives on treatment of uncertainty in SIS reliability assessment.

1.5.3 University of Technology of Troyes

The group at University of Technology of Troyes (UTT) in France has much activities on reliability and dependability analysis. For SIS reliability analysis, Langeron et al. [61] study the merging rules in SIS reliability assessment. The results confirm the needs for advanced methods for complex SISs, and they point to Markov method. Brissaud et al. [9] propose a method to estimate failure rates for SIS reliability analysis. The method contains qualitative and quantitative part such that both feedback data and qualitative influence factors can be considered. Brissaud et al. [7, 8] study the impact of partial testing and provided general formula to quantify SIS reliability for multiple components systems subjected to periodic or non-periodic partial testing.

1.5.4 University of Bordeaux

Together with researchers from Total, the group in University of Bordeaux addressed the issue of SIS classification. Innal et al. [45] examine different SIS operational modes by analyzing their definition in IEC 61508 and IEC 61511, and propose new criteria for classification. They also study the relationship between PFD_{avg} and risk reduction factor and show that following the standard way of calculation, optimistic risk reduction factor may be used. This research group has vast interests in SIS reliability methods. Dutuit et al. [19] apply fault tree to assess the reliability of SIS and point to the needs of using time-dependent reliability performance measure in addition to PFD_{avg} . Dutuit et al. [20] apply different methods and tools for SIS reliability assessment and conclude the advantages and disadvantages of each methods. A thorough discussion of using Petri net for SIS reliability analysis is given in [95].

1.5.5 Tsinghua University

The group at Tsinghua University in China present simple reliability block diagram for SIS reliability verification [25] and make efforts to automatically create Markov models for SIS reliability analysis [26]. Xu et al. [109] investigate the optimal replacement policy for multiple state SIS components where interactions between SIS and EUC are considered. In addition, Xu et al. [109] introduce the concept of safety-related uncertainty to measure the effect of parameter uncertainty on safety and provided four ways to assess this uncertainty.

1.5.6 Tokyo University of Marine Science and Technology

At the Tokyo University of Marine Science and Technology in Japan, Misumi and Sato [72] apply fault tree to model SIS performance, where demand frequency, demand duration and spurious operations are considered. They derive genetic algorithm from the fault tree to calculate the hazardous event frequency, which is used as a basis for SIL allocation. Zhang et al. [112] apply Markov method to study SIS reliability and derive expressions for equivalent mean downtimes (EMDTs). These EMDTs are different from the ones suggested in IEC 61508 even though the two groups of EMDTs lead to similar PFD_{avg} for 1oo2, 1oo2D and 2oo3 system. Consequently, Zhang et al. [112] suggest to use EMDTs derived from Markov model. Yoshimura and Sato [110] investigate the impact of safe failure fraction (SFF) and discuss the necessity of having SFF as a constraints for SIL. Their study claims that SFF have non-negative effect on safety and recommended to apply SFF.

1.5.7 Villanova University

Bukowski [13, 10, 11, 12] from Villanova University and her collaborators apply mainly Markov method to study SIS reliability and investigate the CCF contribution. Bukowski and Lele [13] conduct case study to investigate the CCF impacts from different architectures. Bukowski and Goble simulate the stress-strength failure model to verify the CCF reduction rules. Bukowski [11, 12] apply Markov method to incorporate demand frequency into SIS reliability analysis and demonstrate that using exponentially distributed repair time does not have non-negligible impact on the SIS reliability.

1.5.8 SIS-tech

Started as a Houston based consultancy providing services for SIS related issues, SIS-tech has now expanded into a full range of instrumentation and control services to cover all aspects of the Safety Life-cycle. On their website (<http://sis-tech.com/>), various SIS related information including training courses, conferences and softwares, can be found. In addition, they also publish scientific articles [102, 100, 99, 101] to provide their perspectives and research results on SIS related issues such as CCF, systematic failures, SIL allocation, partial stroke testing. These articles look at SIS reliability from the practitioner's perspectives, which give a good supplement to the more theoretical literature written by academics.

1.5.9 Exida

Exida is another major consulting firm on SIS reliability, with global business operation. They provide certification, training and consulting services beside publishing books and software for the industry. Similar as SIS-tech, various SIS related information can be found on their website (<http://www.exida.com/>). In addition to the more formal articles and reports, Exida also runs a blog with its employees contributing their stories, opinions and reflections on SIS related issues.

1.5.10 Others

Many other groups or individuals have interests on SIS reliability and have made contributions to various aspects. Duijm and Goossens [17] develop, through the Accidental Risk Assessment Methodology for Industries (ARAMIS) project, a method to quantify organizational influence on safety barriers. Sallak et al. [92] study the uncertainty in SIS reliability and applied fuzzy probabilistic approach for determining safety integrity level. Oliverira and Abramovitch [83] extend the PFD_{avg} formula to *koon* systems. Torres-Echeverria et al. [103, 104] study the optimal SIS reliability design and suggest approximation to calculate PFD_{avg} for parallel systems.

1.6 What is a reliability measure?

Before proceeding to the research questions that are further investigated in the articles, we take one step back and discuss the meaning of a quantitative SIS reliability measure. A SIS reliability measure, be it PFD_{avg} or PFH, is a probabilistic statement about the system performance in a future time (interval). Since probability is used, the ontological question of what is probability is inevitably inherited to the SIS reliability measure. It has been debated for hundreds of years whether probability is an objective property of an event or it is merely a subjective “degree of belief” existing in our minds. Three main approaches to probability can be identified [86]:

(i) The classical approach, which derives probability from a set of equally likely outcomes of an experiment and defines $\Pr(A)$ as the number of a favorable outcome A , n_A , divided by the total number of possible outcomes, n .

$$\Pr(A) = \frac{n_A}{n} \quad (1.1)$$

(ii) The frequentist approach, which looks at inherently repeatable experiments and defines $\Pr(A)$ as the ratio between the number of favorable outcomes A , n_A , and the total number of experiments, n , when n is approaching infinite.

$$\Pr(A) = \lim_{n \rightarrow \infty} \frac{n_A}{n} \quad (1.2)$$

(iii) The Bayesian approach, which objects to the objective existence of probability and defines $\Pr(A)$ as a numerical value in the interval $[0, 1]$ representing an individual's degree of belief about whether or not event A will occur.

Whereas the Bayesian school disagrees with the classical and frequentist school's interpretation that probability is an objective property, all three schools follow the Kolmogorov axioms of probability in calculation. This means that whether we believe PFD_{avg} (PFH) is a property of a SIS or a "degree of belief" will not affect the reliability calculation and will lead to the same result. It is only the SIS decision, based on or informed by the reliability measure, will be influenced. Therefore, the ontological meaning of PFD_{avg} (PFH) is not important in reliability quantification. On the other hand, the PFD_{avg} (PFH) value used in decision-making is always an estimate, and we believe a completely objective estimation of PFD_{avg} (PFH) is impossible. The reliability estimate always involves more or less the subjective degree of believe from the analyst. Therefore the SIS decision is not based on a property but a degree of belief.

Another issue with reliability measure is that a comparison between the predicted system performance and the actual performance is difficult even when the concerned system has been operation for a long time or after the system life time. SISs are very reliable systems, we normally do not have enough data to achieve a confident validation of the PFD_{avg} (PFH) estimated in the design phase. Because direct validation of the reliability methods and models is difficult, we have to use other approach to validate our research results, see Section 3.3 for more discussion on validation.

It is also worth mentioning that, according to IEC 61508, PFD_{avg} is the average probability of failure on demand. It is easy to interpret PFD_{avg} wrongly as a conditional probability with the condition being a demand. The PFD_{avg} is actually an average unavailability which does not condition on demand or anything else. This means that the demand does not influence the PFD_{avg} as a reliability measure as such. It is possible to argue that the demand should be taken into consideration in PFD_{avg} calculation, but when the calculation is done, the PFD_{avg} is still an average unavailability that does not condition on demands. The PFH is the average frequency of a dangerous failure, and it is essentially the same as the average rate of occurrence of failures (ROCOF) over a time interval.

1.7 Terms for safety systems

SIS is the name used in the process industry for the kind of safety systems we are dealing with in this thesis, due especially to the influence of IEC 61511. Other industries are using different names for the same kind of safety systems, for example, IEC 61508 uses electrical/electronic/programmable electronic (E/E/PE) safety related system, ISO 26262 uses electrical and/or electronic (E/E) safety related system in the automobile industry, IEC 62061 uses safety related electrical, electronic and programmable electronic control systems (SRECS) for machinery systems, ISO 13849 uses safety related parts of control systems (SRP/CS) for machinery systems, IEC 61513 uses instrumentation and control (I&C) system in nuclear power plants, and IEC 62425 uses safety related railway signaling systems/sub-system/equipment in the railway industry.

The diversity of terms for safety systems in different industries and standards may, to a large extent, be due to the traditions in these industries and the backgrounds of those people behind each standard. It is our opinion that these names do not have non-negligible influence on the reliability analysis of safety system, especially not the core issue of this thesis—reliability quantification. For the convenience of presentation, it is decided to use SIS as a general name. SIS is selected for two reasons: (1) it is widely used in the process industry, which is the sector that had and still have the most active research on functional safety, and (2) SIS is much simpler than other names such as E/E/PE safety related system. In the rest of this thesis, we will use SIS for all relevant safety systems. This also means that the results of this thesis are applicable not only to the process industry, but also to other sectors.

Chapter 2

Research questions and objectives

2.1 Research questions

Reliability estimates (PFD_{avg} or PFH) serve as a basis for many decisions in SIS design and operation. The accuracy of a reliability estimate is important in the sense that an incorrect PFD_{avg} or PFH contributes to the acceptance of an insufficiently reliable design or the rejection of a sufficiently reliable design. The former leads to a SIS with inadequate risk reduction, whereas the later results in unnecessary investment.

All SIS reliability analysis approaches [10, 19, 20, 25, 34, 44, 61, 70, 90] are based on certain assumptions, e.g., the system is assumed to be “as good as new” after a proof test. These assumptions are not valid in all cases and represent significant weaknesses. If the assumptions are used when they should not be, incorrect reliability estimates or significant uncertainty may result, and wrong decisions will follow. Calculation of the reliability when the assumptions are not valid is a challenge in SIS reliability analysis. When the assumptions are valid, reliability analysis may also suffer from various uncertainties [47, 105, 81, 92] with respect to the input data, the model, and the completeness. These uncertainties may not at all be explicitly quantified, so another challenge is how to consider these uncertainties in decision-making. The current SIS classification and reliability measures lacking a scientific foundation, therefore lead to confusions and reluctances among practitioners. Other challenges in SIS reliability analysis include how CCFs [35] can be better account for, issues related to human and organizational factor [93, 94]. Based on a thorough literature survey, the following specific challenges are identified.

2.1.1 Testing strategies

Proof testing is the primary method to detect failures and ensure SIS reliability. But other testing methods are also used in order to meet the increasingly demanding reliability requirements. These testing methods include diagnostic testing, partial testing, and the more recently emerged idea of using demands as tests.

Dangerous detected failures

When calculating PFD_{avg} and PFH according to the formulas in IEC 61508, the DD-failures need to be combined with the DU-failures to calculate the MEDT. An issue with this approach is that as the system expands, more MEDTs need to be calculated. IEC 61508 only provides formulas for up to three components, reliability of systems with more components cannot be calculated. Rausand and Høyland [87] present PFD_{avg} formulas for *koon* systems with the assumption that the contribution of DD-failure is negligible. Both the PDS method [31] and Oliverira and Abramovitch [83] take one step further and developed PFD_{avg} formulas that are able to account for DD-failure for *koon* systems. For PFH calculation, it has been more problematic. The PDS method [31] is the only attempt to develop PFH formulas for *koon* systems, but it failed to properly account for the DD-failures.

Non-perfect proof testing

Most PFD_{avg} and PFH formulas assume that the proof testing is perfect, and thus consider only one proof test interval in the calculation, but there are also a lot of cases where the proof testing cannot detect all failures or the “as good as new” assumption is not valid. In order not to overestimate the SIS reliability [23, 31], the effect of non-perfect proof testing needs to be accounted for. IEC 61508 [39] propose to use proof test converge (PTC) in the calculation of MEDTs, but it is subjected to the main drawback of using MEDTs—cannot be generalized to *koon* systems.

Partial testing

Partial testing is similar to the non-perfect proof testing. They both detect part of the DU-failures. A slight difference is that partial testing is normally used in combination with proof testing, whereas non-perfect proof testing may or may not be combined with overhaul (overhauls restore the system to “as good

as new”). An often used partial testing technique is the partial stroke testing (PST) [2, 3, 68, 99]. Formulas to account for the effect of partial testing are presented for 1oo1 in [68, 67, 99], and numerical approach is employed to solve 1oo2 system in Torres-Echeverra et al. [103]. More recently general formulas are derived in [7, 8] for systems with *koon* configurations. The general formulas can take care of both periodical and non-periodical partial testing, but it failed to account for CCFs.

Demands as tests

When the demands for a SIF become frequent, the influence of demands on SIS reliability cannot be neglected any more. Since the demand is able to verify the functionality of the SIS, several attempts have been made to use demands as proof tests in SIS reliability analysis [10, 72, 64, 111]. However, a demand is different from a proof test in many respects. A demand comes randomly, whereas a test is pre-scheduled. A test is a proactive approach to detect failure, but a demand may lead to an accident. The test coverages are also different between a proof test and a demand. A demand is able to verify the system level functionality but not the channel level, whereas a proof test carefully examines each channel and verifies their functionality. To use demands as proof tests, not only formulas need to be established, measures to avoid possible abuse are also needed because it may be manipulated to avoid costly proof tests.

It is a challenge to establish formulas to properly account for different testing strategies. Having a general formula that takes care of all testing strategies may not be feasible. A more relevant topic would be to identify possible testing strategies and establish formulas accordingly. Based on a thorough literature review, the following research questions are identified.

- How do we calculate the reliability of *koon* systems when DD-failures and/or non-perfect proof tests cannot be ignored?
- How do we calculate the reliability of *koon* systems subject to proof testing and periodical or non-periodical partial testing?
- How do we account for the effect of using demands as proof tests?

2.1.2 Common cause failures

Common cause failure is a main contributor to SIS unavailability [35, 66]. The accurate modeling of CCFs serves a critical role in decisions based on or informed by SIS reliability. Since the introduction of CCF in the 1960s [35, 86], a high number of CCF models have been proposed, and several initiatives have been taken to collect CCF data, but these efforts have mainly been limited to the

nuclear power industry [77, 96]. For SIS reliability, the industry is, most of the time, satisfied with the beta-factor model [21] and MBF [31] model because of their simplicity together with the fact that CCF data is limited.

It is absolutely fine to use simple models, yet models should not be used just because they are simple. The model must, at the same time, make sense and produce reasonable results. For SIS reliability in particular, if errors are inevitable, they should be on the conservative side with respect to safety. The practitioners have been using the beta-factor model and MBF model without questioning their adequacy, while it is indeed important to ensure that the models are adequate, and for SIS in particular, conservative. To assess whether or not the beta-factor model and MBF model are adequate, a common and precise CCF definition is important. Unfortunately, despite the considerable efforts in CCF studies, a generally accepted CCF definition is still missing. Based on the literature review, it is observed that the primary disagreements in the current CCF definitions [66, 76, 78, 39] are related to the following two questions:

- Must multiple failures occur simultaneously to be a CCF or can the failures be spread out in time?
- Should a CCF always lead to system failure?

Our research questions related to CCFs are therefore:

- What is the proper CCF definition that removes the aforementioned inconsistencies?
- Is it adequate to use beta-factor model and MBF for SIS reliability analysis?

2.1.3 Human and organizational factors

Human and organizational factor (HOF) has significant influences on SIS reliability [6, 17, 94], but systematic studies addressing HOFs have not been seen. HOF influences exist in many phases of the SIS life-cycle. The most significant HOF influence occurs in SIS manufacturing, installation, and operation, where humans have most interactions with the system and is susceptible to commit errors (or omit tasks). A common feature of the HOF influences in these phases is that they are all after the completion of SIS design, where some of the most important decisions are made. It is important to predict the HOF influences in the reliability analysis carried out in design phase. This is particularly challenging because very limited or no data related to HOF in manufacturing, installation, and operation are available in the design phase, nor are HOF models for this purpose. We need to use more “generic” HOF data to estimate SIS reliability. In this regard, the relevant research questions on this issue are.

- What are the useful “generic” HOF data for SIS reliability analysis?
- How can the SIS reliability analysis benefit from the identified HOF data?

2.1.4 SIS classification

Functional safety started out mainly from the process industry, where most SISs are working under infrequent demands, therefore most research has concentrated on PFD_{avg} with the presumption that the systems are in low-demand mode. As the concept of functional safety is getting more popular and spreading out to other sectors, it is more and more frequent that we encounter systems working in high-demand or at the boundary of low- and high-demand. If the IEC 61508 standard is strictly followed, we may run into situations where a system is SIL 2 when it is demanded once per 11 months (high-demand) but is SIL 1 when it is demanded once per 13 months (low-demand), this causes trouble among the practitioners and risks the possibility of abuse. It is important to clarify the SIS classification and reliability measures or propose alternatives.

One particular challenge in SIS classification is that IEC 61508 gives the boundary one demand per year for low- and high-demand mode without any further explanation. On the one hand, it has been realized that there are always problems to use demand frequency as the only criterion since the demand frequency is a continuous parameter. The one demand per year criterion is used pragmatically and scientific arguments are difficult, if not impossible, to find. On the other hand, the standard is explicit about the boundary, so sub-optimal decisions may need to be made to comply with the standards. A possible solution is to remove the SIS classification and to take into account the demand frequency in SIS reliability analysis. Several attempts have been made in this direction with Markov method [11, 45, 72, 64, 111]. The questions emerged in this line of research are:

- How should we classify different SIS operational modes?
- What reliability measure do we use? PFD_{avg} ? PFH? or something else?

2.1.5 State-based reliability methods

Simplified formulas [31, 39, 87] are the most popular SIS reliability calculation method, especially among the practitioners, due to their simplicity. Structural models, such as fault tree (FT) [45, 70, 72, 39] and reliability block diagram (RBD) [87, 39], are also commonly used for slightly more complex SISs. When the complexity increases further, the simplified formulas and structure models found themselves struggling, this is especially true when the dynamic (time-dependent) system behaviors, e.g., the change of PFD as a function of time, is important.

State-based methods are able to capture the time-dependent behaviors of a system. In IEC 61508, Markov method [39, 26, 45] and Petri net [18, 45, 95] are the two recommended state-based methods for complex SIS. Compared to

simplified formulas and structure models, the state-based methods are more sophisticated and flexible. For instance, the demand frequency can easily be integrated into the reliability analysis by using Markov method, and the complicated testing strategies can be readily handled by Petri net. The state-based methods are more abstract and difficult to understand. More competence is required to perform SIS reliability analysis with Markov method or Petri net.

Among the practitioners, there is a general reluctance to apply the state-based methods in projects even though they would yield better results. One important reason of the reluctance may be psychosocial: the practitioners feel the state-based methods are so complicated that they are not able to learn or it does not worth the time to learn when the potential gain is not certain or insignificant. The challenge is to come up with standard ways of applying state-based methods in SIS reliability analysis and demonstrate the advantages and benefits of these methods. In addition, there are also challenges related to the methods themselves, for example, Markov method suffers from state-explosion when the number of components increases and solving a general stochastic Petri net is demanding.

The research questions related to state-based reliability methods are:

- How the state-based methods are used to address issues such as integrating demands into SIS reliability analysis?
- What are the benefits of applying state-based methods?
- How to address the internal issues of state-based methods in the context of SIS reliability analysis?

2.1.6 Uncertainty and decision-making

Reliability analyses are based on simplifications and assumptions about the system and its operating context, SIS is not an exception. Various assumptions about failures, repairs, operating conditions, testings and so on are made in SIS reliability analysis, the resulting PFD_{avg} or PFH is therefore subject to uncertainty. Without knowing the level of uncertainty in the reliability estimate, the SIS suppliers and end-users may make erroneous decisions regarding system configurations, component selections, testings as well as maintenance strategies. Therefore, the uncertainty of SIS reliability estimates need to be aware of, analyzed, managed and considered in decision-making.

Uncertainty is a long discussed topic, a lot of literature is available on this topic [1, 81, 16, 107, 73]. In the nuclear industry [81], three sources of uncertainty are distinguished: completeness uncertainty, model uncertainty, and parameter uncertainty. Until recently, the research in SIS reliability has been limited to parameter uncertainty [6, 106, 92]. Completeness uncertainty and model

uncertainty have not been studied in relation to SIS, even though they may pose significant influences on the reliability estimates.

A few requirements regarding uncertainty are given in IEC 61508 and IEC 61511. The standards require that the failure rates data should have a confidence level of at least 70% [39, 40] to be conservative. To meet this requirement, it is necessary to consider the failure rate as a random variable with a probability distribution that describes our knowledge/belief about the failure rate [28]. IEC 61508 also requires that a confidence level of at least 90% shall be demonstrated on the reliability estimates, in the selection of hardware architectures for the so-called route “2_H” [39]. The PDS method considers factors that are often left out in the SIS reliability calculations: (i) Test independent failures (TIF) that may remain unrevealed due to limitations of the proof testing, and (ii) inclusion of systematic failures in the failure rates. By this, they aim to reduce the uncertainty. In addition, there are suppliers who use “best estimates”, but add conservatism by making the SIL requirement more strict, such that compliance with, for example, SIL 3, is only claimed when $PFD_{avg} \leq 0.7 \cdot 10^{-3}$. These attempts try to control the uncertainty of SIS reliability estimates, but the scope is rather limited and they do not give any explicit information about the level of uncertainty. Systematic consideration of uncertainty of SIS reliability estimates in decisions seems to be lacking. This poses the research questions:

- What are the uncertainties in the context of SIS, and how do they influence the decisions?
- How should the uncertainty be analyzed, represented, and used in decision-making?

2.2 Research objectives

The overall objective of this PhD thesis is *to develop new methods and new concepts for reliability assessment of safety-instrumented systems*. The knowledge generated in the PhD project, should give rise to more rational decision-making related to SIS reliability in design, technology qualification, implementation, and operation, hence contribute to the overall strategy for major risk prevention.

There are many aspects where SIS reliability related new methods and concepts can be developed, to avoid being too general or losing focus, more specific objectives are defined based on the research questions. They are presented in three categories.

2.2.1 Reliability method and models

- Objective 1: Develop simplified formulas for SIS reliability analysis. The new formulas shall be able to account for issues such as DD-failures, non-perfect proof testing and partial testing in a better way, so the analysis result will be more accurate.
- Objective 2: Identify and assess the pros and cons of using demands as proof tests in SIS reliability analysis. Propose possible ways to include the reliability contribution from demands.
- Objective 3: Develop a method to quantify human and organizational influence on SIS reliability when the HOF data directly related to SIS is limited.
- Objective 4: Propose a new CCF definition to clarify confusions and inconsistencies in the existing CCF definitions, and assess the adequacy of the beta-factor model and MBF model in light of the new definition.
- Objective 5: Apply and develop state-based reliability methods in SIS reliability analysis, demonstrate to the practitioners the advantages of state-based method and how they can be implemented.

2.2.2 Classification and reliability measure

- Objective 6: Further develop and refine a common reliability analysis approach for both low- and high-demand modes by using Markov analysis to integrate the demand frequency.
- Objective 7: Propose a common reliability measure which applies to both low- and high-demand modes, and investigate its properties.

2.2.3 Uncertainty and decision-making

- Objective 8: Clarify the concept of uncertainty in the context of SIS reliability analysis and highlight the issues related to the three categories: completeness uncertainty, model uncertainty, and parameter uncertainty.
- Objective 9: Propose a holistic approach to analyze uncertainty in SIS so that more structured inputs are obtained for decision-making.

2.3 Delimitations

This PhD project is limited to quantification of SIS random hardware failures. Other SIS related topics, such as control and management of systematic failures, architecture constraint, and software reliability, are important but not explicitly addressed. This PhD thesis is centered on developing new methods and concepts for better reliability quantification, discussions on issues related to data collection and the physical system are, therefore, kept minimal.

The research during this PhD project is to a large extent theoretical. Most of the examples are not extensive and involve certain levels of abstractions and simplifications. The main results are documented in terms of scientific articles, therefore certain repetitions between different articles should be expected. The methods and models in this thesis are developed for subsystems of SIS with the independent assumption between subsystems. Extension to the whole SIS is straightforward under the framework of IEC 61508.

There is one thing we have to point out and apologize to the readers. For two concepts, we have used different terms in different articles and are not able to change since they are already published. These are proof test and functional test, and PFD_{avg} and PFD. We prefer proof test and PFD_{avg} to functional test and PFD.

Chapter 3

Research methodology and approach

The purpose of PhD education is multi-fold. Beside the quest for new knowledge, it is equally or even more important to provide PhD students with training in research skills. After PhD, the student should become an independent researcher and be able to conduct scientific research alone. This chapter discusses my understanding of research methodology and research approach in general, and those applied in this PhD project in particular.

3.1 What is research?

Research is defined, in Merriam-Webster on-line dictionary [74], as: “a studious inquiry or examination; especially: investigation or experimentation aimed at the discovery and interpretation of facts, revision of accepted theories or laws in the light of new facts, or practical application of such new or revised theories or laws.” The essence of this definition is: search for novelty, either new facts, or new theories, or new applications. The manner of this search is usually not casual but often well organized and systematic, as Creswell [15] stated: “research is a process of steps used to collect and analyze information to increase our understanding of a topic or issue.”

The purpose of research is to discover new “things” through the application of scientific procedures. Yet words like “things” and “novelty” are too general to be practically usable. Whereas in the very early days, research may be performed for the sake of researching, almost all research projects today are purposeful, aiming at a specific phenomenon, theory or problem. The new “things” or “novelty” in research is usually specified in the research objectives, which are established to answer the research questions.

The motivation for researching a certain topic may be divided into two levels. What is the motivation of doing research in general? and why on the specific topic? The answers may be much diversified from different people. For me, I

started the PhD project with the desire to experience more intellectual challenges and to find out whether or not research is the “thing” I wish to pursue in my life. As for the question of why research on reliability of SIS. The reasons are more of practical consideration. Reliability of SIS is an important topic. It is directly related to the safety of human, environment and material asset, and there are still many SIS related issues waiting to be tackled. At the time I was about to finish my master, there was a scholarship on SIS reliability, which happens to be the topic of my master thesis, so why not?

3.2 Classification of research

Research may be classified in different ways depending on the criteria. Based on the intended use, OECD [82] distinguish and define: (1) basic research as experimental or theoretical work undertaken primarily to acquire new knowledge of the underlying foundations of phenomena and observable facts, without any particular application or use in view; and (2) applied research as original investigation undertaken in order to acquire new knowledge. It is, however, directed primarily towards a specific practical aim or objective. The basic research is further divided into: (1a) pure basic research—Research carried out for the advancement of knowledge, without working for long-term economic or social benefits and with no efforts being made to apply the results to practical problems or to transfer the results to sectors responsible for its application; and (1b) oriented basic research—Research carried out with the expectation that it will produce a broad base of knowledge likely to form the background to the solution of recognized or expected current or future problems or possibilities. This PhD project aims to develop new methods and new concepts (which will add to the general knowledge base) for reliability analysis of SIS (which is the recognized problem area). It falls into the category of oriented basic research.

Based on the way research is performed, we may differentiate between descriptive and analytical research [60]. Descriptive research usually uses survey and other fact-finding methods to collect existing data and information. The main characteristic of descriptive research is that the variables are not under the control of the researchers. The results of descriptive research are more information about a subject that can be used to generate hypotheses. Analytical research conducts experiments with controlled variables to test the hypotheses, or studies the existing knowledge and findings to develop new methods or models based on logical reasoning. This PhD project is based on the IEC 61508 framework and probability theory, and uses logical reasoning to derive new methods, and is therefore more into the category of analytical research.

We may also differentiate between exploratory and confirmatory (also called conclusive) research, quantitative and qualitative research, as well as conceptual

and empirical research. A summary of the research types of this PhD project is given in Table 3.1.

Table 3.1 Research types of this PhD project.

| Research types | PhD project |
|----------------|-------------|
| Applied | |
| Pure basic | |
| Oriented basic | √ |
| Descriptive | |
| Analytical | √ |
| Exploratory | √ |
| Confirmatory | |
| Quantitative | √ |
| Qualitative | |
| Conceptual | √ |
| Empirical | |

3.3 Scientific method

Research is an organized and systematic activity. In most research projects, the procedures and steps of the scientific method are followed.

- We start with observations about something that is unknown, unexplained or new, and then to investigate relevant theory for the “something” we observe;
- Based on the investigation, we formulate hypothesis to explain our observations;
- Then, we design and perform experiment, data collection or case study to test the hypothesis;
- The hypothesis is accepted or rejected based on the analysis of the test result. If the hypothesis is rejected, we may choose to modify the hypothesis and test again, or proceed to the next step;
- When the actual research is done, the results are documented and reported to our peer and others.

The main objective of this PhD project is to develop new concepts and methods for SIS reliability quantification. To achieve this objective, we address different facets of this issue. As shown in Fig. 3.1, it is like building a house, the roof (main objective) rests on pillars representing solutions to various aspects or factors in SIS reliability analysis. For the topic of each pillar, the scientific method is more or less followed.

There are, however, two places where the current PhD project deviates from the scientific method. First, we do not have the hypotheses in the traditional

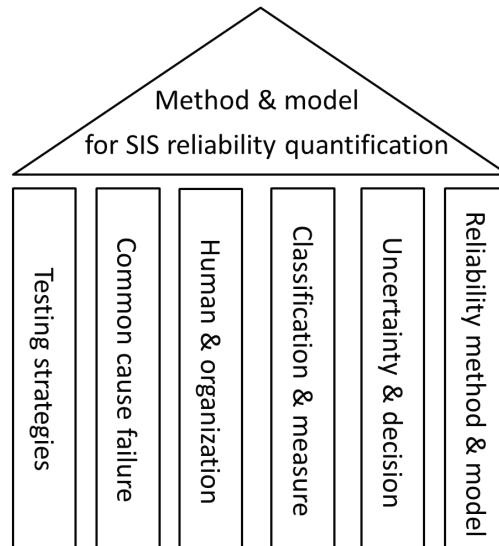


Fig. 3.1 The pillars of the PhD objective.

sense. Instead, we deduct new methods from the reliability and probability theory by careful investigation and sound reasoning. These new methods become our “non-traditional” hypotheses.

It is important that new methods are validated before being accepted for the intended purpose. Due to the nature of our problem, we have our second deviation from the scientific method. In the scientific method, the validation is usually achieved by conducting experiments or case studies. For new methods of SIS reliability analysis, this way of validation has been difficult in a PhD project, because SISs are very reliable system, it takes far more than four years before we can have adequate data to draw a conclusion. We have to use an alternative approach, where the validation is partly achieved by investigating the validity of the our reasoning. It may be difficult to prove that our reasoning is correct, but if any errors in the assumptions or in the reasoning logic are found, we can conclude that the new methods are inappropriate or wrong. In this PhD project, the investigation of reasoning is achieved by subjecting our methods to various peer reviews in group meetings, international conferences and journals. In addition, even if real case studies have been difficult, we may perform pseudo-case studies, where the results from the new methods are compared not with real data, but with results from other exiting methods. By this, we can increase the confidence of the new methods. Pseudo-case studies have been extensively used in the articles.

3.4 Research approach

A research project is a series of activities aiming to create general knowledge or provide solutions to specific problems. It usually begins with the definition of research basis and research questions, and concludes with documentation of the results (sometimes also products). Different approaches may be used along the way to achieve the research results. But whatever research approach is taken, a research project that aims at developing new methods should always include the following main steps (quoted from [57, 65]):

- Identification of research contexts and perspectives
- Discussion of relevant research “gap”, and the associated research questions
- Identification of main assumptions
- Description of theoretical basis
- Description of new methods and models
- Discussion of method/model application areas and constraints

This PhD project takes a quantitative, more specifically quantitative inferential, approach rather than the often used experimental approach. This research approach is similar to the one used in mathematics, where we start from the basic theory (in our case probability and reliability theory), with consideration of relevant assumptions and the nature of the problem, and deduct new methods or formulas by logical reasoning. The deducted new methods and formulas are expected to either take into account factors that are not previously considered in SIS reliability analysis or give more accurate results.

This PhD project is completed with three main stages, which represent the three main activities: (1) identification of research questions and objectives; (2) development of new concepts and methods for the identified questions; (3) summarization of the PhD project and conclusion. The detailed activities and milestones in each stage are illustrated in Fig. 3.2.

The first stage of the PhD project is to identify research questions and establish research objectives. The main activities in this stage are extensive literature study and discussions with advisors. Through literature review, research gaps are identified, and consequently the research questions. It is not possible to address all the research questions in one PhD project, therefore a choice must be made. Based on the literature review, discussions with advisors and own research interest, the initial research objectives are formulated. And the milestone, which indicates the end of the first stage, a PhD project plan is prepared.

With the identified research questions and objectives, new methods and models are proposed after critical investigation of the literature, extensive discussions with advisors and colleagues, and rigorous logical reasoning. The initial proposals are barely good enough. To improve and refine the proposals, we expose the new methods and models to the scrutiny of different groups of experts through various channels, such as internal and external seminars, conference

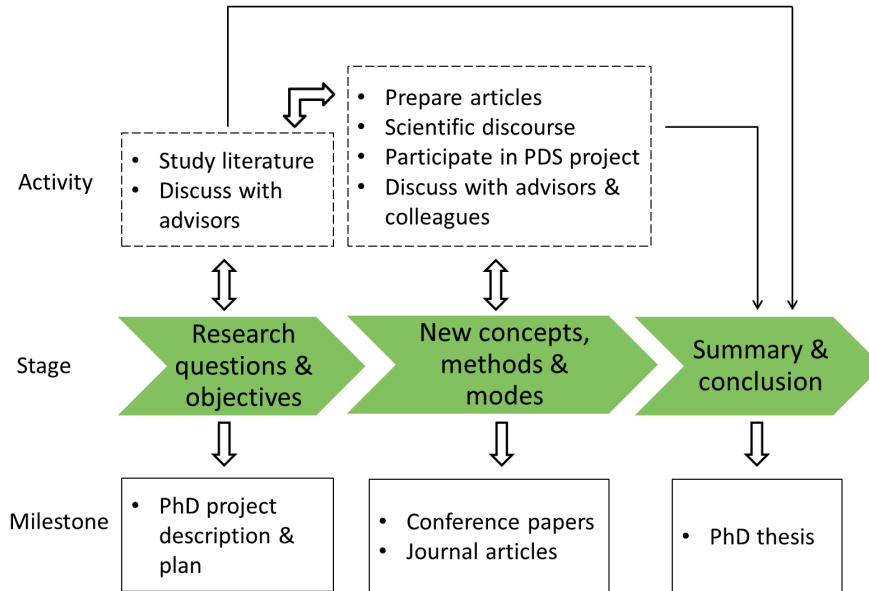


Fig. 3.2 The research activities and milestones.

presentations as well as journal peer reviews. The feedback from these external parties are used to refine the methods and models. The final product of this stage is articles published in conference proceedings and international journals. It is worth mentioning that a PhD project is an iterative process. When new insights are gained in stage 2, it is not uncommon that we go back to the first stage to modify our research questions and objectives.

The third and last stage of the PhD project is to report the findings in terms of a PhD thesis. The thesis includes two parts, a main report documenting the research basis, questions, objectives, approaches and the main contributions, and a list of articles written for the PhD project. At this stage, I summarize and reflect on the PhD project.

Research is no longer (if it ever were) a one man's job, collaboration plays a critical role in the success of any research project. This PhD project is not an exception, we have had various types of collaborations throughout the project, and all have benefited this thesis. All the articles written in this PhD project are product of direct collaboration. The co-authors including advisors, colleagues, and professors from foreign university. They together represent a wide range of expertises and provide constructive inputs and insightful critics. Conferences and seminars are important arenas to get comments and inspirations. Participation in industrial project provides a different perspective on the research topic. Last but not least, the importance of indirect collaborations in forms of reading

literature and having manuscripts reviewed by peers should never be underestimated.

3.5 Whole equals to sum?

In the field of system reliability, the unwritten assumption that system performance is determined by the sum of subsystem and component performance is almost always used, in other words we assume that the performance of the whole system is the sum of the performance of the comprising components. The two classic reliability methods, RBD and FT, are the best representation of this unwritten assumption. Both methods obtain the system performance by decomposing the system to the bottom level and combining the bottom level component performance with logical operation.

System safety has a close relationship with system reliability since the day it was born, and has extensively used methods and tools from system reliability. Inevitably, system safety also inherited the whole equal to sum assumption. But recently, a group of researchers, represented by Nancy Leveson [62], started to question the validity of the whole equal to sum assumption in system safety. They argue that safety is an emergent property of a system, and it is impossible to understand the system safety performance solely by studying the component performance.

In this PhD project, we realize that SIS reliability is intertwined with the field of system safety, but it is indeed a system reliability topic. We believe that SIS reliability performance can be analyzed by studying the SIS subsystems and components. The whole equal to sum assumption is made in this thesis, but in the meantime, we appreciate and are aware of the concerns of using this assumption.

Chapter 4

Main results and future research

4.1 Main results

The main results of this PhD project are documented in the form of ten articles, among which, four articles have been published in relevant international journals, two are currently under review and the other four have been presented in peer reviewed international conferences and published in the conference proceedings. These articles are written to address the research questions identified in Section 2.1. With the ten articles, we aim to achieve the nine research objectives stated in Section 2.2.

In addition to the articles, I also participated in the preparation of the PDS method handbook 2013 [29] during my PhD. This document is not included in the this PhD thesis, but can be purchased through SINTEF safety research (<http://www.sintef.no/pds>).

In this chapter, we summarize the main results and contributions of this PhD project with respect to each objective, such that we are able to evaluate how and to what extent the objectives are met. An overall relationship between the research objectives and the articles are illustrated in Fig. 4.1. The more detailed contributions to each objective are discussed in the following sections.

4.1.1 Contributions to reliability methods and models

Developing new methods and models for SIS reliability quantification has been the main focus of this PhD project. Contributions to the five objectives on this topic are presented in this section.

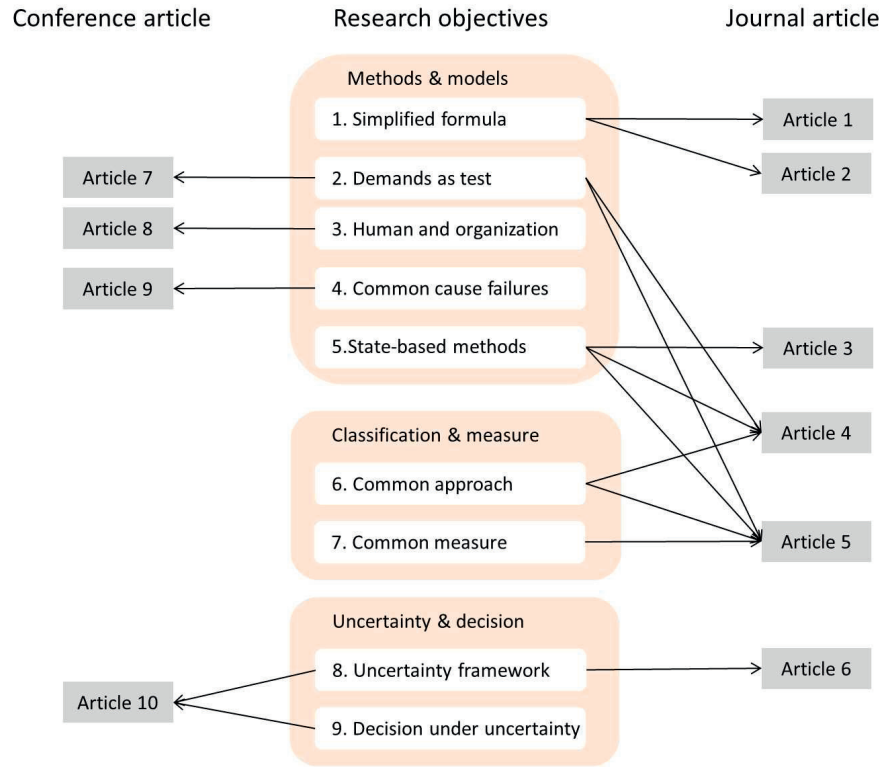


Fig. 4.1 The relationship between research objectives and articles.

Objective 1

The first objective addresses the need for more accurate and comprehensive simplified formulas for PFD_{avg} and PFH calculation, where issues such as DD-failure, non-perfect proof testing and partial testing are important to take into account. The contributions from this PhD project to objective 1 are found in Article 1 [53] and 2 [55], together with the relevant research questions:

- We developed a set of formulas to calculate the PFD_{avg} for *koon* systems when both partial testing and full testing are applied
 - To handle both periodical and non-periodical partial testing;
 - To take into account CCFs and to accommodate the need of using different β -factors for different failure modes;
 - To select cost-effective partial testing strategies.
- We developed a set of formulas to calculate PFH for *koon* systems

- To take into account both DD- and DU-failures;
- To consider the non-perfect proof testing so the result is more accurate.

Simplified formulas are the most popular technique among the practitioners of SIS reliability analysis. Our new formulas are able to systematically address issues such as DD-failure, non-perfect proof testing and partial testing, which can significantly extend the applicability of the simplified formulas and achieve more accurate results. The new formulas are not intended to replace, but to supplement, the existing formulas. The users need to determine what are the important factors to consider in his or her SIS, and decide which formula to use for the particular case.

Both the non-perfect proof testing and the partial testing have been problems of applying simplified formulas to SIS reliability analysis, especially when the system has multiple redundancy and is subject to CCFs. With the contributions in this PhD project, we can easily calculate the SIS reliability in these complicated situations and support related decisions in design and operation, we, therefore, claim that the first objective is, to a large extent, achieved.

Objective 2

The second objective addresses the need of clarification about whether or not we should make use of the information from demands in SIS reliability analysis, and the need of new methods to calculate reliability if we decide to use this information and take demands as some kind of tests. The contributions from this PhD project to objective 2 are found in Article 4 [49], 5 [54] and 7 [48], together with the relevant research questions:

- We identified SIS operation modes where using demands as tests is relevant.
- We compared the characteristics between demands and proof tests to form the basis of using or not using demands as tests.
- We developed formulas to take credits from non-critical demands in PFD calculation.
- We extended and refined the Markov method to take credits from demands in SIS reliability analysis.

Taking credits from demands in SIS reliability analysis has been a controversial topic. The industry wants to use the information about the SIS state from an actual demand to support decisions but is feared of the possible accidents due to the demand. We systematically investigated this issue, and provided a thorough discussion of the pros and cons of using such a “testing strategy”, and highlighted cautions, challenges, and conditions of use. By introducing the “medium demand mode”, we proposed PFD formulas to take credits from the non-critical demands. With the material from this PhD thesis, especially article

7 [48], the decision-makers should have a bigger and better picture of using demands as tests in SIS reliability analysis, and decide whether and how to use the information from demands in SIS related decisions without failing to maintain the due safety level.

Objective 3

The third objective addresses the need to quantify human and organizational influences on the reliability of SIS in the design phase when data are limited. The contributions from this PhD project to objective 3 are found in Article 8 [56], together with the relevant research questions:

- We extended the failure rate model in MIL-HDBK-217F [71] to include human and organizational influences.
- We developed a Bayesian approach to quantify the human and organizational influence on the failure rate, and hence the influence on the SIS reliability.

In SIS reliability design, the component failure rate is usually from the generic database such as offshore reliability data (OREDA) or provided by manufacturers. This kind of failure rate does not reflect the specific influence from the organization, under which the component is operated. On the other hand, for an organization with a database recording the reliability data of its components, the organizational influence on the failure rate is reflected on these organizational specific failure rates (OFR). Even if the OFR of each component, individually, fails to provide enough information for drawing a conclusion of the organization's influence on failure rate, the OFRs, collectively, are adequate for estimating the organization's influence factor on failure rate. By combining the organization's influence factor and the generic or manufacturer provided failure rate, we are able to obtain the OFR of new components in the design phase.

The contribution of this PhD thesis is to provide an approach to extract organizational influence on failure rate from the organization's reliability database and estimate an OFR in the design phase. It addresses a small aspect of the research field of human and organizational factor, but an important one in the SIS design phase.

Objective 4

The fourth objective addresses the need to clarify confusions and to remove inconsistencies in the existing CCF definitions, and the need to assess the adequacy of the current CCF models used in SIS reliability analysis. The contributions from this PhD project to objective 4 are found in Article 9 [51], together with the relevant research questions:

- We proposed a two level CCF definition.
- With the new definition, we clarified the confusions and removed the inconsistencies in the existing CCF definitions.
- We assessed the current CCF models, and concluded that they are adequate with respect to the assumption of simultaneous failures in SIS reliability analysis.
- We compared beta-factor model and MBF model from a practitioners' perspective and identified the conservative models for different system configurations.

Common cause failure is a much discussed topic in SIS reliability analysis because of its significant impact on the results. Several CCF definitions are available and they disagree with each other when it comes to whether or not individual component failures in a CCF need to occur simultaneously and whether it is required to have a system failure for CCF. We proposed a two level CCF definition to resolve these disagreements.

On the component level, we define CCF as an event where (i) a component is failed due to certain cause, and (ii) the same cause has the potential to fail other redundant components. The component level CCF does not have the issue of simultaneous failure or system failure, it suits for data collection which aims at gathering as much CCF information as possible.

On the system level, CCF is defined as an event where (i) multiple redundant component failures are due to a shared cause, and (ii) the multiple component failures lead to a system failure. The system level CCF definition is targeting at CCF models used in reliability analysis, where system failure is concerned. For the issue of simultaneous failures, we do not have this as a condition, instead we have assessed the consequence of using the simultaneous failures assumption in PFD_{avg} calculation, it is shown that, with the virtual component model, the PFD_{avg} will be on the conservative side for most of the SIS configurations.

The beta-factor model and MBF model are commonly used in SIS reliability analysis. We compared these two models from a practitioner's perspective, and presented a table showing the conservative model to use for SISs with different system configurations.

With the contributions in this PhD thesis, the practitioners can have a better picture of CCF modeling in SIS reliability analysis and ensure the result is on the conservative side if error must occur, and the researchers are provided with ideas for further investigation in an area which has been thought of as a mature field by many.

Objective 5

The fifth objective addresses the need of more modeling power to capture more characteristics of SIS reliability behavior, such as dynamics. It is also related

to implementing state-based reliability methods in SIS reliability analysis. The contributions from this PhD project to objective 5 are found in Article 3 [63], 4 [49] and 5 [54] together with the relevant research questions:

- We applied Markov method to two case studies, to exemplify how the SIS reliability analysis may be performed with Markov method and how to obtain time-dependent results.
- We investigated Petri net in the context of SIS reliability analysis, developed Petri net routines to model various aspects of the SIS reliability behavior, and applied Petri net to a case study.

Markov method and Petri net are proved to be useful in modeling special aspects of complex SISs or complex SIS operation strategies in reliability analysis, for example the DD-failure induced proof test and degraded operation. Through the case studies, we showed how the state-based methods can be applied in practical SIS reliability analysis and demonstrated the advantages of these methods.

4.1.2 Contributions to classification and reliability measure

The classification of SIS operation modes has been a controversial topic. On the one hand, using the demand frequency (one demand per year) to distinguish between high- and low-demand is well established thanks to the IEC 61508 standard. On the other hand, such a clear-cut criterion leads to difficulties when the SIS is operated at the boundary of two modes and provides opportunity for abusing. Based on the investigations of this PhD project, we realized that using any specific demand frequency to differentiate high- and low-demand mode would be problematic, since the demand frequency is a continuous parameter. Therefore the focus of this PhD project has been directed to integrating the demand frequency into SIS reliability analysis, hence no classification is needed. A common reliability analysis approach and a common reliability measure can be used throughout the demand frequency spectrum.

Objective 6

The sixth objective addresses the need for a common approach that is capable of integrating the demand frequency into SIS reliability analysis, so that low- and high-demand are harmonized and differentiation is no longer necessary. The main contributions from this PhD project to objective 6 are found in Article 4 [49] and 5 [54] together with the relevant research questions:

- We gave a thorough discussion of the most important issues related to SIS classification.

- We extended and refined the Markov method as a common approach to integrate demand frequency into SIS reliability analysis.
- We applied the common approach to case studies and verified the results with analytical formulas.
- By comparing results of the common approach and the traditional approach, advantages of the common approach were demonstrated.

The common approach integrates demand frequency into SIS reliability analysis, based on the assumptions that the demand verifies the state of the SIS, the demand duration and repair time are exponentially distributed. Even though these assumptions are not fully satisfied, e.g., it is more reasonable to use log-normal distribution for repair time, it is shown that using the exponential distribution does not lead to non-negligible results [12, 49].

The contribution of this PhD thesis represents a scientific discussion of alternative ways to quantify the risk reduction from SISs. It may be used as a supplement for companies to better understand and manage their risk profiles, but is far from replacing the well accepted and widely used IEC 61508 framework. Objective 6 is therefore partial achieved, more work needs to be done to solve the demand mode classification issue.

Objective 7

The seventh objective addresses the need for a new and common reliability measure to replace PFD_{avg} and PFH when the demand rate is integrated in the common reliability analysis approach. This objective is closely linked to the sixth objective, and our main contributions are found in article 4 [49] and 5 [54], which are the same for objective 6:

- We proposed a common SIS reliability measure PFD^* , which can be used for SIS working in both low- and high-demand mode of operation.

The new reliability measure PFD^* is proposed in relation to the common approach. The PFD^* can be considered as an extension of PFD_{avg} , with accounting of the demand frequency. When the demand frequency is low, PFD^* and PFD_{avg} are almost identical, when the demand frequency increases, they start to differ to represent the impact of demands.

PFD^* is easy to understand by the practitioners because of the sister measure PFD_{avg} . It is a practical measure with high likelihood of being implemented with a common approach (not necessarily the one proposed in this thesis). The new reliability measure also represents an attempt to integrate the common approach to the IEC 61508 framework with possibility of using SIL level.

4.1.3 Contributions to uncertainty and decision-making

It is our standpoint that all reliability and risk analyses are merely tools to provide inputs for better and more rational decision-making, if there is no decision to make, a reliability or risk analysis should never be initiated. In the context of this PhD project, the SIS reliability analysis is used to support SIS related decisions in design, manufacturing and operation. This naturally brings the last two objectives of this PhD project to the issue of SIS related decision-making under uncertainty.

Objective 8

The eighth objective addresses the need to clarify the the concept of uncertainty assessment in SIS reliability estimates, by adopting the uncertainty categorization used in the nuclear industry and pointing to the source of uncertainty for SIS analysts and decision-makers. The main contributions from this PhD project to objective 8 are found in Article 6 [52] together with the relevant research questions:

- We adopted the three categories classification of uncertainty from the nuclear industry into SIS reliability analysis.
- We identified and discussed sources of the completeness, model, and parameter uncertainty in SIS reliability estimate.
- We argued that the three categories classification of uncertainty is useful to treat uncertainties in SIS reliability estimate and provided a thorough discussion, which may frame future development of methods and models.

In this PhD thesis, we have not come up with novel ideas about uncertainty, instead, we used the existing concepts and arguments and applied them to our problem—SIS reliability assessment. By discussing each uncertainty category, we concluded that the completeness uncertainty is the most important to address in decisions under uncertainty, followed by model uncertainty and parameter uncertainty.

We also highlighted the importance of communication of the uncertainty in SIS reliability estimate to the decision-maker and emphasized the dependency on the analyst in determining the uncertainty level. With the contributions in this thesis, the uncertainty issue in SIS reliability estimate should be better understood, and direction of effort is pointed out.

Objective 9

The last objective addresses the need for a holistic approach to uncertainty assessment of SIS reliability estimates, with such an approach, the decision-makers can have an overall picture of the uncertainties and make better decisions. The main contributions from this PhD project to objective 9 are found in Article 6 [52] and 10 [50] together with the relevant research questions:

- We developed an approach to determine the level of uncertainty in SIS reliability estimates by systematically considering completeness, model, and parameter uncertainty.
- We suggested an approach to take into consideration the uncertainty level in SIS related decisions.
- The application of the proposed approaches are illustrated by a case study, and the impacts are demonstrated.

The contributions made to objective 9 are mainly for practitioners. The proposed uncertainty determination approach is simple and practical, but also pragmatic. A solid scientific foundation is missing, significant subjective judgments based on experiences are needed. It represents the first attempt to establish a holistic approach to treat uncertainty in SIS and provide suggestion for decision-making, which can be further developed and adjusted according to individual projects.

Uncertainty is a controversial and much debated topic. People with different backgrounds, e.g., engineering, psychology, statistics, sociology and etc. may have very different opinions. We addressed the uncertainty in SIS from an engineers' perspective. With the proposed approach, we can systematically account for the identified uncertainties and make decisions accordingly. In this sense, we have achieved objective 9.

4.2 Future research

This PhD thesis focuses on the reliability quantification of SIS hardware, but all related topics are not discussed. Several important areas for future research are identified and given in this section¹.

The current SIS reliability quantification, including this thesis, looks primarily at the random failures and CCFs. Systematic failures other than CCFs are not included in the reliability quantification. The IEC standards give requirements to qualitatively control systematic failures, but it is worth the effort to investigate whether or not and how we should quantify systematic failure. The

¹ Only future research areas closely related to the quantification of SIS are given, more general future research areas are not provided.

PDS method [31] proposed a new classification for random failure and systematic failure, as well as an approach to quantify the systematic failure. This can serve as a starting point for future research. Human and organizational factors are usually blamed as a significant source of systematic failure, in this thesis, we proposed an implicit approach to model HOF influence on failure rate, future research may use a more traditional approach to explicitly consider HOF influence on SIS reliability.

Software failures are not at all discussed in this thesis, it is an important topic, especially in software-intensive SISs such as those in aviation and automobile. Similar to systematic failures, the standards focus on qualitative approach to ensure the software reliability. It is our opinion that quantification of software reliability is an important topic for future research, since more and more SIL requirements are allocated with quantitative and semi-quantitative approaches that do not distinguish hardware and software in the reliability allocation process.

Safe failure fraction (SFF) is another reliability measure besides PFD_{avg} and PFH, and is used in relation to verify the architect constraints. In the second edition of IEC 61508 [39], the definition of safe failure is changed to exclude those failures that neither lead to a dangerous failure nor to a spurious operation. Some equipment suppliers start to have problems to meet the SFF requirement based on the new definition. A future research area is therefore to investigate SFF calculation and discuss the rationale of architect constraints and SFF.

Spurious operation is another area of further research for those who are interested in SIS reliability quantification. Spurious operation may, on the one hand, serve as some kind of successful proof tests that verifies the functional state of SIS and increases the SIS reliability. On the other hand, for certain component or SIS, e.g., valves, the spurious operation may introduce extra stresses and wear, hence negatively affect the reliability. Spurious operation needs to be avoid also because the possible risk it may pose, e.g., premature activation of airbags may injure or even kill the passengers. Efforts to define and clarify the concept of spurious operation are made in [69], future research may use the results in [69] as a basis and quantitatively integrate spurious operations into SIS reliability analysis.

The methods and concepts developed in this PhD project are applicable to all relevant phases of the SIS life cycle. We tried to keep the whole life cycle in mind when we developed these methods and concepts, yet we were nevertheless biased to a perspective where less attention is paid to the operational phase, due to the fact that most efforts of SIS reliability analysis are in the design phase. The need of updating SIS reliability analyses in the operational phase to better manage risk is evident. Some initiatives have been taken in the Norwegian oil and gas industry to collect operational data and update the proof test interval [32]. However, SIS reliability analysis in operation is still a premature area and more research is needed.

Chapter 5

Acronyms and abbreviations

| | |
|--------------------|---|
| ABS | Anti-lock breaking system |
| BOP | Blowout preventer |
| CCF | Common cause failure |
| DD | Dangerous detected |
| DHSV | Down hole safety valve |
| DP | Dynamic positioning |
| DU | Dangerous undetected |
| E/E/PE | Electrical, electronic, programmable electronic |
| E/E/PES | Electrical, electronic, programmable electronic system |
| EUC | Equipment under control |
| FMEDA | Failure modes, effects and diagnostic analysis |
| FSA | Functional safety assessment |
| FTA | Fault tree analysis |
| HFT | Hardware fault tolerance |
| HIPPS | High integrity pressure protection system |
| HOF | Human and organizational factors |
| ICDE | International Common Cause Data Exchange |
| IEC | International Electrotechnical Committee |
| IEEE | Institute of Electrical and Electronic Engineers |
| ISO | International Organization for Standardization |
| MBF | Multiple Beta factor |
| MEDT | Mean equivalent downtime |
| NTNU | Norwegian University of Science and Technology |
| NOG | Norwegian oil and gas association |
| OFR | Organization specific failure rate |
| OLF | Oljeindustriens landsforening (Eng: The Norwegian Oil Industry Association) |
| OREDA | Offshore Reliability Data |
| PDF _{avg} | Probability of failure on demand |
| PFH | Probability of a dangerous failure per hour |

| | |
|--------|---|
| PST | Partial stroke testing |
| PTC | Proof test coverage |
| RAMS | Reliability, availability, maintainability, and safety |
| RBD | Reliability block diagram |
| ROCOF | Rate of occurrence of failures |
| SFF | Safe failure fraction |
| SIF | Safety instrumented function |
| SIL | Safety integrity level |
| SINTEF | Foundation of Science and Technology at the Norwegian Institute of Technology |
| SIS | Safety-instrumented system |
| SRCS | Safety-related electrical control system |
| SRS | Safety requirement specification (may also mean safety-related system) |
| TIF | Test independent failure |
| TU/e | Eindhoven University of Technology |
| UTT | University of Technology of Troyes |

References

- [1] Abrahamsson, M. (2002). *Uncertainty in Quantitative Risk Analysis - Characterisation and Methods of Treatment*. PhD thesis, Department of Fire Safety Engineering, Lund University, Lund, Sweden.
- [2] Ali, R. and Jero, L. (2003). Reliability and asset management: Smart positioners in safety instrumented systems. *Petroleum Technology Quarterly*, 8:137–140.
- [3] Ali, R. and Goble, W. (2004). Smart positioners to predict health of ESD valves. In *Proceedings of the annual symposium on instrumentation for the process industries*.
- [4] ARC (2008). Process safety system market shows unprecedented growth. Technical report, ARC Advisory Group.
- [5] BP (2010). Deepwater horizon accident investigation report. Technical report, BP. (<http://www.bp.com/sectiongenericarticle800.do?categoryId=9048918&contentId=7082603>).
- [6] Brissaud, F., Barros, A., and Bérenguer, C. (2010a). Handling parameter and model uncertainties by continuous gates in fault tree analyses. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, 224:253–265.
- [7] Brissaud, F., Barros, A., and Bérenguer, C. (2010b). Probability of failure of safety-critical systems subject to partial tests. In *Proceedings of the Annual Reliability and Maintainability Symposium*.
- [8] Brissaud, F., Barros, A., and Berenguer, C. (2012). Probability of failure on demand of safety systems: impact of partial test distribution. *Journal of Risk and Reliability*, 226(4):426–436.
- [9] Brissaud, F., Charpentier, D., Fouladirad, M., Barros, A., and Berenguer, C. (2010c). Failure rate evaluation with influencing factors. *Journal of Loss Prevention in the Process Industries*, 23:187–193.
- [10] Bukowski, J. (2001). Modeling and analyzing the effects of periodic inspection on the performance of safety-critical systems. *IEEE Transactions on Reliability*, 50:321–329.

- [11] Bukowski, J. (2006a). Incorporating process demand into models for assessment of safety system performance. In *Proceedings of RAMS'06 Symposium*, Alexandria, VI, USA.
- [12] Bukowski, J. (2006b). Using Markov models to compute PFD_{ave} when repair times are not exponentially distributed. In *Proceedings of the annual reliability and maintainability symposium*, Newport Beach, CA, USA.
- [13] Bukowski, J. V. and Lele, A. (1997). Case for architecture-specific common cause failure rates and how they affect system performance. In *Proceedings of the Annual Reliability and Maintainability Symposium*, pages 153–158.
- [14] Chen, H., Moan, T., and Verhoeven, H. (2008). Safety of dynamic positioning operations on mobile offshore drilling units. *Reliability Engineering and System Safety*, 93(7):1072–1090.
- [15] Creswell, J. W. (2008). *Educational Research: Planning, Conducting, and Evaluating Quantitative and Qualitative Research*. Prentice Hall, New Jersey.
- [16] De Rocquigny, E., Devictor, N., and Tarantola, S. (2008). *Uncertainty in Industrial Practice: A Guide to Quantitative Uncertainty Management*. Wiley, Chichester, UK.
- [17] Duijm, N. and Goossens, L. (2006). Quantifying the influence of safety management on the reliability of safety barriers. *Journal of Hazardous Materials*, 130:284–292.
- [18] Dutuit, Y., Chatelet, E., Signoret, J. P., and Thomas, P. (1997). Dependability modelling and evaluation using stochastic Petri nets: Application to two test cases. *Reliability Engineering and System Safety*, 55(2):117–124.
- [19] Dutuit, Y., Innal, F., Rauzy, A., and Signoret, J. (2008a). Probabilistic assessments in relationship with safety integrity levels by using fault trees. *Reliability Engineering and System Safety*, 93:1867–1876.
- [20] Dutuit, Y., Rauzy, A., and J-P, S. (2008b). A snapshot of methods and tools to assess safety integrity levels of high-integrity protection systems. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, 222:371–379.
- [21] Evans, M. G. K., Parry, G. W., and Wreathall, J. (1984). On the treatment of common-cause failures in system analysis. *Reliability Engineering*, 9:107–115.
- [22] Gibson, J. J. (1961). The contribution of experimental psychology to the formulation of the problem of safety - a brief for basic research. *Behavioral Approaches to Accident Research*, pages 77–89.
- [23] Goble, W. (2011). Getting good proof test coverage numbers. (http://www.exida.com/index.php/blog/indepth/getting_good_proof_test_coverage_numbers).
- [24] Goble, W. M. and Brombacher, A. C. (1999). Using a failure modes, effects and diagnostic analysis (fmeda) to measure diagnostic coverage in pro-

- programmable electronic systems. *Reliability Engineering and System Safety*, 66(2):145–148.
- [25] Guo, H. and Yang, X. (2007). A simple reliability block diagram method for safety integrity verification. *Reliability Engineering and System Safety*, 92(9):1267–1273.
- [26] Guo, H. T. and Yang, X. H. (2008). Automatic creation of Markov models for reliability assessment of safety instrumented systems. *Reliability Engineering and System Safety*, 93(6):829–837.
- [27] Haddon, W. J. (1980). The basic strategies for reducing damage from hazards of all kinds. *Hazard prevention*, 16:8–12.
- [28] Hamada, M. S., Wilson, A. G., S., R. C., and Martz, H. F. (2008). *Bayesian Reliability*. Springer, London.
- [29] Hauge, S., Kråkenes, T., Hokstad, P., Håbrekke, S., and Jin, H. (2013). *Reliability Prediction Method for Safety Instrumented Systems*. SINTEF, Trondheim.
- [30] Hauge, S., Lundteigen, M. A., Hokstad, P., and Håbrekke, S. (2010a). *Instrumented Systems – PDS Example Collection*. SINTEF, Trondheim.
- [31] Hauge, S., Lundteigen, M. A., Hokstad, P., and Håbrekke, S. (2010b). *Reliability Prediction Method for Safety Instrumented Systems*. SINTEF, Trondheim.
- [32] Hauge, S., Lundteigen, M. A., and Rausand, M. (2009). Updating failure rates and test intervals in the operational phase: A practical implementation of IEC 61511 and IEC 61508. In Briš, R., Soares, C. G., and Martorell, S., editors, *Reliability, Risk and Safety: Theory and Applications (ESREL 2009): Proceedings of The European Safety and Reliability Conference*, pages 1715–1722. CRC Press, London.
- [33] Hauge, S. and Onshus, T. (2010). *Reliability Data for Safety Instrumented Systems*. SINTEF, Trondheim.
- [34] Hokstad, P. and Corneliussen, K. (2004). Loss of safety assessment and the IEC 61508 standard. *Reliability Engineering and System Safety*, 83(1):111–120.
- [35] Hokstad, P. and Rausand, M. (2008). Common cause failure modeling: Status and trends. In Misra, K. B., editor, *Handbook of Performability Engineering*, chapter 39, pages 621–640. Springer, London.
- [36] Hollnagel, E. (2004). *Barriers And Accident Prevention*. Ashgate, London.
- [37] IEC 60601 (2007). *Medical Electrical Equipment*. International Electrotechnical Commission, Geneva.
- [38] IEC 61508 (1998). *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems. Part 1-7*. International Electrotechnical Commission, Geneva.
- [39] IEC 61508 (2010). *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems. Part 1-7*. International Electrotechnical Commission, Geneva.

- [40] IEC 61511 (2003). *Functional Safety: Safety Instrumented systems for the Process Industry Sector, Part 1-3*. International Electrotechnical Commission, Geneva.
- [41] IEC 61513 (2004). *Nuclear Power Plants – Instrumentation and Control for Systems Important to Safety - General Requirements for Systems*. International Electrotechnical Commission, Geneva.
- [42] IEC 62061 (2005). *Safety of Machinery – Functional Safety of Safety Related Electrical, Electronic and Programmable Electronic Control Systems*. International Electrotechnical Commission, Geneva.
- [43] IEC 62425 (2007). *Railway Applications – Communication, Signalling and Processing Systems - Safety Related Electronic Systems for Signalling*. International Electrotechnical Commission, Geneva.
- [44] Innal, F. (2008). *Contribution to Modelling Safety Instrumented Systems and to Assessing Their Performance Critical Analysis of IEC 61508 Standard*. PhD thesis, University of Bordeaux.
- [45] Innal, F., Dutuit, Y., Rauzy, A., and Signoret, J.-P. (2010). New insight into the average probability of failure on demand and the probability of dangerous failure per hour of safety instrumented systems. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, 224.
- [46] ISO 26262 (2011). *Road Vehicles – Functional Safety, Part 1-10*. International Organization for Standardization, Geneva.
- [47] Janbu, A. F. (2009). Treatment of uncertainty in reliability assessment of safety instrumented systems. Master's thesis, Norwegian University of Science and Technology, Trondheim, Norway.
- [48] Jin, H., Lundteigen, M. A., and Rausand, M. (2011a). Can functional tests be replaced by inspection after demands. In *7th Global Congress on Process Safety*.
- [49] Jin, H., Lundteigen, M. A., and Rausand, M. (2011b). Reliability performance of safety instrumented systems: A common approach for both low-and high-demand mode of operation. *Reliability Engineering and System Safety*, 96:365–373.
- [50] Jin, H., Lundteigen, M. A., and Rausand, M. (2011c). Uncertainty assessment of reliability estimates for safety instrumented systems. In *Advances in Safety, Reliability and Risk Management ESREL 2011*.
- [51] Jin, H., Lundteigen, M. A., and Rausand, M. (2012a). Common cause failures in safety instrumented systems: Concepts and analytical approaches. In *11th International Probabilistic Safety Assessment and Management Conference and the Annual European Safety and Reliability Conference 2012, 25-29 June 2012, Helsinki, Finland*.
- [52] Jin, H., Lundteigen, M. A., and Rausand, M. (2012b). Uncertainty assessment of reliability estimates for safety instrumented systems. *Proceedings of*

- the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, 226:646–655.
- [53] Jin, H., Lundteigen, M. A., and Rausand, M. (2013a). New PFH-formulas for k-out-of-n:F-systems. *Reliability Engineering and System Safety*, 111:112–118.
- [54] Jin, H., Lundteigen, M. A., and Rausand, M. (2013b). New reliability measure for safety instrumented systems. *International Journal of Reliability, Quality, and Safety Engineering*, 20:1–16.
- [55] Jin, H. and Rausand, M. (2013). Reliability of safety-instrumented systems subject to partial testing and common-cause failures. *submitted for publication*.
- [56] Jin, H., Rausand, M., Mosleh, A., and Haugen, S. (2012c). Quantification of organizational influences on failure rate: A Bayesian approach. In *IEEE International Conference on Industrial Engineering and Engineering Management 2012*.
- [57] Johannessen, J. A. (2006). *Vitenskapsstrategi og Vitenskapsfilosofi*. Fagbokforlaget, Oslo.
- [58] Knegetering, B. and Brombacher, A. (2000). Method to prevent excessive numbers of markov states in markov models for quantitative safety and reliability assessment. *ISA Transactions*, 39(3):363–369.
- [59] Knegetering, B. and Brombacher, A. C. (1999). Application of micro markov models for quantitative safety assessment to determine safety integrity levels as defined by the iec 61508 standard for functional safety. *Reliability Engineering and System Safety*, 66(2):171–175.
- [60] Kothari, C. (2009). *Research Methodology: Methods and Techniques*. New Age International Ltd. (<http://books.google.no/books?id=8c6gkbKi-F4C>).
- [61] Langeron, Y., Barros, A., Grall, A., and Berenguer, C. (2008). Combination of safety integrity levels (SILs): A study of IEC61508 merging rules. *Journal of Loss Prevention in the Process Industries*, 21:437–449.
- [62] Leveson, N. (2011). *Engineering a Safer World*. MIT press, Cambridge, USA.
- [63] Liu, Y., Jin, H., Lundteigen, M. A., and Rausand, M. (2012). Reliability modeling of safety-instrumented systems by Petri nets. *Submitted for publication*.
- [64] Liu, Y. L. and Rausand, M. (2011). Reliability assessment of safety instrumented systems subject to different demand modes. *Journal of Loss Prevention in the Process Industries*, 24(1):49–56.
- [65] Lundteigen, M. A. (2009). *Safety Instrumented Systems in the Oil and Gas Industry: Concepts and Methods for Safety and Reliability Assessments In Design and Operation*. PhD thesis, Norwegian University of Science and Technology, Department of Productions and Quality Engineering.

- [66] Lundteigen, M. A. and Rausand, M. (2007). Common cause failures in safety instrumented systems on oil and gas installations: Implementing defense measures through function testing. *Journal of Loss Prevention in the Process Industries*, 20:218–229.
- [67] Lundteigen, M. A. and Rausand, M. (2008a). Partial stroke testing of process shutdown valves: How to determine the test coverage. *Journal of Loss Prevention in the Process Industries*, 21:579 – 588.
- [68] Lundteigen, M. A. and Rausand, M. (2008b). Partial stroke testing of process shutdown valves: How to determine the test coverage. *Journal of Loss Prevention in the Process Industries*, 21:579–588.
- [69] Lundteigen, M. A. and Rausand, M. (2008c). Spurious activation of safety instrumented systems in the oil and gas industry: Basic concepts and formulas. *Reliability Engineering and System Safety*, 93:1208–1217.
- [70] Lundteigen, M. A. and Rausand, M. (2009). Reliability assessment of safety instrumented systems in the oil and gas industry: A practical approach and a case study. *International Journal of Reliability, Quality, and Safety Engineering*, 16:187–212.
- [71] MIL-HDBK -217F (1991). Reliability prediction of electronic equipment. Handbook, U.S. Department of Defense, Washington, DC.
- [72] Misumi, Y. and Sato, Y. (1999). Estimation of average hazardou-event-frequency for allocation of safety-integrity levels. *Reliability Engineering and System Safety*, 66:135–144.
- [73] Mosleh, A., Siu, N., Smidts, C., and Lui, C. (1994). *Model Uncertainty: Its Characterization and Quantification*. U.S. Nuclear Regulatory Commission, Washington DC, 2nd edition.
- [74] MWOD. Merriam-Webster online dictionary.
- [75] NAE (2011). *Macondo Well Deepwater Horizon Blowout: Lessons for Improving Offshore Drilling Safety*. The National Academies Press.
- [76] NASA (2002). Probabilistic risk assessment procedures guide for NASA managers and practitioners. Technical report, NASA Office of Safety and Mission Assurance, Washington, DC.
- [77] NEA (1994). International Common Cause Failure Data Exchange (ICDE) project.
- [78] NEA (2004). International common-cause failure dat exchange. ICDE general coding guidelines. Technical note NEA/CSNI/R(2004)4. Technical report, Nuclear Energy Agency.
- [79] NIRS (2010). Fact sheet on Fukushima nuclear power plant. (<http://www.nirs.org/reactorwatch/accidents/Fukushimafactsheet.pdf>).
- [80] NOG (2004). Application of IEC 61508 and IEC 61511 in the Norwegian petroleum industry. Technical report, Norwegian Oil Industry Association, Stavanger, Norway.

- [81] NUREG 1885 (2009). Guidance on the treatment of uncertainties associated with PRAs in risk-informed decision. Technical report, United States Nuclear Regulatory Commission.
- [82] OECD. Organization for economic co-operation and development: Glossary of statistical terms. (<http://stats.oecd.org/glossary/>).
- [83] Oliveira, L. F. and Abramovitch, R. N. (2010). Extension of ISA TR84.00.02 PFD equations to KooN architectures. *Reliability Engineering and System Safety*, 95:707 – 715.
- [84] OREDA (2009). *OREDA Reliability Data*. OREDA Participants, Available from: Det Norske Veritas, NO 1322 Høvik, Norway, 5th edition.
- [85] Perrow, C. (1999). *Normal Accidents: Living with High-Risk Technologies*. Princeton University Press, updated edition.
- [86] Rausand, M. (2011). *Risk Assessment; Theory, Methods, and Applications*. Wiley, Hoboken, NJ.
- [87] Rausand, M. and Høyland, A. (2004). *System Reliability Theory; Models, Statistical Methods, and Applications*. Wiley, Hoboken, NJ., 2nd edition.
- [88] Reason, J. (1990). *Human Error*. Cambridge University Press, Cambridge, UK.
- [89] Reason, J. (1997). *Managing the Risks of Organizational Accidents*. Ashgate, London.
- [90] Rouvroye, J. and Van Den Bliet, E. (2002). Comparing safety analysis techniques. *Reliability Engineering and System Safety*, 75(3):289 – 294.
- [91] Rouvroye, J. L. and Brombacher, A. C. (1999). New quantitative safety standards: different techniques, different results. *Reliability Engineering and System Safety*, 66:121–125.
- [92] Sallak, M., Simon, C., and Aubry, J.-F. (2008). A fuzzy probabilistic approach for determining safety integrity level. *IEEE Transaction on Fuzzy Systems*, 16:239–248.
- [93] Schönbeck, M. (2007). Human and organizational factors in the operational phase of safety instrumented systems: A new approach. Master's thesis, Norwegian University of Science and Technology, Trondheim, Norway.
- [94] Schönbeck, M., Rausand, M., and Rouvroye, J. (2010). Human and organisational factors in the operational phase of safety instrumented systems: A new approach. *Safety Science*, 48(3):310 – 318.
- [95] Signoret, J.-P., Dutuit, Y., Cacheux, P.-J., Folleau, C., Collas, S., and Thomas, P. (2013). Make your Petri nets understandable: Reliability block diagrams driven Petri nets. *Reliability Engineering and System Safety*, 113:61 – 75.
- [96] SKI (2010). CCF analysis of high redundancy systems, safety/relief valve data analysis and reference BWR application. SKI Technical report 91:6. Technical report, Swedish Radiation Safety Authority.
- [97] Sklet, S. (2006a). Safety barriers: Definition, classification, and performance. *Journal of Loss Prevention in The Process Industries*, 19:494–506.

- [98] Sklet, S. (2006b). *Safety Barriers on Oil and Gas Platforms. Means to Prevent Hydrocarbon Releases*. PhD thesis, Norwegian University of Science and Technology, Department of Engineering Design and Materials.
- [99] Summers, A. and Zachary, B. (2000). Partial-stroke testing of safety block valves. *Control Engineering*, 47(12):87–89.
- [100] Summers, A. E. (2000). Viewpoint on isa tr84.0.02 – simplified methods and fault tree analysis. *ISA Transactions*, 39(2):125–131.
- [101] Summers, A. E. (2003). Introduction to layers of protection analysis. *Journal of Hazardous Materials*, 104(1-3):163–168.
- [102] Summers, A. E. and Raney, G. (1999). Common cause and common sense, designing failure out of your safety instrumented systems (sis). *ISA Transactions*, 38(3):291–299.
- [103] Torres-Echeverra, A., Martorell, S., and Thompson, H. (2009). Modelling and optimization of proof testing policies for safety instrumented systems. *Reliability Engineering and System Safety*, 94:838 – 854.
- [104] Torres-Echeverra, A., Martorell, S., and Thompson, H. (2009). Modelling and optimization of proof testing policies for safety instrumented systems. *Reliability Engineering and System Safety*, 94(4):838 – 854.
- [105] W Mechri, W., Simon, C., and Othman, K. (2011). Uncertainty analysis of common cause failure in safety instrumented systems. *Proceedings of The Institution of Mechanical Engineers Part O-Journal of Risk and Reliability*, 225:450–460.
- [106] Wang, Y., West, H. H., and Mannan, M. S. (2004). The impact of data uncertainty in determining safety integrity level. *Process Safety and Environmental Protection*, 82:393–397.
- [107] Winkler, R. L. (1999). Uncertainty in probabilistic risk assessment. *Reliability Engineering and System Safety*, 54:127–132.
- [108] Xinhua (2011). Flaws in railway signal system lead to fatal collision: railway authorities. (http://news.xinhuanet.com/english2010/china/2011-07/28/c_131014639.htm).
- [109] Xu, M., Chen, T., and Yang, X. (2012). The effect of parameter uncertainty on achieved safety integrity of safety system. *Reliability Engineering and System Safety*, 99(0):15 – 23.
- [110] Yoshimura, I. and Sato, Y. (2008). Safety achieved by the safe failure fraction (sff) in iec 61508. *IEEE Transactions on Reliability*, 57:662–669.
- [111] Yoshimura, I. and Sato, Y. (2009). Estimation of calendar-time- and process-operative-time-hazardous-event rates for the assessment of fatal risk. *International Journal of Performability Engineering*, 5:377–386.
- [112] Zhang, T., Long, W., and Sato, Y. (2003). Availability of systems with self-diagnostic components applying Markov model to IEC 61508-6. *Reliability Engineering and System Safety*, 80(2):133 – 141.

Part II
Articles

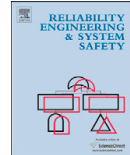
Article 1 (journal)

New PFH-formulas for k -out-of- n :F-systems
–In *Reliability Engineering and System Safety*



Contents lists available at SciVerse ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

New PFH-formulas for k -out-of- n :F-systems

Hui Jin*, Mary Ann Lundteigen, Marvin Rausand

Department of Production and Quality Engineering, Norwegian University of Science and Technology, NO 7491 Trondheim, Norway

ARTICLE INFO

Article history:

Received 24 November 2011

Received in revised form

5 November 2012

Accepted 7 November 2012

Available online 22 November 2012

Keywords:

Safety instrumented systems

Reliability

PFH

Proof-test coverage

DD-failures

ABSTRACT

Simplified formulas are popular for reliability analysis of safety instrumented systems (SISs). Both the IEC 61508 standard and the PDS-method provide such formulas for calculation of the average frequency of dangerous failures per hour (PFH). These formulas give reasonably accurate values for the PFH, but both of them also have significant weaknesses. The IEC-formulas can only be applied to systems with up to three elements while the PDS-formulas do not properly account for dangerous detected failures and are not able to include the effects of non-perfect proof-testing. This article presents new PFH-formulas for general k -out-of- n -systems, that take into account both dangerous detected and dangerous undetected failures and also allow for non-perfect proof-testing. The proposed PFH-formulas are compared with the IEC-formulas and the PDS-formulas for some selected systems in a case study, which shows that the new formulas represent an improvement compared to the IEC- and PDS-formulas.

© 2012 Elsevier Ltd. All rights reserved.

1. Introduction

IEC 61508 [12] classifies safety instrumented systems (SISs) into low-demand, high-demand, and continuous modes of operation, according to how often the systems are demanded. When the demand rate is less than once per year, the SIS is said to operate in low-demand mode; if not, the SIS is said to operate in high-demand mode. Continuous mode of operation refers to the situation where the SIS function is part of normal operation and is used continuously.

Different reliability measures are used for the three operational modes. The average frequency of dangerous failures per hour (PFH) is used for a SIS operating in high-demand and continuous mode, and the average probability of failure on demand (PFD) is used in low-demand mode [12]. Extensive research has been carried out related to modeling and calculation of the PFD [2,4,7,8,13,16,18,22], while modeling and calculation of the PFH have received much less attention.

The PFH may be calculated based on the simplified formulas [8,12], fault tree analysis [12,13], Markov models [12], and Petri nets [12–14]. Some researchers prefer not to distinguish the SIS operational modes and use a common reliability measure with basis in Markov modeling [3,13–15,17,19,23]. Despite the limitations in modeling capacity, the simplified formulas are still preferred by most practitioners, due to their simplicity.

Simplified PFH-formulas are presented in IEC 61508 [12] and in the PDS¹-method handbook [8]. These formulas are referred to

as the IEC-formulas and the PDS-formulas, respectively, in the rest of this article. The two sets of formulas give reasonably accurate values for the PFH, but improvements may still be made. The IEC-formulas can only be applied to SIS subsystems with at most three elements, and a generalization to subsystems with more elements is lacking. The PDS-formulas can be used for a general subsystem, but dangerous detected (DD) failures and non-perfect proof-testing are not sufficiently accounted for.

The objective of this article is to develop new PFH-formulas for general k -out-of- n (k -out-of- n) F SIS subsystems (i.e., subsystems that fail when at least k of its n elements fail), where DD-failures and non-perfect proof-testing are taken into account. The PFH-formulas propose a new quantification approach for the contribution from independent failures to the PFH, while the contribution from common cause failures (CCFs) is, as in the PDS-formulas, based on the multiple beta-factor (MBF) model [20]. In the proposed PFH-formulas, the possibility to reveal dangerous failures of redundant elements during a demand is disregarded.

The rest of the article is organized as follows. Various model considerations and assumptions are presented in Section 2. Section 3 gives a brief introduction to the IEC-formulas. In Section 4, the PDS-formulas for PFH-calculation are presented. Based on the PDS-formulas, new PFH-formulas including DD-failures and non-perfect proof-testing are proposed in Section 5. Section 6 compares the proposed new formulas with the IEC-formulas and the PDS-formulas. Concluding remarks are given in Section 7.

* Corresponding author. Tel.: +47 73597123.

E-mail address: hui.jin@ntnu.no (H. Jin).¹ PDS is the Norwegian acronym for "Reliability and availability of computer-based safety systems." The PDS-method is developed by the Norwegian Research

(footnote continued)

Institute, SINTEF, for SIS reliability analysis. It is a well accepted method in the oil and gas industry.

2. Model considerations

2.1. System and subsystem

Reliability is not calculated for a SIS as such, but for a safety instrumented function (SIF) that is performed by a SIS. A SIS may perform one or more SIFs. The part of a SIS that performs a specified SIF may be split into three main subsystems: (1) input elements, such as sensors and transmitters, (2) logic solver(s), and (3) final elements, such as valves and circuit breakers. A subsystem often comprises the same type of elements,² but diverse elements are also used. A SIF for overpressure protection may require, for example, pressure transmitters, a programmable logic controller (PLC), and shutdown valves. In this article, formulas are presented for a *single* subsystem of identical elements, but it is straightforward to extend the calculation to the whole SIF.

2.2. *k*-out-of-*n* system

Redundancy is often used to improve the SIS reliability. For a subsystem with *n* elements, all elements do not necessarily need to function for the subsystem to function. A *k*oo:n:F-subsystem fails (F) if at least *k* of its *n* elements fail. Similarly, a *k*oo:n:G-subsystem is functioning (i.e., is “good,” G) if at least *k* of its *n* elements are functioning. A *k*oo:n:F-subsystem is seen to be the same as (*n*−*k*+1)oo:n:G-subsystem. In this article, the *k*oo:n:F-subsystem is used to simplify the notation, but conversion to *k*oo:n:G terminology can be easily achieved.

2.3. Testing strategy

SISs are exposed to two main types of failures; those that prevent the execution of the SIF and those that do not. The first type is referred to as dangerous failure, and the latter is called safe failure [12]. PFH (and PFD) is a reliability measure with respect to dangerous failures, therefore safe failures are not further discussed. Dangerous failures can be split into DD-failures and DU (dangerous undetected)-failures. The DD-failures are detected by diagnostic testing, and the DU-failures are mainly revealed by manual and periodic proof-testing.

Diagnostic testing is able to detect some of the dangerous failures without fully executing the main function. For example, the diagnostic testing may reveal drifting in the signal conversion of a pressure transmitter without activating the transmitter. The interval between consecutive diagnostic tests is called diagnostic test interval and is denoted by τ_1 [12]. This interval is usually short ranging from milliseconds to hours (in extreme cases). The fraction of dangerous failures that can be detected by diagnostic tests is called diagnostic coverage [12].

The diagnostic testing cannot detect all dangerous failures, so proof-tests are performed to reveal the rest of the failures. A proof-test usually disturbs the process to some extent and is associated with certain costs. The frequency of such tests is much lower than for diagnostic tests. The proof-test interval, τ , may vary from months up to a couple of years.

In many reliability analyses, the proof-test is assumed to reveal all failures. This is, in practice, difficult to achieve even for a moderately complex SIS. There may be certain failures that remain hidden until a major overhaul, a real demand, or the end of the SIS lifetime. An overhaul is a thorough examination and renewal of the system, and after an overhaul, the system is

² IEC61508 [12] distinguishes between the terms element and channel. A channel performs a separate function and can comprise one or more elements. In this article, we use the term element with the same meaning as channel.

assumed to be “as good as new.” Overhauls are usually performed less frequent than proof-tests due to the significant cost. A typical overhaul interval, τ_2 , is in the order of years.

The role of proof-tests for improving the SIS reliability is evident in low-demand mode, but when the demand rate increases, the value of proof-tests is reduced, as the possibility of revealing a failure before a demand is reduced. For some high-demand systems, proof-testing is not performed at all.

2.4. Common cause failures

CCFs may contribute significantly to the PFH. Several CCF-models may be used in SIS reliability analyses. The standard beta-factor model [5] is by far the most popular model due to its simplicity, but it only differentiates between failures of single elements and failures of all elements, and uses the same relative proportion β of CCFs, for systems with different degrees of redundancy. While this is adequate for systems with two elements, it may be insufficient for systems with three or more elements.

Several extensions have been made to account for the limitations of the standard beta-factor model. Among others, the multiple beta-factor (MBF) model is recommended in both the IEC 61508 [12] and the PDS-method [8]. The MBF-model introduces a correction factor to β in the reliability quantification for each *k*oo:n:F-subsystem (presented for *k*oo:n:G-subsystem in [8,12]). The MBF-model is used in this article. For details of the MBF-model, readers are referred to [10,11], or [20].

2.5. Model assumptions

The following assumptions are made as a basis for developing new PFH-formulas:

- The elements considered are identical and have the same constant failure rates.
- DD-failures and DU-failures are mutually exclusive, such that an element can have a DD-failure or a DU-failure, but the presence of both a DD-failure and a DU-failure of the same element is not possible.
- When a DD-failure is revealed, the equipment under control (EUC) is immediately brought to a safe state.
- The MBF-model is used for CCF-modeling.
- A common factor β is, for simplicity, used for DD- and DU-CCFs, but the formulas can easily be extended to accommodate different β -factors.
- The rate of independent (ID) failures is approximated by the *total* failure rate, such that λ_{DU} instead of $(1-\beta) \cdot \lambda_{DU}$ is used for independent DU-failures. The result of this approximation is conservative.
- Combinations of CCFs and ID-failures that lead to subsystem failure are neglected for subsystems with three or more elements.
- Redundant element failures that are revealed in a demand and subsequently repaired are not taken into account in the following PFH-formulas.

3. IEC-formulas

IEC 61508 [12] presents PFH-formulas for some commonly used systems: 1oo1:F, 1oo2:F, 2oo2:F, 2oo2D:F, 2oo3:F and 3oo3:F (note that the formulas in IEC 61508 are presented using the *k*oo:n:G terminology). These formulas calculate the PFH by using the *channel-equivalent mean downtime*, t_{CE} and/or the *voted group-equivalent mean downtime*, t_{GE} . DD-failures and non-perfect

proof-testing are both considered in the calculation of t_{CE} and t_{GE} . The IEC-formulas are not presented in this article, and readers are referred to part 6 of [12]. The IEC-formulas are available only for subsystems with up to three elements. This is largely due to the use of equivalent mean downtimes. For more complex subsystems, other equivalent mean downtimes beside t_{CE} and t_{GE} need to be calculated. This is rather complicated and a formula for a general $koon:F$ -subsystem is therefore difficult to obtain.

4. PDS-formulas

The PDS-method [8] presents PFH-formulas for general $koon:F$ -subsystems. The PFH contributions from CCFs and ID-failures are treated independently, and the PFH is calculated as

$$PFH = PFH_{CCF} + PFH_{ID} \tag{1}$$

For a $1oon:F$ -subsystem, any element failure leads to subsystem failure. It is therefore not necessary to consider CCFs, and the PFH is equal to the sum of the failure rates of all elements. Since all elements are assumed to be identical, we have

$$PFH = n \cdot \lambda_{DU} \tag{2}$$

where λ_{DU} is the DU-failure rate of an element.

For a $koon:F$ -subsystem, where $k > 1$, the CCF-contribution to PFH is accounted for by using the MBF model and is expressed as

$$PFH_{CCF} = C_{(n-k+1)oon} \cdot \beta \cdot \lambda_{DU} \tag{3}$$

where β is the conditional probability of the failure of at least one more element, when we know that one element has failed, and $C_{(n-k+1)oon}$ is a correction factor for β in a $koon:F$ -subsystem. The correction factor is a special feature of the MBF model, and recommended values are given in [8,12].

Proof-testing is performed with intervals of length τ and it is assumed that the tests are perfect such that all failures are revealed and corrected in every proof-test. To calculate the PFH, we therefore need to consider only one proof-test interval. Since the n elements are identical and independent, the number of element with DU-failures, $K_{ID}(\tau)$, in a test interval is binomially distributed for the $koon:F$ -subsystem:

$$\Pr(K_{ID}(\tau) = i) = \binom{n}{i} (1 - e^{-\lambda_{DU}\tau})^i (e^{-\lambda_{DU}\tau})^{n-i} \quad \text{for } i = 0, 1, \dots, n \tag{4}$$

The probability that the subsystem fails due to independent DU-failures in a test interval is

$$\Pr(K_{ID}(\tau) \geq k) = \sum_{i=k}^n \Pr(K_{ID}(\tau) = i) \tag{5}$$

In all realistic applications, $\lambda_{DU}\tau$ is small (e.g., $\lambda_{DU}\tau < 0.01$), such that we can use the approximations $1 - e^{-\lambda_{DU}\tau} \approx \lambda_{DU}\tau$ and $e^{-\lambda_{DU}\tau} \approx 1$. The probability (4) can hence be approximated by

$$\Pr(K_{ID}(\tau) = i) \approx \binom{n}{i} (\lambda_{DU}\tau)^i = \frac{n!}{(n-i)!} \cdot \frac{(\lambda_{DU}\tau)^i}{i!} \tag{6}$$

We observe that

$$\begin{aligned} \Pr(K_{ID}(\tau) = k+1) &\approx \frac{n!}{(n-(k+1))!} \cdot \frac{(\lambda_{DU}\tau)^{k+1}}{(k+1)!} \\ &= \frac{n-k}{k+1} \cdot \lambda_{DU}\tau \cdot \Pr(K_{ID}(\tau) = k) \end{aligned} \tag{7}$$

For all realistic applications, the factor $(n-k/k+1) \cdot \lambda_{DU}\tau$ is a very small number (the factor is more insignificant when we consider $k+2$ or more failures), and we may therefore approximate (5) by $\Pr(K_{ID}(\tau) \geq k) \approx \Pr(K_{ID}(\tau) = k)$

Let $M_{ID}(\tau)$ be the number of subsystem failures due to independent DU-failures in the proof-test interval $(0, \tau)$. Since DU-failures

are only revealed at time τ , $M_{ID}(\tau)$ can only take the values 0 and 1, and the expected number of $M_{ID}(\tau)$ is $E(M_{ID}(\tau)) = \Pr(K_{ID}(\tau) \geq k) \approx \Pr(K_{ID}(\tau) = k)$. The average frequency of subsystem failures due to independent DU-failures per hour, PFH_{ID} , is hence

$$PFH_{ID} = \frac{E(M_{ID}(\tau))}{\tau} \approx \frac{n!}{(n-k)!} \cdot \frac{(\lambda_{DU}\tau)^k}{k!\tau} \tag{9}$$

The total PDS-formula for PFH of a $koon:F$ -subsystem, where $k > 1$, becomes

$$\begin{aligned} PFH &= PFH_{CCF} + PFH_{ID} \\ &\approx C_{(n-k+1)oon} \cdot \beta \cdot \lambda_{DU} + \frac{n!}{(n-k)!} \cdot \frac{(\lambda_{DU}\tau)^k}{k!\tau} \end{aligned} \tag{10}$$

5. New PFH-formulas

5.1. Dangerous detected failures

DD-failures are often ignored in SIS reliability analyses since it is assumed that when a DD-failure occurs, the EUC that is protected by the SIF, is immediately brought to a safe state. This assumption is not always fulfilled. First, the diagnostic test interval is not always negligible, meaning that a DD-failure is not detected immediately after its occurrence. Second, switching to a safe state immediately after a revealed DD-failure may not be possible or practicable. Sometimes, the operational philosophy may also allow the SIS to operate in a *degraded* mode.

5.1.1. PDS-method

The PDS-method [8] accounts for DD-failures by treating them as mutually exclusive from DU-failures and adding their contribution to (10).

For a $1oon:F$ -subsystem, the total PFH becomes

$$PFH = n \cdot (\lambda_{DU} + \lambda_{DD}) \tag{11}$$

where λ_{DD} is the rate of DD-failures.

Following the same arguments as for (10), the PFH-formula for a $koon:F$ -subsystem, where $k > 1$, can be expressed as

$$\begin{aligned} PFH &\approx C_{(n-k+1)oon} \cdot \beta \cdot (\lambda_{DU} + \lambda_{DD}) \\ &\quad + \frac{n!}{(n-k)!} \cdot \left(\frac{(\lambda_{DU}\tau)^k}{k!\tau} + \frac{(\lambda_{DD}\tau_1)^k}{k!\tau_1} \right) \end{aligned} \tag{12}$$

where τ_1 is the diagnostic test interval. The other parameters are as above.

When multiple elements need to fail to give subsystem failure ($k > 1$), the PDS-formulas consider situations where all failures are either DU-failures or DD-failures. Combinations of DU-failures and DD-failures leading to a subsystem failure are not considered.

5.1.2. New PFH-formulas covering DD-failures

The PFH-formulas of the PDS-method can be extended to cover the situation where a combination of DU-failures and DD-failures leads to a dangerous subsystem failure. We will first illustrate the approach by studying a $2oo2:F$ -subsystem.

2oo2:F-subsystem. This subsystem is a parallel system of two identical and independent elements, and the subsystem fails only when both elements fail. Two combinations of dangerous failures will give a dangerous subsystem failure in the proof-test interval $(0, \tau)$:

- (a) First a DU-failure occurs on one element at some time t in $(0, \tau)$, and then a dangerous failure (DU or DD) occurs on the other element in the remaining part of the interval, i.e., in (t, τ) . The rate of dangerous (D) failures is $\lambda_D = \lambda_{DU} + \lambda_{DD}$. The element to fail first with a DU-failure can be one out of two.

When the first failure has occurred, there is only one option for the second failure. We can therefore express the probability of this option as:

$$\Pr(\text{Option a}) = 2 \int_0^\tau (1 - e^{-\lambda_D(\tau-t)}) \cdot \lambda_{DU} e^{-\lambda_{DU}t} dt \approx (\lambda_{DU}\tau)^2 + \lambda_{DU} \cdot \lambda_{DD}\tau^2 \quad (13)$$

To obtain the result in (13), we have used the approximation $1 - e^{-x} \approx x - x^2/2$ when x is small.

(b) First a DD-failure occurs on one element at some time t in $(0, \tau)$, and then a D-failure occurs on the other element before the DD-failure is restored. We have assumed that the EUC immediately will be brought to a safe state when a DD-failure is revealed. We have further assumed that the diagnostic testing is done with intervals of length τ_1 . The first DD-failure will hence occur in such a diagnostic test interval and will not be revealed until the end of this interval. If a D-failure occurs in the remaining part of the diagnostic test interval, the subsystem will fail. When we know that a DD-failure has occurred in a diagnostic test interval, the time U it occurred in the interval will be uniformly distributed with probability density function $f_U(u) = 1/\tau_1$ for all u in this particular diagnostic test interval [21]. The probability of a D-failure after a DD-failure has occurred will be the same for all diagnostic test intervals, and we therefore consider the first interval $(0, \tau_1)$, to simplify the notation.

Similar as for option (a), the element to fail first can be one out of two and the probability of the second option can therefore be expressed as

$$\Pr(\text{Option b}) = 2 \int_0^\tau \left(\int_0^{\tau_1} (1 - e^{-\lambda_D(\tau_1-u)}) \cdot \frac{1}{\tau_1} du \right) \cdot \lambda_{DD} e^{-\lambda_{DD}t} dt \approx \lambda_{DD} \lambda_D \tau_1 \tau \quad (14)$$

In these calculations, we have disregarded the possibility of more than one dangerous subsystem failure in the same proof-test interval. For a realistic SIF, the probability of two or more dangerous failures in the same proof-test interval will be negligible.

The two options are mutually exclusive and the probability of a dangerous subsystem failure is

$$\Pr(\text{Option a}) + \Pr(\text{Option b})$$

The probability of a dangerous subsystem failure in $(0, \tau)$ can be written as

$$\Pr(\text{System fails in } (0, \tau)) \approx (\lambda_{DU}\tau)^2 + (\lambda_{DU}\tau)(\lambda_{DD}\tau) + (\lambda_{DD}\tau)(\lambda_D\tau_1)$$

The PFH_{ID} of the 2oo2:F-system in $(0, \tau)$ is therefore

$$\text{PFH}_{ID} \approx \frac{(\lambda_{DU}\tau)^2}{\tau} + \frac{(\lambda_{DU}\tau)(\lambda_{DD}\tau)}{\tau} + \frac{(\lambda_{DD}\tau)(\lambda_D\tau_1)}{\tau} \quad (15)$$

2oon:F-subsystem. The PFH in $(0, \tau)$ for this system can be found in the same way as for the 2oo2:F-subsystem. The two elements that will fail can be selected among the n elements in $\binom{n}{2}$ different ways. The rest of the calculation is the same as for the 2oo2:F-subsystem and the PFH for the 2oon:F-subsystem in $(0, \tau)$ becomes

$$\text{PFH}_{ID} \approx \frac{n}{2} \cdot \left[\frac{(\lambda_{DU}\tau)^2}{\tau} + \frac{(\lambda_{DU}\tau)(\lambda_{DD}\tau)}{\tau} + \frac{(\lambda_{DD}\tau)(\lambda_D\tau_1)}{\tau} \right] \quad (16)$$

Again, we note that when $\lambda_{DD} = 0$, we get the same results as in Section 4.

We want to generalize the result and will therefore rewrite (16) slightly as

$$\text{PFH}_{ID} \approx \frac{n!}{(n-2)!} \left[\frac{(\lambda_{DU}\tau)^2}{2!\tau} + \frac{(\lambda_{DU}\tau)(\lambda_{DD}\tau)}{2!\tau} + \frac{(\lambda_{DD}\tau)(\lambda_D\tau_1)}{2!\tau} \right] \quad (17)$$

Compared with the PDS-formulas, two extra terms $(\lambda_{DU}\tau)(\lambda_{DD}\tau)/2!\tau$ and $(\lambda_{DD}\tau)(\lambda_D\tau_1)/2!\tau$ (note: $\lambda_D = \lambda_{DD} + \lambda_{DU}$) are added in (17). Since τ is significantly longer than τ_1 , and λ_{DU} and λ_{DD} are in the same order of magnitude, $(\lambda_{DU}\tau)^2/2!\tau$ and $(\lambda_{DU}\tau)(\lambda_{DD}\tau)/2!\tau$ are the dominating terms in equation (17).

koon:F-subsystem. By using the same arguments as above, we can show that the PFH of a *koon:F*-subsystem due to independent failures can be written as

$$\text{PFH}_{ID} \approx \frac{n!}{(n-k)!} \cdot \left(\frac{(\lambda_{DU}\tau)^k}{k!\tau} + \lambda_{DD} \cdot \sum_{j=1}^k \frac{(\lambda_{DU}\tau)^{k-j} (\lambda_D\tau_1)^{j-1}}{(k-j+1)j!} \right) \quad (18)$$

The derivation of (18) is based on the same approach as above, but rather tedious and is not included here.

The PFH-formula for *koon:F*-subsystem, for $k > 1$, is therefore

$$\text{PFH} \approx C_{(n-k+1)\text{oon}} \cdot \beta \cdot \lambda_D + \frac{n!}{(n-k)!} \cdot \left(\frac{(\lambda_{DU}\tau)^k}{k!\tau} + \lambda_{DD} \cdot \sum_{j=1}^k \frac{(\lambda_{DU}\tau)^{k-j} (\lambda_D\tau_1)^{j-1}}{(k-j+1)j!} \right) \quad (19)$$

Remark: The assumption in Section 2.5 that the EUC is immediately brought to a safe state when a DD-failure is revealed is not always realistic. The switching to a safe state may take rather long time for some systems. Then, given a DD-failure, the time allowing more failures to occur needs to be adjusted to reflect this problem, and hence (18) and (19) need to be adjusted. Fortunately, as shown later, extending this time does not have any significant influence on the PFH-value.

5.1.3. New approximation formula for PFH

Since $\tau \gg \tau_1$, the terms containing τ_1 in the sum in (19) will be significantly smaller than the term without τ_1 . We may therefore use the following approximation formula for PFH:

$$\text{PFH} \approx C_{(n-k+1)\text{oon}} \cdot \beta \cdot \lambda_D + \frac{n!}{(n-k)!} \cdot \left(\frac{(\lambda_{DU}\tau)^k}{k!\tau} + \frac{\lambda_{DD} \lambda_{DU}^{k-1} \tau^k}{k!\tau} \right) = \frac{\lambda_D}{\lambda_{DU}} \cdot \left(C_{(n-k+1)\text{oon}} \cdot \beta \cdot \lambda_{DU} + \frac{n!}{(n-k)!} \cdot \frac{(\lambda_{DU}\tau)^k}{k!\tau} \right) \quad (20)$$

i.e., only the term for $j=1$ in the sum in (19) is included. It is noted that when λ_{DD} is disregarded, such that $\lambda_D = \lambda_{DU}$, the new approximation formula (20) is identical to (19) as well as (10) in Section 4.

5.2. Non-perfect proof-testing

In many SIS reliability studies, the proof-test is assumed to have perfect coverage, such that all elements are “as good as new” after the test. A proof-test is, however, seldom perfect, and failures may remain unrevealed after the test. Proof-tests of pressure transmitters are, for example, performed after the transmitters are isolated from the process. This is because pressurizing a pipeline/vessel to the trip pressure may, itself, lead to an unsafe situation. When such a proof-test is performed, some DU-failures, for example caused by contamination in the pressure-sensing lines, may remain hidden after the test. Non-perfect proof-testing is discussed by [1,12,6] for low-demand systems, but similar studies for high-demand systems are missing. This section extends the PDS-formulas for PFH to cover non-perfect proof-testing.

5.2.1. Proof-test coverage

DU-failures that are detected neither by diagnostic testing nor by proof-testing may be revealed during an overhaul, or will remain unrevealed until the end of the system's life/mission. The fraction of DU-failures that are revealed by proof-tests is called the proof-test coverage (PTC) [12]. The PTC is also called functional test coverage in some references, e.g., [15]. The fraction of DU-failures that are not revealed by proof-tests is then (1 – PTC).

5.2.2. Proof-test and diagnostic coverage

After an overhaul, it is realistic to assume that the SIS is “as good as new.” It is hence necessary only to consider one overhaul interval when calculating the PFH. If overhaul is not carried out, some DU-failures may remain unrevealed until the end of the life of the SIS. The time interval to be considered when calculating the PFH will then be the lifetime of the SIS. Both time intervals are here denoted τ_2 .

To calculate the PFH, consider the following two cases:

- (a) Both diagnostic testing and proof-testing are applied. The diagnostic tests have a coverage less than 100% and the proof-tests have a coverage equal to 100% (i.e., perfect proof-testing). This means that no overhaul is needed. The overall PFH-value can be calculated by (20) and the PFH_{ID} by (18).
- (b) In this case, we only consider DU-failures. Both proof-testing and overhaul are applied. The proof-tests have a coverage less than 100%, but the overhaul reveals all failures. The PFH-formula for this situation is what we want to develop in this section.

Comparing the two cases (a) and (b), analogies can be drawn. The role of proof-testing in situation (b) is analogous to the role of diagnostic testing in case (a). Both of them are performed with a certain interval and can only reveal a fraction of failures. The role of proof-testing in the PFH-formula in case (b) is equivalent to the role of diagnostic testing in the PFH-formula in case (a). The corresponding parameters are listed in Table 1.

The role of overhaul in situation (b) is analogous to the role of proof-testing in situation (a). Both of them are performed with a much longer interval (than the counterpart in their respective situations) and are assumed to reveal all failures. The role of overhaul in PFH-formula for situation (b) is equivalent to the role of proof-testing in PFH-formula for situation (a). The corresponding parameters are listed in Table 2.

5.2.3. New PFH-formula with PTC

The PFH-formula with PTC (situation (b)) can be derived from (18). By replacing λ_{DU} , λ_{DD} , λ_D , τ , and τ_1 in (14) with $(1-PTC)\cdot\lambda_{DU}$, $PTC\cdot\lambda_{DU}$, λ_{DU} , τ_2 and τ , respectively, the formula PFH_{ID} with PTC for a $koon:F$ -subsystem, where $k > 1$, becomes

$$PFH_{ID} \approx \frac{n!}{(n-k)!} \cdot \left(\frac{[(1-PTC)\cdot\lambda_{DU}\tau_2]^k}{k!\tau_2} \right)$$

Table 1
Proof-testing in situation (b) compared to diagnostic testing in situation (a).

| Parameters | Proof-testing in situation (b) | Diagnostic testing in situation (a) |
|---------------------------|--------------------------------|-------------------------------------|
| Coverage | PTC | λ_{DD}/λ_D |
| Test interval | τ | τ_1 |
| Failure rate (total) | λ_{DU} | λ_D |
| Failure rate (undetected) | $(1-PTC)\cdot\lambda_{DU}$ | λ_{DU} |
| Failure rate (detected) | PTC λ_{DU} | λ_{DD} |

Table 2
Overhaul in situation (b) compared to proof-testing in situation (a).

| Parameters | Overhaul in situation (b) | Proof-testing in situation (a) |
|---------------------------|---------------------------|--------------------------------|
| Coverage | 100% | 100% |
| Test interval | τ_2 | τ |
| Failure rate (total) | λ_{DU} | λ_D |
| Failure rate (undetected) | 0 | 0 |
| Failure rate (detected) | λ_{DU} | λ_D |

$$+ PTC \cdot \lambda_{DU} \cdot \sum_{j=1}^k \frac{[(1-PTC)\cdot\lambda_{DU}\tau_2]^{k-j}(\lambda_{DU}\tau)^{j-1}}{(k-j+1)j!} \quad (21)$$

In (21), DD-failures are not accounted for. The same way of including DD-failures in (20) can be used to add DD-failures into (21), i.e., adding the factor: λ_D/λ_{DU} . Together with the CCF-contribution, PFH with PTC for a $koon:F$ -subsystem, where $k > 1$, can be calculated by

$$PFH \approx \frac{\lambda_D}{\lambda_{DU}} \cdot \left(C_{(n-k+1)oon} \cdot \beta \cdot \lambda_{DU} + \frac{n!}{(n-k)!} \cdot \left[\frac{[(1-PTC)\cdot\lambda_{DU}\tau_2]^k}{k!\tau_2} + PTC \cdot \lambda_{DU} \cdot \sum_{j=1}^k \frac{[(1-PTC)\cdot\lambda_{DU}\tau_2]^{k-j}(\lambda_{DU}\tau)^{j-1}}{(k-j+1)j!} \right] \right) \quad (22)$$

Observe that when PTC = 100%, (21) is the same as (9) and (22) is the same as (20).

6. Case study

A simple case study is carried out to compare the results obtained by the proposed PFH-formulas with results obtained by the IEC- and PDS-formulas. The comparison is made only for ID-failures. This is (1) because we want to highlight the improvement in the calculation of ID-failures, and (2) because the IEC- and PDS-formulas are based on different CCF models. However, the readers should be aware that if the contribution from CCF had been included, it would in most cases have a dominating effect.

In the case study, we consider a subsystem of a SIS comprising n pressure transmitters of the same type. The relevant parameters for a pressure transmitter are given in Table 3. The failure data are from [9] while the test intervals are assumed. The diagnostic test interval in Table 3 is significantly longer than for most SISs. This is done to show that even with such a long diagnostic test interval, the two proposed formulas give rather close results. Such a long diagnostic test interval may, however, be relevant in extreme cases. The mean repair time, MRT, is assumed to be negligible (i.e., 0 h) to have the same basis when comparing IEC-formulas and other formulas, but it can be shown that the results are not significantly changed when a typical MRT, such as 8 h, is used.

6.1. New PFH-formulas with DD-failures

Assuming perfect proof-testing, the PFH_{ID} (i.e., restricted to independent failures) for the transmitters is calculated for some common $koon:F$ -subsystems in Table 4 based on the IEC-formulas, the PDS-formulas, and the two new formulas (19) and (20). Table 4 shows that the PDS-formulas give more conservative results than the IEC-formulas. This is, to a large extent, because the CCF-fraction is not subtracted when considering independent failures in the PDS-formulas (i.e., the reduction factor $(1-\beta)$ is not used for the independent failure rate). The same applies for formulas (19) and (20)). The PFH-values obtained by the new formulas are even more

Table 3
Data used in PFH-calculation for pressure transmitters.

| Parameters | Value |
|--|-----------------|
| DU failure rate (λ_{DU}) | 0.3E-6 per hour |
| DD failure rate (λ_{DD}) | 2.0E-6 per hour |
| Dangerous failure rate (λ_D) | 2.3E-6 per hour |
| Proof-test interval (τ) | 4380 h |
| Beta factor for DU and DD (β) | 0.05 |
| Diagnostic test interval (τ_1) | 8 h |
| Mean repair time, MRT | 0 h |

Table 4
PFH_{ID}-values obtained by various formulas [(1-β)-factor is ignored].

| Subsystem | IEC [12] | PDS [8] | Proposal (19) | Approx. (20) |
|-----------|----------|----------|---------------|--------------|
| 2oo2: F | 3.60E-10 | 4.26E-10 | 3.06E-9 | 3.02E-9 |
| 2oo3: F | 1.08E-9 | 1.28E-9 | 9.18E-9 | 9.07E-9 |
| 3oo3: F | 4.58E-13 | 5.18E-13 | 4.04E-12 | 3.97E-12 |
| 3oo4: F | N/A | 2.07E-12 | 1.62E-11 | 1.59E-11 |

conservative than the results from the PDS-formulas, because combinations of DD- and DU-failures leading to subsystem failure are taken into consideration in the new formulas.

The diagnostic test interval is not part of the formula (20), but the PFH-values obtained by this formula are seen to be very close to those obtained by (19), even for an unusually long diagnostic test interval (the shorter the diagnostic test interval, the less likely a failure will occur before the DD-failure is repaired). In most cases, it is therefore adequate to use the approximation formula (20). Moreover, this also confirms that the assumption of achieving a safe state immediately after a revealed DD-failure has insignificant influence on the PFH-value. Hence the concern about assumptions in (19) is alleviated.

Diagnostic coverage is an important parameter in the SIS reliability analysis. Fig. 1 shows the PFH_{ID} as a function of the diagnostic coverage for a 2oo3:F-subsystem calculated by the IEC-, the PDS-, and the proposed formulas, respectively. The PFH_{ID}-values obtained by the approximation formula (20) are not included since they are almost identical to the proposed formula (19). In Fig. 1, the dangerous failure rate λ_D is kept constant and as given in Table 3. The DD- and DU-failure rates vary with the diagnostic test coverage. The rest of the data are as given in Table 3.

Fig. 1 shows that the proposed PFH-formulas give higher PFH_{ID}-values than the IEC- and PDS-formulas. When the diagnostic coverage is 0, which is the same as no diagnostic testing, the proposed formulas and the PDS-formulas give the same PFH_{ID}, and higher than the PFH-value obtained by the IEC-formulas. This is because the CCF-fraction is not subtracted when considering independent failures in the proposed formulas and the PDS-formulas. Fig. 1 also shows that the relationship between the diagnostic coverage and the PFH-value is linear when using the proposed formula, while the IEC- and the PDS-formulas suggest a non-linear relationship. Fig. 1 illustrates the benefit of improving the diagnostic coverage.

When the CCF-fraction β is subtracted for independent failures in the PDS-formulas and in the proposed new formulas (19) and (20), the results are shown in Table 5. The IEC-formulas and the PDS-formulas now give close results. The proposed new formulas give, however, more accurate PFH-values.

Remark: Given the parameters in this case study, it is calculated that the PFH contribution from CCF is in the order of 10^{-8} per hour. Compared to PFH contribution from the ID-failures in Tables 4 and 5, the PFH contribution from CCF is dominant. If the

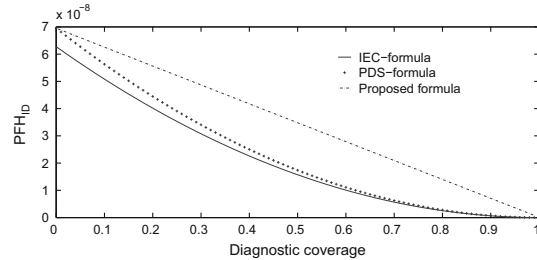


Fig. 1. PFH_{ID} for different diagnostic coverages, for a 2oo3:F-subsystem.

Table 5
PFH_{ID}-values obtained by various formulas [(1-β)-factor is included].

| Subsystem | IEC [12] | PDS [8] | Proposal (19) | Approx. (20) |
|-----------|----------|----------|---------------|--------------|
| 2oo2: F | 3.60E-10 | 3.85E-10 | 2.76E-9 | 2.73E-9 |
| 2oo3: F | 1.08E-9 | 1.15E-9 | 8.28E-9 | 8.18E-9 |
| 3oo3: F | 4.58E-13 | 4.45E-13 | 3.47E-12 | 3.40E-12 |
| 3oo4: F | N/A | 1.78E-12 | 1.39E-11 | 1.36E-11 |

CCF is included in the case study, the results from different formulas will be rather similar.

6.2. New PFH-formulas with PTC

In order to include the effect of non-perfect proof-testing, both the IEC-formulas and the proposed formulas use the PTC and an overhaul interval in the PFH calculation. Comparisons between results from the IEC-formulas and the proposed new formulas are made for different PTC-values when the overhaul interval τ_2 is 5 years and 10 years, respectively. The results are given in Table 6.

Table 6 shows that the proposed formula (22) gives more conservative results than the IEC-formulas. This is because cases where the last failure is a DD-failure, are not considered in the IEC-formulas for PFH, and also because the CCF-fraction is not subtracted when calculating PFH_{ID}. The proposed formula can also be used to calculate the PFH for a general kooF-subsystem, which is not possible with the IEC-formulas. The results indicate that the PTC has a significant influence on the PFH_{ID}. This influence increases when the overhaul interval increases. For a 3oo4:F-subsystem, the PFH_{ID} can increase by a factor of 10–20 times from 100% PTC to 80% PTC.

Tables 4 and 6 show that (20) and (22) give identical results when PTC is 100%. This result is obvious since overhaul is not necessary when the proof-tests are perfect. In practice, however, proof-tests are seldom perfect and overhauls are necessary.

Fig. 2 shows the PFH_{ID} as a function of the proof-test coverage, for a 2oo3:F-subsystem. The data in Table 3 are used, and the overhaul interval is 5 years. The figure shows that the proposed formula gives more conservative results than the IEC-formulas, and when the PTC is reduced, the difference between the two formulas is more significant.

7. Concluding remarks

Simplified formulas are popular in SIS reliability analysis, especially among practitioners. IEC 61508 and the PDS-method provide different version of PFH-formulas. The PFH-values obtained by these formulas are reasonably accurate, but both approaches have weaknesses. The IEC-formulas can only handle subsystems with up to three elements, and the PDS-formulas do

Table 6
PFH_{ID}-values obtained by the IEC-formulas and the proposed formulas with PTC.

| Subsystem | PTC (%) | Overhaul every 5 years | | Overhaul every 10 years | |
|-----------|---------|------------------------|---------------|-------------------------|---------------|
| | | IEC [12] | Proposal (22) | IEC [12] | Proposal (22) |
| 2oo2: F | 100 | 3.60E-10 | 3.02E-9 | 3.60E-10 | 3.02E-9 |
| | 95 | 5.20E-10 | 4.38E-9 | 6.98E-10 | 5.89E-9 |
| | 90 | 6.80E-10 | 5.74E-9 | 10.36E-10 | 8.76E-9 |
| | 85 | 8.40E-10 | 7.10E-9 | 13.74E-10 | 11.64E-9 |
| | 80 | 10.00E-10 | 8.46E-9 | 17.12E-10 | 14.51E-9 |
| 2oo3: F | 100 | 1.08E-9 | 9.07E-9 | 1.08E-9 | 9.07E-9 |
| | 95 | 1.56E-9 | 13.15E-9 | 2.09E-9 | 17.68E-9 |
| | 90 | 2.04E-9 | 17.23E-9 | 3.11E-9 | 26.29E-9 |
| | 85 | 2.52E-9 | 21.32E-9 | 4.12E-9 | 34.91E-9 |
| | 80 | 3.00E-9 | 25.39E-9 | 5.14E-9 | 43.52E-9 |
| 3oo3: F | 100 | 4.58E-13 | 3.97E-12 | 4.58E-13 | 3.97E-12 |
| | 95 | 9.53E-13 | 7.59E-12 | 1.72E-12 | 13.40E-12 |
| | 90 | 16.29E-13 | 12.91E-12 | 3.77E-12 | 30.18E-12 |
| | 85 | 24.84E-13 | 19.91E-12 | 6.63E-12 | 54.31E-12 |
| | 80 | 35.20E-13 | 28.59E-12 | 10.30E-12 | 85.78E-12 |
| 3oo4: F | 100 | N/A | 1.59E-11 | N/A | 1.59E-11 |
| | 95 | N/A | 3.04E-11 | N/A | 5.36E-11 |
| | 90 | N/A | 5.16E-11 | N/A | 12.07E-11 |
| | 85 | N/A | 7.96E-11 | N/A | 21.72E-11 |
| | 80 | N/A | 11.44E-11 | N/A | 34.31E-11 |

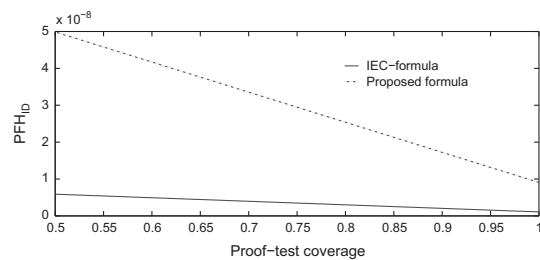


Fig. 2. PFH_{ID} for different proof-test coverages, for a 2oo3:F-subsystem.

not adequately account for DD-failures and non-perfect proof-testing.

This article has proposed a set of new PFH-formulas for general *koo*:F-subsystems. The proposed formulas are more flexible than the IEC-formulas [12] and can be used for subsystems with more complex configurations. Compared to the PDS-formulas [8], the proposed formulas account for DD-failures in a more appropriate way, and non-perfect proof-testing can be included.

A case study of pressure transmitters is given in this article. Comparing the results from the proposed formulas with those from the IEC-formulas and the PDS-formulas shows that the proposed formulas give more conservative results. This is as expected since combinations of DD- and DU-failures leading to subsystem failure are considered. The results also show that non-perfect proof-testing has a significant influence on the PFH-values.

It is, therefore, important to examine the perfect proof-test assumption. If it is not fulfilled, the PTC must be included in the PFH calculation and overhaul of SIS may need to be exercised.

References

- [1] Baradits G. Safety instrumented system management. PhD thesis. Hungary: University of Pannonia; 2010.
- [2] Bukowski J. Modeling and analyzing the effects of periodic inspection on the performance of safety-critical systems. *IEEE Transactions on Reliability* 2001;50:321–9.
- [3] Bukowski J. Incorporating process demand into models for assessment of safety system performance. In: Proceedings of RAMS'06 symposium. Alexandria, VI, USA; 2006.
- [4] Bukowski J. Using Markov models to compute PFD_{ave} when repair times are not exponentially distributed. In: Proceedings of the annual reliability and maintainability symposium. Newport Beach, CA, USA; 2006.
- [5] Fleming KN. A reliability model for common mode failures in redundant safety systems. Technical Report GA-A13284, General Atomic Company, San Diego, CA; 1975.
- [6] Goble W. Getting good proof test coverage numbers. Last accessed August 3 2011. <http://www.exida.com/index.php/blog/indepth/getting_good_proof_test_coverage_numbers/>; 2011.
- [7] Guo H, Yang X. A simple reliability block diagram method for safety integrity verification. *Reliability Engineering and System Safety* 2007;92(9):1267–73.
- [8] Hauge S, Lundteigen MA, Hokstad P, Håbrekke S. Reliability prediction method for Safety Instrumented Systems. Trondheim: SINTEF; 2010.
- [9] Hauge S, Onshus T. Reliability data for safety instrumented systems. Trondheim: SINTEF; 2010.
- [10] Hokstad P, Corneliussen K. Loss of safety assessment and the IEC 61508 standard. *Reliability Engineering and System Safety* 2004;83(1):111–20.
- [11] Hokstad P, Maria A, Tomis P. Estimation of common cause factors from systems with different numbers of channels. *IEEE Transactions on Reliability* 2006;55(1):18–25.
- [12] IEC 61508. Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 1–7. Geneva: International Electrotechnical Commission; 2010.
- [13] Innal F. Contribution to modelling safety instrumented systems and to assessing their performance critical analysis of IEC 61508 standard. PhD thesis. France: University of Bordeaux; 2008.
- [14] Innal F, Dutuit Y, Rauzy A, Signoret J. New insight into the average probability of failure on demand and the probability of dangerous failure per hour of safety instrumented systems. *Journal of Risk and Reliability* 2010;224:75–86.
- [15] Jin H, Lundteigen MA, Rausand M. Reliability performance of safety instrumented systems: a common approach for both low- and high-demand mode of operation. *Reliability Engineering and System Safety* 2011;96:365–73.
- [16] Langeron Y, Barros A, Grall A, Berenguer C. Combination of safety integrity levels (sils): a study of IEC 61508 merging rules. *Journal of Loss Prevention in the Process Industries* 2008;21(4):437–49.
- [17] Liu YL, Rausand M. Reliability assessment of safety instrumented systems subject to different demand modes. *Journal of Loss Prevention in the Process Industries* 2011;24(1):49–56.
- [18] Lundteigen MA, Rausand M. Reliability assessment of safety instrumented systems in the oil and gas industry: a practical approach and a case study. *International Journal of Reliability, Quality, and Safety Engineering* 2009;16:187–212.
- [19] Misumi Y, Sato Y. Estimation of average hazardous-event-frequency for allocation of safety-integrity levels. *Reliability Engineering and System Safety* 1999;66:135–44.
- [20] Rausand M. Risk assessment; theory, methods, and applications. Hoboken, NJ: Wiley; 2011.
- [21] Rausand M, Høyland A. System reliability theory; models, statistical methods, and applications. 2nd edition Hoboken, NJ: Wiley; 2004.
- [22] Rouvroye J, Van den Bliet E. Comparing safety analysis techniques. *Reliability Engineering and System Safety* 2002;75(3):289–94.
- [23] Youshiamura I, Sato Y. Estimation of calendar-time- and process-operative-time-hazardous-event rates for the assessment of fatal risk. *International Journal of Performability Engineering* 2009;5:377–86.

Article 2 (journal)

Reliability of safety-instrumented systems subject to partial testing
and common-cause failures

–Accepted for publication in *Reliability Engineering and System
Safety*

Reliability of safety-instrumented systems subject to partial testing and common-cause failures

Hui Jin*, Marvin Rausand*

Department of Production and Quality Engineering, Norwegian University of Science and Technology, NO 7491 Trondheim, Norway

Abstract

Partial testing is sometimes used as a supplement to proof testing to improve the reliability of safety-instrumented systems (SISs) in low-demand mode of operation. This article studies the effect of partial testing on SIS reliability. Simplified formulas are developed to include both partial and proof testing in the calculation of the average probability of failure on demand (PFD_{avg}). The proposed formulas can handle situations where partial testing is performed periodically and non-periodically. Common-cause failures (CCFs) are treated by using the beta-factor model, and different β -factors can be included for different failure modes. The proposed formulas are compared with existing results for partial verification. A case study is presented to demonstrate the applicability. The proposed formulas can serve as a valuable tool for selecting a cost-effective strategy for partial testing.

Keywords: Safety-instrumented systems, partial tests, proof tests, PFD_{avg} , common-cause failures

1. Introduction

Reliability analysis of safety-instrumented systems (SISs) has attracted a lot of attention in the recent years and significant contributions have been made to improve the analyses. Requirements for SIS reliability analyses are given in IEC 61508 [8] and several application-specific standards,

*Corresponding author:
Email address: hui.jin@ntnu.no (Hui Jin)

such as IEC 61511 [9] for the process industry. This article is limited to SISs operating in low-demand mode, meaning that the SIS is normally in a passive state and will only be activated when a demand occurs. The frequency of demands is assumed to be less than once per year [8]. An emergency shutdown system in a process plant is an example of such a low-demand SIS. The reliability of a low-demand SIS is quantified as the average probability of failure on demand (PFD_{avg})¹. This means that if a demand occurs, the SIS will, on average, fail to carry out its required safety-instrumented function (SIF) with probability PFD_{avg} .

To reduce the PFD_{avg} , we may increase the component reliability, increase the redundancy level, perform more frequent proof tests, and/or improve the system's protection against common-cause failures (CCFs). The component reliability has been improved to such a level that further improvement is difficult and may not be cost-effective; more redundancy will lead to higher cost, a more complex system, and often more spurious trips. In some applications, the space is limited, and high redundancy may not be feasible. The positive effect of increased redundancy may also be lost due to CCFs. Increased frequency of proof testing may therefore be the preferred strategy if the SIS reliability has to be improved, especially for existing SISs where modification of the hardware is expensive.

Reliability improvement by more frequent proof tests does not come without a cost. Proof testing requires resources in the form of man-hours, equipment, and coordination. More importantly, proof testing often disturbs the production and leads to production downtime. To avoid the loss of production, alternative test methods have been proposed to replace some of the proof tests. One such proposal is the use of partial stroke testing (PST) for safety valves. Compared with a proof test where all the dangerous failure modes of the valve are tested, only some few failure modes are tested in a PST. A PST of a shutdown valve, for example, can partly detect the failure mode "fail to close on command", but is not able to detect the failure mode "leakage in closed position." In some companies, the SIS elements are partly operated in-between proof tests without any careful examination of all failure modes. By this procedure, the companies are able to detect certain failure modes without proof testing, and the PFD_{avg} may be reduced without changing the proof

¹ PFD_{avg} is the average unavailability of the safety function, the word "reliability" is used in a general sense to describe the reliability performance of SIS.

test frequency, or the PFD_{avg} is maintained with less frequent proof tests. This type of partial testing will hereafter be called Δ -testing, and may often be performed without any extra production disturbances during planned or unplanned production stops.

Methods for PFD_{avg} calculation have been heavily investigated [3, 4, 10, 11, 12, 14, 16], but the effect of Δ -testing is not systematically accounted for. Summers and Zachary [17] present an approximation formula for a single item subject to Δ -testing. This formula is elaborated in [13] and is widely accepted. Torres-Echeverria et al. [18] propose analytical expressions for the PFD_{avg} of parallel systems, solved by numerical methods. A common limitation is that these methods are based on the assumption of periodic Δ -tests. The work by Brissaud et al. [1] is important in this respect since it proposes formulas that can calculate the PFD_{avg} for general k -out-of- n (*koon*) systems subject to non-periodic Δ -testing. However, the formulas do not account for CCFs, which is a main contributor to the PFD_{avg} [7].

The objective of this article is to develop PFD_{avg} formulas for *koon* systems that take into account the effect of both non-periodic Δ -testing and CCFs. The proposed formulas should give similar results as the widely accepted formulas for special cases such as single items (i.e., 1oo1 systems) with periodic Δ -testing, and *koon* systems without Δ -testing. When CCFs are not considered, the proposed formulas should also give similar results as Brissaud et al. [1] for *koon* systems with Δ -testing, even if the two sets of formulas are developed in completely different ways.

The rest of this article is organized as follows. A brief account of failure classification is given in section 2. Section 3 presents PFD_{avg} formulas considering only independent failures; verifications are given through special cases and a numerical example. In section 4, CCFs are included in PFD_{avg} formulas for SISs subject to Δ -testing. A case study of shutdown valves is presented in section 5, and concluding remarks are given in section 6.

2. Failure classification

Failures of SISs may be classified as dangerous (D) and safe (S) failures. A failure is dangerous if the SIF is prohibited by the failure, and safe otherwise. S-failures are assumed to have negligible effect on the PFD_{avg} , since PFD_{avg} is a reliability measure with respect to D-failure and the repair

of S-failures is usually completed in a short time and a controlled environment possibly with additional safety measure implemented. D-failures can be further split into dangerous detected (DD) and dangerous undetected (DU) failures. DD-failures are failures detected by diagnostic testing and DU-failures are failures only detected by proof testing and partly by Δ -testing. Diagnostic tests are performed rather frequently, often more frequent than once per minute. If a DD-failure is repaired immediately after it is detected and the repair time is negligible, or the equipment under control (EUC) is immediately brought to a safe state when a DD-failure is revealed, the PFD_{avg} contribution from DD-failures will be negligible. In the following, we therefore consider only DU-failures.

When both proof testing and Δ -testing are used, the DU-failures may be further split into two categories: (a) DU-failures that can be detected by both proof testing and Δ -testing, and (b) DU-failures that are detected by proof testing but not by Δ -testing.

We define the Δ -test coverage (ΔTC) as the fraction θ of the DU-failures that can be detected by Δ -testing.

$$\theta = \frac{\lambda_a}{\lambda}$$

where λ is the total DU-failure rate and λ_a is the rate of type a failures. The rate of type b failures is then $\lambda_b = (1 - \theta)\lambda$.

CCFs deserve special attention, due to their significant impact on PFD_{avg} . A CCF is defined as a failure that is the result of one or more events, causing concurrent failures of two or more components, leading to a system failure [8]. Several models, such as the beta-factor model [2] and the multiple beta-factor model [4], may be used to quantify the effect of CCFs on the SIS reliability. The beta-factor model is by far the most commonly used CCF model in SIS reliability analyses, mainly due to its simplicity.

3. PFD_{avg} formulas with Δ -testing

We first consider only independent DU-failures and develop PFD_{avg} formulas for a SIS subsystem subject to both proof testing and Δ -testing. CCFs are included into the formulas in Section 4. The subsystem under consideration is a *koon* system, i.e., the subsystem is functioning when k or

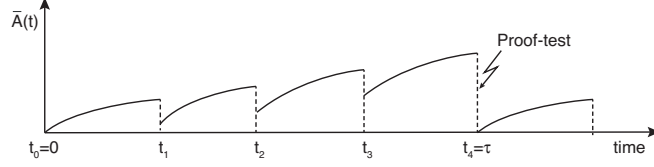


Figure 1: Safety unavailability with Δ -testing and proof test at time $\tau = t_4$.

more of the n channels are functioning. Both proof testing and Δ -testing are used to detect DU-failures. When a DU-failure is detected in a proof test, a repair action is carried out to restore the subsystem to an “as good as new” state. We may therefore consider only one proof test interval to determine the PFD_{avg} . Δ -tests are performed within the proof test interval and are only able to detect type a failures. An as good-as-new-state can therefore not be claimed after a Δ -test, as illustrated in Fig. 1, when Δ -tests are performed at time t_1 , t_2 , and t_3 .

3.1. Model assumptions

To calculate the PFD_{avg} , several assumptions need to be made:

- The channels in the *koon* system are identical and have the same constant DU-failure rate λ . The Δ TC is θ . The rate of type a failures is $\lambda_a = \theta\lambda$, and the rate of type b failures is $\lambda_b = (1 - \theta)\lambda$.
- All channels are in a fully functioning state at time $t = 0$.
- In a proof test interval τ , m tests are performed. The first $m-1$ tests are Δ -tests with intervals: t_1, t_2, \dots, t_{m-1} ; and the m -th test is a proof test (see Fig.1).
- All the tests are performed simultaneously for all the n channels.
- All DU-failure modes are revealed in a proof test, and repair is initiated immediately after the test. An as-good-as-new state is assumed after a proof test (or after the repair action following a proof test).
- Only type a failures are revealed in a Δ -test, and these failures are repaired immediately. After a Δ -test, no type a failure exist, but there may be type b failures.

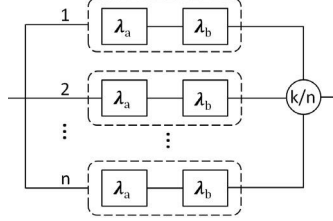


Figure 2: Reliability block diagram for a *koon* system subject to Δ -testing

- A type *b* failure is not at all affected by Δ -tests, i.e., neither Δ -tests nor the following repair would detect and repair type *b* failures.
- The test and repair time are negligible and the effect of DD-failures is not considered.
- The effect from a real demand functioning as a test is not considered.
- We assume that a CCF takes down all channels of the subsystem, and use the beta-factor model for CCF modeling.
- When a type *a* or a type *b* failure occurs, the channel is in a dangerously failed state.

3.2. Formulas for independent DU-failures

When all DU-failures are independent, the reliability of a *koon* system, subject to both Δ -testing and proof testing, with type *a* and type *b* failures, may be modeled by a reliability block diagram as shown in Fig. 2.

The PFD_{avg} in the interval $[0, \tau]$ is equal to the average safety unavailability in this interval

$$\text{PFD}_{\text{avg}} = \frac{1}{\tau} \int_0^{\tau} \bar{A}(t) dt = \frac{1}{\tau} \sum_{i=1}^m \int_{t_{i-1}}^{t_i} \bar{A}(t) dt \quad (1)$$

where t_i is the time of the i -th Δ -test for $i = 1, \dots, m-1$, t_m is the time of a proof test, $t_0 = 0$, and $\bar{A}(t)$ is the safety unavailability function of the subsystem at time t .

In the first interval $[t_0, t_1]$, the subsystem is assumed to be fully functioning at time $t_0 = 0$, and

the safety unavailability function is equal to the unreliability function of a *koon* system

$$\bar{A}(t) = F^{koon}(t)$$

where $F^{koon}(t)$ is the unreliability (i.e., cumulative distribution) function of a *koon* system at time t .

In the interval $(t_{i-1}, t_i]$ for $i = 2, 3, \dots, m$, the subsystem may or may not be in a fully functioning state at the beginning of the interval. The safety unavailability function is therefore not equal to the unreliability function of a *koon* system. At time t_{i-1} , a Δ -test has just been completed and no type a failure can exist. But the subsystem may have a random number of type b failures at t_{i-1} . This random number is denoted N_b and takes value in $i = 2, 3, \dots, n$. The safety unavailability function $\bar{A}(t)$ in $(t_{i-1}, t_i]$ can be conditioned on the number of type b failures at t_{i-1}

$$\bar{A}(t) = \sum_{j=0}^n \Pr(N_b = j \mid t_{i-1}) \bar{A}(t \mid N_b = j, t_{i-1})$$

where $\Pr(N_b = j \mid t_{i-1})$ is the probability of having j type b failures at t_{i-1} , and $\bar{A}(t \mid N_b = j, t_{i-1})$ is the safety unavailability function of a *koon* system in the interval $(t_{i-1}, t_i]$, $i = 2, 3, \dots, m$, given j type b failures (j channels have DU-failure) at t_{i-1} .

Since all the channels are independent and identical, the probability of having j type b failures at t_{i-1} follows a binomial distribution. Since the channels have constant failure rate, the probability is [15]

$$\Pr(N_b = j \mid t_{i-1}) = \binom{n}{j} (1 - e^{-\lambda_b t_{i-1}})^j (e^{-\lambda_b t_{i-1}})^{n-j}$$

When there are j type b failures at t_{i-1} and $j > n - k$, the *koon* system is failed (unavailable) in the interval $(t_{i-1}, t_i]$ for $i = 2, 3, \dots, m$.

$$\bar{A}(t \mid N_b = j, t_{i-1}) = 1 \quad \text{for } j > n - k$$

Otherwise, if $j \leq n - k$, the *koon* system is degraded to a *koo*($n - j$) system. This means that $n - j$ channels can fail in the interval $(t_{i-1}, t_i]$, $i = 2, 3, \dots, m$. When more than $n - j - k$ of them fail,

the subsystem is failed. The unavailability function of this subsystem is equal to the unreliability function of a $koo(n-j)$ system.

$$\bar{A}(t | N_b = j, t_{i-1}) = F^{koo(n-j)}(t | t_{i-1}) \quad \text{for } j \leq n-k$$

where $F^{koo(n-j)}(t | t_{i-1})$ is the unreliability function of a $koo(n-j)$ at time t , given it has survived to time t_{i-1} .

The PFD_{avg} in the interval $(t_{i-1}, t_i]$ is then

$$\begin{aligned} \text{PFD}_{\text{avg}_i} &= \frac{1}{\tau_i} \int_{t_{i-1}}^{t_i} \bar{A}(t) dt = \frac{1}{\tau_i} \int_{t_{i-1}}^{t_i} \sum_{j=0}^n \Pr(N_b = j | t_{i-1}) \bar{A}(t | N_b = j, t_{i-1}) dt \\ &= \frac{1}{\tau_i} \int_{t_{i-1}}^{t_i} \left(\sum_{j=0}^{n-k} \binom{n}{j} (1 - e^{-\lambda_b t_{i-1}})^j (e^{-\lambda_b t_{i-1}})^{n-j} F^{koo(n-j)}(t | t_{i-1}) + \sum_{j=n-k+1}^n \binom{n}{j} (1 - e^{-\lambda_b t_{i-1}})^j (e^{-\lambda_b t_{i-1}})^{n-j} \right) dt \\ &= \sum_{j=0}^{n-k} \binom{n}{j} \frac{1}{\tau_i} \int_{t_{i-1}}^{t_i} (1 - e^{-\lambda_b t_{i-1}})^j (e^{-\lambda_b t_{i-1}})^{n-j} F^{koo(n-j)}(t | t_{i-1}) dt \\ &\quad + \sum_{j=n-k+1}^n \binom{n}{j} \frac{1}{\tau_i} \int_{t_{i-1}}^{t_i} (1 - e^{-\lambda_b t_{i-1}})^j (e^{-\lambda_b t_{i-1}})^{n-j} dt \end{aligned}$$

Given that the i -th Δ -test interval is $\tau_i = t_i - t_{i-1}$ and given the memoryless property of components with constant failure rate [15], we have

$$\text{PFD}_{\text{avg}_i} = \sum_{j=0}^{n-k} \binom{n}{j} (1 - e^{-\lambda_b t_{i-1}})^j (e^{-\lambda_b t_{i-1}})^{n-j} \frac{1}{\tau_i} \int_0^{\tau_i} F^{koo(n-j)}(t) dt + \sum_{j=n-k+1}^n \binom{n}{j} (1 - e^{-\lambda_b t_{i-1}})^j (e^{-\lambda_b t_{i-1}})^{n-j} \quad (2)$$

For a $koon$ system with no test in the interval $(t_{i-1}, t_i]$, if the subsystem is fully functioning at t_{i-1} , the PFD_{avg} ($\text{PFD}_{\text{avg}_i, \text{basic}}^{koon}$) in $(t_{i-1}, t_i]$ is calculated, according to [4], by

$$\text{PFD}_{\text{avg}_i, \text{basic}}^{koon} = \frac{1}{\tau_i} \int_{t_{i-1}}^{t_i} F^{koon}(t | t_{i-1}) dt = \frac{1}{\tau_i} \int_0^{\tau_i} F^{koon}(t) dt \approx \frac{n!(\lambda \tau_i)^{n-k+1}}{(n-k+2)!(k-1)!} \quad (3)$$

Inserting (3) for a $koo(n-j)$ system into (2), we have

$$\begin{aligned}
\text{PFD}_{\text{avg}_i} &= \sum_{j=0}^{n-k} \binom{n}{j} (1 - e^{-\lambda_b t_{i-1}})^j (e^{-\lambda_b t_{i-1}})^{n-j} \text{PFD}_{\text{avg}_i, \text{basic}}^{koo(n-j)} + \sum_{j=n-k+1}^n \binom{n}{j} (1 - e^{-\lambda_b t_{i-1}})^j (e^{-\lambda_b t_{i-1}})^{n-j} \\
&\approx \sum_{j=0}^{n-k} \binom{n}{j} (1 - e^{-\lambda_b t_{i-1}})^j (e^{-\lambda_b t_{i-1}})^{n-j} \frac{(n-j)! (\lambda \tau_i)^{n-j-k+1}}{(n-j-k+2)! (k-1)!} \\
&+ \sum_{j=n-k+1}^n \binom{n}{j} (1 - e^{-\lambda_b t_{i-1}})^j (e^{-\lambda_b t_{i-1}})^{n-j} \tag{4}
\end{aligned}$$

The PFD_{avg} in the interval $[0, \tau]$ is then

$$\begin{aligned}
\text{PFD}_{\text{avg}} &= \frac{1}{\tau} \sum_{i=1}^m \int_{t_{i-1}}^{t_i} \bar{A}(t) dt = \frac{1}{\tau} \sum_{i=1}^m \tau_i \text{PFD}_{\text{avg}_i} \\
&\approx \frac{1}{\tau} \sum_{i=1}^m \sum_{j=0}^{n-k} \binom{n}{j} \tau_i (1 - e^{-\lambda_b t_{i-1}})^j (e^{-\lambda_b t_{i-1}})^{n-j} \frac{(n-j)! (\lambda \tau_i)^{n-j-k+1}}{(n-j-k+2)! (k-1)!} \\
&+ \frac{1}{\tau} \sum_{i=1}^m \sum_{j=n-k+1}^n \binom{n}{j} \tau_i (1 - e^{-\lambda_b t_{i-1}})^j (e^{-\lambda_b t_{i-1}})^{n-j} \tag{5}
\end{aligned}$$

When $\lambda \tau_i$ and $\lambda_b \tau$ are small (i.e., less than 0.01), the approximations, $1 - e^{-\lambda \tau_i} \approx \lambda \tau_i$, $1 - e^{-\lambda_b t_{i-1}} \approx \lambda_b t_{i-1}$ and $(e^{-\lambda_b t_{i-1}})^{n-j} \approx 1$ can be used. Then (4) and (5) become

$$\text{PFD}_{\text{avg}_i} \approx \sum_{j=0}^{n-k} \binom{n}{j} (\lambda_b t_{i-1})^j \frac{(n-j)! (\lambda \tau_i)^{n-j-k+1}}{(n-j-k+2)! (k-1)!} + \sum_{j=n-k+1}^n \binom{n}{j} (\lambda_b t_{i-1})^j \tag{6}$$

$$\text{PFD}_{\text{avg}} \approx \frac{1}{\tau} \sum_{i=1}^m \sum_{j=0}^{n-k} \binom{n}{j} \tau_i (\lambda_b t_{i-1})^j \frac{(n-j)! (\lambda \tau_i)^{n-j-k+1}}{(n-j-k+2)! (k-1)!} + \frac{1}{\tau} \sum_{i=1}^m \sum_{j=n-k+1}^n \binom{n}{j} \tau_i (\lambda_b t_{i-1})^j \tag{7}$$

Moreover, when the Δ -tests are performed periodically with interval $\tilde{\tau}$, i.e., $\tau_i = \tilde{\tau}$ for all i , $t_i = i \cdot \tilde{\tau}$ and $\tilde{\tau} = \frac{\tau}{m}$; the PFD_{avg} formula is simplified to

$$\text{PFD}_{\text{avg}} \approx \frac{1}{m} \sum_{i=1}^m \sum_{j=0}^{n-k} \binom{n}{j} ((i-1) \lambda_b \tilde{\tau})^j \frac{(n-j)! (\lambda \tilde{\tau})^{n-j-k+1}}{(n-j-k+2)! (k-1)!} + \frac{1}{m} \sum_{i=1}^m \sum_{j=n-k+1}^n \binom{n}{j} ((i-1) \lambda_b \tilde{\tau})^j \tag{8}$$

3.3. Partial verification

This section verifies the proposed formulas by: (1) Comparing the formulas for special cases with widely accepted formulas and (2) comparing, for an example, numerical results with the existing results.

3.3.1. Without Δ -tests

When there is no Δ -test, the only test is the proof test at time τ (i.e., $m=1$ and $\tau_1=\tau$); and $j=0$ since it is assumed there is no failure at time 0. The PFD_{avg} in the interval $[0, \tau]$ by (7) becomes

$$\text{PFD}_{\text{avg}} \approx \frac{n!(\lambda\tau)^{n-k+1}}{(n-k+2)!(k-1)!} \quad (9)$$

This is identical to the PFD_{avg} formula in Rausand and Høyland [15] for a *koon* system with proof test interval τ .

3.3.2. Periodic Δ -tests for 1oo1 systems

For a subsystem, where $m-1$ periodic Δ -tests are conducted with interval $\tilde{\tau}$ in each periodic proof test interval τ , $\tau = m\tilde{\tau}$. For a 1oo1 system, inserting $k=1$ and $n=1$ into (8), we obtain

$$\begin{aligned} \text{PFD}_{\text{avg}} &\approx \frac{1}{m} \sum_{i=1}^m \left(\frac{\lambda\tilde{\tau}}{2} + \lambda_b(i-1)\tilde{\tau} \right) = \frac{(\lambda_a + \lambda_b)\tilde{\tau}}{2} - \lambda_b\tilde{\tau} + \frac{1}{m} \sum_{i=1}^m \lambda_b i\tilde{\tau} \\ &= \frac{\lambda_a\tilde{\tau}}{2} - \frac{\lambda_b\tilde{\tau}}{2} + \frac{\lambda_b\tilde{\tau}(m+1)}{2} = \frac{\lambda_a\tilde{\tau}}{2} + \frac{\lambda_b m\tilde{\tau}}{2} = \frac{\lambda_a\tilde{\tau}}{2} + \frac{\lambda_b\tau}{2} \\ &= \frac{\theta\lambda\tilde{\tau}}{2} + \frac{(1-\theta)\lambda\tau}{2} \end{aligned} \quad (10)$$

The result in (10) corresponds to the formulas in Lundteigen and Rausand [13] and Summers and Zachary [17] for 1oo1 systems with Δ -test interval $\tilde{\tau}$ and proof test interval τ .

3.3.3. Numerical example

A set of PFD_{avg} formulas are given for *koon* systems subject to Δ -tests without CCFs in Brissaud et al. [1]; and a case example is presented. We apply the proposed formulas (5&7) to the same case, and compare the result with the one in Brissaud et al. [1]. The subsystem configuration

Table 1: Parameters for the numerical example—adopted from Brissaud et al. [1]

| Property | Parameter | Value |
|-------------------------|----------------|--------------------|
| Configuration | <i>koon</i> | 2oo5 |
| Failure rate | λ | 10^{-5} per hour |
| ΔTC | θ | 0.5 |
| Δ -test interval | $\tilde{\tau}$ | 2190 hours |
| proof test interval | τ | 8760 hours |

Table 2: PFD_{avg} results from different formulas.

| ΔTC | Brissaud et al. [1] | Proposal (5) | Proposal (7) |
|--------------|----------------------|----------------------|----------------------|
| $\theta=0.5$ | $6.61 \cdot 10^{-6}$ | $6.73 \cdot 10^{-6}$ | $7.44 \cdot 10^{-6}$ |

and relevant data are from Brissaud et al. [1] and given in Table 1. PFD_{avg} results from different formulas are given in Table 2. It can be seen that (5) gives a result rather close to Brissaud et al. [1], whereas the result from (7) is overly conservative. This shows that the approximation in (7) is not suitable, because in the current example, $\lambda\tilde{\tau} \approx 0.02$ and $\lambda_b\tau \approx 0.09$, using approximations $1-e^{-\lambda\tau_i} \approx \lambda\tau_i$, $1-e^{-\lambda_b t_{i-1}} \approx \lambda_b t_{i-1}$ and $(e^{-\lambda_b \tau_{i-1}})^{n-j} \approx 1$ will give a conservative result.

4. Formulas including CCFs

The CCFs are included in the PFD_{avg} by the beta-factor model, and the CCFs are included as a virtual component in series with the independent subsystem in Fig. 1. The two failure modes (type *a* and *b*) may have different β -factors, e.g., for valves, type *a* failure may be failure to close (FTC) and type *b* failure may be leak in closed position (LCP), the β of FTC is usually different from the β of LCP. In order not to lose generality, β_a and β_b are used to differentiate the CCF of type *a* and *b* failures. The reliability block diagram of the *koon* system is now as shown in Fig. 3. The total PFD_{avg} can be calculated by

$$PFD_{avg,total} \approx PFD_{avg} + PFD_{avg,a}^{CCF} + PFD_{avg,b}^{CCF}$$

where PFD_{avg} is the independent failure contribution—calculated by (5) for the *koon* system, and $PFD_{avg,a}^{CCF}$ and $PFD_{avg,b}^{CCF}$ are the respective CCF contributions from type *a* and *b* failures, calculated

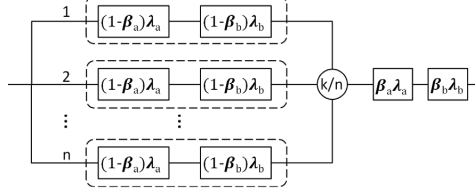


Figure 3: Reliability block diagram of a koon system subject to Δ -test and CCFs.

by (5) for a lool system.

Replacing λ and λ_b in (5) with $\beta_a \lambda_a$ and 0, respectively, for a lool system, the CCF contribution from type a failures is obtained

$$\text{PFD}_{\text{avg},a}^{\text{CCF}} \approx \frac{1}{\tau} \sum_{i=1}^m \frac{\beta_a \lambda_a \tau_i^2}{2}$$

Replacing both λ and λ_b in (5) with $\beta_b \lambda_b$ for a lool system, the CCF contribution from type b failures is obtained

$$\text{PFD}_{\text{avg},b}^{\text{CCF}} \approx \frac{1}{\tau} \sum_{i=1}^m \left(\frac{\beta_b \lambda_b \tau_i^2 e^{-\beta_b \lambda_b \tau_{i-1}}}{2} + (1 - e^{-\beta_b \lambda_b \tau_{i-1}}) \tau_i \right)$$

Therefore, the formula for total PFD_{avg} in interval $[0, \tau]$ is

$$\begin{aligned} \text{PFD}_{\text{avg},\text{total}} &\approx \frac{1}{\tau} \sum_{i=1}^m \sum_{j=0}^{n-k} \binom{n}{j} \tau_i (1 - e^{-(1-\beta_b)\lambda_b \tau_{i-1}})^j (e^{-(1-\beta_b)\lambda_b \tau_{i-1}})^{n-j} \frac{(n-j)! [((1-\beta_a)\lambda_a + (1-\beta_b)\lambda_b)\tau_i]^{n-j-k+1}}{(n-j-k+2)!(k-1)!} \\ &+ \frac{1}{\tau} \sum_{i=1}^m \sum_{j=n-k+1}^n \binom{n}{j} \tau_i (1 - e^{-(1-\beta_b)\lambda_b \tau_{i-1}})^j (e^{-(1-\beta_b)\lambda_b \tau_{i-1}})^{n-j} \\ &+ \frac{1}{\tau} \sum_{i=1}^m \frac{\beta_a \lambda_a \tau_i^2}{2} + \frac{1}{\tau} \sum_{i=1}^m \left(\frac{\beta_b \lambda_b \tau_i^2 e^{-\beta_b \lambda_b \tau_{i-1}}}{2} + (1 - e^{-\beta_b \lambda_b \tau_{i-1}}) \tau_i \right) \end{aligned} \quad (11)$$

When $\beta_b \lambda_b \tau_{i-1}$ is small, the approximations, $1 - e^{-\beta_b \lambda_b \tau_{i-1}} \approx \beta_b \lambda_b \tau_{i-1}$ and $e^{-\beta_b \lambda_b \tau_{i-1}} \approx 1$ can be used, and $\text{PFD}_{\text{avg},b}^{\text{CCF}}$ becomes

$$\text{PFD}_{\text{avg},b}^{\text{CCF}} \approx \frac{1}{\tau} \sum_{i=1}^m \left(\frac{\beta_b \lambda_b \tau_i^2}{2} + \beta_b \lambda_b \tau_{i-1} \tau_i \right)$$

Together with the conditions that $(1 - \beta_b)\lambda_b\tau_i$ and $(1 - \beta_b)\lambda_b t_{i-1}$ are small, the formula for total PFD_{avg} becomes

$$\begin{aligned}
\text{PFD}_{\text{avg,total}} &\approx \frac{1}{\tau} \sum_{i=1}^m \sum_{j=0}^{n-k} \binom{n}{j} \tau_i ((1 - \beta_b)\lambda_b t_{i-1})^j \frac{(n-j)! [((1 - \beta_a)\lambda_a + (1 - \beta_b)\lambda_b)\tau_i]^{n-j-k+1}}{(n-j-k+2)!(k-1)!} \\
&+ \frac{1}{\tau} \sum_{i=1}^m \sum_{j=n-k+1}^n \binom{n}{j} \tau_i [(1 - \beta_b)\lambda_b t_{i-1}]^j \\
&+ \frac{1}{\tau} \sum_{i=1}^m \frac{\beta_a \lambda_a \tau_i^2}{2} + \frac{1}{\tau} \sum_{i=1}^m \left(\frac{\beta_b \lambda_b \tau_i^2}{2} + \beta_b \lambda_b t_{i-1} \tau_i \right) \tag{12}
\end{aligned}$$

When the β -s for type a and b failures are identical, i.e., $\beta_a = \beta_b = \beta$, the total PFD_{avg} is simplified to

$$\begin{aligned}
\text{PFD}_{\text{avg,total}} &\approx \frac{1}{\tau} \sum_{i=1}^m \sum_{j=0}^{n-k} \binom{n}{j} \tau_i ((1 - \beta)\lambda_b t_{i-1})^j \frac{(n-j)! ((1 - \beta)\lambda_b \tau_i)^{n-j-k+1}}{(n-j-k+2)!(k-1)!} \\
&+ \frac{1}{\tau} \sum_{i=1}^m \sum_{j=n-k+1}^n \binom{n}{j} \tau_i ((1 - \beta)\lambda_b t_{i-1})^j \\
&+ \frac{1}{\tau} \sum_{i=1}^m \left(\frac{\beta \lambda_b \tau_i^2}{2} + \beta \lambda_b t_{i-1} \tau_i \right) \tag{13}
\end{aligned}$$

5. Case study

Shutdown systems are among the most used SISs in the process industry. Experience has shown that about 50% of the shutdown system failures are due to the failure of final elements – the shutdown valves [6]. It is therefore important to improve the reliability (availability) of these valves. PST is sometimes implemented to fulfill this purpose. The main DU-failure modes for a shutdown valve are FTC and LCP [6]. A PST may detect FTC failures but not LCP failures, whereas a proof test can detect both failure modes. Therefore, an FTC failure is a type a failure, and an LCP failure is a type b failure. To calculate the PFD_{avg} of the shutdown valves, the formulas proposed in this article can be used.

We consider valves connected in a 1oo2 configuration. The relevant parameters are given

Table 3: Parameters for shutdown valves.

| Property | Parameter | Value |
|-------------------------|-----------|------------------------------|
| Configuration | $koon$ | 1002 |
| Failure rate | λ | $0.8 \cdot 10^{-6}$ per hour |
| CCF of type a failure | β_a | 0.05 |
| CCF of type b failure | β_b | 0.1 |
| ΔTC | θ | 0.65 |
| proof test interval | τ | 8760 hours |

Table 4: PFD_{avg} of valves with different PST strategies.

| PST strategy | Proposal (11) | Proposal (12) |
|----------------|----------------------|----------------------|
| Monthly PST | $1.44 \cdot 10^{-4}$ | $1.44 \cdot 10^{-4}$ |
| Quarterly PST | $1.54 \cdot 10^{-4}$ | $1.54 \cdot 10^{-4}$ |
| Biannually PST | $1.86 \cdot 10^{-4}$ | $1.86 \cdot 10^{-4}$ |
| Without PST | $3.64 \cdot 10^{-4}$ | $3.64 \cdot 10^{-4}$ |

in Table 3. The total failure rate is from the PDS data handbook [5]. The ΔTC is adopted from Lundteigen and Rausand [13]. Different failure modes are due to different causes and mechanisms, thus different β -factors are assumed for type a and b failures. The proof test interval is set to be a year.

PFD_{avg} of shutdown valves subject to different PST strategies are calculated by using (11) and (12) and given in Table 4. It is seen that formula (12) gives approximately the same result as (11). We also observe that the PFD_{avg} is significantly reduced (by 50%) with a biannual PST, whereas further increased PST frequency brings less significant PFD_{avg} reduction. It is therefore important to select a cost-effective PST strategy; the proposed formulas may be an adequate tool for this purpose.

6. Concluding remarks

In this article, we have studied the reliability of a low-demand SIS subject to both proof testing and intermediate partial testing called Δ -testing. Simplified formulas are developed to calculate the PFD_{avg} for $koon$ systems with identical channels. Both periodic and non-periodic Δ -testing are covered and special attention is given to including CCFs. The proposed formulas are compared

with existing formulas for specific cases, and give similar results. A case study of shutdown valves is presented. CCFs are modeled by the beta-factor model and it is shown that different beta-factors for different failure modes are well taken care of by the proposed formulas. Decision-making related to Δ -testing strategies can benefit from the proposed formulas.

The proposed formulas are presented for a situation where Δ -testing and proof testing are applied to detect failures. The formulas can also be used to calculate PFD_{avg} for a *koon* system in a more general situation, where a fixed period of time (after which the subsystem is renewed) is considered and a non-perfect testing technique is applied (periodically or non-periodically) to detect the DU-failure. For example, a subsystem subject to non-perfect proof testing and periodic overhaul.

7. Acknowledgments

The authors would like to thank the reviewers of this article for well-considered and helpful inputs and comments.

References

- [1] Brissaud, F., Barros, A., Berenguer, C., 2012. Probability of failure on demand of safety systems: impact of partial test distribution. *Journal of Risk and Reliability* 226(4), 426–436.
- [2] Fleming, K. N., Mosleh, A., Deremer, R. K., 1985. A systematic procedure for the incorporation of common cause events into risk and reliability models. *Nuclear Engineering and Design* 93 (3), 245–273.
- [3] Guo, H., Yang, X., 2007. A simple reliability block diagram method for safety integrity verification. *Reliability Engineering and System Safety* 92 (9), 1267–1273.
- [4] Hauge, S., Lundteigen, M. A., Hokstad, P., Håbrekke, S., 2010. Reliability prediction method for safety instrumented systems. SINTEF, Trondheim.
- [5] Hauge, S., Onshus, T., 2010. Reliability data for safety instrumented systems. SINTEF, Trondheim.
- [6] Hoekstra, B., 2005. Safety integrity – not only a matter of reliable hardware. *Business Briefing: Exploration and Production: The Oil and Gas Review*, 114–117.
- [7] Hokstad, P., Rausand, M., 2008. Common cause failure modeling: Status and trends. In: Misra, K. B. (Ed.), *Handbook of Performability Engineering*. Springer, London, Ch. 39, pp. 621–640.
- [8] IEC 61508, 2010. Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems. Part 1-7. International Electrotechnical Commission, Geneva.

- [9] IEC 61511, 2003. Functional safety: safety instrumented systems for the process industry sector, part 1-3. International Electrotechnical Commission, Geneva.
- [10] Innal, F., 2008. Contribution to modelling safety instrumented systems and to assessing their performance critical analysis of IEC 61508 standard. Ph.D. thesis, University of Bordeaux, France.
- [11] Jin, H., Lundteigen, M. A., Rausand, M., 2011. Reliability performance of safety instrumented systems: A common approach for both low-and high-demand mode of operation. *Reliability Engineering and System Safety* 96, 365–373.
- [12] Langeron, Y., Barros, A., Grall, A., Berenguer, C., 2008. Combination of safety integrity levels (SILs): A study of IEC 61508 merging rules. *Journal of Loss Prevention in the Process Industries* 21 (4), 437 – 449.
- [13] Lundteigen, M. A., Rausand, M., 2008. Partial stroke testing of process shutdown valves: How to determine the test coverage. *Journal of Loss Prevention in the Process Industries* 21 (6), 579–588.
- [14] Lundteigen, M. A., Rausand, M., 2009. Reliability assessment of safety instrumented systems in the oil and gas industry: A practical approach and a case study. *International Journal of Reliability, Quality, and Safety Engineering* 16, 187–212.
- [15] Rausand, M., Høyland, A., 2004. *System Reliability Theory; Models, Statistical Methods, and Applications*, 2nd Edition. Wiley, Hoboken, NJ.
- [16] Rouvroye, J., Van den Bliet, E., 2002. Comparing safety analysis techniques. *Reliability Engineering and System Safety* 75 (3), 289 – 294.
- [17] Summers, A., Zachary, B., 2000. Partial-stroke testing of safety block valves. *Control Engineering* 47 (12), 87–89.
- [18] Torres-Echeverria, A., Martorell, S., Thompson, H., 2009. Modelling and optimization of proof testing policies for safety instrumented systems. *Reliability Engineering and System Safety* 94, 838 – 854.

Article 3 (journal)

Reliability modeling of safety-instrumented systems by Petri nets
–Submitted to *Reliability Engineering and System Safety*

Is not included due to copyright

Article 4 (journal)

Reliability performance of safety-instrumented systems: A common approach for both low- and high-demand mode of operation
–In *Reliability Engineering and System Safety*



Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Reliability performance of safety instrumented systems: A common approach for both low- and high-demand mode of operation

Hui Jin ^{*}, Mary Ann Lundteigen, Marvin Rausand

Department of Production and Quality Engineering, Norwegian University of Science and Technology, NO 7491 Trondheim, Norway

ARTICLE INFO

Article history:

Received 5 July 2010
 Received in revised form
 15 November 2010
 Accepted 20 November 2010
 Available online 25 November 2010

Keywords:

Markov model
 Safety instrumented systems
 High-demand
 Hazardous event frequency
 Demand rate

ABSTRACT

Safety instrumented systems (SISs) are usually divided into two modes of operation, low-demand and high-demand. Unfortunately, this classification is not easy to justify and the available formulas that are used to quantify the reliability performance in these two modes of operation are unable to capture combined effects of functional testing, spurious activations, and successful responses to demands. This article discusses some important modeling issues for SIS reliability performance quantification, and demonstrates their implementation in a Markov model. The accuracy of the Markov model for a simple case study of a pressure transmitter is verified through comparison with a scenario-based formula, and it is shown that the Markov approach gives a sufficiently accurate result for all demand rates, covering both low- and high-demand modes of operation.

© 2010 Elsevier Ltd. All rights reserved.

1. Introduction

Safety instrumented systems (SISs) are widely used to prevent hazardous events, and to mitigate their consequences to humans, the environment, and material and financial assets. A SIS generally consists of one or more input elements (e.g., sensors, transmitters), one or more logic solvers (e.g., programmable logic controllers [PLC], relay logic systems), and one or more final elements (e.g., safety valves, circuit breakers). The main elements of a SIS are illustrated in Fig. 1.

The required functionality and reliability of a SIS are usually deduced from overall hazard and risk analyses. Without proper design, construction, and follow-up, the SIS may fail to provide the necessary risk reduction and a number of standards and guidelines have been developed to assist in designing and implementing SISs. One such standard is IEC 61508 [6], that outlines key requirements to all phases of the SIS life cycle. The principles introduced in this generic standard, are also reflected in application specific standards, such as IEC 61511 [7] for the process industry, IEC 62425 [8] for the railway industry, and ISO/DIS 26262 [11] for the automobile industry.

IEC 61508 differentiates between two modes of SIS operation: low-demand and high-demand. The classification of operational modes is based on two criteria: (1) How often the SIS is expected to operate in response to demands? (2) The expected time that a failure may remain unrevealed, taking into account the functional

test frequency. According to IEC 61508, a SIS is operating in the high-demand mode if the demand rate is greater than once per year, or greater than twice the frequency of functional tests. If the demands occur close to continuously, the mode of operation is sometimes referred to as continuous, rather than high-demand. In the rest of this article, high-demand also covers the continuous mode of operation, unless otherwise stated. When the demand rate is less than once per year, and less than twice the functional test frequency, the SIS is operating in low-demand mode. Typical high-demand SISs are dynamic positioning (DP) systems for ships and offshore platforms, anti-lock braking systems (ABS) for automobiles, and railway signaling systems, whereas typical low-demand SISs include emergency shutdown systems (ESD), fire and gas detection systems, process shutdown systems (PSD), and airbag systems in automobiles.

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 [15]. A railway signaling system may, for example, set a green (go) signal if the following rail section is free, and a red signal if this rail section is occupied. According to IEC 61508, a safety integrity level (SIL) should be allocated to each SIF. The standard defines four SILs, where SIL 4 gives the highest and SIL 1 the lowest requirements. In order to claim that a SIF has a certain SIL, it is necessary to achieve a certain reliability. IEC 61508 defines two reliability measures for this purpose: (i) the average probability of failure on demand (PFD) and (ii) the probability of failure per hour (PFH), and suggests using PFD as a reliability measure for low-demand SISs and PFH for high-demand SISs. The SIL ranges for PFD and PFH specified by IEC 61508 are given in Table 1.

^{*} Corresponding author.

E-mail address: hui.jin@ntnu.no (H. Jin).

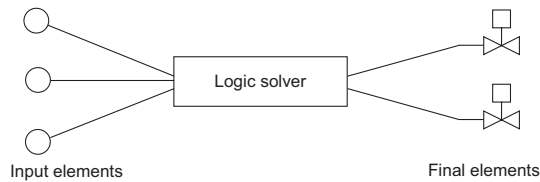


Fig. 1. The main SIS elements.

Table 1
SIL requirements [6].

| SIL | PDF | PFH |
|-----|-------------------------------|-------------------------------|
| 4 | $\geq 10^{-5}$ to $< 10^{-4}$ | $\geq 10^{-9}$ to $< 10^{-8}$ |
| 3 | $\geq 10^{-4}$ to $< 10^{-3}$ | $\geq 10^{-8}$ to $< 10^{-7}$ |
| 2 | $\geq 10^{-3}$ to $< 10^{-2}$ | $\geq 10^{-7}$ to $< 10^{-6}$ |
| 1 | $\geq 10^{-2}$ to $< 10^{-1}$ | $\geq 10^{-6}$ to $< 10^{-5}$ |

It is generally accepted that PFD is a meaningful reliability measure for a low-demand SIS, but there are different opinions about the adequacy of the PFH for a high-demand SIS [1,14].

Despite the presumably clear split between the low-demand and the high-demand mode of operation, there are still some issues that cause confusion and problems in the quantification of SIS reliability performance. First, the rationale behind using once per year or twice the frequency of functional tests as the borderline is not well explained in IEC 61508, or anywhere else [10]. Second, for some SIFs, the various elements have different demand rates. Parts of the logic solver may, for example, be operated more often than the input and final elements, making it difficult to define the mode of operation. Third, the classification disregards the aspect of the demand duration. Even for rare demands, the demand, once it occurs, may give “sub-demands” during an extended period of time. The SIS may therefore be in the low-demand mode between demands, and in the high-demand mode while responding to the demand. A typical example is a blow-out preventer (BOP) that is used to stop uncontrolled flow from oil wells during drilling. Situations that call for full closure of the BOP are rare, but when the BOP has been activated, it must be able to withstand the well pressure for hours and even weeks. Neither the classification nor the proposed reliability performance measure for high demand systems, the PFH, are able to treat these issues.

Instead of drawing a clear borderline between low-demand mode and high-demand mode of operation, some authors suggest to incorporate the rate of demands into the analysis by using Markov modeling [1,14,10]. The interpretation of PFH is questioned by the same authors, and a common measure for use with both low-demand and high-demand mode is suggested [1,14]. Bukowski [1] calculates the probability of being in a state “of fail dangerous and process requires shutdown” (PFDPRS) based on a Markov model, while Misumi and Sato [14] use fault tree analysis to develop analytical formulas for what they call the “average hazardous event frequency”. These proposals are promising for the quantification of SIS reliability performance in general, but need further development to reflect all relevant modeling aspects.

The objectives of this article are to (i) clarify important modeling aspects for low-demand and high-demand SISs, (ii) summarize and discuss some of the key limitations related to measures like PFD and PFH, and (iii) suggest and verify a Markov model for quantification of SIS reliability performance that caters for modeling considerations in both low-demand and high-demand mode of operation.

The rest of the article is organized as follows. Section 2 discusses a number of important modeling issues and Section 3 highlights some of the weaknesses of PFD and PFH, in light of the modeling issues that are addressed in Section 2. The model, which is based on a Markov transition diagram, is presented in Section 4. In Section 5, a scenario-based model for SIS reliability performance assessment is developed and the applicability of the Markov model is demonstrated through a simple case study of a pressure transmitter, and by comparison with the scenario-based model. Finally, concluding remarks are given in Section 6.

2. Modeling considerations

The starting point of a reliability performance analysis of a SIS is always to acquire knowledge about the system, under which modes and conditions it will operate, and how the system should respond to system failures and other foreseeable events. In this article, the system comprises both the SIS and the system to be protected, which is sometimes referred to as the equipment under control (EUC) [6]. Important issues to address are, for example, the nature of the demands, the desired states for the various operating modes, such as start-up, normal operation, shutdowns, and foreseeable abnormal events.

The following list of questions should be addressed in the quantification of the SIS reliability performance:

- What is the safe state, i.e., the desired state of the EUC in response to a hazardous event or a SIS failure?
- Where in the sequence of protection layers is the SIS placed?
- What type of hazardous events may occur if the SIS, and subsequent protection layers, fail to perform on demand?
- What is the testing strategy for the SIS?
- What are the potential consequences of spurious activations, on the EUC and on the SIS components?
- What are the demand rate and the demand duration?

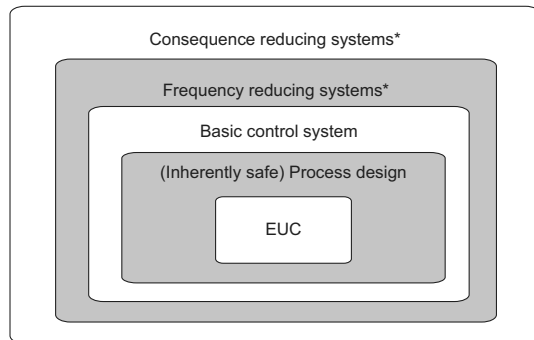
In addition, it is important to identify the main properties of the SIS, by reviewing the component functions and their interrelationship, such as architecture and voting.

2.1. Definition of safe state

The SIS must be designed to take the EUC to a safe state in response to a demand. Unfortunately, it is not always straightforward to define the safe state, and the EUC may have different safe states during normal operation, compared to start-up, shutdown, and so on. In some cases, the safe state is to maintain the state before the demand occurred, while in other cases, it means to stop the EUC. When the safe state is defined, the SIS design must also consider “fail-safe” operation, meaning that the SIS automatically takes the EUC to a safe state in response to foreseeable SIS failures, such as loss of power supply and loss of signal.

Some SISs, like the ones we mentioned above as examples of high-demand systems, return the EUC to the normal operating state after the demand. This is, for example, the case for a DP system where external forces (e.g., wave forces) are acting on one side of an offshore platform, and the DP system is required to maintain its position by imposing compensating thrust force on the other side of the platform. When the external forces disappear, the DP system returns to a state where it is ready to respond to other external forces. A railway signaling system is always ready to respond to a new request when the previous train has left the rail section.

For the SISs that we mentioned as typical low-demand systems, it is common that the EUC remains in the safe state after the SIS has responded to a demand. The SIS is only reset when a decision has



* SIS, mechanical systems, manual intervention, and so on

Fig. 2. Protection layers.

been taken to restart the EUC. In the event of a gas leakage, the ESD system stops the process by closing dedicated ESD valves. The ESD system maintains this state, until the leakage point has been repaired and the operators have decided to restart the EUC. The automatic train protection (ATP) system operates in the same way; if a train has been stopped by the ATP, it is not possible to continue driving unless a decision has been made to suspend the ATP signal and restart the train.

2.2. Sequence of protection layers

Several independent protection layers are often used for the same EUC, to ensure that the desired risk reduction is achieved. ATP and railway signaling systems are examples of two independent protection layers used to avoid train accidents. Protection layers may also be implemented by physical barriers, pure mechanical systems, and administrative procedures.

The “onion model” in Fig. 2 is sometimes used to illustrate the sequence of protection layers [3,7]. The sequence starts from the center and proceeds outwards, first with frequency reducing layers and then with consequence reducing layers. The purpose of the frequency reducing protection layers is to prevent a hazardous event from occurring, for example a gas leakage, while the consequence reducing measures aim to stop the development into accidents (e.g., explosion, fires) involving harm to humans, the environment, or material and financial assets. High-demand SISs are often of the first category, and low-demand of the latter.

In the reliability performance quantification, it is important to take the activation sequence into account. Does the SIS perform a SIF as the last protection layer, or is the function performed as an intermediate layer? If the SIS is used to mitigate the consequences of a hazardous event, and it appears as the last in line, a SIS failure may directly lead to an accident.

2.3. Definition of hazardous event

A hazardous event is sometimes defined as the first significant deviation from the normal situation that may, if not controlled, develop into an accident [15]. As argued above, a high-demand SISs often contributes to reduce the likelihood of such events. For consequence reducing SISs (usually low-demand SISs), it is the accident frequency, and not the hazardous event frequency that is reduced. For simplicity, the approach to reliability performance quantification of SISs, presented in this article, uses the term *hazardous event frequency* (HEF) for both modes of operation, but the reader should be aware of the differences in the interpretation.

Yoshimura and Sato [16] propose three categories of hazardous events, which we adopt in this article: (1) *Repeatable-hazardous event*, where the hazardous event does not necessarily have severe consequences, even if the SIS fails. As an example, consider a car that starts to slide on an icy road. Even if the ABS brakes fail, the car may stay on the road if the driver manages to keep control. The hazardous event may reoccur as long as the hazard (i.e., the icy road) is present. (2) *Renewable fatal hazardous events*, where the consequence of the hazardous event is fatal to the EUC (and the SIS), but not in a way that prevents the systems from being restored within reasonable time. An example is a minor gas leakage that has occurred due to a leaking flange, and where the normal operating state of the production line (and the SIS) is restored after having performed necessary repair, replacements, and overhauls. (3) *Non-renewable fatal hazardous events*, where the damage is extensive, and no recovery is possible. The accident with Deepwater Horizon in the Gulf of Mexico in 2010 is an example of an event of this category.

2.4. Testing strategies

The SIS components are exposed to two main types of failures, safe failures and dangerous failures [6,7]. Safe failures are failures that do not have any effect on the ability of the SIS to perform its functions, or alternatively, that the component goes to its fail-safe state. The latter example is often referred to as a spurious trip or spurious activation [12]. Dangerous failures are failures that may prevent the SIS from performing on demand. The dangerous failures may be further split into two sub-categories: Dangerous detected (DD) failures, that are detected by online diagnostics, and dangerous undetected (DU) failures, that remain hidden until the SIS function is fully operated during a functional test, in a real demand situation, or (in some cases) during a spurious activation.

Functional tests are in many cases performed at regular intervals to reveal and correct DU-failures before a demand occurs. For a low-demand SIS, it is important to perform functional testing to avoid that a DU-failure remains hidden for a long time. The necessity of functional testing for high-demand SISs is not always evident, an issue that is further discussed later in the article.

Diagnostic testing is a feature that is sometimes provided for programmable electronic components. A diagnostic test is able to reveal certain types of failures, such as run-time errors and signal transmission errors, without fully operating the main functions of the component. The diagnostics of a pressure transmitter may reveal drifting in the signal conversion, without the pressure transmitter responding to a high pressure signal.

2.4.1. Effect of functional tests

DU-failures are the main contributors to SIS unreliability, i.e., its inability to perform on demand. In the reliability performance quantification it is important to address the following issues:

- To what extent is the functional test able to reveal all DU-failures?
It is not always practicable or safe to perform a fully realistic functional test of a SIS. To pressurize a pipeline to the trip pressure of a pressure transmitter may, for example, be unsafe, and most pressure transmitters are therefore tested after they have been isolated from the process. Some causes of DU-failures may therefore remain hidden, such as contamination in the pressure sensing lines. The fraction of failures that may be revealed by a functional test is sometimes referred to as the *functional test coverage*.
- To what extent is the functional test necessary?
A high-demand SIS may experience demands more often than it is practical to perform functional tests. It may therefore not be

possible to use functional testing to reveal and correct DU-failures before the next demand. This is not the same as saying that regular functional tests are not necessary for high-demand systems. For a SIS that has redundant components, or where the SIS components receive signals from other systems than the SIS, it is not always possible to confirm that all, and not only some, of the components were functioning as intended. In this situation, it may be important to perform regular testing, to avoid that the SIS is operating with reduced fault tolerance.

- What other events have similar effect as functional testing? Functional testing is usually performed to reveal DU-failures at the component level. A successful response to a demand is also a type of test. The main differences are that a demand is a random event and that the confirmation from successful response is on the system level, rather than the component level—depending on the ability to verify correct reliability performance of each individual component during the demand. A spurious activation of a SIS is also a random event and may verify the function of SIS components. A spurious signal from a pressure transmitter may, for example, cause one or more valves to operate. A spurious activation may not necessarily reveal DU-failures, without careful attention by the operators. Manual checks may be required to verify that all components that should have been affected by the spurious activation, were in fact operated.

2.4.2. Diagnostic testing

Diagnostic testing aims at revealing failures without interrupting the EUC. The fraction of dangerous failures that is revealed by diagnostic testing is often referred to as the *diagnostic coverage* [6,7].

A diagnostic test is run frequently, typically every few seconds, minutes, or few hours. The time delay between the occurrence and the detection of a DD-failure is normally negligible. For a low-demand SIS, this means that there will usually be sufficient time to perform repair and restore the function before the next demand occurs—if the repair is started immediately and completed within a few hours. For a high-demand SIS, the demand rate and the diagnostic test frequency may be of the same order of magnitude, and the validity of this assumption may need to be re-examined.

The effect of diagnostic testing should be carefully considered in light of the demand rate, the diagnostic test coverage, the diagnostic test interval, and the time that is needed to repair the failure.

2.5. Spurious activations

The SIS should be designed to avoid spurious activations, and if a spurious activation occurs, it should bring the EUC to a safe state. This is not always possible and spurious activations may sometimes lead to hazardous events. This is, for example, the case when the airbag system is spurious activated while driving on a motorway. Another problem is that a spurious activation may give very high stresses and thus deteriorate both the SIS and the EUC. An example of this is a downhole safety valve in an oil well. During normal testing, the flow is stopped before the valve is closed and tested. A spurious activation of the valve will be a so-called slam-shut operation where the valve is closed against a flowing well. This operation gives very high stresses to the valve and the valve may not survive more than a few such operations.

Spurious activation of a SIS will normally lead to lost production or low availability of the EUC [12]. Follow-up of spurious activations further takes time and attention from operators and maintenance personnel and human errors may occur during restart of the EUC.

From a reliability perspective, it is noticeable that measures introduced to improve the reliability of a SIS, for example by adding redundancy, will almost inevitably lead to more spurious activations [13].

On the positive side, a spurious activation may serve as a functional test and a confirmation that the SIS was working as intended during a demand-like event. The positive as well as the negative effects should be considered in SIS design and in reliability performance assessments.

2.6. Demand characteristics

All demands have some duration, but the duration may be so short that it can be neglected in the reliability performance analyses. As a result, it is sometimes distinguished between two types of demands: instantaneous demands, with negligible duration, and demands with some duration [14]. Several methods for reliability analysis, such as reliability block diagram and fault tree analysis, are mainly applicable for instantaneous demands.

In reliability performance analyses, it is important to determine if a SIS needs to respond to a demand with duration, as mentioned in the example with the DP system on offshore platforms.

3. HEF versus PFD and PFH

A SIS is used to reduce risk, and IEC 61508 requires that it is demonstrated that the SIS reliability performance is adequate to meet stated risk acceptance criteria. The acceptance criteria are often stated in terms of a maximum tolerable HEF, from which a SIL requirement, and eventually, a PFD or PFH requirement may be deduced [6,7].

3.1. Relationship between HEF and PFD

For a low-demand SIS, HEF is the product of the demand rate, λ_{de} , for the SIS and the conditional probability that the SIS fails to function, PFD, given a demand, such that, $HEF = \lambda_{de} \cdot PFD$ [15]. Note that PFD here should, in principle, cover both the instantaneous activation of the SIS and the successful performance of the SIS during the demand period. An example is a fire pump system that has to start and to pump water as long as it is demanded. In practice, most calculation approaches fail to account for the possibility of having a failure during the demand period.

The PFD is well suited as input parameter to many methods for risk analysis, such as fault tree analysis, event tree analysis, and LOPA [3].

3.2. Relationship between HEF and PFH

Unlike PFD, it is not straightforward to use PFH in traditional risk analysis methods like fault tree analysis, event tree analysis, and LOPA.

For a high-demand SIS, the relationship between HEF and PFH is vague, with the result that several authors give their own interpretations and definitions [9,10,4].

For a SIS operating under (close to) continuous demands, the conditional probability that a demand occurs, given a SIS failure, is very close to 100%. In this case, the HEF is equal to the frequency of dangerous SIS failures, which is PFH. For a SIS operating in high, but not continuous demand mode, it is not easy to calculate the HEF without using a Markov or a similar state model. Intuitively, it may be argued that the HEF in this case is always less than PFH, such that PFH is always a conservative approximation of the HEF, regardless of the demand rate. When the demand rate is close to the borderline between low-demand and high-demand, the approximation

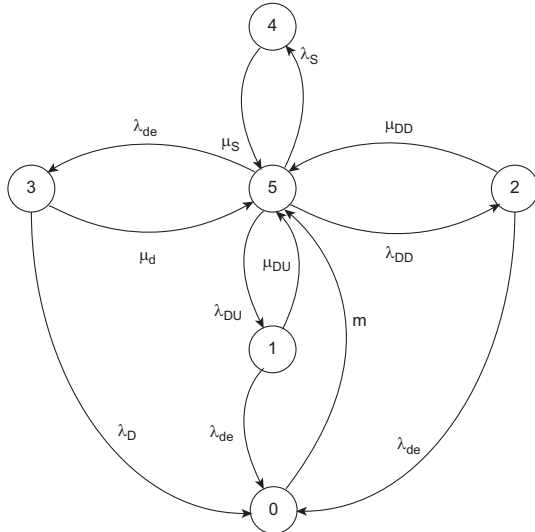


Fig. 3. Markov transition diagram.

may be too conservative. The relationship between PFH and HEF is further complicated when the duration of the demand is significant.

The consequence of having different interpretations of PFH becomes evident in risk analyses. An overall acceptance criterion for a HEF may be broken down to acceptance criteria for the various protection layers. Assume that the acceptance criterion for SIF_j is expressed by using HEF_j, for $j = 1, 2, \dots$. A requirement to HEF_j must then be expressed by PFH_j where:

- For a SIS operating under (close to) continuous demands: $PFH_j \approx HEF_j$.
- For a SIS operating with less frequent demands, for example, close to the borderline between low-demand and high-demand: $PFH_j > HEF_j$.

Remark. IEC 61508 relates each SIL to a fixed range for the PFH. In light of the discussions above, the approach may be questioned since the same PFH may give quite different HEF, depending on the demand rate and the demand duration.

4. A common approach to SISs reliability performance

It is difficult to argue why PFH, and not PFD, should be used as reliability performance measure when the SIS is exposed to demands in the borderline between what IEC 61508 defines as low-demand and high-demand. Why is, for example, the PFD an adequate measure when the demand rate is once every 13 months, but not for once every 11 months? Even for higher demand rates, the PFD may be a well suited measure, but current analytical formulas in, for example, IEC 61508, do not reflect the combined effects of demand rates, demand duration, and functional testing. Some authors propose using a Markov model, which does not distinguish between low- and high-demand mode of operation, for reliability performance quantification of a SIS. This model is well suited for many of the issues mentioned in Section 2 [1,10,16] and is further studied in this article.

4.1. System under consideration

The main difference between a Markov model and the SIS reliability performance quantification methods that are used in IEC 61508 and associated standards and guidelines, is that the demand rate and the demand duration are modeled. To study the main effects of the demand rate and the demand duration, it is sufficient to consider a single SIS component. The state of the EUC is either a non-demand state or a on-demand state. The component under consideration is a single element in a SIS that acts as the last protection layer. The component is subject to functional as well as diagnostic testing. It is assumed that the hazardous event is of the type renewable fatal hazardous event, and that a repair action is needed to return the EUC and the SIS to the normal operating state.

The SIS may be subject to spurious activations. It is assumed that the safe state is when the EUC is stopped. It is further assumed that a spurious activation can only occur if no other failures are present. This assumption may be illustrated for a valve: a valve that is stuck in open position cannot spurious close at the same time. The possibility of having a demand and a spurious activation at the same time is neglected.

4.2. Markov model

A Markov transition diagram for the system is illustrated in Fig. 3, for the system states in Table 2.

The model has six system states, 0,1, . . . ,5, where state 5 is the initial state and state 0 represents the hazardous event/state. If the SIS is not the last protection layer, the hazardous event is a demand for the next barrier.

It is assumed that the system satisfies the Markov property [15], and that all transition rates are constant in time. The failure rates may in practice be different in the various operating states, but this is not accounted for in this article, where the same failure rates are used in on-demand and non-demand states.

The repair rates are also constant, meaning that the DD and DU repair times are exponentially distributed. In reality, the rates are often not constant, but according to Bukkowski [2], this simplification gives reasonable accuracy.

4.2.1. Definition of system states, including safe state

The system includes both the EUC and the SIS. The system state is therefore the combined effect of the SIS state and the demand situation. A SIS has the state “available” when it is able to function if a demand occurs. In this state, the SIS is free from DD- or DU-failures and has not been spurious activated. The SIS is defined as “functioning” when it is responding to a demand. “Safe state” means that the EUC is in a state where it is safe no matter whether there is a demand, or not.

A more specific interpretation of the system states is as follows: State 5 is the normal operating state, where the SIS is available and there is no demand for the activation of the SIS. State 4 represents the safe state, where no hazardous event can happen. The state may

Table 2 System states.

| System state | SIS state | Demand |
|--------------|------------------------------|------------|
| 5 | Available | Non-demand |
| 4 | Safe state | N/A |
| 3 | Functioning | On-demand |
| 2 | DD-failure | Non-demand |
| 1 | DU-failure | Non-demand |
| 0 | Dangerous failure (DU or DD) | On-demand |

Table 3
Markov transition rates.

| Transition rate | Description |
|---|-------------------------------|
| λ_s | Transition rate to safe state |
| μ_s | Restoration rate |
| λ_{de} | Demand rate |
| μ_{de} | Demand duration rate |
| λ_{DD} | DD-failure rate |
| μ_{DD} | DD repair rate |
| λ_{DU} | DU-failure rate |
| μ_{DU} | DU repair time |
| $\lambda_D (= \lambda_{DU} + \lambda_{DD})$ | Dangerous failure rate |
| m | Renewal rate |

be achieved after a spurious activation. State 3 is the state where the SIS is responding to a demand. In state 2, the SIS has a DD-failure while there is no demand for the SIS. State 1 is similar to state 2, but the SIS has a DU- rather than a DD-failure. State 0 is the (renewable) hazardous event, where the SIS has a DU- or DD-failure and there is a demand for the activation of the SIS.

The transition rates and their descriptions are given in Table 3. It is assumed that state 5 is the initial state. The transitions between state 5 and state 4 are due to safe failure and the restoration. The restoration rate μ_s from state 4 to state 5 is calculated as $1/\text{MTTR}_s$, where MTTR_s is the mean restoration time.

4.3. Inclusion of testing strategies

The system is subject to diagnostic testing as well as functional testing. The functional tests are carried out after regular time intervals of length τ .

For DD-failures, it is assumed that a repair action is initiated immediately, such that the downtime due to a DD-failure is limited to the actual repair time. The DD repair rate, μ_{DD} , is therefore calculated from the mean time to repair (MTTR_{DD}) as

$$\mu_{DD} = \frac{1}{\text{MTTR}_{DD}} \quad (1)$$

The downtime due to a DU-failure may be split into an unknown part and a known part. The unknown part is when the DU-failure has not yet been revealed by a test (or demand). If a functional test has identified a DU-failure, the average downtime is equal to $\tau/2$ (e.g., see [15, p. 433]). The mean known downtime is the time to perform a functional test (which is often negligible) and the mean repair time of the DU-failure, MTTR_{DU} . Of the two contributors to the downtime, the unknown part is usually dominating. The DU repair rate, μ_{DU} is therefore calculated as

$$\mu_{DU} = \frac{1}{\tau/2 + \text{MTTR}_{DU}} \quad (2)$$

4.4. Inclusions of demand and hazard event characteristics

The demands are assumed to occur according to a homogeneous Poisson process (HPP) with rate λ_{de} , such that the time between two consecutive demands is exponentially distributed with parameter λ_{de} . The duration of each demand is also assumed to be exponentially distributed with rate μ_{de} . The mean demand duration is therefore $1/\mu_{de}$. It is further assumed that the SIS is "as good as new" after a successful response to a demand.

When a hazardous event occurs (state 0), we assume that the system is restored/renewed to the normal state 5. The renewal time is assumed to be exponentially distributed with rate m .

4.5. Calculations

The Markov model in Fig. 3 is used to calculate the steady state probabilities and visit frequencies for each state. The state transition matrix $\mathbf{A} = \{a_{ij}\}$ is based on the non-zero entries a_{ij} for $i \neq j$ in Fig. 3 and $a_{ii} = -\sum_{j=0}^5 a_{ij}$, $j \neq i$ for $i = 0, 1, \dots, 5$.

The Kolmogorov forward equations [15] give

$$\mathbf{P}(t) \cdot \mathbf{A} = \dot{\mathbf{P}}(t) \quad (3)$$

where $\mathbf{P}(t) = [P_0(t), P_1(t), \dots, P_5(t)]$, $P_i(t)$ is the probability that the system is in state i at time t , and $\dot{\mathbf{P}}(t)$ is the time derivative of $\mathbf{P}(t)$.

For an irreducible Markov process, it can be shown that

$$\lim_{t \rightarrow \infty} P_i(t) = P_i = \text{constant} \quad \text{for } i = 0, 1, \dots, 5 \quad (4)$$

and

$$\lim_{t \rightarrow \infty} \dot{P}_i(t) = 0 \quad \text{for } i = 0, 1, \dots, 5 \quad (5)$$

The steady state probabilities can be calculated from (3)–(5) and the fact that the sum of the steady state probabilities is always equal to 1,

$$\sum_{i=0}^5 P_i = 1 \quad (6)$$

The steady state probability for state i , P_i , is the long-run probability that the system is in state i . P_i can also be interpreted as the mean proportion of time the system is in state i .

The HEF at time t is equal to the visit frequency to state 0, from any other state at time t [15].

$$\text{HEF}(t) = \sum_{i=1}^5 P_i(t) \cdot a_{i0} \quad (7)$$

This means that the HEF for the model in Fig. 3 is equal to

$$\text{HEF}(t) = P_1(t) \cdot \lambda_{de} + P_2(t) \cdot \lambda_{de} + P_3(t) \cdot \lambda_D \quad (8)$$

5. Applicability of the proposed model

This section demonstrates the applicability of the proposed reliability performance model for low-demand as well as high-demand mode of operation. First a scenario-based approach is introduced to calculate the HEF. The accuracy of the HEF calculated by using this scenario-based formula is investigated by comparing it with standard formulas [6] for PFD (for low-demand SIS) and PFH (for high-demand SIS). Thereafter, the HEF calculated by the scenario-based formula is used as the benchmark to demonstrate the applicability and accuracy of the Markov model. This is illustrated through a case study of a *pressure transmitter*. The transmitter is assumed to be an input subsystem of a SIS.

The relevant data is given in Table 4. The failure rates are from the PDS data handbook [5]. Other parameters, such as repair and restoration rates, are based on the authors' judgment.

5.1. Calculation of the HEF by the scenario-based formula

For a single component (a 1oo1 configuration) the HEF can be calculated from a scenario-based formula. Assume that no more than one hazardous event can take place during a functional test interval. For this simple system, we can exhaust the most likely hazardous event scenarios. Three scenarios that may result in a hazardous event are identified.

Assume that the system is put into operation at time $t = 0$. Let the time until a DU-failure be denoted by T_{DU} , the time until a DD-failure by T_{DD} , and the time until a demand by T_{de} . Further, let

Table 4
System specifications.

| Notation | Value |
|------------------------------|-----------------------------|
| λ_{DD} | 3×10^{-7} per hour |
| λ_{DU} | 5×10^{-7} per hour |
| λ_D | 8×10^{-7} per hour |
| λ_s | 5×10^{-7} per hour |
| τ | 6 months |
| Mean repair time (DU and DD) | 8 h |
| Mean restoration time | 1 day |
| Mean renewal time | 7 days |
| Mean demand duration | 12 min |

\tilde{T}_{de} denote the demand duration and \tilde{T}_{DD} the repair time of a DD-failure.

- *Scenario1*: A DU-failure occurs at time t . The demand occurs after the DU-failure, but before the next scheduled functional test at time τ . In this case, the probability of having a hazardous event with scenario 1 (s_1) is

$$P_{s1} = \Pr(T_{DU} < T_{de} \leq \tau) = \int_0^\tau \lambda_{DU} e^{-\lambda_{DU}t} (1 - e^{-\lambda_{de}(\tau-t)}) dt \quad (9)$$

- *Scenario2*: A DD-failure occurs at time t . A demand occurs after the DD-failure and before the failure is repaired. In this case, the probability of having a hazardous event with scenario 2 (s_2) becomes

$$P_{s2} = \Pr(T_{DD} < T_{de} < T_{DD} + \tilde{T}_{DD} \leq \tau) = \int_0^\tau \lambda_{DD} e^{-\lambda_{DD}t} \Pr(t < T_{de} < t + \tilde{T}_{DD} \leq \tau) dt \quad (10)$$

where

$$\Pr(t < T_{de} < t + \tilde{T}_{DD} \leq \tau) = \int_0^{\tau-t} (1 - e^{-\lambda_{de}u}) e^{-\mu_{DD}u} du \quad (11)$$

When the repair time is short, the mean time to repair a DD-failure, τ_{DD} , can be used to calculate the approximate probability of having a demand when repairing a DD-failure, then

$$\Pr(t < T_{de} < t + \tilde{T}_{DD} \leq \tau) \approx 1 - e^{-\lambda_{de}\tau_{DD}} \quad (12)$$

- *Scenario3*: A demand occurs at time t . A dangerous failure occurs during the demand, but before the end of demand. In this case, the probability of having a hazardous event with scenario 3 (s_3) becomes

$$P_{s3} = \Pr(T_{de} < T_D < T_{de} + \tilde{T}_{de} \leq \tau) = \int_0^\tau \lambda_{de} e^{-\lambda_{de}t} \Pr(t < T_D < t + \tilde{T}_{de} \leq \tau) dt \quad (13)$$

where

$$\Pr(t < T_D < t + \tilde{T}_{de} \leq \tau) = \int_0^{\tau-t} (1 - e^{-\lambda_D u}) e^{-\mu_{de}u} du \quad (14)$$

When the demand duration is short, the mean demand duration, τ_{de} , can be used to calculate the approximate probability of having a dangerous failure during a demand, then

$$\Pr(t < T_D < t + \tilde{T}_{de} \leq \tau) \approx 1 - e^{-\lambda_D \tau_{de}} \quad (15)$$

Since two or more of the three scenarios cannot occur at the same time, they are disjoint, and the HEF can be calculated as:

$$HEF = \frac{P_{s1} + P_{s2} + P_{s3}}{\tau} \quad (16)$$

Remark. For scenario 3, there is no strict “upper limit” τ if a demand state is present at time τ . If a demand state is present at time τ , the functional test has to be postponed. This approach is slightly conservative due to the reason that DU- and DD-failures are treated independently.

5.2. The accuracy of the scenario-based formula

In the scenario-based approach, all possible scenarios are, in principle, included, and the HEF calculated by (16) should therefore be close to accurate.

The accuracy of the scenario-based formula is further verified by comparing the result with the HEF calculated by standard formulas for the PFD (in low-demand mode) and PFH (in very high-demand mode).

5.2.1. Low-demand situation

When the demand rate is low, the HEF can be approximated by the product of the PFD and the demand rate [10]. The PFD for a single component is [6]

$$PFD = 1 - e^{-\lambda_D t_{CE}} \quad (17)$$

where t_{CE} is the average downtime after a dangerous failure, which is given by

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \left(\frac{\tau}{2} + MTTR_{DU} \right) + \frac{\lambda_{DD}}{\lambda_D} MTTR_{DD} \quad (18)$$

For the demand rate once per ten years, the HEFs calculated from the scenario-based formula and the standard PFD formula are given in Table 5. It can be seen that the two approaches give almost the same result, which indicates that the accuracy of the scenario-based formula is acceptable for a low-demand SIS. More general evidence of the accuracy of the scenario-based formula in the low-demand mode can be found in Fig. 4, where the HEFs calculated from the scenario-based formula and the PFD for demand rates up to one demand per 1000 h are given. Fig. 4 shows that the HEF is almost the same as the product of the PFD and the demand rate for low demand rates, but when the demands become more frequent, the difference starts to increase.

Table 5
HEF calculated from the scenario-based formula and from a standard PFD formula for one demand per ten years.

| | |
|-------------------------------|----------------------------------|
| HEF _{PFD} | 1.2566×10^{-8} per hour |
| HEF _{scenario-based} | 1.2314×10^{-8} per hour |

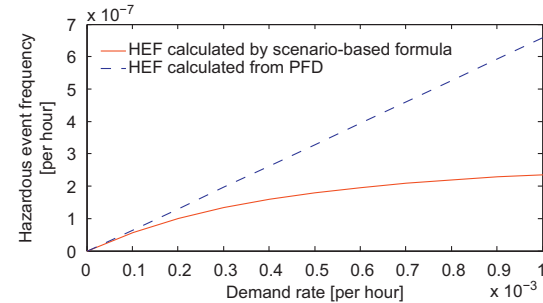


Fig. 4. HEF as a function of the demand rate in low-demand mode.

Table 6

HEF calculated from the scenario-based formula and from a standard PFH formula for one demand per hour.

| | |
|-------------------------------|----------------------------------|
| HEF _{PFH} | 8×10^{-7} per hour |
| HEF _{scenario-based} | 7.9821×10^{-7} per hour |

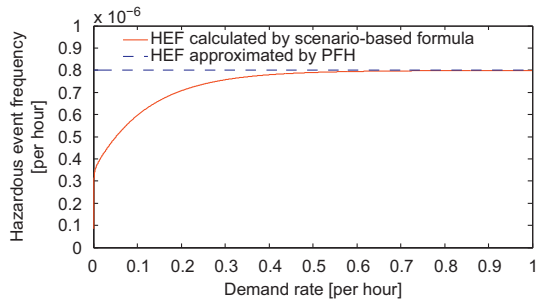


Fig. 5. HEF as a function of the demand rate in high-demand mode.

5.2.2. High-demand situation

When the demand rate is very high, the HEF can be approximated by the PFH, which for a single component is equal to the dangerous failure rate. For a demand rate of one demand per hour, the HEFs calculated from the scenario-based formula and from the standard PFH formula [6] are given in Table 6. The two approaches give similar results, which verifies the accuracy of the scenario-based formula for very high demand rates. More general evidence of the accuracy of the scenario-based formula in high demand situation can be found in Fig. 5, where the HEFs calculated from the scenario-based formula and the PFH for demand rates up to one demand per hour are given. Fig. 5 shows that the HEF calculated by the scenario-based formula is approaching the PFH as the demands tend to be continuous, as discussed in the introduction.

The scenario-based formula gives accurate HEF estimation when the demand rates are low and very high. The HEF calculated by the scenario-based formula increases with the demand rate, this is in accordance with what is expected. So, we may claim that it is adequate to use the scenario-based formula as the benchmark to assess the applicability and accuracy of the Markov model.

5.3. HEFs calculated by using the Markov model and the scenario-based formula

For demand rates from one demand every 10 years to one demand per hour, the HEF calculated by using the Markov model and the HEF calculated by the scenario-based formula are presented in Fig. 6. The HEF from the Markov model is obtained by solving Eqs. (3) and (8) in Matlab.

Fig. 6 shows that the Markov model gives a good approximation to the “scenario-based” HEF through the whole range of demand rates considered. The “error” slightly increases as the demand rate increases, however, the “error” is generally small throughout the whole range with a maximum error less than 10^{-7} per hour. For very high demand rates, the “error” starts to decrease. The HEFs from the two approaches tend to converge at the end. On this basis, the Markov model is claimed to give accurate results for demand rates ranging from one demanded per 10 years to one demand of per hour.

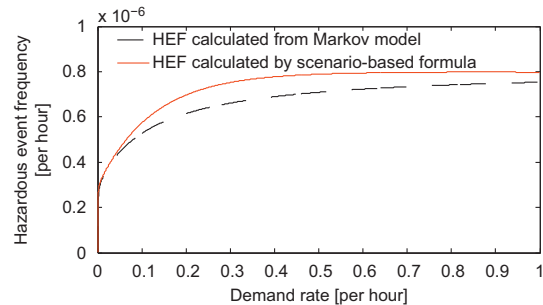


Fig. 6. HEF calculated by using the Markov model and the scenario-based formula.

One concern may be that the Markov model gives “non-conservative” results when the result from the scenario-based formula is used as the benchmark. However, the scenario-based approach gives a slightly conservative result itself, therefore one cannot conclude that the Markov model gives non-conservative results, but rather to conclude that the method gives a result which is fairly close to and at the non-conservative side of a good conservative approximation—and the error is in the order of 10^{-7} per hour, which is rather small.

6. Concluding remarks

This article has given a thorough discussion of a number of important modeling issues related to quantification of SIS reliability performance, both for low-demand and high-demand SISs. Issues like demand duration and verification of functionality by functional testing, successful response to demands and spurious activation are highlighted. The borderline between low-demand and high-demand mode of operation is discussed.

A Markov model for a SIS element including the demand rate is developed. The model can be used to calculate the hazardous event frequency (HEF) for general demand rates, covering both low-demand and high-demand mode of operation.

A scenario-based formula for the HEF is developed. The accuracy of this formula is verified through comparison with the standard formulas for PFD and PFH in IEC 61508. Thereafter the scenario-based formula is used to check the applicability and accuracy of the results obtained by using the Markov model.

It is concluded that the Markov model gives very accurate results for a simple case study of a single pressure transmitter, both for low-demand and high-demand mode. All the modeling issues mentioned above can be illustrated by this simple case study, and all the main results will also be applicable for a more complex multi-component SIS. The detailed analysis of a multi-component system will be more complex from a computational point of view, and the main features of the analysis may easily disappear in the computational details. At the same time, it would be of great interest to study the effects of diagnostic testing, functional testing, and correct response to demands for a more complex system. This is therefore a topic for further research.

Acknowledgments

The authors would like to thank the reviewers of this article for well-considered and useful inputs and comments.

References

- [1] Bukowski J. Incorporating process demand into models for assessment of safety system performance. In: Proceedings of RAMS'06 symposium. Alexandria, VI, USA; 2006.
- [2] Bukowski J. Using markov models to compute PFD_{ave} when repair times are not exponentially distributed. In: Proceedings of the annual reliability and maintainability symposium. Newport Beach, CA, USA; 2006.
- [3] CCPS, Layer of protection analysis; simplified process risk assessment. New York: American Institute of Chemical Engineers; 2001.
- [4] Hauge S, Lundteigen M, Hokstad P, Håbrekke S. Reliability prediction method for safety instrumented systems. Trondheim: Sintef; 2010.
- [5] Hauge S, Onshus T. Reliability data for safety instrumented systems. Trondheim: Sintef; 2010.
- [6] IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related systems, parts 1–7. Geneva: International Electrotechnical Commission; 1998.
- [7] IEC 61511, Functional safety: safety instrumented systems for the process industry sector, parts 1–3. Geneva: International Electrotechnical Commission; 2003.
- [8] IEC 62425, Railway applications—communication, signalling and processing systems—safety related electronic systems for signalling. Geneva: International Electrotechnical Commission; 2007.
- [9] Innal F. Contribution to modeling safety instrumented systems and to assessing their performance critical analysis of iec 61508 standard. PhD thesis, University of Bordeaux; 2008.
- [10] Innal F, Dutuit Y, Rauzy A, Signoret J. New insight into the average probability of failure on demand and the probability of dangerous failure per hour of safety instrumented systems. *Journal of Risk and Reliability* July 2010;224:75–86.
- [11] ISO/DIS 26262, Road vehicles—functional safety, parts 1–10. Geneva: International Organization for Standardization; 2009.
- [12] Lundteigen MA, Rausand M. Spurious activation of safety instrumented systems in the oil and gas industry: basic concepts and formulas. *Reliability Engineering and System Safety* 2008;93:1208–17.
- [13] Lundteigen MA, Rausand M. Reliability assessment of safety instrumented systems in the oil and gas industry: a practical approach and a case study. *International Journal of Reliability, Quality, and Safety Engineering* 2009;16:187–212.
- [14] Misumi Y, Sato Y. Estimation of average hazardous-event-frequency for allocation of safety-integrity levels. *Reliability Engineering and System Safety* 1999;66:135–44.
- [15] Rausand M, Hoyland A. *System reliability theory; models, statistical methods, and applications*. 2nd ed. Hoboken, NJ: Wiley; 2004.
- [16] Youshiamura I, Sato Y. Estimation of calendar-time- and process-operative-time-hazardous-event rates for the assessment of fatal risk. *International Journal of Performability Engineering* 2009;5:377–86.

Article 5 (journal)

New reliability measure for safety-instrumented systems
–In *International Journal of Reliability, Quality and Safety Engineering*


Is not included due to copyright

Article 6 (journal)

Uncertainty assessment of reliability estimates for safety-instrumented systems

–In *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*

Uncertainty assessment of reliability estimates for safety-instrumented systems

Proc IMechE Part O:
J Risk and Reliability
0(0) 1–10
© IMechE 2012
Reprints and permissions:
sagepub.co.uk/journalsPermissions.nav
DOI: 10.1177/1748006X12462780
pio.sagepub.com


Hui Jin, Mary Ann Lundteigen and Marvin Rausand

Abstract

Reliability estimates play a crucial role in decision making related to the design and operation of safety-instrumented systems. A safety-instrumented system is often a complex system whose performance is seldom fully understood. The safety-instrumented system reliability estimation is influenced by several simplifications and assumptions, both about the safety-instrumented system and its operating context, and therefore subject to uncertainty. If the decision makers are not aware of the level of uncertainty, they may misinterpret the results and select a safety-instrumented system design that is either too complex or too simple, or with an inadequate testing strategy, to provide the required risk reduction. This article elucidates the uncertainties related to safety-instrumented system reliability estimation. The article is limited to safety-instrumented systems that are operated in a low-demand mode, for which the probability of failure on demand is the standard reliability measure. The uncertainty of the probability of failure on demand estimate is classified as completeness uncertainty, model uncertainty, and parameter uncertainty and each category is thoroughly discussed. It is argued that the completeness uncertainty is the most important for safety-instrumented system reliability analyses, followed by parameter and model uncertainty. It is further argued that uncertainty assessment should be an integrated part of any safety-instrumented system reliability analysis, and that the analyst should communicate her judgment about the uncertainty to the decision-makers as part of the analysis results.

Keywords

Reliability, uncertainty, safety systems, complexity, reliability models, reliability data

Date received: 30 Mar 2012; accepted: 07 Sep 2012

Introduction

Safety-instrumented systems (SISs) are used in many industrial sectors to detect hazardous events and prevent them from developing into accidents. Reliability requirements for the safety-instrumented functions (SIFs), that are performed by a SIS, shall, according to IEC 61508, be deduced from hazard and risk analyses.

A SIS generally consists of one or more input elements, one or more logic units, and one or more final elements. A very simple SIS configuration is shown in Figure 1. It should, however, be realized that the configurations used in practical applications are often far more complicated. A SIS is installed to protect a system, which we will refer to as the equipment under control (EUC). The design, construction, implementation, and operation of a SIS are subject to the requirements in the generic standard IEC 61508¹ and in application-specific standards, such as IEC 61511² for the process industry, IEC 61513³ for the nuclear industry,

ISO 26262⁴ for the automobile industry, IEC 62278⁵ for the railway industry, and IEC 62061⁶ for machinery systems. The standards require that the SIS reliability is calculated and give guidance on how this can be done.

SIS reliability calculations are based on simplifications and assumptions about the system and its operating context, and the reliability values are therefore subject to uncertainty. Without being aware of the level of uncertainty, decision makers, such as SIS suppliers and end-users, may make improper decisions regarding

Department of Production and Quality Engineering, Norwegian University of Science and Technology, Trondheim, Norway

Corresponding author:

Marvin Rausand, Department of Production and Quality Engineering, Norwegian University of Science and Technology, S.P. Andersens veg 5, Trondheim, NO 7491, Norway.
Email: marvin.rausand@ntnu.no

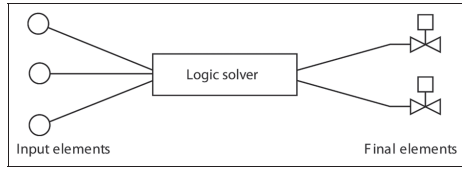


Figure 1. The main SIS elements.

Table 1. SIL requirements for low-demand SIFs¹

| SIL | PFDAvg |
|-----|-------------------------------|
| 1 | $\geq 10^{-2}$ to $< 10^{-1}$ |
| 2 | $\geq 10^{-3}$ to $< 10^{-2}$ |
| 3 | $\geq 10^{-4}$ to $< 10^{-3}$ |
| 4 | $\geq 10^{-5}$ to $< 10^{-4}$ |

PFDAvg: average probability of failure on demand; SIL: safety integrity level.

system configuration, component selection, and testing and maintenance strategies.

SIFs are classified according to how often they are demanded and IEC 61508¹ distinguish between low-demand and high-demand SIFs. A low-demand SIF is demanded less often than once per year and remains dormant until it is activated. The first edition of IEC 61508 also referred to the proof test frequency in the classification into high-demand and low-demand. This requirement has been removed in the second edition, but the scientific community is still debating this matter. Failures may occur and remain undetected until a proof test is carried out. The reliability of a low-demand SIF is measured by the average probability of failure on demand (PFDAvg) and this measure is used to express the reliability requirement to the SIF. In this article, reliability is used as a general term that is synonymous to the term dependability.⁷ The reliability of a system can, for example, be measured by its availability. The PFDAvg is here a measure of the system's unavailability. It should be noted that several SIFs may be implemented by the same SIS.

The IEC standards classify the reliability requirements into four safety integrity levels (SILs), as shown in Table 1. To meet the reliability requirement of SIL 3, for example, the SIF must, on average, not fail more than once per 1000 demands.

In addition to the quantitative requirements in Table 1, the SIS must also meet several qualitative requirements related to architectural constraints, safety management, and so on. These requirements are not discussed in this article; neither are reliability requirements to high-demand SIFs discussed.

Many authors⁸⁻¹¹ discuss uncertainty in risk and reliability analysis, but very few discuss aspects related directly to SIS reliability, and these are mainly limited to the uncertainty of input parameters.¹²⁻¹⁴ Other types

of uncertainty have not been addressed, even though they may have a significant influence on the reliability estimates. Janbu¹⁵ and Jin et al.¹⁶ are two of the few who investigate the uncertainty related to SIF reliability estimates from an overall perspective.

IEC 61508 and IEC 61511 give few requirements that address uncertainty in decision making. The standards add some conservatism to the reliability estimation, by requiring that the failure rates data used should have a confidence level of at least 70%.^{1,2} To meet this requirement, it is necessary to consider the failure rate as a random variable Λ with a probability distribution that describes our knowledge/belief about the failure rate.¹⁷ The value λ_u that is used in the calculations, must fulfill $\Pr(\Lambda \leq \lambda_u) \geq 0.70$, to have a 70% confidence level. IEC 61508 also requires that a confidence level of at least 90% shall be demonstrated on the reliability estimates, in the selection of hardware architectures for the so-called route "2H".¹ Some suppliers use "best estimates", but add conservatism by making the SIL requirement more strict, such that compliance with, for example, SIL 3, is only claimed when $\text{PFDAvg} \leq 0.7 \cdot 10^{-3}$.

The PDS-method¹⁸ (PDS is the Norwegian abbreviation for "Reliability of computer-based safety systems") For more information, see <http://www.sintef.no/PDS>.) extends the formulas in IEC 61508 by introducing additional measures to account for factors that are often left out in the SIF reliability calculations: (i) test independent failures (TIFs) that may remain unrevealed owing to limitations of the proof testing, and (ii) inclusion of systematic failures in the failure rate estimates.

These efforts attempt to reduce/compensate the uncertainty of SIS reliability estimates, but the scope is rather limited. A thorough uncertainty assessment approach for SIS reliability estimates seems to be lacking.

Our point of departure is that we do not believe that it is possible to quantify the uncertainty of a PFDAvg estimate in any objective way. The person most capable of making judgments about the uncertainty is the analyst and they should communicate to the decision-makers their "degree of belief" about the uncertainty, together with the results from the SIS reliability analysis.

The objectives of this article are to elucidate the concept of uncertainty in SIS reliability analysis and to highlight problematic issues related to the three categories: completeness uncertainty, model uncertainty, and parameter uncertainty. After having read the article, we hope that the analyst will be in a better position to judge and present their judgment about the uncertainty of a PFDAvg estimate.

The rest of this article is organized as follows. 'Reliability calculation' presents the various categories of failures that may occur in a SIS, outlines the SIS reliability analysis process, and lists the main simplifications and assumptions that are made. A brief

overview of the most common methods for SIS reliability analysis is also given. ‘What is uncertainty?’ introduces the concept of uncertainty and discusses the classification of uncertainty with respect to SIS reliability estimation. ‘Completeness uncertainty’ presents and discusses main issues related to completeness uncertainty. This is followed by ‘Model uncertainty’ and ‘Parameter Uncertainty’. Finally, concluding remarks are given.

Reliability calculation

Reliability calculations are based on a number of assumptions and simplifications, affecting the scope of the analysis and the ability to represent physical and operational properties of the components and the system. One important assumption is that reliability is best calculated by the use of statistical models, rather than physics-of-failure models. Statistical models express component and system performance by the use of time-to-failure (or repair) distributions. Parameters of the models need to be assigned, and system reliability theory is used to aggregate the information from these models into an overall reliability estimate, such as the PFD_{avg} .

Component failures

Failures of SIS elements may be classified as dangerous and safe failures. Dangerous failures can be further split into dangerous detected (DD) failures and dangerous undetected (DU) failures. DD failures are revealed (almost immediately) by diagnostic testing, while DU failures are only revealed by proof testing or in real demands.

Many of the formulas used for SIS reliability calculation cover only DU failures, under the assumption that DD failures have a negligible impact on the PFD_{avg} . This assumption may be realistic if the diagnostic test interval is negligible and the EUC enters a safe state while the DD failure is repaired. Omitting DD failures when these assumptions are not fulfilled will lead to a biased PFD_{avg} value.

A safe failure is a failure that does not prevent the execution of a SIF or leads to an unsafe state of the EUC. A spurious failure of a SIS element, such as a false alarm or a spurious valve closure, often takes the EUC to a safe state, owing to “fail-safe” design principles. Still, safe failures may have some undesired effects, such as downtime of the (production) system and excessive stresses to SIS elements.

Failures of SIS elements, be it dangerous or safe, can further be split into random hardware failures and systematic failures.

- A *random hardware failure* is a failure, occurring at a random time, which results from one or more of the possible degradation mechanisms in the hardware.¹
- A *systematic failure* is a 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.¹

An example of a random hardware failures is a valve that leaks owing to wear of the valve seat. An example of a systematic failure is a gas detector that is installed in an inappropriate location, for example close to a fan, such that it is not able to detect a gas release. The systematic failure is not easily detected during normal operation or regular proof testing and diagnostic testing. The probability of such failures is often very difficult to estimate.

A systematic failure is also called a *functional failure*, i.e. a failure where the item is still able to operate, but does not perform its specified function. A systematic failure is not caused by physical degradation and is therefore sometimes called a *non-physical failure*.

IEC 61508¹ requires only random hardware failures to be considered in PFD_{avg} calculations, while systematic failures should be controlled and managed by a dedicated safety management program. The main argument for this approach is that systematic failures do not follow the same failure processes as random hardware failures. In principle, a systematic failure is a non-recurring event if the cause of failure is successfully identified and corrected. The standard¹ gives a number of requirements that shall reduce (or ideally prevent) the occurrence of systematic failures.

Several data collection exercises^{19,20} have indicated that many SIS failures are systematic rather than random hardware failures. Based on such data collections, it is sometimes argued that also systematic failures, when studied en bloc, can be considered as random events as they tend to repeat themselves. Even if a systematic failure is corrected, similar types of failure seem to reoccur. One example is that even if a calibration procedure is improved to avoid a particular type of failure, the personnel may have established work habits that does not prevent the failure to reoccur. Consequently, two factors associated with the treatment of random and systematic failures are of interest in the discussion of uncertainty: (i) should or should not systematic failures be included in the SIS reliability estimation, and (ii) if systematic failures are included, to what extent is the assumption about their randomness adequate?

It may be remarked that the IEC 61508 approach will, because of the exclusion of systematic failures, inevitably, give a too-low and non-conservative value for the PFD_{avg} . Some of the systematic failures, however, are manifested as common-cause failures (CCFs) and TIFs, which are partly accounted for in the PFD_{avg} calculation.

CCFs

A CCF is a failure, which is the result of one or more events, causing concurrent failures of two or more separate channels in a multiple channel system, leading to system failure.¹ CCFs may occur because redundant

channels have components of the same type, or because they have the same type of design deficiency or inadequate maintenance, or are located in the same area (and therefore subject to the same exposure). In a SIS, where redundancy is often introduced to enhance reliability, it is important to cater for such failures and this is also a well established practice. Related factors that create uncertainty are linked to the modeling of CCFs and the sparse access to data to support the models.

Test-independent failures

Proof testing is not always fully realistic, since a realistic test may be dangerous or give excessive stresses to the equipment. It is, for example, not relevant to fill a production room with toxic gas to test a gas detector. Instead a small amount of non-toxic gas is injected directly into the detector through a test-pipe. Such a test will reveal most DU failures, but some DU failures may also pass the test and remain undetected. Such failures are called TIF and were introduced as part of the PDS-method.¹⁸ When a TIF is present, the system will not be as-good-as-new after a proof test.

Analysis process

In most cases, a SIS is modeled as a series system of three independent subsystems.

1. Input elements.
2. Logic solver.
3. Final elements.

Each subsystem is then analyzed separately.

Two different types of models are required: Component models and system models. Component models build on time-to-failure distributions and input parameters, such as failure rate, test interval, mean test-time, mean time to repair (MTTR), diagnostic coverage, and proof test coverage. System models describe the interactions between the various SIS elements within a subsystem. Some models are static (e.g. reliability block diagrams and fault trees), while others can describe dynamic features (e.g. Markov models and Petri nets). The models must again be supplemented by a suitable CCF model (e.g. beta-factor or multiple beta-factor model). A range of input parameters are required.

Assumptions and simplifications

All the models are subject to a number of assumptions and simplifications. Typical basic assumptions are given below (the assumptions may be slightly different for individual cases). The impact of these assumptions on the uncertainty need to be studied case by case.

- All elements have constant failure rates (λ).
- All elements are proof tested at the same time at regular proof test intervals (τ).
- All failures are revealed by the test.

- The test time is negligible.
- The repair time of a failure revealed by a proof test is negligible.
- After a test/repair, all elements are as-good-as-new.
- Common-cause failures can be adequately modeled by the standard beta-factor model (β).
- No other types of dependency between elements are relevant.
- DD failures are revealed immediately and a repair action is immediately initiated.
- The system (EUC) is in a safe state when a DD failure is repaired.
- Safe failures are not considered.
- Systematic failures are not considered (but partly included in the estimate of the β -factor).
- Human and organizational errors are not considered.
- Maintenance errors are disregarded.
- The SIS is not influenced by any factors outside (rather limited) physical boundaries of the SIS.

Conflicting objectives

A supplier may sign a contract with an end-user (e.g. an oil company) about a SIS for which a certain number of SIFs and associated SIL-requirements (e.g. SIL 3) have been specified with a basis in standards, such as IEC 61508. The supplier sometimes considers the job to be accomplished when the PFD_{avg} estimate is within the constraints of the SIL requirement and the other requirements in relation to SIL, such as architectural constraints, have been met. The approximation formulas in IEC 61508 disregard systematic failures, but include the contribution from CCFs. This simplistic approach fulfills the requirements in IEC 61508, but may not give a realistic PFD_{avg} estimate (i.e. the PFD_{avg} that is later to be experienced in the operational phase). It can be argued that the avoidance of systematic failures is mainly in the hands of the end-user, since the end-user is often to "blame" for overlooking key requirements (that would have impacted the SIS design) and for introducing failures or not revealing failures during operation and maintenance. The supplier seldom aims towards a status as "world champion" in PFD_{avg} calculations, and from the supplier's perspective, it is of interest to fulfill the end-user's requirements as fast and cheap as possible.

On the other hand, the end-user is responsible for the safety of the installation and should base decisions on a realistic (and usually conservative) estimate of the PFD_{avg} . This will then require more realistic models and a more careful examination of the SIFs and their operating and environmental conditions.

What is uncertainty?

What do we mean by uncertainty?

Uncertainty is a common word in our daily parlance, but is used with different meanings in different contexts.

Related to reliability and risk assessments, the interpretation of uncertainty is still debated.^{21,22} According to our view, probabilities in risk and reliability assessment must be interpreted as subjective probabilities. This also applies for the PFD_{avg} . We use the knowledge available to select appropriate models and input parameters, calculate a value for PFD_{avg} , and call this value our PFD_{avg} estimate. In this process, we are aware that we make a lot of simplifications and approximations that will influence the PFD_{avg} estimate and make our estimate uncertain. As part of the SIS reliability analysis, we should assess this uncertainty and communicate our assessment to the decision maker. The objective of the remaining part of this article is to give guidance to analysts on issues to be aware of when assessing the uncertainty of the PFD_{avg} estimate.

Uncertainty may stem from two main causes, natural variation and the lack of knowledge about the system or process. These categories of uncertainty are referred to as aleatory and epistemic uncertainty, respectively.^{10,23}

- *Aleatory uncertainty*: uncertainty arising from or associated with, the inherent, irreducible, and natural randomness of a system or process.
- *Epistemic uncertainty*: uncertainty owing to lack of knowledge about the performance of a system or process.

The epistemic uncertainty will be reduced when new knowledge becomes available, while the aleatory uncertainty cannot, in principle, be reduced.²⁴ However, several types of uncertainty that in the past were classified as aleatory, are now considered to be epistemic, indicating that the uncertainty classification is not fixed, but may vary as fundamental understanding of natural phenomena increases.²⁵ Some authors therefore take the stand that all uncertainty is epistemic.^{21,26} Despite its limitations, the classification gives a conceptual allocation of uncertainties into controllable and not so easily controllable categories.

How do we assess uncertainty?

Statistical models are used as a basis for estimating risk and reliability parameters, for example, to determine the frequency of accident scenarios in a probabilistic risk assessment (PRA) and the reliability of a SIS. By using statistical models for this purpose, we acknowledge the existence of uncertainty.¹⁰ Epistemic uncertainty as a source of uncertainty is related to how well our models and data are able to assess the behavior of the system. This uncertainty may be addressed by an additional process, i.e. uncertainty assessment. In this article, we use uncertainty assessment to account for the epistemic uncertainty of SIS reliability.

Complexity

New generations of SISs are generally more complex than previous generations. This is especially related to

the programmable parts (i.e. logic solvers and smart sensors), the number of components involved, and the interaction with other systems. The complexity makes it difficult for the analyst to fully understand the behavior of the system (both technical and operational), to identify all failure modes, and to establish adequate models. This issue is addressed in IEC 61508¹ where it is distinguished between type A and type B subsystems, where type B subsystems are more complex and therefore need more careful considerations.

Johansen and Rausand²⁷ list a set of complexity attributes related to (a) the physical system, and (b) the operation of the system. These attributes can be used to indicate the complexity and be a guide to the awareness we should have related to complexity.

Uncertainty classification

The nuclear industry¹⁰ distinguishes between three sources of epistemic uncertainty: completeness uncertainty, model uncertainty, and parameter uncertainty. The same categories are adopted in this article and each of them is discussed in the following.

There is no clear cut borderline between the three categories of uncertainty, and attempts to reduce the uncertainty within one category may influence the uncertainty in another category. For example, the choice of a multi-parameter distribution instead of an exponential distribution may reduce the model uncertainty, but more parameter uncertainty may be introduced. This is also the case with advanced CCF models. The categorization is therefore pragmatic.

Completeness uncertainty

Completeness uncertainty is about factors that are not properly included in the analysis. Failing to include all relevant factors in the analysis will give an incorrect estimate of the reliability, even if the data and model selection is "perfect". We may distinguish between the following.¹⁰

1. *Known completeness uncertainty*, which is owing to factors that are known, but deliberately not included. Reasons for exclusion may be lack of understanding the limitations of the system in its operating context, time or cost constraints, lack of models, lack of data to support the models, or lack of competence in using the models. The known completeness uncertainty reflects assumptions and simplifications that have been made in a trade-off of costs, available resources, competence of analysts, and the state of knowledge about the system and its operating environment. The number of exclusions and their impacts (need to be assessed) may be a measure of the level of uncertainty in a SIS reliability estimate.
2. *Unknown completeness uncertainty*, which is owing to factors that are not known or not identified.

Table 2. The degree of newness of technology.²⁸

| Experience with the operating condition | Level of technology maturity | | |
|---|------------------------------|---|-----------------|
| | Proven | Limited field history or not used by company/user | New or unproven |
| Previous experience | 1 | 2 | 3 |
| No experience by company/user | 2 | 3 | 4 |
| No industry experience | 3 | 4 | 4 |

The factors are truly unknown, and are therefore difficult to account for or make judgments about. The unknown completeness is problematic, as its contribution is invisible. However, indirect factors, i.e. factors that may impact to what extent “we don’t know”, may give an indication of contribution. The use of new technology, or the use of existing technology in new application areas may suggest that the contribution from unknown completeness uncertainty is high compared with when proven technology is used. The classification in Table 2 of the newness of technology may here be useful. In Table 2,²⁸ the newness is classified in four categories, ranging from 1 to 4, where 4 represents the most new and unfamiliar technology. The SIS technology is developing fast, and new and more advanced logic solvers and smart sensors are launched and implemented at high pace.

Additional factors/issues that may influence the (known and unknown) completeness uncertainty include the following.

- Interactions with external systems: a SIS is integrated in a bigger system (e.g. the process) and may interact with the EUC and with other safety and control systems. These interactions may influence (enhance or reduce) the SIS reliability.
- Failure mechanisms that are not known and/or not catered for: such failure mechanisms may be related to stresses during operation and maintenance, and to environmental conditions. Failure mechanisms may also be forgotten owing to inadequate failure analysis, e.g. as part of a FMECA.
- Side-effects of diagnostic testing: diagnostic testing is a means to timely reveal dangerous failures, and thereby increase the SIS reliability. Whether or not such a testing leads to side-effects is seldom evaluated.
- Placement of input elements (e.g. sensors, transmitters): installing input elements at places other than where they should may expose the components to different environmental stresses, and hence the components may get a different reliability behavior.
- Testing and maintenance strategies: complex testing and maintenance strategies are difficult to model in SIS reliability analyses and are therefore simplified in the calculations. This may increase the completeness uncertainty.

- Human and organizational factors: several studies have indicated that human and organizational factors are strongly influencing the SIS reliability,^{29,30} but such factors are usually not included in the analyses.

Including these factors generally leads to a higher PFD_{avg} estimate, but the amount of PFD_{avg} increases the need to be assessed case by case.

Model uncertainty

Model uncertainty arises from the fact that any model, conceptual or mathematical, will inevitably be a simplification of the reality it is designed to represent.^{22,24} Several authors have discussed the choice of models for SIS reliability analysis and given recommendations. One of the first articles with this purpose is Rouvroye and Brombacher.³¹

Component models

Almost all SIS reliability analyses assume that the elements have constant failure rates. This assumption implies that the elements do not show any deterioration and that they are as-good-as-new as long as they are functioning. This assumption may be adequate for electronic and some electrical items, and for mechanical items that are regularly maintained and upgraded/replaced if deterioration is revealed.

In some applications, such as in subsea oil and gas production systems, the items are left alone for a long time (e.g. 8 years) without any type of preventive maintenance. Some of these are mechanical items that are exposed to sea water, high pressure, and a corrosive environment. This indicates that the items will deteriorate with time and that the constant failure rate assumption is not adequate. If, for example, the life distribution of a component is Weibull distributed with a shape parameter that is greater than one, and we use a constant failure rate model, we will over-estimate the probability of failure (i.e. be conservative) in the first part of the item’s life and under-estimate the probability of failure in the last part of the item’s life. A deteriorating item will not be as-good-as-new after a successful proof test.³² This problem is very seldom catered for in SIS reliability analyses.

Component models must also take into consideration issues related to testing and maintenance, such as

the coverage of diagnostic tests, the coverage of proof tests, the possible use of partial stroke testing of shut-down valves,³³ and several more.

System models and methods

Several methods are used to model the interactions between SIS elements, and calculate PFD_{avg} . The most common are:

- (a) simple approximation formulas;³⁴
- (b) IEC 61508 approximation formulas;¹
- (c) the PDS method;¹⁸
- (d) reliability block diagrams;
- (e) fault tree analysis;
- (f) Markov methods;
- (g) Petri nets.³⁵

These methods can be used to analyze both low-demand and high-demand SIFs. The sequence in which the methods are listed indicates their applicability to an increasing system complexity. The first five methods consider the SIS to be a static system without any dynamic properties, while Markov methods and Petri nets can incorporate some dynamic effects owing to testing and maintenance.

It is often claimed³⁶ that CCFs are more crucial for the SIS reliability than independent element failures. It is therefore important how CCFs are incorporated into the methods. In some methods, we may choose among various implicit CCF models,³⁷ while other methods come with a dedicated CCF model (the PDS method). Some methods are mainly based on explicit modeling of CCFs, rather than implicit. To choose the “best” CCF model is a difficult task and the SIS analysts therefore too often select the simplest possible model—the beta-factor model. The beta-factor model is listed as an adequate CCF model in IEC 61508¹ and the choice of this model is therefore compatible with the standard; and in most cases, leads to conservative PFD_{avg} estimates.

In most cases, other dependencies than CCFs are not covered in the SIS reliability analyses. Among such dependencies are cascading failures and negative dependencies. A special challenge is related to modeling dependencies that are partly within and partly between SIS channels and modules. As discussed by Lundteigen and Rausand,³⁶ these dependencies can be an important source of model uncertainty.

Dynamic effects may be related to phased mission, the effect of DD failures and safe failures, and testing procedures. An example of such a testing procedure is to carry out a full proof test of similar channels each time a DD failure is restored—either in addition to the planned proof test or by postponing the planned proof test.³⁸ Another example is to supplement the proof testing with regular inspections (e.g. once a week) where some failure possibilities may be partly examined. The inspection may, for example, involve moving a valve slightly to check that it is not stuck.

Model selection

The most adequate model/method is determined by the assumptions and simplifications. As long as the analyst is competent and familiar with the different methods, it does not matter very much if they choose the most simple method that fits the assumptions or they choose a more advanced method. Liu et al.³⁸ analyze the same SIS with different methods and find that the reliability estimates are similar. The approximation formulas give the most conservative estimates and the conservativeness decreases with increasing method complexity—which is expected since the complex methods are based on more detailed modeling. Too few and simple systems are, however, analyzed to give any firm and general conclusions. Rouvroye and Brombacher³¹ and Rouvroye and van den Blik³⁹ find that different methods may result in different SILs. Their findings are in conflict with the conclusion in Liu et al.³⁸ and may be caused by the differences in the level of complexity of the systems that were studied.

The causes (assumptions and simplifications) of model uncertainty are the same as for known completeness uncertainty. It is, therefore, not obvious that uncertainties can uniquely be classified as model uncertainty or known completeness uncertainty. Some sources, such as the PDS method,¹⁸ do not differentiate between completeness uncertainty and model uncertainty, but use the term model uncertainty to represent both.

Model uncertainty has been studied by several authors. Among these are Zio and Apostolakis⁴⁰ and Droguett and Mosleh.⁴¹ The model uncertainty issue is not significant in SIS reliability analysis, as we account for the uncertainty by the assumptions and simplifications (the main causes of model uncertainty) as part of known completeness uncertainty.

Parameter uncertainty

Parameter uncertainty is related to uncertainty of the parameter values used in the quantification.¹⁰ In the current context, these parameters comprise component failure rates, mean repair times, common-cause beta-factors, test coverage factors, and so on. Failure rates are available in data sources, such as OREDA¹⁹ and Hauge and Onshus.²⁰ (A survey of reliability data sources is given on <http://www.ntnu.edu/ross/info/data>.) Estimates of some of the other parameters may be found in Hauge and Onshus,²⁰ partly based on expert judgment.

Several uncertainties are related to the provision of input parameters, and we discuss some of these.

Failure rates

A SIS is often a vital safety barrier and is designed to be highly reliable. Few failures are, therefore, expected to occur even during a long operating period, and the

failure rate estimates based on experience data become rather uncertain. Another problem is that the failure rates we find, for example, in OREDA,¹⁹ are based on data from components that were installed several years (often 10–15 years) before the data collection exercise was terminated. Owing to the rapid technological development of, for example, smart sensors, the failure rate estimates may not at all represent the technology that will be used in the new SIS.

The operational and environmental conditions of the elements used in a new SIS are sometimes very different from the conditions under which the data were collected. For electronic components, this issue is handled by the approach outlined in MIL-HDBK-217F.⁴² For more complicated equipment, such as SIS elements, the approach in MIL-HDBK-217F is too simple and we have to use more advanced approaches, such as the one described by Brissaud et al.⁴³

OREDA¹⁹ and Hauge and Onshus²⁰ are both based on recorded maintenance actions. These data sources will, therefore, not contain all safe failures, since some of these can be reset without any formal maintenance action.

Common cause failure rates

Very few data sources are available for CCF rates. The only exception is for the nuclear power industry⁴⁴ that has established the International Common-Cause Data Exchange database.⁴⁵ The authors are not aware of any similar initiative for any non-nuclear sector. CCF rates are highly dependent on the physical conditions and the operational and environmental conditions and it is therefore difficult to claim that a CCF rate in one installation will be similar to the CCF rate in another installation.

IEC61508¹ has, therefore, chosen another approach where the factor β of the beta-factor model is determined by a checklist in Part 6 of the standard. The checklist is based on around 40 questions, is generic, and is intended for all types of SIS. An immediate observation is that the number of questions related to human and organizational factors is low compared with the importance of these factors. This issue is further discussed by Rahimi et al.²⁹ Several other approaches may be used to determine the β -factor. Among these is the unified partial method (UPM) that has been extended by using influence diagrams.⁴⁶

Test coverage

Several authors^{33,47–49} have discussed possible approaches to determine the test coverage—mainly based on expert judgment. These efforts are, however, limited and little guidance is available on how to estimate the test coverage factor, both for diagnostic and proof testing, and the values used in many SIS reliability analyses are therefore, at best, guesstimates.

Uncertainty propagation

Parameter uncertainty is the most studied type of uncertainty^{22,24,50} and is usually analyzed by Monte Carlo simulation. An uncertainty distribution—sometimes expressed by an error factor—is given for the main parameters, a value from each distribution is chosen at random and an output value is generated. This is repeated a high number of times and we say that the uncertainty is propagated through the model to give an uncertainty distribution of the output measure of interest (in our case the PFD_{avg}).⁵¹ Such a simulation module is a separate module of many computer programs for reliability analysis, such as fault tree analysis. Some authors also use an approach based on fuzzy number arithmetic⁵² and Dempster-Shafer theory⁵³ to propagate the uncertainty of the parameters.

Concluding remarks

This article has discussed a number of issues related to the uncertainty of the PFD_{avg} estimate of a SIS operating in low-demand mode. The authors believe that this type of discussion is important, as it may frame future development of methods and models for treating uncertainty in reliability analyses. It is argued that the three perspectives of uncertainty contributions, the completeness, model, and parameter uncertainty, are very useful for this purpose and a thorough discussion about the possible ways to treat them in the analyses have been made for each category. It is argued that uncertainty assessment is an important part of a SIS reliability analysis and that the uncertainty should be communicated to the relevant decision makers together with the PFD_{avg} estimate.

The persons who are best capable of assessing the uncertainty is the analyst who knows how the various attributes of the SIS are implemented in the models and in the analyses. The authors do not believe that it is possible to present any objective estimate of the uncertainty, so the analyst has to judge the different contributors to the uncertainty and present their best “degree of belief”.

Of the three categories, completeness uncertainty is judged to be the most important. We realize that parameter uncertainty may lead to different SIL ratings, but the decision maker normally has a good picture of this category of uncertainty. It is those we do not know that we fail to consider in decision making. This completeness category is split into two sub-categories; known and unknown completeness uncertainty. For the known completeness uncertainty, the analyst is aware of the relevant issues and has deliberately excluded them from the analysis. This type of simplifications can, in some cases, be compensated for by using conservative approximations. For the unknown completeness uncertainty, the analyst does not know what they do not know and does not include. This uncertainty is most prevalent for new technology and partly

known technology in new areas of application. The analyst may be warned about the possible uncertainty by using the classification of newness proposed by Det Norske Veritas (DNV).²⁸

Model uncertainty is linked to the completeness uncertainty. The choice of model/method is strongly dependent on the assumptions and simplifications made. If the analyst is competent and familiar with the limitations of the various methods, it is not very important which method they choose, as long as the method fits to the assumptions made.

As for parameter uncertainty, the technological development in the SIS area is running fast, and the failure rate estimates in data sources may, therefore, be outdated. Another issue is that the failure rate estimates may not fit to the current operational context and we may need to extrapolate the estimates from the known to the new application, this is also discussed in Sallak et al.¹² An approach for this purpose is outlined by Brissaud et al.⁴⁵

An important area of further research is to develop new frameworks and methods that integrate uncertainty assessment with SIS reliability analyses. Current approaches that focus primarily on the treatment of parameter uncertainty are not sufficient, as they do not include other, and sometimes more important, sources of uncertainty. In fact, current approaches in the literature may be a false comfort and give inappropriate guidance in the decision making about SIS design and risk management of facilities in which the SIS is installed.

Funding

This research received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

Acknowledgments

The authors would like to thank the reviewers of this article for well considered and useful inputs and comments.

References

- IEC 61508. Functional safety of electrical/electronic/programmable electronic safety-related systems. Part 1-7. Geneva: International Electrotechnical Commission, 2010.
- IEC 61511. Functional safety: safety instrumented systems for the process industry sector. Part 1-3. Geneva: International Electrotechnical Commission, 2003.
- IEC 61513 Nuclear power plants – instrumentation and control for systems important to safety – general requirements for systems. Geneva: International Electrotechnical Commission, 2004.
- ISO 26262 Road vehicles – functional safety. Geneva: International Electrotechnical Commission, 2011.
- IEC 62278 Railway applications – specification and demonstration of reliability, availability, maintainability and safety (RAMS). Geneva: International Electrotechnical Commission, 2002.
- IEC 62061 Safety of machinery – functional safety of safety-related electrical, electronic and programmable electronic control systems. Geneva: International Electrotechnical Commission, 2005.
- IEC 60050-191 International electrotechnical vocabulary. Chapter 191: dependability and quality of service. Geneva: International Electrotechnical Commission, 1990.
- De Rocquigny E, Devictor N and Tarantola S. *Uncertainty in industrial practice: a guide to quantitative uncertainty management*. Chichester, UK: Wiley, 2008.
- Mosleh A, Siu N, Smidts C, et al. *Model uncertainty: its characterization and quantification*. Washington DC: US Nuclear Regulatory Commission, 2nd ed. 1994.
- NUREG 1885. Guidance on the treatment of uncertainties associated with PRAs in risk-informed decision. Technical report, Washington DC: US Nuclear Regulatory Commission, 2009.
- Winkler RL. Uncertainty in probabilistic risk assessment. *Rel Engng Sys Saf* 1999; 54: 127–132.
- Sallak M, Simon C and Aubry J-F. A fuzzy probabilistic approach for determining safety integrity level. *IEEE Trans Fuzzy Sys* 2008; 16: 239–248.
- Wang Y, West HH and Mannan MS. The impact of data uncertainty in determining safety integrity level. *Process Saf Environm Protection* 2004; 82: 393–397.
- Brissaud F, Barros A and Bérenguer C. Handling parameter and model uncertainties by continuous gates in fault tree analyses. *Proc IMechE, Part O: J Risk and Reliability* 2010; 224: 253–265.
- Janbu AF. *Treatment of uncertainty in reliability assessment of safety instrumented systems*. Master's thesis, Norwegian University of Science and Technology, Trondheim, Norway, 2009.
- Jin H, Lundteigen MA and Rausand M. Uncertainty assessment of reliability estimates for safety instrumented systems. In: *Advances in safety, reliability and risk management ESREL 2011* (ed. C. Guedes Soares), CRC Press, London: 2213–2221.
- Hamada MS, Wilson AGSRC and Martz HF. *Bayesian reliability*. New York, NY: Springer, 2008.
- Hauge S, Lundteigen MA, Hokstad P, et al. Reliability prediction method for safety instrumented systems – PDS method handbook. SINTEF report A13503, SINTEF Safety Research, Trondheim, Norway, 2010.
- OREDA. *OREDA reliability data*. OREDA Participants, Available from: Det Norske Veritas, NO 1322 Høvik, Norway, 5th ed., 2009.
- Hauge S and Onshus T. Reliability data for safety instrumented systems – PDS data handbook. SINTEF report A13502, SINTEF Safety Research, Trondheim, Norway, 2010.
- Aven T. *Risk analysis: assessing uncertainties beyond expected values and probabilities*. Chichester, UK: Wiley, 2008.
- Rausand M. *Risk assessment; theory, methods, and applications*. Hoboken, NJ: Wiley, 2011.
- Parry GW. The characterization of uncertainty in probabilistic risk assessments of complex systems. *Rel Engng Sys Saf* 1996; 54: 119–126.
- Abrahamsson M. *Uncertainty in quantitative risk analysis - characterisation and methods of treatment*. PhD thesis,

- Department of Fire Safety Engineering, Lund University, Lund, Sweden, 2002.
25. Faber M. On the treatment of uncertainties and probabilities in engineering decision analysis. *J Offshore Mechanics and Arctic Engng* 2005; 127: 243–248.
 26. Kieureghian A and Ditlevsen O. Aleatory or epistemic? Does it matter? *Structural Safety* 2009; 31: 102–112.
 27. Johansen IL and Rausand M. Complexity in risk assessment of sociotechnical systems. In: PSAM11 & ESREL 2012 June 25–29, 2012 (Proceedings from this conference has yet not been published), Helsinki, Finland, 2012.
 28. DNV Qualification of new technology. Recommended Practice DNV-RP-A203, Det Norske Veritas, Høvik, Norway, 2011.
 29. Rahimi M, Rausand M and Lundteigen MA. Management factors that influence common-cause failures of safety-instrumented systems in the operational phase. In: *Advances in Safety, Reliability, and Risk Management, ESREL 2011* (ed. C. Guedes Soares), pp. 2036–2044. London, CRC Press.
 30. Schönbeck M, Rausand M and Rouvroye J. Human and organisational factors in the operational phase of safety instrumented systems: A new approach. *Safety Sci* 2010; 48(3): 310–318.
 31. Rouvroye JL and Brombacher AC. New quantitative safety standards: different techniques, different results. *Rel Engng Sys Saf* 1999; 66: 121–125.
 32. Rausand M and Vatn J. Reliability modeling of surface controlled subsurface safety valves. *Rel Engng Sys Saf* 1998; 61: 159–166.
 33. Lundteigen MA and Rausand M. Partial stroke testing of process shutdown valves: How to determine the test coverage. *J Loss Prevention in the Process Ind* 2008; 21: 579–588.
 34. Rausand M and Høyland A. *System reliability theory: models, statistical methods, and applications*. 2nd ed. 2004. Hoboken, NJ: Wiley.
 35. Dutuit Y, Rauzy A and J-P S. A snapshot of methods and tools to assess safety integrity levels of high-integrity protection systems. *Proc IMechE, Part O: J Risk and Reliability* 2008; 222: 371–379.
 36. Lundteigen MA and Rausand M. Common cause failures in safety instrumented systems on oil and gas installations: Implementing defense measures through function testing. *J Loss Prevention in the Process Ind* 2007; 20: 218–229.
 37. Hokstad P and Rausand M. Common cause failure modeling: Status and trends. In: Misra KB (ed.) *Handbook of performability engineering*, 2008, pp.621–640. London: Springer.
 38. Liu Y, Jin H, Lundteigen MA, et al. Reliability modeling of safety-instrumented systems by Petri nets. 2012. Submitted for publication. Submitted to Reliability Engineering and System Safety.
 39. Rouvroye JL and van den Blik EG. Comparing safety analysis techniques. *Rel Engng Sys Saf* 2002; 75: 289–294.
 40. Zio E and Apostolakis G. Two methods for the structured assessment of model uncertainty by experts in performance assessments of radioactive waste repositories. *Rel Engng Sys Saf* 1996; 54: 225–241.
 41. Drogue E and Mosleh A. Bayesian methodology for model uncertainty using model performance data. *Risk Analysis* 2008; 28: 1457–1476.
 42. MIL-HDBK-217F Reliability prediction of electronic equipment. Handbook, Washington, DC: US Department of Defense, 1991.
 43. Brissaud F, Charpentier D, Fouladirad M, et al. Failure rate evaluation with influencing factors. *J Loss Prevention in the Process Ind* 2010; 23: 187–193.
 44. Rasmuson D, Mosleh A and Wierman T. Insight from analysing the nuclear regulatory commission's common-cause failure database. *Proc IMechE, Part O: J Risk and Reliability* 2008; 222: 533–544.
 45. NEA International common-cause failure data exchange. ICDE general coding guidelines. Technical report R(2004)4, Nuclear Energy Agency, Paris, 2004.
 46. Zitrou A, Bedford T and Walls L. An influence diagram extension of the unified partial method for common cause failures. *Quality Technol Quantitative Mgmt* 2007; 4: 111–128.
 47. Hokstad P, Fløtten P, Holmström S, et al. A reliability model for optimization of test schemes for fire and gas detectors. *Rel Engng Sys Saf* 1995; 47: 15–25.
 48. Bukowski JV. Impact of proof test effectiveness on safety instrumented system performance. In: *Proceedings of the annual reliability and maintainability symposium (RAMS 2009)*, 2009.
 49. Brissaud F, Barros A and Béranger C. Probability of failure of safety-critical systems subject to partial tests. In: *Proceedings of 2010 the annual reliability and maintainability symposium (RAMS 2010)*, Fort Worth, TX, San Jose, CA, January 25–28, 2010.
 50. Thunnissen DP. *Propagating and mitigating uncertainty in the design of complex multidisciplinary systems*. PhD thesis, California Institute of Technology, Pasadena, CA, 2005.
 51. NASA Probabilistic risk assessment procedures guide for NASA managers and practitioners. Technical report, NASA Office of Safety and Mission Assurance, Washington, DC, 2002.
 52. W Mechri W, Simon C and Othman K. Uncertainty analysis of common cause failure in safety instrumented systems. *Proc IMechE, Part O: J Risk and Reliability* 2011; 225: 450–460.
 53. Simon C and Weber P. Imprecise reliability by evidential networks. *Proc IMechE, Part O: J Risk and Reliability* 2009; 223: 119–131.

Article 7 (conference)

Can functional tests be replaced by inspection after demand?
–In *7th Global Congress on Process Safety*

Is not included due to copyright

Article 8

Quantification of organizational influences on failure rate: A Bayesian approach
–In *IEEE International Conference on Industrial Engineering and Engineering Management*

Quantification of Organizational Influences on Failure Rate: A Bayesian Approach

Hui Jin^{1,2}, Marvin Rausand¹, Ali Mosleh², Stein Haugen¹

¹Department of Production and Quality, Norwegian University of Science and Technology, Trondheim, Norway

²Center for Risk and Reliability, University of Maryland, College Park, Maryland, USA
(hui.jin@ntnu.no, marvin.rausand@ntnu.no, mosleh@umd.edu, stein.haugen@ntnu.no)

Abstract—This paper studies the organizational influences on failure rates. The failure rate model in MIL-HDBK-217F is extended to include organizational factors, and a Bayesian approach is proposed to quantify the organizational influences. In contrast to most explicit organizational models, this paper focuses on extracting information from failure rate data. The proposed Bayesian approach, however, can be combined with the explicit models by using their results as prior information, hence obtain more rigorous result. A numerical example is included to illustrate the model and approach.

Keywords – Bayesian, organizational influences, failure rate, quantification

I. INTRODUCTION

Reliability plays an important role in system design and development, especially for safety-related systems whose failure may lead to harm to human, the environment, and material and financial assets. A central concept in reliability-related activities is the failure rate (function) that describes the “prone to failure” of an item¹ [1].

The failure rate of an item is determined by the inherent reliability of the item and its operating conditions. The operating conditions may be further divided into the environmental/physical (E/P) conditions and organizational conditions. The E/P conditions cover the “hard” factors such as temperature, humidity, and pressure that influence the failure rate. The organizational conditions (also called organizational factors) cover the “soft” factors that influence the failure rate. The organizational influences may be direct or indirect through meta-level factors such as maintenance strategy, personnel training, and working practice. In this paper, we consider the overall organizational influences, therefore, these meta-level factors are not explicitly treated, instead they are implicitly included as part of the organizational factors.

In reliability design, a recurring problem is the lack of quality data for failure rate estimation. The failure data obtained from laboratory tests are valid only for the laboratory testing E/P conditions and contain no information about the organizational influences. Models have been proposed to include the plant-specific E/P conditions to the laboratory failure data, and then estimate the plant-specific failure rate [15], but these models do not account for the organizational influences. Failure data from actual

operation of the items (i.e., field data) cover both the plant-specific E/P conditions and the organizational influences, but the amount of data is usually too limited to draw direct relationships between the organizational factors and the failure rate. Instead, failure rates for industry average E/P conditions and organizational influences are usually provided, i.e., generic failure rates (GFRs) found in databases such as the offshore reliability database OREDA [2].

Many authors have investigated organizational influences on system performance and accidents. These studies range from qualitative accident investigation to quantitative methods to include human and organizational factors into probabilistic safety assessment. Some of the well-known qualitative models are the Swiss cheese model [3], the risk management framework proposed by Rasmussen [4] and the STAMP model [5]. Several models have been proposed to quantify organizational influences. Early examples are MACHINE [6], WPAM [7], the SAM [8] framework and the ω -factor model [9]. In the Accidental Risk Assessment Methodology for IndustrieS (ARAMIS) [10] project, methodology was developed to quantify organizational influences on reliability of safety barriers. Øien [11] used a risk influence diagram to quantify organizational influences on leak events on offshore installations and suggested using indicators to monitor these influences. This line of research is followed by BORA [12] and the Risk OMT [13] project. For a more extensive review on organizational factors, the readers are referred to [14].

Despite the research efforts related to organizational factors, no quantification model has received wide popularity and acceptance. Most of the models focus on incorporating organizational influences to the risk analysis; few have directly considered the organizational influences on the failure rates. At the same time, it is argued that the failure rate of the same item varies significantly between organizations [14]. Therefore quantification of organizational influences on failure rates is a field that calls for more research.

A pertinent question is: Does an organization have the same influences on the failure rates of different items? Since the organization culture, the management style, and the operating philosophy for an organization are not likely to be significantly different for different items, it is reasonable to assume that an organization has similar influences on the failure rate of different items [9].

Many industries collect field data and estimate GFRs for relevant items. One example is the offshore oil and gas

¹Item is used to denote any component, subsystem, or system that can be considered as an entity.

industry that provides GFRs through the OREDA project [2]. On the other hand, organizations that have been in business for a while usually have their own failure databases containing organization-specific failure rates (OFRs). When these organizations design new systems, they prefer the OFRs to the GFRs, since the OFRs are more relevant to their organizations. These organizations may have problems when using items that they have no or little experience with, because the OFRs are either unavailable or have a big uncertainty due to the limited experience. In these cases the GFRs are usually resorted to.

A relevant question is now whether it is possible to combine the assessed organizational factors and the GFR to obtain an OFR for an item that the organization does not have much experience with.

The objective of this paper is to develop an approach to extract information from those items that an organization has experience with, and use this information to assess the organizational influences on failure rates. The assessment result is used to account for the organizational influences on failure rates of items that the organization has no or limited experience with. Therefore, the organization can use OFR even when the items are new to it.

The rest of this paper is organized as follows: Section II extends the failure rate model in MIL-HDBK-217F to include organizational factors. In section III, A Bayesian approach is proposed to estimate parameters in the model presented in section II. An example is given in section IV to illustrate the proposed approach. And this leads to the final discussion and conclusions in section V.

II. FAILURE RATE MODEL

MIL-HDBK-217F [15] has been the main reliability data source for electronic components. In MIL-HDBK-217F it is assumed that the failure rate λ^j of item i is constant and can be specified as:

$$\lambda^j = \lambda_b^i \pi_r^j \pi_A^j \pi_R^j \pi_S^j \pi_C^j \pi_Q^j \pi_E^j \quad (1)$$

where λ_b^i is the baseline failure rate of item i , under a set of standard conditions and the actual conditions j are taken into account as π factors that modify the baseline failure rate. For further details about this model, see [15].

In the MIL-HDBK-217F model, most of the π factors are related to the E/P conditions and little or no attention is given to the organizational factors. To account for the organizational influences on the failure rate, extension is proposed based on the following assumptions:

- The organizational influences on the failure rate do not change with the item or the E/P conditions.
- The organization's E/P conditions are the same as the industry average, but the E/P conditions for different items do not need to be the same.

- Constant failure rate is assumed for the item and the organizational factor influences the failure rate in a linear way.
- The main E/P conditions are beyond the control of the specific organizational. A possible influence of organization factors on E/P conditions is not considered in the model.

For an item i , operated by organization A, under E/P conditions j , the failure rate can be written as

$$\lambda_A^j = \lambda_b^i \pi_{EP}^j \pi_o^A \quad (2)$$

where π_{EP}^j is a (combined) modification factor representing the actual E/P conditions, and π_o^A is a modification factor representing the actual organizational factors.

When item i is operated under industry average E/P conditions by organization A, the failure rate λ_A^i can be derived from (2)

$$\lambda_A^i = \lambda_b^i \overline{\pi_{EP}} \pi_o^A \quad (3)$$

where $\overline{\pi_{EP}}$ represents influences from the industry average E/P conditions.

Considering organization B hands over the operation of item i to organization A without changing the E/P conditions (i.e., only the organizational factors are changed), we may define the relative organizational influence factor between A and B as

$$r_{AB} = \frac{\pi_o^A}{\pi_o^B} \quad (4)$$

By combining (2) and (3), the following relationships can be derived

$$r_{AB} = \frac{\lambda_b^i \pi_{EP}^j \pi_o^A}{\lambda_b^i \pi_{EP}^j \pi_o^B} = \frac{\lambda_A^j}{\lambda_B^j} = \frac{\lambda_b^i \overline{\pi_{EP}} \pi_o^A}{\lambda_b^i \overline{\pi_{EP}} \pi_o^B} = \frac{\lambda_A^i}{\lambda_B^i} \quad (5)$$

When r_{AB} and λ_B^i (λ_B^j) are known, λ_A^i (λ_A^j) can be calculated.

We now assume that a specific organization is operating an item i under industry average E/P conditions. Based on (5), the GFR (λ_G^i) and OFR (λ_A^i) for the item have the following relationship

$$r_A = \frac{\lambda_A^i}{\lambda_G^i} \quad (6)$$

Since the organizational influences on the failure rate do not change with the item or the E/P conditions, r_A is the same for all (most) of the items in the organization. An organization normally has a high number of items, thus a significant amount of data can be used to estimate

r_A . The factor r_A is assumed to be a random variable with a probability distribution.

III. BAYESIAN QUANTIFICATION APPROACH

In this section, a Bayesian approach is used to quantify the organizational influences on the failure rate. This approach makes use of the GFRs from a generic data source, such as OREDA, and the OFRs from the organization in question. Details about Bayesian reliability are not given, and readers may consult [16] for more information. The general format of the approach is as follows.

$$\varphi(r_A | E) = \frac{L(E | r_A)\varphi(r_A)}{\int_{\omega_A} L(E | r_A)\varphi(r_A)dr_A} \quad (7)$$

where $\varphi(r_A)$ is the prior distribution of r_A , $L(E | r_A)$ is the likelihood of the evidence (i.e., observed data) E when r_A is given, $\varphi(r_A | E)$ is the posterior distribution of r_A given the evidence E .

A. Data

Two types of data are needed in the proposed approach:

- The OFRs of the n items that are operated by organization A, λ_A^i , $i = 1, 2, \dots, n$.
- The GFRs of the items corresponding to the OFRs, i.e., λ_G^i , $i = 1, 2, \dots, n$.

The OFRs and GFRs are estimates of their true values, such that applying (6) to the OFRs and GFRs results in a set of r_A^i -s instead of the true values (r_A). The r_A^i -s are evidences that can be used to estimate r_A .

Remark: There may be cases where an item is so specific to the organization and no GRF for this item is available, or the organization average E/P conditions for an item is different from the industry average E/P conditions. In either case, the information contained in the OFR of that item cannot be used in the estimation of r_A .

B. Prior distribution

The estimation of r_A may be based on statistical failure rate data or explicit modeling of how an organization influences the failure rate. The Bayesian approach may combine both. The failure rate data are used as evidences and the results from explicit modeling can serve as prior information. For example, in the ω -factor model, an approach to quantify organizational influences is proposed. With this approach, the ω -factor can be estimated. By simple re-parameterization, the ω -factor can be converted to r_A and used as prior for Bayesian updating. For details of the ω -factor model, see [9].

There is no restriction on the form of the prior distribution and both nonparametric and parametric distributions can be used. The parametric distributions are normally easier to handle in calculation. To simplify the matter, in this paper a lognormal distribution is used as the prior: $r_A \sim LN(\theta_0, \omega_0)$.

$$\varphi(r_A) = \varphi(r_A | \theta_0, \omega_0) = (r_A \omega_0 \sqrt{2\pi})^{-1} e^{-\frac{(\ln r_A - \ln \omega_0)^2}{2\omega_0^2}} \quad (8)$$

where $\theta_0 = (r_A)_{50}$ and $r_{\underline{A}} = \theta_0 e^{\omega_0^2/2}$ are the medium and mean of the prior distribution, respectively. The variance for r_A is $\text{var}(r_A) = r_{\underline{A}}^2 (e^{\omega_0^2} - 1)$.

C. Likelihood function and posterior distribution

To obtain the posterior distribution, an important step is to determine the likelihood function. The evidences are $E = [r_A^1, r_A^2, \dots, r_A^n]$. We follow an approach proposed by Mosleh and Apostolakis [17]. Assuming that the different pieces of evidence are independent, we get

$$\begin{aligned} L(E | r_A) &= L(r_A^1, r_A^2, \dots, r_A^n | r_A) \\ &= L(r_A^1 | r_A) L(r_A^2 | r_A) \dots L(r_A^n | r_A) = \prod_{i=1}^n L(r_A^i | r_A) \end{aligned} \quad (9)$$

Using the multiplicative error model of [17], the likelihood of observing r_A^i , given r_A is the true value, follows a lognormal distribution.

$$L(r_A^i | r_A) = LN(r_A^i | r_A) = (r_A \sigma \sqrt{2\pi})^{-1} e^{-\frac{(\ln r_A^i - \ln r_A)^2}{2\sigma^2}} \quad (10)$$

where σ is the strength of or the confidence in the evidences, and should be specified by the analysts.

Inserting (10) into (9), and then (8) and (9) into (7) yields

$$\begin{aligned} \varphi(r_A | E) &= \frac{1}{k} \left(\prod_{i=1}^n (r_A \sigma \sqrt{2\pi})^{-1} e^{-\frac{(\ln r_A^i - \ln r_A)^2}{2\sigma^2}} \right) \times \\ & (r_A \omega_0 \sqrt{2\pi})^{-1} e^{-\frac{(\ln r_A - \ln \omega_0)^2}{2\omega_0^2}} \end{aligned} \quad (11)$$

where k is the normalization factor

$$\begin{aligned} k &= \int_{r_A} \left(\prod_{i=1}^n (r_A \sigma \sqrt{2\pi})^{-1} e^{-\frac{(\ln r_A^i - \ln r_A)^2}{2\sigma^2}} \right) \times \\ & (r_A \omega_0 \sqrt{2\pi})^{-1} e^{-\frac{(\ln r_A - \ln \omega_0)^2}{2\omega_0^2}} dr_A \end{aligned}$$

When the lognormal prior paired with a lognormal likelihood function, the posterior is also a lognormal distribution. In the case of one piece of evidence, i.e., $n = 1$, we have

$$\varphi(r_A | E) = LN(r_A | \theta_1, \omega_1) = (r_A \omega_1 \sqrt{2\pi})^{-1} e^{-\frac{(\ln r_A - \ln \theta_1)^2}{2\omega_1^2}} \quad (12)$$

where: $\theta_1 = \theta_0^{\omega_b} (r_A^1)^{\omega_b}$, $\omega_a = \frac{\sigma^2}{\omega_0^2 + \sigma^2}$, $\omega_b = \frac{\omega_0^2}{\omega_0^2 + \sigma^2}$,
and $\omega_1 = \left(\sqrt{\frac{1}{\omega_a^2} + \frac{1}{\sigma^2}}\right)^{-1}$.

Equation (12) can be easily generalized to accommodate n pieces of evidence by using the equation iteratively.

Given the prior distribution parameters θ_0 , ω_0 and the confidence in the evidences σ , the posterior distribution of r_A can be obtained. Thus, the OFR distribution can be estimated by combining r_A and the GFR of the item of interests according to (6). It is worth to notice that the resulting OFR is a failure rate based on industry average E/P conditions, for the plant-specific failure rate, the OFR needs to be further modified according to the plant-specific E/P conditions.

IV. NUMERICAL EXAMPLE

An example using hypothetical data is presented in this section to illustrate the proposed model and approach. Ten item samples are assumed for this example.

TABLE I.
GFR, OFR AND r_A^i FOR THE EXAMPLE.

| i | 1 | 2 | 3 | 4 | 5 |
|---|--------|--------|-------|-------|-------|
| $\bar{\lambda}_G^i$ (10^{-6} per hour) | 166.07 | 354.71 | 20.52 | 72.61 | 13.64 |
| $\bar{\lambda}_A^i$ (10^{-6} per hour) | 64.77 | 258.94 | 8.41 | 30.50 | 15.96 |
| r_A^i | 0.39 | 0.73 | 0.41 | 0.42 | 1.17 |
| i | 6 | 7 | 8 | 9 | 10 |
| $\bar{\lambda}_G^i$ (10^{-6} per hour) | 24.450 | 113.47 | 0.970 | 6.790 | 2.810 |
| $\bar{\lambda}_A^i$ (10^{-6} per hour) | 33.25 | 103.26 | 5.22 | 5.02 | 1.24 |
| r_A^i | 1.36 | 0.91 | 5.38 | 0.74 | 0.44 |

The GFRs, see the second row of Table I, are from OREDA [2] for 10 random items. The OFRs of organization A for the same items are assumed and listed in the third row of Table 1. The r_A^i -s are calculated according to (6) and given in the fourth row of Table 1. Further assume a lognormal prior, $r_A \sim LN(\theta_0, \omega_0)$ with $\theta_0 = 1$, $\omega_0 = 0.6$. σ is set to 5 to represent a relatively low confidence in the evidences.

Suppose organization A does not have experience with one type of pressure transmitter, we show how to estimate failure rate of this type of pressure transmitter when it is operated by A. Suppose the GFR of the pressure transmitter has a lognormal distribution [18] with a median equal to 3×10^{-7} per hour and an error factor equal to 2. We have $\bar{\lambda}_G^{PT} \sim LN(3 \times 10^{-7}, 0.421)$ (see [1] for equations to convert error factor to lognormal parameter).

Applying (12) 10 iterations for the data in Table 1 yields posterior distribution, $r_A \sim LN(0.9608, 0.9478)$. The prior and posterior distributions are plotted in Fig. 1.

The $\bar{\lambda}_A^{PT}$ can be calculated using (6). Since both $\bar{\lambda}_G^{PT}$ and r_A are given as probability distribution, the distribution of $\bar{\lambda}_A^{PT}$ is calculated using Monte Carlo simulation. The results are shown in Fig. 2. The median OFR of the pressure transmitter, when operated by A, is 2.88×10^{-7} per hour, with a standard deviation 6.88×10^{-7} .

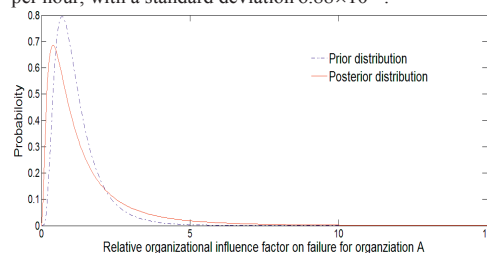


Fig. 1. Prior and posterior distribution of r_A .

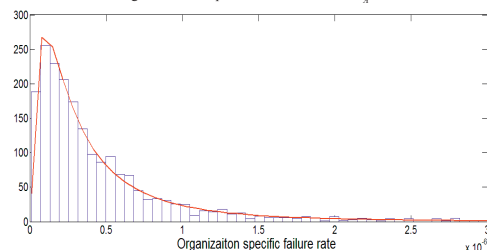


Fig. 2. Organization A specific failure rate of the pressure transmitter.

V. DISCUSSION AND CONCLUSIONS

In this paper, the MIL-HDBK-217F failure rate model is extended to include the organizational factors and a Bayesian approach is proposed to quantify the organizational influences on failure rate. Compared with most studies that attempt to explicitly model organizational influences, our approach is to extract information from the failure rate data. At the same time, the results from other explicit models can be included as prior information in the proposed approach. Hence, the proposed approach can be combined with other models to make maximum use of the available information for failure rate estimation.

It is worth pointing out that when designing a new system, the available data are usually GFRs, and using the proposed model will lead to OFRs. Both GFRs and OFRs are based on the industry average E/P conditions. To obtain the plant specific failure rate, the OFRs need to be further modified by considering the specific E/P conditions.

In addition, it is assumed that organizational influences on failure rate do not change with the items within the organization. This may not always be true. The main

organizational influences affect failure rates through operation and maintenance, so items frequent operated and maintained are less influenced by the organizational factor than those that are not. To cope with this issue, we may categorize items according to the organizational influences, and estimate separate factors for each category.

The model and approach in this paper are proposed for individual organizations. In some industries significant differences in terms of failure rates exist among sub-organizations within a big organization. Take offshore petroleum industry as an example, different failure rates may be observed for the same item in different offshore installations within an oil company. This is because installations have their local cultures, work practices and operation philosophy etc. This issue can be accommodated by extending the proposed model to sub-organizations: Using sub-OFRs and OFRs to replace OFRs and GFRs in the original model, respectively. The only requirement is that the sub-organizations and the organization have the same average E/P conditions. And it is noticed that at the sub-organization level less failure rate data are available.

ACKNOWLEDGMENT

The first author thanks Det Norske Veritas (DNV) for providing travel grant for his visit to the University of Maryland College Park.

REFERENCES

- [1] M. Rausand and A. Høyland, *System Reliability Theory: Models, Statistical Methods and Applications* (2nd. ed.), New York, USA: Wiley, 2004.
- [2] OREDA, *Offshore Reliability Data Handbook*, Trondheim, Norway: SINTEF, 2002.
- [3] J. Reason, *Managing the Risks of Organizational Accidents*, UK: Ashgate, Aldershot 1997.
- [4] J. Rasmussen, "Risk management in a dynamic society: a modeling problem," *Safety Science*, vol. 27, pp. 183-213, 1997.
- [5] N. Leveson, "A new accident model for engineering safer systems," *Safety Science*, vol. 42, pp. 237-270, 2004.
- [6] D.E. Embrey, "Incorporating management and organizational factors into probabilistic safety assessment," *Reliability Engineering and System Safety*, vol. 38, pp. 199-208, 1992.
- [7] K. Davoudian et al., "The work process analysis model (WPAM)," *Reliability Engineering and System Safety*, vol. 45, pp. 107-125, 1994.
- [8] D.M. Murphy and M.E. Paté-Cornell, "The SAM framework: modeling the effects of management factors on human behavior in risk analysis," *Risk Analysis*, vol. 16, pp. 501-515, 1996.
- [9] A. Mosleh et al., "The ω -factor approach for modeling the influence of organizational factor in probabilistic safety assessment," in *IEEE sixth annual human factor meeting*, Orlando, Florida, 1997.
- [10] N.J. Duijm and L. Goossens, "Quantifying the influence of safety management on the reliability of safety barriers," *Journal of Hazardous Materials*, vol. 130, pp. 284-292, 2006.
- [11] K. Øien, "A framework for the establishment of risk indicators," *Reliability Engineering and System Safety*, vol. 74, pp. 147-167, 2001.
- [12] T. Aven, et al., "Barrier and operational risk analysis of hydrocarbon releases (BORA-Release): Part I: Method description," *Journal of Hazardous Materials*, vol. 137, pp. 681-691, 2006.
- [13] B.A. Gran et al., "Evaluation of the Risk OMT model for maintenance work on major offshore process equipment," *Journal of Loss Prevention in the Process Industries*, vol. 25, pp. 582-593, 2012.
- [14] M. Schönbeck et al., "Human and organizational factors in the operational phase of safety instrumented systems: A new approach," *Safety Science*, vol. 48, pp. 310-318, 2010.
- [15] MIL-HDBK-217F, "Reliability prediction of electronic equipments," Department of defense, Washington D.C., 1990.
- [16] M.S. Hamada et al., *Bayesian Reliability*, USA: Springer, 2008.
- [17] A. Mosleh and G. Apostolakis, "Model for the Use of Expert Opinions," in *Low Probability, High Consequence Risk Analysis: Issues, Method and Case Studies*, R.A. Waller and V.T. Covello, Eds. New York, USA: Plenum Press, 1984.
- [18] WASH-1400-MR, "Reactor safety study: An assessment of accident risks in US. Commercial nuclear power plants," Nuclear Regulatory Commission, Washington D.C., 1975.

Article 9 (conference)

Common-cause failures in safety-instrumented systems
–In *PSAM 11 & ESREL 2012*

Is not included due to copyright

Article 10 (conference)

Uncertainty assessment of reliability estimates for safety-instrumented systems
–In *ESREL 2011*

Is not included due to copyright

