Doctoral theses at NTNU, 2009:9

Mary Ann Lundteigen

# Safety instrumented systems in the oil and gas industry:

## Concepts and methods for safety and reliability assessments in design and operation

Mary Ann Lundteigen

Doctoral Thesis

Doctoral theses at NTNU, 2009:9

NTNU
Norwegian University of
Science and Technology
Thesis for the degree of
doktor ingeniør
Faculty of Engineering Science and Technology
Department of Production and Quality Engineering

NTNU
Norwegian University of
Science and Technology

NTNU
Norwegian University of
Science and Technology

NTNU

ISBN 978-82-471-1385-1 (printed ver.)
ISBN 978-82-471-1386-8 (electronic ver.)
ISSN 1503-8181

Mary Ann Lundteigen

# Safety instrumented systems in the oil and gas industry:

## Concepts and methods for safety and reliability assessments in design and operation

Thesis for the degree of philosophiae doctor

Trondheim, January 2008

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

NTNU
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

ISBN  978-82-471-1385-1 (printed ver.)
ISBN 978-82-471-1386-8 (electronic ver.)
ISSN 1503-8181

Doctoral Theses at NTNU, 2009:9

Printed by Tapir Uttrykk

Mary Ann Lundteigen

# Safety instrumented systems in the oil and gas industry

## Concepts and methods for safety and reliability assessments in design and operation

Thesis for the degree of philosophiae doctor

Trondheim, November 2008

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

NTNU
Norwegian University of
Science and Technology

# Preface

This thesis is the result of a PhD project at the Department of Production and Quality Engineering, the Norwegian University of Science and Technology (NTNU). The work was carried out from October 2005 till November 2008.

The PhD project has been carried out in close collaboration with my main supervisor, Professor Marvin Rausand at Department of Production and Quality Engineering (NTNU), and his contributions are reflected in several articles. The co-supervisor has been Professor Tor Onshus at Department of Engineering Cybernetics (NTNU). He has contributed with his broad industrial network within the oil and gas industry.

The PhD project has been a unique opportunity for making contributions to a field in which I take great interest, namely reliability of safety instrumented systems. Previously, I have worked with safety instrumented systems from a more practical viewpoint. This knowledge has been used as basis for the development of new concepts and methods which I hope will lead to safer and more reliable design and operation of such systems.

Trondheim,
February 2009

*Mary Ann Lundteigen*

# Acknowledgements

Taking a PhD is a personal project, but it could not been carried out without the support of others. First, I would like to thank my main supervisor, Professor Marvin Rausand, for all his support, guidance and encouragement. I have seen it been mentioned before, but I would like to repeat it here: If I ever get to supervise a PhD student, he will serve as a role model.

I would also like to thank my co-supervisor, Professor Tor Onshus, for sharing his industrial network with me and giving me some guidance on how to connect to the oil and gas industry during the project.

One particular useful connection has been with StatoilHydro at Stjørdal, and I would like to thank Bjørnar Berg and Espen Sørensen for involving me in their work.

On two articles, I have collaborated with researchers from SINTEF. This has lead to fruitful discussions, and I would like to thank my co-authors Stein Hauge from SINTEF Department for Safety and Reliability and Odd Nordland from SINTEF Department of Software Engineering, Safety, and Security for this collaboration. I would also like to thank Hans Berstad from SINTEF Department of Applied Cybernetics, who shared his extensive and detailed knowledge on safety instrumented systems with me in several industry projects before I started the PhD study.

At the Department of Production and Quality Engineering, we have weekly meetings where PhD students present their plans, articles, and preliminary results. These meetings have been a valuable arena for getting feedback on own work. I would therefore like to thank all participants in the RAMS group for their support throughout the project.

It is difficult to start a PhD project without the support of my employer at that time, SINTEF Department of Applied Cybernetics. I highly appreciate that they have given me the time to carry out this project.

Finally, I would like to thank my husband, Egil, and my children, Vegard and Eirik, for their patience and for giving me something else to concentrate on than the PhD project. I would also like to thank my brother, Alf, my parents, and my parents-in-law for their support and practical help along the way.

# Summary

This PhD thesis proposes new methods and gives new insight to safety and reliability assessments of safety instrumented systems (SISs). These systems play an important role in many industry sectors and are used to detect the onset of hazardous events and mitigate their consequences to humans, the environment, and material assets.

This PhD thesis focuses on SIS applications in the oil and gas industry. Here, the SIS must respond to hazardous events such as gas leakages, fires, and overpressurization. Because there are personnel onboard the oil and gas installations, the operations take place in a vulnerable marine environment, and substantial values are associated with the offshore facilities, the reliability of SIS is of great concern to the public, the authorities, and the plant owners.

The objective of this PhD project has been to *identify* some of the key factors that influence the SIS reliability, *clarify* their effects on reliability, and suggest means to *improve* the treatment of these factors in safety and reliability assessments in design and operation.

The PhD project builds on concepts, methods, and definitions in two key standards for SIS design, construction, and operation: IEC 61508 and IEC 61511. IEC 61508 is a generic standard, and applies to more than one industry sector and to SIS manufacturers who develop new products for safety applications. IEC 61511 is a process sector standard and applies to SISs that are based on well proven or certified components.

The main contributions from this PhD project are:

- A product development model that integrates reliability, availability, maintainability, and safety (RAMS) requirements with product development.
- An approach for how to demonstrate compliance to IEC 61508.
- An approach for how to carry out reliability analysis of complex SIS.
- A clarification of the concepts of architectural constraints and safe failure fraction (SFF), and a discussion of why the SFF may not be suited as a design parameter.

- A clarification and classification of the concept of spurious activations and spurious activation rate.
- An approach for how to determine the test coverage of partial stroke testing of shutdown valves.
- An approach for how to defend against common cause failures (CCFs) in the operational phase.
- An approach for how to use field data to monitor and act upon the SIS reliability performance.

It has been important to share the contributions and ideas for further work with other researchers. The contributions have been presented in ten articles, where five have been published in international journals, two have been submitted for publication, and three have been presented at conferences and in conference proceedings.

The contributions are also directed to the industry and the actors that are involved in SIS design, construction, and operation. Even if the oil and gas industry is the main focus area of the PhD project, the results may be relevant for other industry sectors as well.

SIS manufacturers and SIS designers face a large number of requirements from authorities, oil companies, international standards, and so on. At the same time, they are requested to use the safety life cycle model in IEC 61508 as basis for their product development. This PhD thesis links the safety life cycle model in IEC 61508 to a more general product development model, where IEC 61508 requirements are discussed in light of other RAMS requirements.

SIS manufacturers who develop products for more than one industry sector must often adhere to IEC 61508 as well as sector specific standards. Some of the sector specific standards build directly on IEC 61508, while others have been developed prior to IEC 61508 and may use different concepts and approaches. This PhD thesis describes an approach for qualification of a software development platform in light of these challenges.

SIS designers have to balance the SIS reliability with the practicality of performing functional tests. Functional tests are important means to reveal SIS failures, but the tests often require process shutdowns. Partial stroke testing is a valve test that does not require full valve closure, but the test efficiency is highly influenced by the test coverage. This PhD thesis suggests a way to determine the test coverage, taking into account application specific considerations and generic data for valve failures.

Traditionally, the oil and gas industry has aimed at keeping the SIS as simple as possible, and here, reliability block diagrams have been well suited for reliability analysis. However, technology development challenges the principle of simplicity, and then fault tree analysis may be better suited to achieve complete reliability models and for involving design engineers in the model construction and verification. Many software tools for fault tree analysis make non-conservative estimates for the reliability of periodically tested SISs, which may not be acceptable when the estimates are used as basis for selecting hardware architecture. This PhD thesis proposes a conservative calculation approach for fault tree analysis that builds on calculation methods that the oil and gas industry are familiar with.

The architectural constraints are used in IEC 61508 and IEC 61511 to restrict the freedom in selecting hardware architecture and to avoid that architecture is determined based on reliability calculations alone. The architectural constraints, and in particular the SFF, have been questioned by many researchers, SIS designers, manufacturers, and end users. The insight that is provided in this PhD thesis to the desired and undesired properties of the SFF and the architectural constraints may therefore be of interest to several parties. In addition, IEC 61508 and IEC 61511 committees may find the clarification and discussion useful as they are now in the process of evaluating whether or not to keep these concepts in future revisions of the standards.

Spurious activations of SIS may lead to production losses, loss of confidence to the SIS, and more undesired events due to the increased number of shutdowns and start-ups. IEC 61508 and IEC 61511 do not give explicit constraints for the spurious activation rate, but oil companies must still consider this issue because of operational and safety considerations. To account for spurious activations when selecting SIS design requires insight to why spurious activations occur and how the spurious trip rate may be estimated. This PhD thesis introduces three new definitions related to spurious activation; spurious operation, spurious trip, and spurious shutdown, as a means to clarify the underlying causes of spurious activations and how they are to be included when calculating the spurious trip rate.

Oil companies have to align their operation and maintenance according to requirements in IEC 61508 and IEC 61511. Two areas where the IEC standards may require some adjustments to the way of operating and maintaining a SIS are the handling of CCFs and the follow-up of SIS safety integrity performance. This PhD thesis suggests an approach on how to defend against CCFs that may be implemented with current practises for planning, execution, and follow-up of functional testing and inspection activities. The PhD thesis also presents an approach for how field data may be used to monitor the safety integrity and for making adjustments to the test intervals.

There are several areas of further research. One area is related to implementation of new approaches and concepts from this PhD project into existing industry practises. Another area is to develop and improve existing concepts and methods for reliability and safety assessments to account for new technologies and new ways of operating oil and gas facilities.

# About this thesis

The PhD thesis is written for scientists, safety professionals, managers, and other personnel with knowledge or interest in safety and reliability assessments. Some knowledge about the offshore oil and gas industry is beneficial. It is also an advantage to understand the concepts and main principles of the IEC 61508 and IEC 61511 standards.

The thesis has three parts; Part I Main report, Part II Articles, and Part III Supplementary information. A list of acronyms and abbreviations and a glossary are provided at the end of the thesis.

Part I starts with a brief introduction to safety instrumented systems (SIS) and why they are important in many industry applications, and continues with a presentation of research challenges, objectives, and main results. The main research principles and the approach are also presented.

Part II comprises the ten articles that have been developed as part of the PhD project. Here, five articles are published in international journals, two articles have been submitted for publication, and three articles have been presented in conferences and conference proceedings.

Part III gives supplementary information on SIS and SIS related standards and guidelines. Readers who are not familiar with IEC 61508 and IEC 61511, may find it beneficial to read Part III in addition to the introductory sections in Part I.

# Contents

## Part I Main report

**Part II Articles**

## Part III Supplementary information

# Part I

# Main report

# 1

# Introduction

## 1.1 Background

Our safety is increasingly taken care of by safety instrumented systems (SISs), where electrical, electronic, and/or programmable electronic (E/E/PE) devices interact with mechanical, pneumatic, and hydraulic systems. Such systems are, for example, frequently used in cars. When you press the brake pedal while driving, your pedal force may not necessarily be added directly to the car brakes. Instead, a PE device may convert the pedal force to an electrical signal which is then used to activate the brake blocks.

During heavy braking, you may experience that the pedal pulses even if you apply a constant force. In this case, your car has an anti-lock braking system that prevents the wheels from locking by repeatedly releasing and applying braking force. This system helps you as a driver to maintain control over the car. If you still loose control and drive into the ditch, the electronic based air bag system will release and reduce the extent of damages.

SISs have a much wider application area than the car example. They are of vital importance at process plants to detect the onset of hazardous events, for example a release of some hazardous material, and for mitigating their consequences to humans, the environment, and material assets.

SISs are also found in many transportation systems. One example is railway signalling systems, where SISs are used to set light signals and operate switches. If the train enters a rail section without permission, for example a train passing a red light (‘stop’) signal, there may be an additional SIS, the automatic train protection system, that forces the train to start immediate retardation. SISs are also an integral part of aircraft and air traffic control systems, to ensure safe operation of aircrafts in air as well as on ground.

So, when you drive to work or travel by plane to a distant location, you rely on the SIS to respond to hazardous events. And you may ask: How reliable are these systems and how can we make sure that they provide the necessary protection?

This PhD thesis addresses these questions and suggests methods and concepts to be used by researchers, reliability analysts, design engineers, and end users for their joint effort in building and operating safe SIS.

The main focus is SIS applications in the oil and gas industry, and particularly in light of IEC 61508 and IEC 61511, two standards that are widely accepted for SIS design and operation. Even so, many of the basic principles and research results apply to other industry sectors as well.

### 1.1.1 Safety instrumented systems

The main purpose of a SIS is to bring the plant or an equipment to a safe state if an hazardous event occurs. Hazardous events may be gas leakages or too high or too low pressures, temperatures, and liquid levels. If the SIS fails to perform the intended functions, the event may develop into an accident, for example an explosion.

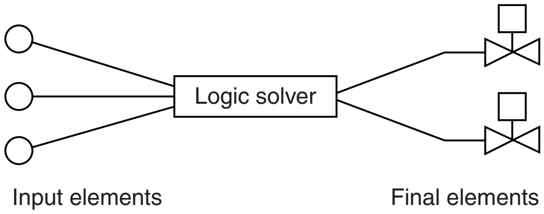


**Fig. 1.1.** Simplified illustration of a SIS

A SIS may be split into three main subsystems as illustrated in Fig. 1.1; input elements, logic solvers, and final elements. These three subsystems are used to perform safety instrumented functions (SIFs).

A more detailed presentation of SIS and SIS related concepts is given in Part III, Chapter 4.

### 1.1.2 Safety and reliability assessments

Safety and reliability assessments play an important role in SIS design, construction, and operation. Such assessments are used to select and qualify a SIS for a particular application with the given functional and reliability requirements. When the SIS is put into operation, data may be collected to update the safety and reliability assessments and verify that the SIS continues to meet the specified requirements.

Safety and reliability assessments comprise activities such as reliability modeling and calculations, design reviews, testing, and failure analysis.

The purpose of a design review is to examine the documentation of hardware and software and evaluate if all the stated requirements are catered for. Failure analysis is often performed as part of the design review, to ensure that all failure causes and effects are identified and handled in the SIS design. One frequently used method is the failure modes and effect analysis (FMEA) [108]. In the operation phase, failure analysis may be used to determine corrective actions and ways to prevent similar failures in the future.

Reliability modeling may be performed by the use of reliability block diagrams, Markov state transition diagrams, fault tree analysis, petri-net, or binary decision diagrams [108, 81, 48, 38, 112, 18]. Quantitative results may be obtained by approximation formulas [108, 24, 114], or by exact formulas [18, 112]. Many calculation methods that are used with periodically tested SIS are based on approximations [48, 100, 114].

Testing may be performed once the SIS hardware and software have been constructed or purchased. Testing of hardware and the integrated software and hardware may start with individual components and end with the SIF loops. Software testing may follow the V model. The V model combines a top-down software design approach with a bottom up testing strategy [38, 116]. In the operational phase, testing is a key activities to reveal hidden SIS failures and to verify that any modification to the SIS hardware or software leads to the intended result.

The stated requirements are given in regulations and standards. National and international regulatory authorities provide overall requirements for SIS design, implementation, and operation. For the detailed implementation of these requirements, the regulations often refer to international standards like IEC 61508 and IEC 61511. IEC 61508 was introduced in 1998, while IEC 61511 was published in 2003, as the process sector implementation of the IEC 61508. In this PhD thesis, these two standards are often referred to as “the IEC standards”.

Other sectors and application areas have also developed their own standards based on IEC 61508, or modified existing standards to reflect the IEC 61508 requirements, for example IEC 62061 [41] for machinery control systems, IEC 62425 [45] for railway signalling systems, IEC 61513 [40] for nuclear power plants, and IEC 60601[36] for medical equipment.

A more detailed presentation of IEC 61508, IEC 61511, and other related standards is given in Part III, Chapter 5.

### 1.1.3 IEC 61508 and IEC 61511

IEC 61508 and IEC 61511 outline requirements, principles, and methods for safety and reliability assessments, and indicate at what point in time such assessments should be performed.

The main purpose of the IEC standards is to define a unified approach to safe and reliable SIS design, implementation, and operation. Even if some of the principles, concepts, and methods have been used in previous standards, IEC 61508 and IEC 61511 represent a further development, taking into account the challenges and opportunities of using E/E/PE technology. The standards do not only address technical aspects, but also work processes, procedures, and tools necessary to specify, develop, operate, and maintain SIS hardware and software.

IEC 61508 organizes its requirements according to a safety life cycle. The safety life cycle comprises 16 phases and is illustrated in Fig. 1.2. IEC 61511 uses a similar life cycle model. A more detailed discussion of the safety life cycle phases is given in Part III, chapter 5.3.

Two concepts are used to describe the desired safety and reliability performance; the functional safety requirements, stating *what* the SIS is required to do, and the safety integrity requirements, stating *how well* the SIS is required to perform. IEC 61508 and IEC 61511 distinguish between four safety integrity levels (SIL), ranging from SIL 1 to SIL 4 where SIL 1 is the least and SIL 4 is the most reliable level. For each SIF, the SIL is selected so that the necessary risk reduction is achieved.

A SIL requirement gives restrictions and guidance on the selection of hardware, software, and associated tools, procedures, and work processes. If a SIS implements several SIFs that have different SIL requirements, the strictest SIL requirement applies to any shared components like for example a logic solver.

Safety integrity is split into three parts: Hardware safety integrity, software safety integrity, and systematic safety integrity. To meet a SIL requirement, it is necessary to demonstrate that all parts achieve the specified SIL. If, for example, it is confirmed that a SIF meets SIL 2 in terms of hardware safety integrity, we can not claim compliance to this SIL unless the systematic and software safety integrity also meet SIL 2.

Verification of adequate hardware safety integrity is a two step process. First, it is required to calculate the reliability of the SIFs and compare the results with the SIL requirement, and second it is required to determine the architectural constraints.

IEC 61508 uses probability of a dangerous failure per hour (PFH) for a SIS that operates continuously and probability of failure on demand (PFD) for a SIS that operates on demand. A reliability target range is specified for each SIL. The PFD target range for a SIL 2 safety function is, for example, between $1 \cdot 10^{-3}$ and $1 \cdot 10^{-2}$. This means that a SIL 2 safety function must perform its intended functions in (at least) 99 out of 100 demands. The IEC standards suggest using the beta factor model for including common cause failures (CCFs) in the calculations, and IEC 61508, ISA TR 84.00.02 [48], and the PDS method [114] give some practical examples on how the model can be applied for different hardware configurations.

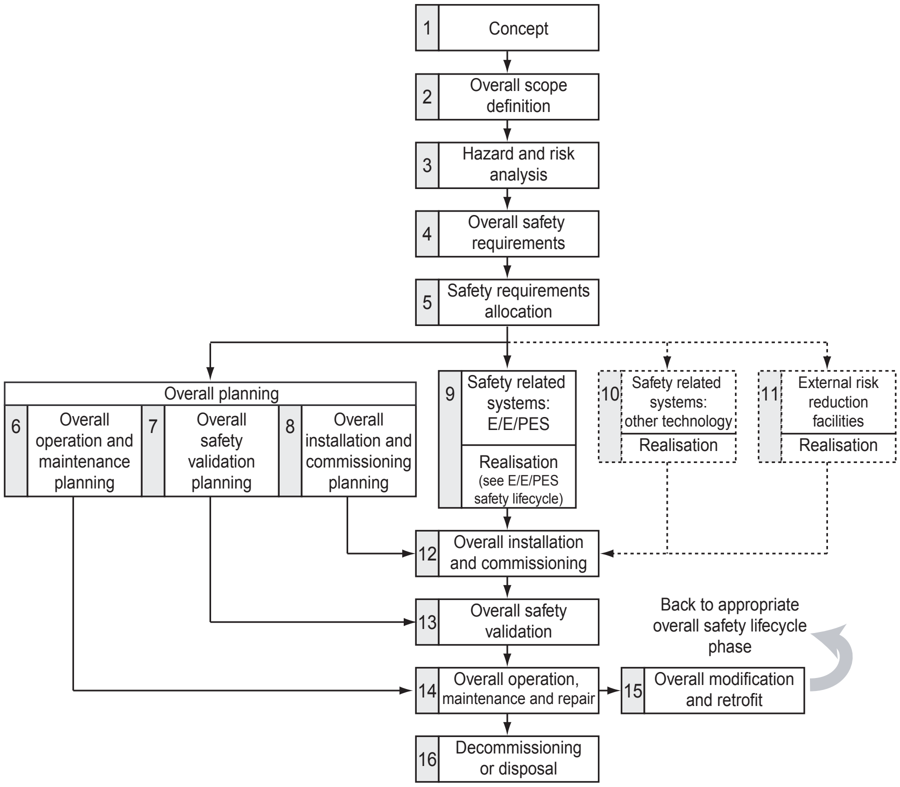

1 Concept
2 Overall scope definition
3 Hazard and risk analysis
4 Overall safety requirements
5 Safety requirements allocation
Overall planning
6 Overall operation and maintenance planning
7 Overall safety validation planning
8 Overall installation and commissioning planning
9 Safety related systems: E/E/PES
Realisation (see E/E/PES safety lifecycle)
10 Safety related systems: other technology
Realisation
11 External risk reduction facilities
Realisation
12 Overall installation and commissioning
13 Overall safety validation
14 Overall operation, maintenance and repair
15 Overall modification and retrofit
Back to appropriate overall safety lifecycle phase
16 Decommissioning or disposal

**Fig. 1.2.** Safety life cycle (from [38])

The architectural constraints are used to determine the minimum hardware fault tolerance, taking into account some key properties such as the component complexity and the safe failure fraction (SFF). The SFF is the proportion of "safe" failures among all failures. A "safe" failure is either a failure that is safe by design, or a dangerous failure that is immediately detected and corrected. The IEC standards define a safe failure as a failure that does not have the potential to put the SIS in a hazardous or fail-to-function state. A dangerous failure is a failure that can prevent the SIS from performing a specific SIF, but when detected soon after its occurrence, for example by online diagnostics, the failure is considered to be "safe" since the operators are notified and given the opportunity to implement compensating measures and necessary repairs. In some cases, the SIS may automatically respond to a dangerous detected failure as if it were a true demand, for example, causing shutdown of a process section or the whole plant.

To ensure compliance with software and safety integrity requirements, the standards promote verification and validation in various stages of the SIS life cycle, including design reviews, commissioning, testing, and audits. The key audit activity is functional safety assessment (FSA). This is an extended review were compliance to all requirements of the IEC 61508 or IEC 61511 is investigated.

The introduction of the IEC standards has lead to a more unified approach to SIS design, construction, and operation. However, the standards also give new challenges to the industry, as they have to adapt their current practises to new concepts, principles, and requirements. The concepts, principles, and requirements are not always fully understood, which in some cases lead to unintended use.

The implications of IEC 61508, and related standards as IEC 61511, are extensively discussed in the literature [5, 11, 128, 12, 109, 110, 24, 116, 125, 121, 13]. Still, SIS manufacturers, SIS designers, and end users seem to request more guidance on how to adapt to the IEC requirements.

## 1.2 Research challenges and questions

Based on a thorough literature review[1] and discussion with SIS manufacturers and end users, some overall challenges include:

- Some of the key concepts that have been introduced with IEC 61508 and IEC 61511 are not well defined and fully understood.
- As a result, many concepts are applied differently leading to different, and not always comparable results.
- There seems to be insufficient attempts to analyze key factors that influence reliability, and provide guidance on their constraints and recommended use.
- SIS manufacturers, system integrators, and end users still seem to lack guidance on how to adjust their current work processes, tools, and procedures to IEC 61508 and related standards.

More specifically, the following specific challenges related to safety and reliability assessments have been identified.

### 1.2.1 RAMS requirements from the SIS producer's perspective

SIS manufacturers must often adhere to IEC 61508 when designing and constructing *new* SIS devices. IEC 61511 does, for example, direct SIS manufacturers back to IEC 61508 for design and qualification of new SIS devices. For SIS manufacturers, it may therefore be advantageous to align their product development process with the framework in IEC 61508, but IEC 61508 does not provide all necessary requirements for SIS development. Manufacturers also face other

[1] with basis in Part II and Part III.

safety, availability, maintainability, and safety (RAMS) requirements from customers and authority regulations and directives.

Many authors address product development models and product development challenges [103, 10, 78, 61, 15, 25, 26, 80]. Product development is viewed from different angles; The producer (e.g., manufacturer, system integrator) perspective, consumer (e.g., end user) perspective, or a combination of the two perspectives. Unfortunately, none of the models indicate how RAMS requirements can be catered for in the context of IEC 61508. Relevant research questions to address are therefore:

- What are the RAMS requirements from a SIS producer's perspective?
- How can a product development model reflect RAMS requirements in light of the requirements in IEC 61508?

### 1.2.2 Adoption of IEC 61508 requirements

Industry specific standards are used to integrate the IEC 61508 requirements with sector specific considerations, design principles, and terms. For SIS manufacturers who develop equipment or systems for more than one industry sector, it is important to have methods and tools that comply with IEC 61508 as well as with the sector specific standards. However, many SIS manufacturers find this task overwhelming, and seek guidance on how to demonstrate that their products meet the relevant requirements. A relevant research question to address are therefore:

- What approach may be taken for qualifying a product according to the IEC 61508 and relevant sector specific requirements?

### 1.2.3 Reliability analysis of complex SIS

As mentioned in Section 1.1.2, there are several approaches for calculating the SIS reliability. Obtaining a point value of the reliability, for example for the average PFD, is not the only purpose of such an analysis. The analysis should help designers understand the functionality of the SIS and give advice to how the SIS design can be improved. Such improvements may be related to physical design changes, changes to the voting logic, improved diagnostic test routines, protection against common cause failures (CCF), and so on. An important objective of reliability analysis is therefore to provide a decision basis which is possible to comprehend by design engineers who are usually not trained in reliability engineering.

The reliability analysis approaches have different strengths and weaknesses. Many SISs include complex interactions of pneumatic, hydraulic, electrical, and programmable electrical components, and in this case it is necessary to select a method that can capture the complexity and at the same time contribute with more insight to how the SIS works among SIS designers, operators, and maintenance personnel. These strengths and weaknesses are best demonstrated by case studies. Case studies are therefore often requested and welcomed to share experience and increase the awareness to their practical use. Relevant research questions to address are therefore:

- What kind of reliability modeling and calculation approaches are suitable for complex SISs, taking into account the need to provide information that may be possible to comprehend by SIS designers, operators, and maintenance personnel?
- What kind of practical considerations can be made to the handling of CCFs?

### 1.2.4 The ambiguity of the architectural constraints

In the design phase, the PFD is calculated based on generic data (e.g., generic failure rates). This initial PFD estimate, which is sometimes referred to as the predicted performance [80], may be uncertain due to a number of reasons. Following the recommended approach in IEC 61508 and IEC 61511, the contribution from software failures and systematic failures are often excluded. In addition, the effects of operational and environmental conditions on the SIS hardware may not be fully known and catered for in the input data. Assumptions and simplifications that are made for the reliability modeling and analysis may also influence to what extent the predicted PFD gives a realistic indication of the performance.

Based on these arguments, IEC 61508 and IEC 61511 have included a set of additional requirements to achieve a sufficiently robust hardware architecture. These requirements are referred to as *architectural constraints*, and their intention is to have one (or more) additional channels that can activate the SIF in case of a fault within the SIS. The architectural constraints prevent SIS designers and system integrators from selecting architecture based on PFD calculations alone, and the requirements may therefore be seen as restrictions in the freedom to choose hardware architecture.

The architectural constraints are sometimes interpreted as a mistrust to the quantitative reliability analysis. Reliability experts frequently debate whether or not the architectural constraints are necessary. It is particularly the suitability of the safe failure fraction (SFF) that has been questioned [66, 47, 111].

A thorough analysis of the architectural constraints and the SFF, and their intended and non-intended effects on reliability seems to be missing. A relevant research question to address is therefore:

- How do the architectural constraints affect reliability, and in particular, the SFF?

### 1.2.5 The concept of spurious activations

The main focus of IEC 61508 and IEC 61511 is to ensure that the SIS is able to perform on demand. Limited focus is given to spurious activations and their causes and effects. IEC61508 has no requirements related to spurious activations. IEC 61511 requires that a maximum *spurious trip rate* is specified, but the standard does not provide any definition of a spurious trip or guidance on how the rate should be estimated and catered for when selecting SIS design.

To estimate the spurious trip rate, the oil and gas industry often uses the formulas presented in [122, 48, 114, 116]. When comparing these formulas, it is evident that there is no unique interpretation of the spurious trip concept. While the PDS[2] method [114] defines a spurious trip as a spurious *activation* of a single SIS element or of a SIF, ANSI/ISA 84.00.01 [8] refers to a spurious trip as a non-intended process shutdown. As a result, the concept of spurious trip is rather confusing and it is difficult to compare the spurious trip rate in different applications. Relevant research questions to address are therefore:

- What is meant by spurious activation?
- How may spurious activation be classified?
- What factors should be considered when calculating the spurious activation rate?

### 1.2.6 Defense against CCFs in the operational phase

End users need to have work practises, procedures, tools, and personnel competence to maintain the desired SIS performance. Safety and reliability assessments often indicate that the most important contributor to SIS failure is CCFs. CCFs may affect several redundant components, and thereby violate the intended tolerance against hardware failures.

The events, acts, and conditions that lead to CCFs may be introduced in design as well as in the operational phase. For design and construction, checklists have been developed to ensure that measures are taken to reveal and avoid introducing CCFs. Similar tools seem to be missing for SIS follow-up in the operational phase.

Relevant research questions to address are therefore:

- How are CCFs introduced in the operational phase?
- How can CCFs be identified, analyzed and prevented during SIS operation and maintenance?

[2] PDS is the Norwegian abbreviation of “reliability of computer-based safety systems”.

### 1.2.7 The reliability effects of introducing partial stroke testing

Partial stroke testing (PST) is sometimes introduced to improve reliability of shutdown valves. The reliability gain may be used to improve safety and/or to reduce costs [68]. The magnitude of reliability improvement is influenced by the *PST coverage* factor, which expresses to what extent failures can be revealed during PST compared to functional tests.

While several authors have discussed how to take credit for PST in reliability calculations [6, 4, 64, 76, 120], little guidance has been given on how to determine the PST coverage factor. Lundteigen and Rausand [68] show that past data indicate quite different PST coverage, and ISA TR 84.00.03 and Goble [23] suggest using FMEA to determine the PST coverage. Relevant research questions to address are therefore:

- What factors influence the PST coverage?
- What PST coverage may be claimed for shutdown valves based on historical data?
- What methods can be used to determine the PST coverage factor, taking into account application specific conditions and technology?

### 1.2.8 SIS performance monitoring in the operational phase

Monitoring reliability performance of safety functions was a legal requirement in Norway even before the introduction of the IEC standards. Unfortunately, the current performance indicators and targets are not fully suited for follow-up of SIL requirements.

The industry also seems to lack a common approach to how field data can be utilized for maintenance management, for example for making decisions on how frequent the functional tests should be executed based on the field experience. Two approaches are included in OLF-070 [100]. Unfortunately, these approaches have not been widely adopted by the Norwegian oil and gas industry, and changes to the test intervals are today mainly based on qualitative considerations. Relevant research questions to address are therefore:

- How can field data be used to monitor the safety integrity during operations?
- How can field data be used to make decisions regarding the functional test intervals?

## 1.3 Research objectives

The main objective of the PhD project has been to *identify* some of the key factors that influence the SIS reliability, *clarify* their effects on reliability, and suggest means to *improve* the treatment of these factors in safety and reliability assessments in design and operation.

Based on the main objective and the research questions, the more specific objectives have been to:

1. Propose a RAMS management approach that relates IEC 61508 requirements to other RAMS requirements.
2. Demonstrate how SIS manufacturers can achieve compliance to the IEC 61508 requirements as well as sector specific requirements, by using a software development platform as a case study.
3. Contribute with new perspectives and approaches for reliability analysis of complex SIS.
4. Clarify how the requirements for architectural constraints may affect reliability, taking both intended and unintended effects into account.
5. Provide definitions for spurious activation, and suggest which factors to address when calculating the spurious activation rate.
6. Propose a framework for calculating the PST coverage, that takes design features as well as plant specific features into account.
7. Propose a CCF defense approach that can improve the awareness, understanding, and control of CCFs during execution and follow-up of functional tests and inspections.
8. Propose a practical approach for using field data for monitoring safety integrity performance and for making decisions on how to adjust the functional test intervals.

The numbering does not indicate a prioritization of the objectives. The purpose of the numbering is for reference only.

## 1.4 Delimitations

The main focus is SIS applications in the oil and gas industry and within the context of IEC 61508 and IEC 61511, and most practical examples, terms, and concepts are selected from this industry sector. It is assumed that the SIS is operating on demand, rather than continuously or in the high demand mode. This assumption applies to most SIS on oil and gas installations.

The selected research areas are based on own interests (what I would like to learn more about), on IEC 61508 and IEC 61511 (what I should know something about), on discussions with other reliability experts, for example in the IEC 61508 and IEC 61511 committee, on the stated research questions, on research challenges identified in SINTEF projects, and, finally, on practical challenges experienced through participation in the analysis of SIS failures reported for the Kristin installation that is operated by StatoilHydro. This means that there may be other relevant factors that influence the SIS reliability, for example handling of uncertainty, that are not covered in this PhD project.

## 1.5 Structure of the thesis

The thesis comprises three main parts; Part I Main report, Part II Articles, and Part III Supplementary information.

Part I gives a brief presentation of the research area, the research approach, and the main results. Part I also gives ideas for areas of further research. The main report builds on ten research articles, and the reader is directed back to these articles for additional details on the main results.

Part II includes the ten research articles that have been published during the PhD project, in international journals or in conference proceedings.

Part III provides supplementary information on SIS and SIS related standards, and gives readers an opportunity for more insight to these areas.

### 1.5.1 Journal articles

| | Reference |
|---|---|
| **Article 1:**<br>Nordland, Odd and Lundteigen, Mary Ann. Safety qualification of a software development environment. *International Journal of Performability Engineering (IJPE)*, Volume 3, p. 75-89, 2007 | [87] |
| **Article 2:**<br>Lundteigen, Mary Ann and Rausand, Marvin. 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*, Volume 20, p. 218-229, 2007 | [67] |
| **Article 3:**<br>Lundteigen, Mary Ann and Rausand, Marvin. Spurious activation of safety instrumented systems in the oil and gas industry: Basic concepts and formulas. *Reliability Engineering and System Safety*, Volume 93, p. 1208-1217, 2008 | [70] |
| **Article 4:**<br>Lundteigen, Mary Ann and Rausand, Marvin. Partial stroke testing of process shutdown valves: How to determine the test coverage. *Journal of Loss Prevention in the Process Industries*, Volume 21, p. 579-588, 2008 | [69] |
| **Article 5:**<br>Lundteigen, Mary Ann and Rausand, Marvin. Architectural constraints in IEC 61508: Do they have the intended effect? *Reliability Engineering and System Safety*, Volume 94, p.520-525, 2009 | [71] |
| **Article 6:**<br>Lundteigen, Mary Ann and Rausand, Marvin. Reliability assessment of safety instrumented systems in the oil and gas industry: A practical approach and a case study. *Submitted to Journal of Reliability, Quality and Safety Engineering* | [65] |
| **Article 7:**<br>Lundteigen, Mary Ann, Rausand, Marvin, and Utne, Ingrid. Development of safety instrumented systems – RAMS engineering and management from a producer perspective. *Submitted to Reliability Engineering and System Safety* | [72] |

### 1.5.2 Conference articles

| | Reference |
|---|---|
| **Article 8:**<br>Lundteigen, Mary Ann and Rausand, Marvin. The effect of partial stroke testing on the reliability of safety valves. In *Risk, Reliability and Societal Risk*, Volume 3. Taylor & Francis 2007, p. 2479-2486 | [68] |
| **Article 9:**<br>Hauge, Stein and Lundteigen, Mary Ann. A new approach for follow-up of safety instrumented systems in the oil and gas industry. In *Safety, Reliability and Risk Analysis: Theory, Methods and Applications*, Volume 3. CRC Press. 2008, p. 2921-2928 | [28] |
| **Article 10:**<br>Lundteigen, Mary Ann and Rausand, Marvin. Assessment of hardware safety integrity requirements. In *I: Reliability of Safety-Critical Systems: Proceedings of the 30th ESReDA Seminar*. European Commission, Joint Research Centre p. 185-198 | [66] |

# 2

# Research principles and approach

The main reasons for starting a PhD project have been to:

- Acquire a state of the art knowledge within my areas of interest; SIS and safety and reliability analysis.
- Be able to understand and use methods for safety and reliability assessments, and learn more about their strengths and limitations.
- Develop research skills, ranging from the design and execution of research projects, to the writing of scientific articles and presentation of research results.
- Contribute with new concepts and methods that may be recognized by other researchers within the same research area.
- Develop international and national networks with reliability and SIS experts.

The overall approach for meeting these objectives are outlined in the following sections.

My scientific background is natural science with specialization in cybernetics. Cybernetics concern automatic control, and many applications build on technologies that are frequently used for SIS.

Most of my work experience is related to the oil and gas industry, with particular focus on instrumentation and maintenance. I have obtained field experience from having worked on offshore oil and gas installations. It was during this period my interest in SIS emerged, an interest that has been further developed through research activities and now finally, in a PhD project. I hope that future research will benefit from the skills that I have developed during the PhD project.

## 2.1 Research principles

### What is research?

Research may be defined as a detailed study of a subject, especially in order to discover (new) information or reach a (new) understanding (Cambridge Dictionaries Online). The study should be systematic, and the subject may, for example, be literature, theory, materials, or a system. The primary objectives of research are to acquire and exploit new knowledge.

Many research (or scientific) methods within social as well as natural science require the use of experiments. An experiment is a test under controlled conditions that is made to demonstrate a known truth, examine the validity of a hypothesis, or determine the suitability of something previously untried. A difference between my work and classical (natural science) research, is that I develop new methods and concepts based on reasoning rather than by performing experiments. I define reasoning as the process where formal logic arguments, existing methods, and knowledge are used as building blocks to derive new relationships or insight.

We may distinguish between three types of research based on the intended use OECD [98]: (i) *Basic research* is 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, (ii) *applied research* is original investigation undertaken in order to acquire new knowledge. It is, however, directed primarily towards a specific practical aim or objective, and (iii) *oriented basic research* is 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. While the main purpose of (i) and (iii) is to acquire new knowledge, the main purpose of (ii) is to solve a particular problem.

The research performed as part of my PhD project may be classified as oriented basic research because the focus is on the development of new concepts and methods that may fulfil current need, and which may form a basis for further research that may meet the needs of the future.

### When is a research method sustainable?

Any new method should not be accepted before it has been proved valid for its intended purpose. Without experiments, we may investigate the method’s validity by investigating the validity of the reasoning. If some of the initial assumptions are incorrect or the formal logic used to support the new method is wrong or incorrectly used, we may conclude that the method is not valid at all or just valid within a more narrow application area than originally planned. It is also possible to perform case studies where the method is tested for an example application. In this case, we may validate the results by qualitative or expert judgments, or preferably, compare the results with outcomes from other recognized and comparable methods.

In my research, I have tried to use both validation approaches. I have justified the arguments and assumptions used in method development. By peer review, the arguments, the assumptions, and also the formal logic have been verified. I have also included case studies, or given examples, that illustrate how the method may be applied. The methods presented in article 6 (on reliability analysis of complex SIS) and article 9 (on SIS performance monitoring) have been used in industry projects.

Method validity is not the only quality measure of research methods. According to the Norwegian Research Council [94], research quality is related to three aspects:

- Originality; to what extent the research is novel and has innovative use of theory and methods.
- Solidity; to what extent the statements and conclusions in the research are well supported.
- Relevance; to what extent the research is linked to professional development or is practical and useful to society.

I have published articles in journals and conferences with referee as a means to verify that my research approaches fulfil the requirements to originality, solidity, and relevance. By presenting some of the results in relevant fora, like the PDS forum[1] and the IEC 61511 technical committee, I have also obtained additional confirmation of the research relevance. However, additional case studies should be performed to obtain more insight on how the results may be applied and integrated into the SIS life cycle phases.

The main type of research in this thesis is development of concepts and methods meant for practical applications in the oil and gas industry. The purpose has been to develop new theoretical models, frameworks, and methods based on existing methods within functional analysis, causal analysis, and reliability modeling.

I do not think research should be performed as an individual project. I think the research quality improves from the interaction between researchers, and between researchers and the industry. New ideas form the basis for new knowledge, and may often occur unexpectedly when a problem or a system is viewed from different angles and perspectives. Even though a PhD project is a rather individual activity, I have tried to discuss ideas and results with different actors.

First to mention is the fruitful discussions with my main supervisor, who has challenged me on the quality of reasoning and the application of theory. Second, I have participated in several related activities, which are further explained in Section 2.2. Through these activities, I have been able to raise my understanding of SIS and SIS related standards and identify new research areas.

To be successful in research, it is essential to cope with criticism. A necessary basis for handling criticism is always to aim for high quality research that is worthwhile defending.

[1] PDS is the acronym for “pålitelighet og tilgjengelighet av datamaskinbaserte sikringssystemer” (Norwegian for “Reliability and availability of computer based safety systems”). The PDS forum is a forum for Norwegian vendors and users of control and safety systems.

I think that the way a researcher copes with criticism may be a measure of the researchers integrity or confidence in own research. Being exposed to criticism, for example in a response from a reviewer on a new journal article, should start a two step process. First, it is important to analyze the criticism carefully; Does it represent a new perspective to my research, and which I have not been aware of or considered sufficiently? Does it pinpoint a gap or a weakness in my research, for example the assumptions? In this case, the criticism represents valuable input to my research, and potentially, a starting point of a new collaboration among researchers. If the criticism turns out to be invalid or pointless, even after having explored the pearls of wisdom that may be buried in it, I think it is still worth a well founded reply. The second step should therefore always be to give well founded replies regardless of validness of the criticism. By this approach, I think that my integrity as a researcher increases, in my own eyes as well as others.

## 2.2 Research approach

High quality research requires a documented and logical design of the research project. A research project is a sequence of activities or work packages that build onto each other. It starts with the definition of research basis and research questions and ends up with the research results. A research project should provide answers to the initially stated questions, provide new methods, highlight their application areas, and suggest new perspectives and ideas for further work.

A research project should include the following main steps (derived from [62]):

1. Identification of research context and perspectives
2. Discussion of relevant research problems (“gaps”), and the associated research questions
3. Identification of main assumptions
4. Description of theoretical basis
5. Description of new methods and models
6. Discussion of methods/model application areas and constraints

My PhD project has been divided into the three main activities: (1) Development of the PhD project plan, (2) development of research articles, and (3) development of the PhD main report (thesis). In addition, I have participated in a number of related activities which have supported my research.

The research activities and how they relate to the research results are illustrated in Fig. 2.1. The project plan development started with a literature review and an initial identification of research gaps. The activity then continued with a discussion of research topics, research questions, and research approach. The research questions that have been addressed in this PhD project have been partly selected from the literature review and partly from topics where I would like to

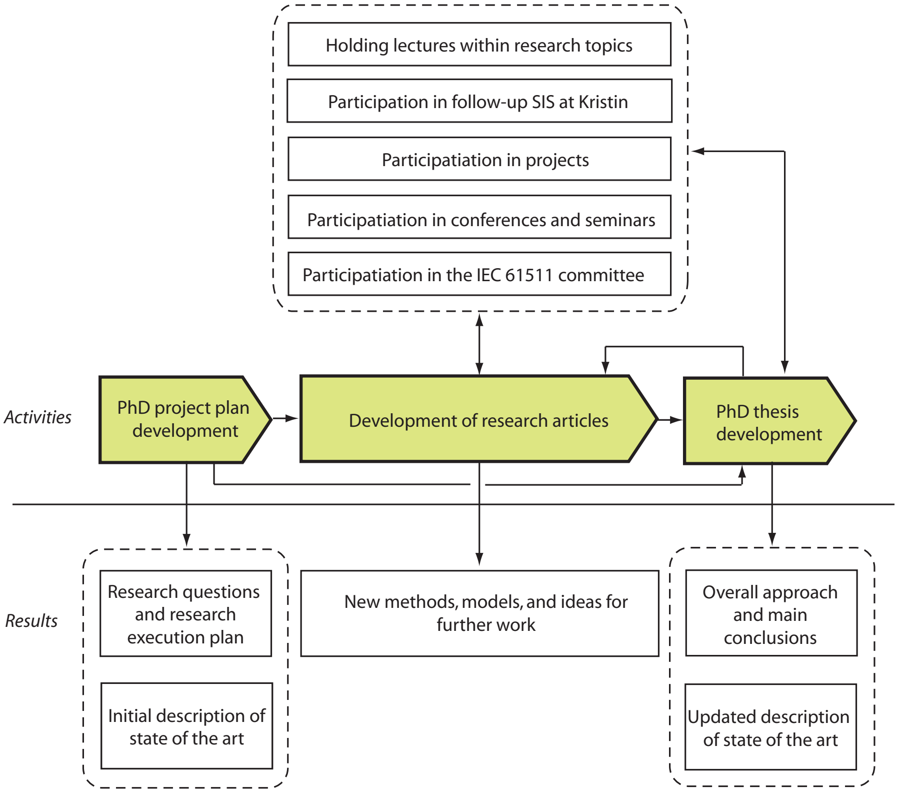

Holding lectures within research topics
Participation in follow-up SIS at Kristin
Participiatiation in projects
Participiatiation in conferences and seminars
Participiatiation in the IEC 61511 committee
Activities
PhD project plan development
Development of research articles
PhD thesis development
Results
Research questions and research execution plan
Initial description of state of the art
New methods, models, and ideas for further work
Overall approach and main conclusions
Updated description of state of the art

**Fig. 2.1.** Research execution plan

increase my competence. The PhD project plan resulted in an initial state of the art description, formulation of research questions, and a research execution plan.

The research articles have been developed following the same research steps. The new methods and models and their theoretical basis are also presented there. Most of the articles are written together with my main supervisor, Professor Marvin Rausand as we have mutual interest in the research field.

Two articles have been written with researchers from SINTEF, Odd Nordland and Stein Hauge. The article with Odd Nordland documents some of the results from an industry project where SINTEF performed reliability analysis of a new railway signaling system. The article with Stein Hauge has been based on a research project that is funded by the Norwegian Research Council and the PDS forum (referred to as the PDS-BIP project).

The PhD main report (thesis) describes the research basis, research questions, and research approach, and outlines the main results from the research articles. The development of the PhD thesis has been an iterative process as new results, ideas and insight have been obtained from the research articles and other related activities, like:

- Participation in follow-up of SIS at Kristin: Kristin in a condensate field outside Norway and which is operated by StatoilHydro at Stjørdal. The Kristin offshore installation is built according to the OLF-070 [100], and the follow-up must be aligned with the IEC 61508 and IEC 61511 requirements. Here, I have been able to participate in the analysis of SIS failures that have been reported for the installation.
- Participation in projects:
  - PDS-BIP project: This project comprises several research activities. I have contributed to two research reports: The first report describes the current status and challenges related to implementation of the IEC 61508 and IEC 61511 requirements for new installations on the Norwegian continental shelf. The second report describes a guideline for follow-up of safety integrity for SIS in the operational phase.
  - Industry project on investigating draw-work brake problems: The project was led by Professor Michael Golan at the department of Petroleum Engineering and Applied Geophysics (NTNU), and I have contributed with qualitative reliability analysis of control and safety functions that were implemented for the brakes.
  - Industry project on reliability analysis of workover systems: I have performed qualitative and quantitative reliability analysis of well isolation for workover systems.
- Participation in conferences and seminars: I have participated and presented results in the ESREL conference two times. In addition, I have held presentations in the PDS forum and at some industry related conferences. I have also been invited and participated in company internal seminars on IEC 61508 and IEC 61511.
- IEC 61511 technical committee work: I am participating in the IEC 61511 technical committee on behalf of the PDS forum. The technical committee is responsible for maintaining the IEC 61511. Through this work, I am able to better understand intention behind the requirements and to meet and discuss key issues of SIS design, construction, and operation with SIS experts from many different countries. A revision of the IEC 61511 has now been initiated, and here I may be able to influence the future content of the standard.

I have prepared and held lectures on all topics that are covered in my articles and some related areas. Holding lectures have been a way to improve my understanding of fundamental issues within reliability as well as on the methods that are frequently used for safety and reliability assessments. In addition, the presented material is subject to a quality check by the participating students.

### Quality assurance

An essential part of the quality assurance has been carried out through publication in international journals and conferences with referee. In addition, the relevance and solidity have been confirmed by sharing research ideas and results at international conferences and in relevant forums like the PDS forum and the technical committee for the IEC 61511 standard.

# 3

# Main results and further work

## 3.1 Main results

The ten research articles represent and describe the main results of this PhD project. The relationships between the articles and the research objectives are illustrated in Fig. 3.1. Eight research objectives were stated in Section 1.3. The purpose of this chapter is to evaluate to what extent these objectives have been met.

In Table 3.1, I have indicated how different target groups may use the results from this PhD project. The rationale behind this table is further elaborated in Section 3.2.

**Table 3.1.** Subjects of interest for different target groups

| **Target groups** | **Subjects of interest** | **Article ref.** |
|---|---|---|
| Academics (other researchers): | Spurious activation | 3 |
| | Architectural constraints | 5,10 |
| Industry - end users: | Defenses against CCFs | 2 |
| | Use of field data | 9 |
| Industry - SIS designers, manufacturers: | Compliance to IEC standards | 1 |
| | Product development - RAMS | 7 |
| | Partial stroke testing | 4,8 |
| | Architectural constraints | 5,10 |
| | Analysis of complex SIS | 6 |
| Authorities | Defenses against CCFs | 2 |
| Education: | Concept clarification | All |

### 3.1.1 Contributions to objective 1

The first objective addresses the need for SIS manufacturers, SIS designers, and system integrators to have a holistic view on RAMS requirements, and not on

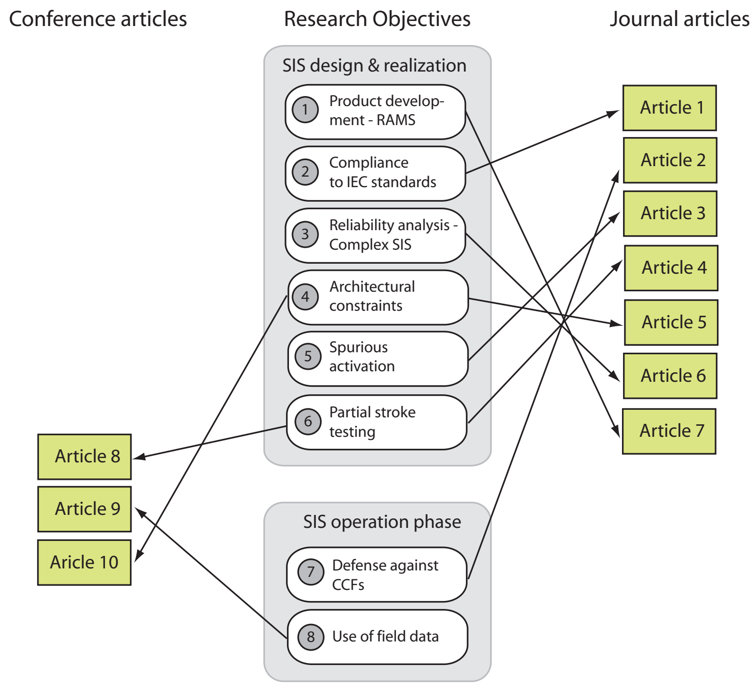


**Fig. 3.1.** Relationships between research objectives and research articles

IEC 61508 and related standards alone. The research questions associated with the objective are discussed in Section 1.2.1 and article 7 [72]. The main contributions from this PhD project are:

- Identification of RAMS requirements for a SIS producer.
- Development of a product development model that integrates these requirements, and demonstrates its application for a SIS.

I consider the contributions as a first step towards meeting objective 1. To fully meet the objective, the framework should provide more in-depth guidance on each of the RAMS aspects. Currently, the framework is more detailed on issues related to IEC 61508 compared to product safety, availability, maintenance, and maintainability. A particular area of interest is to balance safety integrity and (production) availability.

### 3.1.2 Contributions to objective 2

The second objective addresses the need for more guidance on how to demonstrate compliance to the IEC 61508 and sector specific standards. The research questions associated with the objective are discussed in Section 1.2.2 and article 1 [87]. The main contributions from this PhD project are:

- A clarification of how EN 50126, EN 50128, and EN 50129 for railway signaling systems relate to the IEC 61508 requirements for a software development platform.
- A practical approach for how to demonstrate compliance to IEC 61508 and sector specific requirements.

Article 1 is the only publication in this PhD project that is directed towards another industry sector than the oil and gas industry. The article builds on a SINTEF project where I was the project leader and where the reliability of a railway signaling system was investigated. The article has been included because the results are applicable for the oil and gas industry: Some overall principles for handling sector specific and generic standards are discussed and the software development platform may be used in many industry sectors, including the oil and gas industry.

Many industry specific standards for SIS software and hardware design were developed prior to the release of IEC 61508. Some of the standards have later been updated to reflect IEC 61508, but there are often inconsistencies due to the sector specific considerations. As IEC 61508 acceptance increases among national authorities, the regulations often make reference to the IEC 61508 as well as the sector specific standards. For SIS manufacturers and SIS designers, it is necessary to demonstrate compliance to both categories of standards.

My view is that the contributions from this PhD project are important to ease the adoption of the IEC standards. Case studies are useful to demonstrate the process of compliance. A limitation may be that verification of application software is not addressed. A software development platform can provide programmers with suitable tools for software development, but is not able to verify if the tools are used correctly and if the software specification is adequate and correctly interpreted through the software code. IEC 61508 and EN 50128 propose several methods that are suitable for revealing software failures and weaknesses, but the standards may provide too much freedom in the selection of methods.

### 3.1.3 Contributions to objective 3

The third objective addresses the need to improve current methods for reliability analysis of complex SIS, taking into account that the methods should still be possible to comprehend by design engineers and that the methods should cater for the main properties of periodically tested systems. The research questions associated with the objective are discussed in Section 1.2.3 and article 6 [65]. The main contributions from this PhD project are:

- A detailed description of a complex SIS, represented by a case study of a workover system for well interventions.
- An approach for how to model CCFs and to make conservative approximations for the PFD with fault tree analysis.

- A recommendation on the use of minimal cut sets as basis for communicating findings from reliability analyses to decision makers and practitioners.

In my view, the contributions support the stated objectives. I realize that the arguments for using fault tree analysis are mainly based on the identified limitations of reliability block diagrams. The main reasons for taking this approach are that (i) both fault trees and reliability block diagrams are widely accepted in the oil and gas industry, and (ii) fault trees are (like reliability block diagrams) easy to comprehend by SIS designers and practitioners and it is therefore easier for the reliability analysts to use their expertise for verifying the reliability models.

One immediate question that the reader may ask is why a new approach for fault tree analysis is necessary when several software tools are available that supports such analyses.

The first response to this question is that most software tools for fault tree analysis use non-conservative approximations for periodically tested components. This may not be acceptable when the PFD estimates are used as basis for selecting hardware architecture. Many reliability analysts may ask how important the conservative versus the non-conservative estimation is, in particular if the *same* tool is used to analyze and compare different hardware configurations. I partly agree with this argument, but in practise, the results are being compared even if different calculation approaches are used. Many decision makers do not have sufficient insight to judge how the calculation approach influences the PFD estimate. I therefore think that we, as researchers, as a minimum should aim for calculation approaches that make conservative rather than non-conservative approximations.

A second response to this question is related to how the CCFs are treated. Most fault tree analysis tools require explicit modeling of CCFs in the fault trees, and this is not always a suitable approach for reliability analysis of complex SIS. As demonstrated by a case study, there may be dependencies between components that are modeled at different locations in the fault tree. For the reliability analyst, it is not easy to decide how to model CCFs and where to incorporate them as basic events. In addition, the size of the fault tree may be overwhelming and the possibility for making errors during modeling or model revisions may increase.

A third response to the question is related to the use of already well known formulas in the oil and gas industry. Many reliability analysts are familiar with reliability block diagrams and related approximation formulas in IEC 61508 and the PDS method. The advantage of the proposed approach is that these well known formulas are applied for the minimal cut sets. The system is considered as a series of cut parallel structures in a reliability block diagram, where each minimal cut set is a 1-out-of-$n$. Here, 1-out-of-$n$ means that at least one out of $n$ components must function for the configuration to perform its intended function.

One area that is not sufficiently addressed in the proposed approach is the handling of $k$-out-of-$n$ voted configurations with $k \geq 2$. For a $k$-out-of-$n$ configuration, the same components may be element of more than one minimal set. For the calculations, the “repeated” components may be considered as associated components. Rausand and Høyland [108] has proved that the upper bound approximation holds even with associated components. This means that the PFD estimate will be conservative rather than non-conservative.

In the article, it is recommended to define these subsystems as single elements in the fault tree, and use approximation formulas provided in IEC 61508 or by the PDS method to calculate the contributions from independent failures and CCFs. The mixing of explicit modeling of CCF (in fault trees) and implicit modeling through the minimal cut sets add some unwanted, and perhaps unnecessary, complexity to the proposed approach. More research may be required to develop alternatives for handling CCFs.

I have not investigated other modeling approaches, like Markov methods, Petri net, and Monte Carlo simulations. Even if these methods are more difficult to comprehend by practitioners, they may add new insight to the behavior of complex SIS which is not catered for in fault trees and reliability block diagrams.

### 3.1.4 Contributions to objective 4

The forth objective concerns the need to clarify the reliability effects of the requirements for architectural constraints in IEC 61508 and IEC 61511, and addresses in particular the suitability of the SFF. The research questions associated with the objective are discussed in Section 1.2.4 and articles 5 [66] and 10 [71]. The main contributions from this PhD project are:

- A clarification of why the SFF may credit unsafe SIS design solutions.
- Two case studies that demonstrate the reliability effects of using the SFF as a design parameter.
- New insight to why more hardware fault tolerance does not always give the intended reliability improvements.

Regarding article 5, the most recent of the two articles, I have got feedback from members of the IEC 61511 technical committee that supports my view and compliments the way the analysis has been performed. For this reason, I think that the contributions meet the research objective. The discussion of architectural constraints should continue and be used as motivation for development of new methods and guidelines that reduce uncertainty in reliability modeling and reliability calculations.

Article 5 and 10 argue that a high SFF is not always good for safety. There are two ways to reduce the unintended effects of the SFF. First, to exclude the non-critical failures from the SFF formula, an approach that has been suggested by the PDS method [114]. Second, to find ways to penalize high safe and dangerous detected failure rates in the same way as high dangerous undetected failure rates are penalized through the PFD calculations. This may be an area of further research.

### 3.1.5 Contributions to objective 5

The fifth objective concerns how to define and classify spurious activations. The research questions associated with the objective are discussed in Section 1.2.5 and article 3 [70]. The research objective was formulated based on a question I asked myself when I tried to compare how the spurious trip rates were calculated. It seems that different approaches are used without giving much reflection to under which assumptions they are valid. The main contributions from this PhD project are:

- Definition and classification of spurious activation including spurious operation, spurious trip, and spurious shutdown.
- Clarification of the causes of spurious activation.
- Discussion of the differences between safe CCFs and traditional (dangerous) CCFs.
- Generic approach for calculation of spurious trip rate.
- A comparison between the generic approach and two other approaches that are frequently used to calculate the spurious trip rate, the PDS method and the ISA approach.

I think that my contributions represent new perspectives to the discussion on spurious activation. Traditionally, spurious activations in the oil and gas industry have been seen as a non-safety issue, and that the main consequences of such activations are production losses. For this reason, the spurious activations are not given much attention in IEC 61508 and IEC 61511.

In other industry sectors, the link between spurious activation and safety is more evident and reflected in regulations and guidelines. A spurious trip of a railway signaling system may lead to a situation where the train location status is not fully known and where manual traffic management is required before a restart of the system is made. For a car, a spurious release of an air bag system or the brakes may lead to collision or the car driving off the road.

Traditionally, IEC 61508 and related standards have been applied for emergency shutdown systems, process shutdown systems, fire and gas systems, and HIPPS. With the increased recognition of the standards, many oil companies assign SIL requirements to other safety critical systems such as well intervention systems, drilling systems, navigation systems, and ballast systems. For these systems, it is often important to also focus on the rate of spurious activations as they may lead to hazardous events. Whereas traditional SISs often have a well defined safe state, this is not always the case for other safety critical systems. The safe state of a ballast system may in some cases be to stop pumps and close valves, while in other situations, for example if the ballast tanks take in water, it may be important to run pumps and keep valves open to retain equilibrium of the installation.

One aspect that could have been investigated further, is how a spurious activation may improve the actual (field) reliability. Spurious activations may often lead to partial or complete functional test of SIFs, but more guidance should be provided on how much credit to take from such activations. It is important to emphasize that giving credit to spurious activations is an issue for the operational phase, and should not be used as an argument for designing SISs that are prone to this type of failures.

### 3.1.6 Contributions to objective 6

The sixth objective concerns the need to clarify the reliability gain from introducing partial stroke testing (PST). The research questions associated with the objective are discussed in Section 1.2.7 and articles 4 [68] and 8 [69]. The main contributions from this PhD project are:

- An approach for how to determine the PST coverage based on experience data.
- A clarification of the concept PST coverage and its main elements.
- A new framework for how to determine the PST coverage, taking into account the application specific conditions.

Several articles are published on how to determine the effect of PST on the PFD, but little attention is given to how the PST coverage is determined. We may ask why this is important, since most analyses indicate a PST coverage in the range from 60% to 70%.

My main argument is that PST may easily be introduced on false premises. This means that decision makers are not sufficiently aware of the conditions under which the PST gives the intended results, and in what situations frequent PST may introduce new risks. I strongly think that analysis should be used to raise awareness of the assumptions, conditions, and limitations of using PST.

I think that the new framework represents new ideas and new insight to the reliability effects of PST, and that the contributions therefore fulfil the intent of the objective. Still, I think the framework needs further development. One issue is the selection of questions that are used to determine the PST reliability factor. The questions should be discussed with the industry and in particular with end users, valve vendors, and vendors of PST technology. The discussions may lead to new questions, modification of the existing ones, and perhaps an update of the weights that have been assigned for each question.

At present, little field data are available on what type of failures that have been revealed by PST, and if functional tests have revealed failures that should have been detected by PST. Further analysis of field data may therefore be required to improve the framework.

### 3.1.7 Contributions to objective 7

The seventh objective addresses CCFs and how they may be catered for in the operational phase. The research questions associated with the objective are discussed in Section 1.2.6 and article 2 [67]. The main contributions from this PhD project are:

- A clarification of CCF causes and CCF classification in the context of a SIS that is subject to regular functional testing.
- A clarification of the differences and similarities between systematic failures and CCFs.
- A new framework on defense against CCFs that may be integrated with current practises for functional testing and inspection.

The new framework is not theoretically complicated, but includes small modification to existing practises that may increase the awareness, competence, and treatment of CCFs. By implementing this framework, we are able to follow up the assumptions that were taken during the SIS design phase and to avoid that the attention to CCFs ends when the SIS design has been completed.

I am a little pessimistic about the adoption of the framework in the industry. It seems to me that implementation and follow up of new initiatives may be difficult due to limited resources. As national authorities like the Petroleum Safety Authority (PSA) are concerned with the increasing level of SIS complexity and dependencies, we may expect that a future revision of the regulations will pay more attention to defense against CCFs in design as well as operation. I have also proposed an amendment on defense against CCFs to existing requirements on maintenance planning and execution in IEC 61511.

### 3.1.8 Contributions to objective 8

The eighth objective concerns the need to collect field data and use this information for follow-up of SIS performance in the operational phase. The research questions associated with the objective are discussed in article 9 [28]. The main contributions from this PhD project are:

- An approach for how to use field data for monitoring safety integrity.
- A procedure for when and how to adjust the functional test intervals.

Based on discussions and feedback from the oil and gas industry, I feel that the contributions almost fulfil the objective. Two critical points have been raised; (1) that the new approach does not cater for situations with insufficient operation time or few observations, and (2) that more flexible adjustments than doubling and halving should be allowed for the functional test interval. Regarding (1), I fully agree that the approach needs to be improved. But for systems like fire and gas detection system, the number of components is sufficiently high to achieve a rather good indication of performance at least with two years operation time.

Regarding (2), the oil companies often prefer to adjust the intervals in small steps and within the normal scheduling regime. A typical scheduling regime is functional testing every month, every three months, every sixth months, every year, and every two years. So, in most cases doubling and halving are adequate alternatives. Still, I think the approach would benefit from being more flexible.

The contributions from this PhD project have therefore, in collaboration with the co-author of article 9, been developed further in a SINTEF report to account for few observations, limited observation time, and more flexible adjustments of the functional test interval.

The contributions to objective 8 address analysis of SIS failures, but to confirm SIS performance it may be necessary also to consider other data like the spurious activation rates and the demand rates. The demand rate does not influence the SIS performance, but rather the SIS performance requirement (SIL). If more frequent demands than initially assumed are experienced, it may be necessary to increase the SIL to meet the acceptance criteria.

## 3.2 Discussion

### Relating the results to the safety life cycle

This PhD project contributes with new approaches and concepts within the following phases of the SIS life cycle, see also Fig. 3.2:

- SIS realization phase, in particular in the design selection process: Articles 1, 3-7, 8 and 10.
- SIS operation and maintenance phase, in particular for data collection and analysis and the execution of functional testing: Articles 2 and 9.
- SIS modification phase, in particular for decision making related to SIS performance deviations: Article 9.

IEC 61508 and IEC 61511 also use the concept of management of functional safety. Management of functional safety includes all activities that are necessary to ensure that the organization involved in the various SIS life cycle phases has the necessary competence, procedures, and practises in place to achieve the functional safety and safety integrity requirements of the SIS. Article 1 may be considered as a contribution here, since it specifically addresses the adoption of the IEC requirements.

### What are the most important contributions from the PhD project?

The contributions may be viewed in light of different target groups, as indicated in Table 3.1. For other researchers, I think the most important contribution is

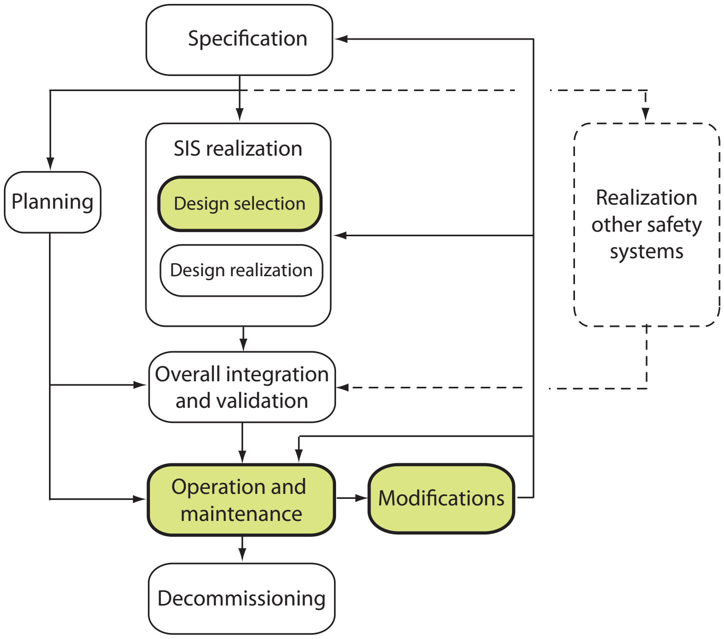


**Fig. 3.2.** The contributions from this PhD project in a safety life cycle perspective

the article on spurious activation. This article indicates several areas of further research, for example related to avoidance of spurious activations, on how to improve the calculation methods for spurious activation rate, and how to credit spurious activations as functional tests in the operational phase. Other researchers may also find the articles on the architectural constraints interesting, for example the discussion of the reliability effects of hardware fault tolerance and the need for having other means to account for uncertainty than the architectural constraints.

The most important contribution for the end users, like the oil and gas companies, is the approach on the use of field data to monitor SIS performance and update the functional test intervals. I hope the end users also find the approach on defense against CCF useful, but I think it is necessary to first get the national authorities' attention to this issue. The authorities are therefore a target group for the article on defense against CCFs. Both approaches may be easily integrated with current practises and tools associated with SIS follow-up and maintenance management.

The decision on whether or not to invest in PST technology is often taken in an initial design phase, and the decision is highly influenced by the PST coverage. SIS designers and end users may therefore find the approach for determining the PST coverage factor useful.

The article on the architectural constraints may also be of interest for both SIS designers and end users. The article may increase the awareness to some unintended effects using the SFF as a design parameter, and thereby help SIS designers and end users in their evaluation and selection of SIS components. In addition, the article highlights some concerns about the architectural constraints, for example related to added complexity.

The article on the architectural constraints is also a contribution to the IEC 61508 and IEC 61511 committee, in their evaluation of whether or not to keep the architectural constraints, and in particular the SFF, as design parameters in future revisions of the standards. This is an issue that is heavily discussed in the technical committees right now as both standards are under revision.

All articles may be relevant for educational purposes, as they outline and clarify many concepts, principles, and approaches for safety and reliability assessments within the context of IEC 61508 and IEC 61511.

Personally, I feel that the most important contribution is to be able to provide new insight to methods and concepts that are recognized and found useful by other researchers and experts within the same area.

### 3.2.1 Handling of uncertainty

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

Uncertainty is a concept that expresses our degree of knowledge about the system [82]. While uncertainty analysis is a key element of reliability assessments in nuclear and space industries [82, 32], it is not given the same attention in guidelines and standards for SIS for the oil and gas industry. As uncertainty is an area where I believe more research should be performed, I have made some reflections on the underlying causes of uncertainty using the calculated PFD as an example.

The calculated PFD is one out of several inputs that influences SIS design. Other inputs may be related to other requirements in IEC 61508 and IEC 61511, such as systematic safety integrity, software safety integrity, and architectural constraints. Decision makers may also have to balance safety requirements with production availability and maintenance strategies.

As illustrated in Fig. 3.3, the calculated PFD is influenced by three main factors: (i) the model, (ii) the data, and (iii) the calculation approach. The uncertainty associated with the PFD depends on whether or not the model, the data, and the calculation approach reflect the main properties of the SIS in question.

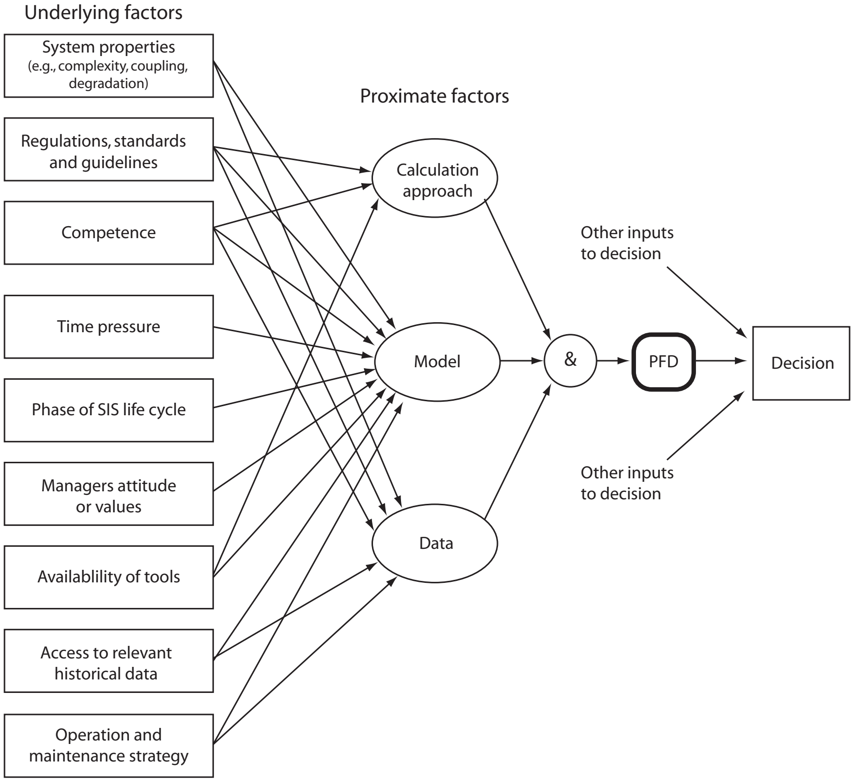


**Fig. 3.3.** Factors that influences the PFD

As indicated in Fig. 3.3, this is not only a question of the competence of the reliability analysts.

In the following, we elaborate on how the underlying factors in Fig. 3.3 may influence the level of uncertainty of the PFD.

### Uncertainty related to the system model

The system model represents our interpretation of some real phenomena, for example a SIS. A system model may be developed in two steps: first the construction of a functional and/or architecture model and second the development of one or more reliability models.

The system model expresses our degree of knowledge regarding:

- The system architecture or structure. How are the components configured and how do they interact when performing a SIF?
- The degree of coupling or dependencies between redundant components, systems, and functions. What components may share common root causes and/or coupling factors?

- System properties, like for example life distribution of SIS components. Can we, for example, assume that the time to failure is exponentially distributed?
- The modes under which the SIS operates. Is the SIS operated continuously or on demand, and must the SIS respond to other hazardous events in other modes than normal operation, for example start-up and when the plant is shutdown.
- The maintenance and testing strategies. Can we assume an "as good as new" condition after functional test.
- Other operational assumptions, like for example the downtime distribution of SIS components. Can we assume that the downtime is exponentially distributed?

As indicated in Fig. 3.3, we may assume that the model construction is influenced by:

- Regulations, standards, and guidelines: Different industry sectors may prefer and therefore highly recommend different modeling strategies. We may assume that many reliability analysts choose reliability block diagrams because IEC 61508 gives practical examples and formulas for calculating the PFD using this approach.
- Competence: We may expect that previous experience and knowledge highly influence the selection of modeling approach. Some have limited theoretical background in mathematics and statistics, and may prefer the simpler modeling approaches like fault tree analysis and reliability block diagrams, while others having this competence may explore the benefits of the Markov methods, petri-net, binary decision diagrams, and Monte Carlo simulations.
- Time pressure: In many SIS design and construction projects, the reliability analysts may have limited time available to perform the calculations and may for this reason be forced to select simpler models rather than detailed ones.
- Phase of SIS life cycle: In an early design phase, the reliability analysts may choose a simple reliability model for rough prediction and comparison between different SIS design alternatives. In a later phase, the reliability model may be updated and extended with more features.
- Managers attitudes or values: If the organization does not see the need in performing safety and reliability assessments, other than for satisfying a regulation, the reliability analysts may be forced to limit the scope and ambition of the analysis.
- Available tools: Reliability analysts may prefer software tools that are available in-house, instead of purchasing new tools.
- Access to relevant data: Experience data, if available, may give guidance on the dominating failure modes to consider for the analysis.
- Operation and maintenance strategies: Operation and maintenance strategies indicate whether or not the planned and unplanned down times should be considered in the analysis.

### Uncertainty related to data

The reliability model describes the relationship between input parameters (e.g., failure rates, functional test intervals, mean restoration times) and output parameters (e.g., PFD, beta-factor, diagnostic coverage, SFF). The level of uncertainty associated with the input data may be influenced by:

- Relevance: To what extent the data is relevant for the technology being used and its operating and environmental conditions.
- Quality: To what extent the data fulfil the quality specifications, for example in terms of completeness and classification.
- Amount: How many failures that have been observed for a population of components, and the length of the observation period.

Uncertainty associated with the amount of data is often referred to as statistical uncertainty, and may be expressed using one of the three models [82]:

- Probability density function
- Cumulative distribution function
- Displaying selective percentiles, for example a confidence level of 90% of the parameter value

The statistical uncertainty may be reduced with increasing amount of relevant data and/or with increasing observation time.

As indicated in Fig. 3.3, there are several underlying factors that may influence to what extent we achieve relevant, high quality, and a sufficient amount of data:

- System properties: We want to reflect the system properties through degradation models. The expected degradation mechanisms under the given operating and environmental conditions (e.g., arctic environment) may deviate from the degradation shown in experience data, and such aspects are important to cater for when selecting input data.
- Regulations, standards, and guidelines: Regulations, standards, and guidelines may provide recommendations or requirements regarding uncertainty handling. IEC 61508 requires that any failure rate data should have a confidence level of at least 70%. This means that the probability that the true value is less than the used value is at least 70% [108, 38].
- Competence: If data are not available or not directly relevant for the technology in question, it may be necessary to determine the values of the input parameters by expert judgments [30, 99, 106] or Bayesian methods [82, 9]. With expert judgments, the plant operators and maintenance personnel may be asked how likely or how often a particular event, for example a valve failure, may occur. When we use Bayesian methods, we determine conditional probabilities or failure distributions, based on our prior knowledge (e.g., observations or distributions) about the system or its components.

- Access to relevant historical data: Many historical data bases provide failure rates that are based on a number of installations and with components having different technologies. This means that access to underlying information is required to make proper selection of input parameters. In addition, the completeness of failure recording, the amount of data and the observation time are factors that influence to what extent we can rely on historical data.
- Operation and maintenance strategies: Such strategies may give insight to the mean time to repair, the mean downtime, and the distribution of down times.

Data requirements and model selection are closely related. It is often pointless to select a modeling approach that uses parameters where data is not available. For example, the nuclear power industry collects data on CCFs [83, 84, 85, 86] and suggests comprehensive methods for calculating the contribution from CCFs, but similar initiatives have not been taken in the oil and gas industry. For practical purposes, we should therefore balance the modeling approach with the availability of data.

### Uncertainty related to calculation approaches

The PFD may be calculated by using mathematically exact expressions or approximation formulas [108]. Often, the two approaches give minor differences in the results. We may therefore rank the calculation approach as the least important contributor to uncertainty compared to aspects of model and data. What method to select can therefore be reduced to a question of preferences. The reliability analysts preference may be influenced by competence, availability of tools, and recommendations provided in relevant standards.

An issue that is sometimes raised, is whether to use the *average* or *time dependent* PFD. Some authors think that the average PFD is misleading since the PFD in approximately 50% of the time is higher than this value [18]. Currently, the IEC 61508 and the IEC 61511 suggest using the average PFD. However, new revisions of the standards may call for other practises.

### Other perspectives to uncertainty

Perrow [107] distinguishes between systems that have linear and complex interactions. Linear interaction means that there is a direct and deterministic relationship between the inputs and the outputs. For complex interactions, this relationship is not visible or not possible to comprehend. We may therefore assume that uncertainty increases with increasing complexity, due to the difficulty of constructing adequate architecture and reliability models.

Perrow also characterizes systems by their degree of coupling. Coupling expresses the degree of dependencies between system components, and may vary from loose to tight. According to Perrow, both systems with linear and complex interactions may have tight and loose coupling. To cater for tight coupling in the

PFD calculations, we would need a comprehensive set of data that expresses this coupling. In practise, it is often difficult to identify data at this level of detail, at least for the oil and gas industry where limited focus is given to CCFs in the data collection process. For this reason, we may assume that uncertainty increases with increasing coupling due to the lack of adequate data.

Some authors distinguish between epistemic or aleatory uncertainty [82, 32]. Both concepts are usually discussed in relationship with data. Epistemic uncertainty is the uncertainty caused by our incapability to interpret the real world. Aleatory uncertainty expresses the uncertainty that is due to inherent, irreducible, randomness of the world. While epistemic uncertainty is often associated with non-observable quantities (like for example the failure rate), we associate aleatory uncertainty with observable quantities.

To what extent aleatory uncertainty exists and is a relevant issue to consider, are still under debate among researchers. Personally, I think that aleatory uncertainty is a useful concept for describing our inability to explain *all* aspects of the world. Saying this, it is important to treat aleatory and epistemic uncertainty as time dependent properties. As our knowledge about how systems work increases, we may expect that some of the aleatory uncertainty is converted to epistemic uncertainty. But even if our knowledge increases, the nature may develop new relationships and introduce new aleatory uncertainty. This may be an issue for models used to describe climatic changes.

### Uncertainty analysis versus sensitivity analysis

Sensitivity analysis is often mentioned in the same context as uncertainty analysis, but the two types of analysis have slightly different meaning. While uncertainty analysis is a tool for evaluating the degree of knowledge or confidence in the results, the sensitivity analysis is used to improve the way we can interpret the results. When we perform sensitivity analysis, we investigate how variations in input data (model input parameters, assumptions) cause changes to the model output parameters [82].

A number of importance ranking measures have been developed to support sensitivity analyses, for example Birnbaum's measure, the improvement potential measure, and the Fussel-Vesely's measure [108, 82].

Sensitivity analyses may be used to complement uncertainty analyses. In the nuclear industry, such analyses may be used to demonstrate that the system does not exceed the specified safety margin [32]. The safety margin is here defined as the difference between an acceptance criterion and the result that are obtained by calculations.

## 3.3 Further work

Specific areas for further research are indicated in each of the articles. In this section, some overall recommendations for further research are given.

One research area is related to the assessment of uncertainty. While the nuclear power industry [32] and the aerospace industry [82] frequently discuss uncertainty and sensitivity analyses, these are barely recognized by IEC 61508, IEC 61511, OLF-070 [100], and ANSI/ISA 84.00.01 [8].

The oil and gas industry uses the architectural constraints to reduce the consequences of uncertain reliability predictions. However, in my PhD project, I have concluded that the architectural constraints may not have the intended effect on safety and reliability. Further research may look at alternative strategies for achieving adequate boundaries for SIS design, for example by developing practical approaches for uncertainty handling in the context of IEC 61508 and IEC 61511 frameworks. I think that uncertainty analysis should not be restricted to parametric uncertainty, but also include the model construction and calculation approaches.

I think that sensitivity analyses should be used more frequently in relationship with PFD calculations to increase the robustness of the calculated results. An area of further research may therefore be to find practical ways to implement such sensitivity analyses. I use the term “practical approaches” rather than “theoretical approaches”, since the theoretical basis may be considered as mature and that the main challenge is to develop methods that are possible to comprehend by engineers and reliability analysts working in the oil and gas industry. The guidelines developed by ISA on safety integrity calculation methods [48] discuss parametric uncertainty and sensitivity analysis. These guidelines may be a good starting point for developing an overall approach to uncertainty and sensitivity analysis.

I have previously indicated that there is a relationship between spurious activations and safety integrity. The spurious activations may have a positive effect on safety integrity, if we assume that a spurious activation is similar to a functional test. At the same time, spurious activations may have a negative impact on safety integrity due to the stress imposed on components that are affected. In addition, spurious activations may lead to hazardous events if the safe state is different for different operating situations. An area of further research is to develop a better understanding of the relationship between spurious activations and safety integrity. A related area is to develop strategies for how to take credit of spurious activations as functional tests.

In the PhD project, I have not studied continuously operating (high demand) SIS. At the same time, I have indicated that such systems already exist on oil and gas installations and that attempts are made to qualify them according to IEC 61508 and IEC 61511. So far, IEC 61511 only considers on demand SIS. A number of methods exist for calculating the probability of dangerous failures per hour (PFH) [41, 38], which is the reliability measure used for continuously operating SIS. However, the interpretation of the PFH is sometimes questioned [46]. An area of further research may therefore be to investigate and improve current methods for calculating the PFH.

# Part II

# Articles

# Article 1

Safety qualification of a software development platform
*International Journal of Performability Engineering*, Volume 3, p. 75 – 89, 2007

Is not included due to copyright

# Article 2

Common cause failures in safety instrumented systems on oil and gas installations: Implementing defenses measures through function testing
*Journal of Loss Prevention in the Process Industries*, Volume 20, p. 218 – 229, 2007

Available online at www.sciencedirect.com

ScienceDirect

Journal of Loss Prevention in the Process Industries 20 (2007) 218–229

Journal of Loss Prevention in the process industries

www.elsevier.com/locate/jlp

# Common cause failures in safety instrumented systems on oil and gas installations: Implementing defense measures through function testing

Mary Ann Lundteigen*, Marvin Rausand

*Department of Production and Quality Engineering, The Norwegian University of Science and Technology, 7491 Trondheim, Norway*

Received 27 December 2006; received in revised form 9 March 2007; accepted 9 March 2007

**Abstract**

This paper presents a common cause failure (CCF) defense approach for safety instrumented systems (SIS) in the oil and gas industry. The SIS normally operates in the low demand mode, which means that regular testing and inspection are required to reveal SIS failures. The CCF defense approach comprises checklists and analytical tools which may be integrated with current approaches for function testing, inspection and follow-up. The paper focuses on how defense measures may be implemented to increase awareness of CCFs, to improve the ability to detect CCFs, and to avoid introducing new CCFs. The CCF defense approach may also be applicable for other industry sectors.

*Keywords:* Common cause failures; Safety instrumented systems; Defense measures; Function testing; Inspection

## 1. Introduction

Safety instrumented systems (SIS) are used in the oil and gas industry to detect the onset of hazardous events and/or to mitigate their consequences to humans, material assets, and the environment. 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 parts of a SIS are illustrated in Fig. 1.

A SIS may perform several safety (instrumented) functions (SIF) and is sometimes referred to as a safety barrier or a protection layer (Sklet, 2006). Related SIFs may be combined into more comprehensive protection systems, like fire and gas detection systems and emergency shutdown systems.

The standards IEC 61508 (1998) and IEC 61511 (2003) are extensively used in the oil and gas industry, during all phases of the SIS life cycle. Both standards use safety integrity level (SIL) as a measure of SIS reliability. To enhance the reliability, redundancy is often introduced in the SIS architecture. Independence between safety barriers is achieved by combining diversity in design (e.g., by using diverse technology, diverse design and implementation approaches) with diversity in follow-up of SIS in the operational phase (e.g., by using different operation and maintenance procedures, scheduling or staff).

Common cause failures (CCF) are a serious threat to SIS reliability (Smith & Simpson, 2005; Summers & Raney, 1999; Edwards & Watson, 1979), and may lead to simultaneous failures of redundant components and safety barriers. IEC 61511 (2003) defines a CCF as *a failure which is the result of one or more events*, *causing failures of two or more separate channels in a multiple channel system*, *leading to a system failure*. A channel is a single redundant path within a SIF, or alternatively a single SIF in case more than one SIF is required to obtain the necessary risk reduction.

Causes of potential CCFs may be introduced in design as well as in the operational phase. In the design phase, CCF causes may be a result of inadequate understanding of failure mechanisms and responses, improper selection of hardware components, and so forth. In the operational phase, CCF causes may, for example, be introduced because of improper testing, human errors during operation

*Corresponding author. Tel.: +47 73 59 7101; fax: +47 73 59 7117.
*E-mail address:* mary.a.lundteigen@ntnu.no (M.A. Lundteigen).

0950-4230/$ - see front matter © 2007 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jlp.2007.03.007

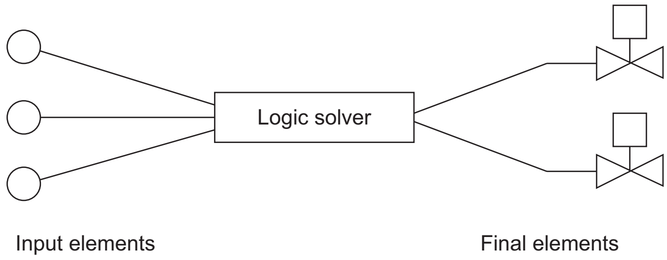


Fig. 1. Main parts of a safety instrumented system.

and maintenance, and environmental stresses outside the design envelope.

Many authors find it useful to split CCF causes into *root causes* and *coupling factors* (Parry, 1991; Paula, Campbell, & Rasmuson, 1991). A root cause is a basic cause of a component failure (e.g., a corrosive environment), while a coupling factor explains why several components are affected by the same root cause (e.g., inadequate material selection for several valves).

The nuclear industry is very concerned with CCFs, and is recording and analyzing CCF events (NUREG/CR-5460, 1990; NUREG/CR-5485, 1998; NEA, 2004, 2002, 2003, 2004). Several guidelines have been developed for qualitative and quantitative analysis of CCFs. The Nuclear Energy Agency (NEA) has initiated the International Common Cause Data Exchange (ICDE) project to encourage collection and analysis of data related to CCF events. Several analyses of CCF data that give insight into why CCFs occur have been published.

The oil and gas industry is mainly focusing on CCFs in the design phase of the SIS, while CCFs are given much less attention in the operational phase. The oil companies have systematically collected reliability data for more than 25 years through the OREDA project (Langseth, Haugen, & Sandtorv, 1998; Sandtorv, Hokstad, & Thompson, 1996). The data collection is based on maintenance reports from single item failures. This approach does not easily provide information about CCFs and the status related to CCFs is therefore not fully known. The Norwegian Petroleum Safety Authority (PSA) is, however, increasingly concerned with how new technology, standardization, and new operational concepts may reduce the independence between SIFs (Hauge et al., 2006).

Function testing and inspection are key activities for a SIS operating in the low demand mode. Low demand means that the SIS experiences few demands, typically less than once every year. Function testing and inspection are influencing the occurrence of CCFs in the operational phase because: (i) main types of CCFs can be identified and corrected through efficient testing and inspection procedures, and (ii) inadequate procedures and human errors may cause simultaneous failures of several components (Hirschberg, 1991; Johanson et al., 2003; Pyy, Laakso, & Reiman, 1997).

The objective of this paper is to propose a CCF defense approach which is able to improve the awareness to CCFs, prevent CCFs from being introduced during the execution of function tests and inspections, identify CCFs and CCF causes and select efficient defenses against future CCFs. The CCF defense approach is designed to be integrated with current practices related to execution and follow-up of function testing and inspection in the oil and gas industry. The CCF defense approach has been developed for SIS applications in the Norwegian oil and gas industry, but should be applicable also to other industry sectors.

The rest of the paper is organized as follows. In Section 2 we describe how CCFs currently are handled in the Norwegian oil and gas industry. Section 3 describes how diagnostic testing, function testing, and visual inspections may influence the occurrence of CCFs. In Section 4 we clarify and discuss the definition of a CCF and indicate how CCFs may be classified. The new CCF defense approach is described in Section 5. We conclude in Section 6 with a brief discussion of the proposed approach and give some recommendations for further work in Section 7.

## 2. The oil and gas industry's approach to CCFs

Recent SIS applications for the Norwegian oil and gas industry are built according to IEC 61508 (1998) and IEC 61511 (2003). The Norwegian Oil Industry Association (OLF) has developed a guideline on the practical application of IEC 61508 (1998) and IEC 61511 (2003) in the oil and gas industry, that is referred to as the OLF-070 (OLF-070, 2004) guideline. The standards and the guideline require that the effect of CCFs is taken into account in reliability calculations. IEC 61508 (1998) recommends using the $\beta$-factor model (e.g., see Rausand & Høyland, 2004), where $\beta$ is the conditional probability of a CCF, when a failure has occurred. An extended version of the $\beta$-factor model, called the PDS method (Sintef, 2006), is frequently used in the Norwegian oil and gas industry.

The IEC standards have few specific requirements related to CCFs in the operational phase, and this may be a reason why CCFs are not given much attention in this phase. Another reason may be that there is a general lack of knowledge on how CCFs affect operation and maintenance, since CCFs are not recorded and analyzed. There is no guidance in OREDA (2002) on how to collect data on CCFs, even though CCFs are mentioned in connection with fire and gas detectors. ISO 14224 (2006) recognizes the importance of sector specific CCF data for SIL analysis, and suggests that CCF data are derived from analysis of single failures rather than being recorded directly. Currently, however, data related to CCFs are not collected.

IEC 61508 (1998), part 6, Humphreys (1987), and Smith and Simpson (2005) provide checklists that can be used to determine an application specific $\beta$ value, while the PDS method suggests generic $\beta$ values for various SIS components. The generic values are based on previous estimates combined with expert judgments, and may not reflect the plant specific conditions. The checklists are not always sensitive to single improvements, and a new or improved defense tactic in the operational phase may therefore not lead to a reduction of the estimated $\beta$-factor.

To save money and ease operation and maintenance, the technical solutions become more and more standardized. The same type of PLCs is, for example, used in several SIS applications. This standardization may reduce the independence between SIS applications (Hauge et al., 2006). New operational concepts, like remote monitoring and control, may introduce additional risks (Johnsen, Lundteigen, Fartun, & Monsen, 2005; Sintef, 2003). Sintef, the Norwegian research organization, has recently carried out two studies that analyze CCFs and the level of independence in typical SIS applications on oil and gas installations (Hauge, Hokstad, Herrera, Onshus, & Langseth, 2004; Hauge et al., 2006). The first study was initiated by SIS vendors, system integrators and end users participating in a network on the application of the PDS method in Norway. The second study was initiated by Hydro, the Norwegian oil company. Unfortunately, there has, so far, not been any follow-up of these studies.

## 3. Diagnostic testing, function testing and visual inspection

Diagnostic testing, function testing, and visual inspections are important means to verify that the SIS is able to perform its safety functions and to reveal any failures that may impede the SIS from functioning on demand. Failures that may prevent the SIS from functioning on demand are referred to as *dangerous* failures by IEC 61508 (1998) and IEC 61511 (2003).

Diagnostic testing is online means to detect deviations, degradations and discrepancies, and is usually performed by dedicated software and hardware, implemented inherently in the components (e.g., watchdogs) or added to the SIS configuration (e.g., read-back of status signals from field elements for comparison with output signals set by the PLC). Failures detected by diagnostic testing are called *dangerous detected* failures in IEC 61511 (2003). The diagnostic software and hardware usually do not test the complete SIF, but give alarm upon various abnormalities (e.g., drift, exceeded cycle time, and communication error) on component level. Diagnostic alarms that share the same cause may indicate the presence of a CCF.

Function testing and visual inspections are offline means to detect SIS failures and are performed at regular intervals. The objective of function testing is to confirm the correct functionality and to reveal undetected failures that may impede the SIS from functioning on demand. Visual inspection looks for observable deterioration and unauthorized modifications. Failures revealed by function testing and inspection are called *dangerous undetected* failures in IEC 61511 (2003). The interval between function tests (or inspections) has a direct influence on the SIF's probability of failure on demand.

In most cases, function testing and inspection are executed manually. However, new technology has been developed for automated testing, for example, partial stroke testing of valves (Lundteigen & Rausand, 2007; Summers & Zachary, 2000). In the future it is expected that new oil and gas installations may be built for more extensive use of automated testing and inspection, but for the current oil and gas installations (that may stay in operation for another two decades) it is not realistic to expect major changes in the function testing and inspection strategies.

This paper focuses on current approaches to function testing, and how defense measures may be implemented to increase awareness of CCFs, to improve the ability to detect CCFs, and to avoid introducing new CCFs.

Function testing and inspection generally comprise the following six tasks:

(1) *Scheduling*: Today, function testing and inspections are scheduled automatically by the maintenance management system. At a predefined time, the function test or inspection is submitted as a work package that includes the test or inspection procedure.
(2) *Preparation*, *execution*, *and restoration*:
   (a) *Preparation*: Before the test or inspection is executed, it is required to do certain preparations; to obtain work permits, find the necessary documentation, to coordinate with other involved disciplines and, in some cases, to perform a job safety analysis. Job safety analysis is commonly used in the oil and gas industry to prepare for critical and complex work activities with a potentially high risk to humans, equipment or the environment. A function test or inspection does not always require a job safety analysis. This depends on the complexity of the work, and the total amount of ongoing activities in the same area.
   (b) *Execution*: The prescribed steps in the test or inspection procedure are executed, including setting necessary overrides and inhibits.
   (c) *Restoration*: After the test or inspection is completed, the affected components are put back into operation in a safe and adequate manner. This may involve opening/closing of isolation valves, following interlock procedures, resetting solenoids and valves and removing inhibits and overrides.
(3) *Failure reporting*: Deviations and failures are reported through the maintenance management system by the personnel executing the function test or inspection. Failures and deviations may be recorded as free text, as numerical values (e.g., pressure readings) or by using pre-defined classification systems of failure causes, detection method, and failure effects.
(4) *Failure analysis*: The purpose of the failure analysis is to assess the SIS performance and compare with the target performance (SIL requirements). The SIS performance in the operational phase is usually derived from the

number of dangerous failures detected during a function test, inspection, and real demands. To ensure that the quality of the recorded data is adequate, it is often necessary to reassess the initial failure classification and review the free text descriptions. Performance monitoring has also been done prior to the introduction of the IEC 61508 (1998) and the IEC 61511 (2003). On the Norwegian continental shelf, it has, for several years, been required to report the status of safety barriers. The main difference between the previous approach and the IEC 61508 (1998)/IEC 61511 (2003) requirements, is the focus on the performance of safety functions rather than on safety components.

(5) *Implementation*: It is necessary to prepare and implement corrective means related to the recorded failures. It is expected that failures detected by diagnostic testing, function testing, and inspection are corrected immediately to reduce the unavailability of the SIF. In cases where failures are not possible to correct immediately, compensating measures must be implemented.

(6) *Validation and continuous improvements*: At regular intervals, it is necessary to review current work practices and procedures and to analyze how they comply with the overall objective of SIS follow-up, which is to maintain the SIS performance during operation and maintenance. It may be relevant to review the extent of overdue tests, the adequacy of the failure classification system and the failure reporting procedures, SIF performance versus SIL targets, quality and scope of proof test execution (HSE, 2002). Any deviations or deficiencies should be captured and used to improve SIS follow-up.

## 4. Definition and classification of CCFs

### 4.1. The main attributes of CCFs

There is no generally accepted definition of CCF. This means that people in different industry sectors may have different opinions of what a CCF is. Smith and Watson (1980) review nine different definitions of CCF and suggest that a definition must encompass the following six attributes: (1) the components affected are unable to perform as required, (2) multiple failures exist within (but not limited to) redundant configurations, (3) the failures are "first in line" type of failures and not the result of cascading failures, (4) the failures occur within a defined critical time interval (e.g., the time a plane is in the air during a flight), (5) the failures are due to a single underlying defect or a physical phenomenon (the common cause of failures), and (6) the effect of failures must lead to some major disabling of the system's ability to perform as required.

All these attributes are reflected in the CCF definition that is used by the nuclear power industry (NEA, 2004). Concerning attribute (4), the ICDE project defines the critical time interval to be the time between two consecutive inspections. IEC 61508 (1998) and IEC 61511 (2003) do not include the critical time aspect in their definition of CCF. It is, however, natural to restrict the analysis to dependent failures occurring within the same function test interval. All critical failures should, at least in principle, be identified and corrected as part of the function test and repair action. A failure in the next interval will therefore be a single failure, even if it is dependent on a (corrected) failure in the previous interval. To clarify when dependent failures are defined as CCF during failure analysis, the following attributes may be applied: (1) the CCF event comprises multiple (complete) failures of two or more redundant components or two or more SIFs due to a shared cause, (2) the multiple failures occur within the same inspection or function test interval, and (3) the CCF event leads to failure of a single SIF or loss of several SIFs.

### 4.2. Classification of CCF attributes

Failure classification systems may be used to identify potential failures and to structure both causes and effects. Some authors distinguish between pre-operational and operational failure causes (Humphreys & Jenkins, 1991; Watson & Edwards, 1979), some use the concept of root causes and coupling factors, where the root causes may be further split into trigger events, conditioning events and proximate causes (Parry, 1991; Mosleh et al., 1994). Here, a proximate cause is a readily identifiable cause of failure, a conditioning event is a condition that predisposes the component to failure, and a triggering event is an event that initiates the transition to the failed state. The nuclear power industry has established classification systems for CCF causes and differentiate between various types of root causes and coupling factors (NEA, 2004; NUREG/CR-5460, 1990; NUREG/CR-5485, 1998). One such classification system is shown in Table 1. The operational failure causes proposed by, for example, by Humphreys and Jenkins (1991), overlap quite well with the coupling factors.

In many cases, CCF analysis is often limited to dependent failures within a single SIF since the reliability is estimated for each SIF separately. Cooper, Lofgren, Samanta, and Wong (1993) have introduced common failure mechanisms as an alternative concept to CCFs, to ensure that also CCFs affecting different SIFs are identified and followed up. A common failure mechanism comprises failures that share failure mechanisms, design or function, and time of occurrence. Failures that are classified with common failure mechanisms do therefore share the same coupling factors.

CCF causes are often identical to the systematic failure causes. Systematic failures are in IEC 61508 (1998) and IEC 61511 (2003) defined as failures that are due to design, implementation or operational related errors. The IEC standards suggest, as a general rule, not to quantify systematic failures. However, some systematic failures are quantified through the modeling of CCFs.

It may be convenient to distinguish between classification systems for failure reporting and classification systems for in-depth failure analysis. For failure reporting it is important that the taxonomy is intuitive and easy to understand, giving an initial and rough classification. For failure analysis one may add more detailed taxonomy, as suggested in OREDA (2002).

## 5. New CCF defense approach

In this section, we describe a new CCF defense approach which may be integrated with current approaches for function testing, inspection and follow-up. The new approach focuses on the following key aspects: (1) to avoid introducing CCFs during function testing and inspection, (2) to identify CCFs and CCF causes based on failure reports, and (3) to use the insight of failure causes to select efficient means to defend against future CCFs. The approach may be integrated into existing function testing and inspection related work processes, and has been designed to avoid any significant additional workload on plant workers. The approach builds on experience from the nuclear power industry (Hellstrøm, Johanson, & Bento, 2004; Hirschberg, 1991; Johanson et al., 2003; Parry, 1991; Paula et al., 1991; NUREG/CR-5460, 1990), the process industry (Summers & Raney, 1999), the oil and gas industry (Hauge et al., 2004, 2006) and own experience from maintaining SIS on oil and gas installations.

Table 1
ICDE classification of common causes (NEA, 2004)

| Classification of root causes | Classification of coupling factors |
|---|---|
| State of other components | Same/similar hardware |
| Design, manufacture or construction inadequacy | Hardware design |
| | System design |
| Human actions | Hardware quality deficiency |
| Maintenance | Same/similar operational conditions |
| Internal to component | Maintenance/test schedule |
| Procedure inadequacy | Maintenance/test procedure |
| Abnormal environmental stress | Maintenance/test staff |
| Other | Operation procedure |
| | Operation staff |
| | Same/similar environmental exposure |
| | Internal |
| | External |
| | Other |

The CCF defense approach follows the main tasks of function testing and inspection that are described in Section 3 and illustrated in Fig. 2. The six activities are based on checklists and analytical methods like operational sequence diagrams (OSD), influence diagrams and cause-defense matrices.

### 5.1. Task 1: ensure that necessary improvements are captured when scheduling

Scheduling of function test and inspection procedures is usually performed automatically and with predefined intervals by the maintenance management system. During the scheduling process, a work package is created specifying the type of resources, estimated number of hours needed to perform the work and the test procedure to be used. An important defense against CCFs is to ensure that any corrections and improvements to the test procedure are captured when new function test or inspection work packages are created.

### 5.2. Task 2: avoid introducing CCFs during preparation, execution, and restoration

Experience shows that CCFs are often introduced during maintenance due to human errors, erroneous procedures and deficient work processes (Hellstrøm et al., 2004; Pyy et al., 1997). Human errors may be deliberate actions (e.g., carelessness due to inappropriate understanding of the

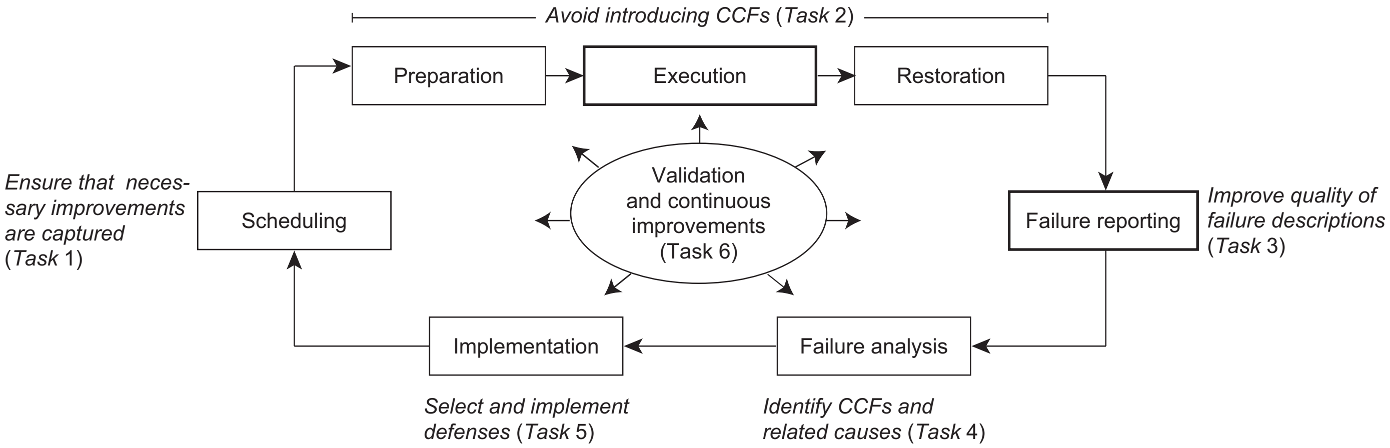

Avoid introducing CCFs (Task 2)
Preparation
Execution
Restoration
Ensure that necessary improvements are captured (Task 1)
Scheduling
Validation and continuous improvements (Task 6)
Failure reporting
Improve quality of failure descriptions (Task 3)
Implementation
Failure analysis
Select and implement defenses (Task 5)
Identify CCFs and related causes (Task 4)

Fig. 2. Main concepts of the CCF defense approach.

risks involved), accidental omission (e.g., forgetting parts of the instructions or leaving components inadvertently inoperative), or inadequate execution of the prescribed instructions (e.g., improper adjustments, miscalibration of equipment, improper bypassing). Deficient work processes may lack adequate coordination between maintenance disciplines, be based on deficient procedures or inadequate selection of tools.

Recommended defenses should be applied by the field technicians, and comprise means to improve self-checking, improve work planning and preparation, improve the operability readiness control, increase the respect to procedures, and verify adequate training of personnel (Hellstrøm et al., 2004). During execution of the tasks it is required to maintain a high awareness to CCF causes.

Separate checklists are suggested for the three tasks: preparation, execution, and restoration. Often, similar components (e.g., pressure transmitters) within the same area are tested simultaneously. In this case, the preparation checklist may be applied once, while the execution and restoration checklist must be repeated for each component tested or inspected.

Checklist for preparation:

(1) Have potential human errors during execution and restoration been identified and discussed?
(2) Have human error incidents been experienced during previous execution?
(3) Have compensating measures been identified and implemented to avoid human errors?
(4) Are the personnel executing the test familiar with the testing and calibration tools?
(5) Are the calibration tools calibrated?
(6) Does the procedure have known deficiencies, like ambiguous instructions?
(7) Does the procedure describe necessary steps to safely restore the SIS?

Checklist for execution:

(1) Are the components operated within the specified environmental and operating conditions? (E.g., within the specified temperature or pressure range, humidity constraints, vibration constraints, flow composition, and so on.)
(2) Are the components protected against damage from nearby work activities?
(3) Are process connections free from plugging and (if relevant) heat-traced?
(4) Are all field SIS components (constituting the safety function being tested) labeled?
(5) Are additional components that are operated during SIS function testing and inspection sufficiently labeled?

Checklist for restoration:

(1) Has the physical restoration (e.g., isolation valves and bypasses) been verified (e.g, by a colleague)?
(2) Have all suspensions of inhibits and overrides been verified and communicated?
(3) Are any remaining inhibits, overrides or bypasses logged, and compensating measures identified and implemented?
(4) Has the safety function been verified before start-up?

Any question given an answer “no” indicates a deviation (or a potential cause) that may lead to a CCF. Deviations should therefore be discussed and compensating measures or corrections implemented.

### 5.3. Task 3: improve the quality of failure reporting

The maintenance management systems that are currently used in the oil and gas industry are not suited for direct recording of CCFs. CFFs have to be identified from the recorded single failure events. The nuclear industry applies a similar approach (Hirschberg, 1991). Unfortunately, the failure classification systems used for failure reporting have ambiguous taxonomy that may be interpreted differently by different persons. In addition, the failure classes are incomplete and insufficient to use for further in-depth analysis of failure causes. It is therefore necessary to record free text descriptions of failure causes, effects and detection methods in order to verify the initial failure classification and provide necessary information to decide whether or not a CCF has occurred.

Analysis of CCFs is not the only reason for using extra time on failure descriptions. Databases like OREDA (2002) also require access to more in-depth descriptions of failure causes and effects. Any deficient information may be difficult to collect at a later stage since the involved personnel may (due to offshore work schedules) be off for three or four weeks at a time.

A set of questions has been proposed for use by field technicians during failure recording, and may be added as default text in the input field for free-text description. The questions enable a more complete description of failures and failure causes.

Checklist questions for failure reporting:

(1) How was the failure discovered or observed? (Incidental, by diagnostics, during function testing, inspection or repair, upon a demand or by review/audit.)
(2) What is believed to be the cause(s) of failure? (Several possible explanations may be included.)
(3) What was the effect of the failure on the safety function? (Loss of complete function, degraded, none.)
(4) Was the component tested or inspected differently than described in the test or inspection procedure, and why was the approach different?
(5) Has the component been overexposed (operational or by environmental stresses), and if so, what may be the related causes?
(6) Have—to your knowledge—similar failures been experienced previously?

### 5.4. Task 4: identify CCFs through failure analysis

Failure analysis of recorded failures is usually performed by system or equipment responsible engineers. It is proposed to use failure reports generated by the maintenance management system to identify CCFs. This is in line with ISO 14224 (2006) and what is also done in the nuclear power industry (Hirschberg, 1991). The nuclear power plants have for several years collected and shared CCF data, through, for example, the ICDE project. Our main objective is to identify CCFs for the purpose of selecting appropriate and plant specific defenses. In light of ISO 14224 (2006), it may be required also to develop procedures and systems for collecting and sharing data on CCFs.

The starting point for the failure analysis is the failure reports and supplementary failure descriptions (free text) in the maintenance management system. It is suggested to identify CCFs through a four step process: (1) review the failure descriptions and verify (and if necessary correct) the initial failure classification, (2) perform an initial screening that captures failures that (a) have similar design or physical location, (b) share failure causes, (c) have been discovered within the same test or inspection interval, and (d) the failure causes are not random (as defined by IEC 61508, 1998 and IEC 61511, 2003), (3) perform a root cause and coupling factor analysis by using influence diagrams, and (4) list the root cause and coupling factors in a cause-defense matrix as shown in Table 2. Whereas corrective work packages are generated automatically when single failures are registered in the maintenance management system, step 1–step 4 must be performed as additional activities.

Step 1 is necessary for validating single failures as well as CFF causes and effects to ensure appropriate follow-up. Step 2 raises attention to failures that have common failure mechanisms, and that have not been detected by diagnostics. If failures detected by diagnostics are not repaired within a prescribed time, or if the same type of dangerous detected failures occurs rather frequently, they should be included in the analyses as well.

In step 3, it is proposed to identify the root causes and coupling factors by using a root cause and coupling factor analysis diagram. The main objective is to get more insight into the CCF causes, and thereby have a well-prepared basis for selecting suitable defenses. The analysis should be performed by a group of relevant personnel, rather than by individuals, and may include plant workers as well as engineers. A separate diagram may be constructed for each CCF identified in step 2. The root cause and coupling factor diagram may start with a description of the CCF, including the failure mode and the components having caused the failure, as shown in Fig. 3. The failure mode is the non-fulfillment of the required SIS performance. From there, the root cause and coupling factor diagram is drawn from right to left through iterative asking for underlying failure causes.

The CCF causes are always a result of a root cause and a coupling factor, indicated by an "and" gate in Fig. 3. In some cases it may, however, be difficult to determine the root causes (due to inadequate failure descriptions). In this case, one may focus on the coupling factors and still find adequate defenses against future CCFs. The analysis stops when no further insight into failure causes is available.

The diagram may also be used pro-actively, to identify failure causes that may lead to CCFs in the near future. In this case, one may extend the diagram with analysis of other relevant SIS components that may lead to loss of the safety function, as illustrated in Fig. 3 by dashed arrows and nodes. Relevant components may, in this context, mean redundant components. To identify potential failure causes, one may use a simple checklist of typical failure causes, for example the one shown in Table 1.

The application of the checklist may be illustrated for a pressure transmitter in a pipeline. A pressure transmitter performs the following subfunctions; to sense the pipeline pressure, convert the pressure reading to an analogue signal and transmit the pressure reading to the logic solver. Failure of one of the subfunctions leads to failure of the pressure transmitter. The root causes and coupling factors may be analyzed for each subfunction failure. The root causes of sensing failures may, for example,

Table 2
Simplified cause-defense matrix

| CCF | Root cause | Coupling factor | Defense alternatives | R | C | Impact (H/L) | Cost (H/M/L) |
|---|---|---|---|---|---|---|---|
| Failure of ESD valves | Solenoid stuck due to pollution in hydraulic supply | Same design | Implement regular quality check of hydraulics | √ | √ | M | L |
| | | Hook-up to same hydraulic supply | Installing filters in hydraulic supply | √ | | H | M |
| | | | Replacing existing solenoids with new and more robust ones | | | | |

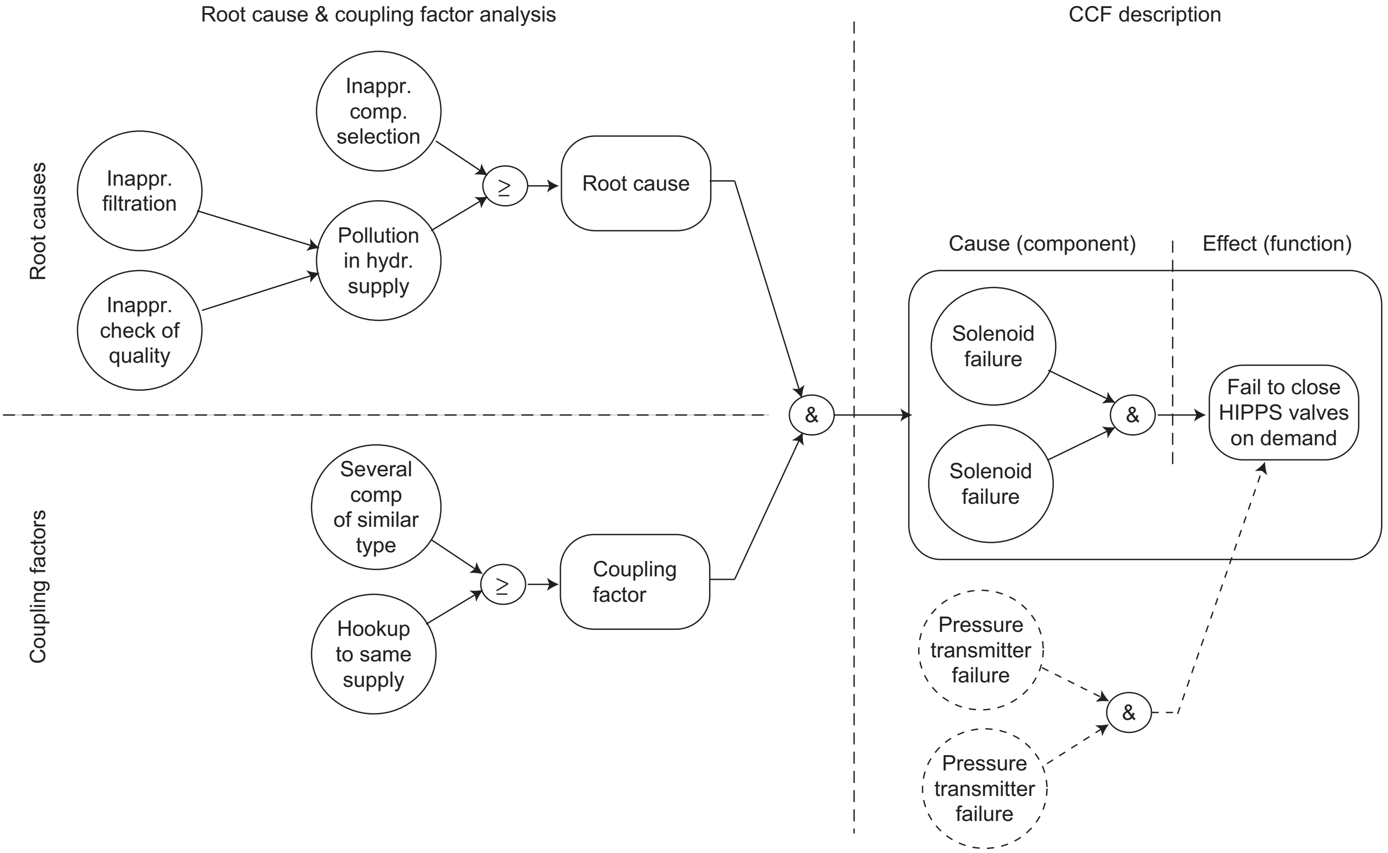


Fig. 3. Root cause and coupling factor analysis diagram.

be construction inadequacy (e.g., too small dimension of pressure sensing line) or human actions (e.g., leaving the transmitter isolated). Several pressure transmitters may fail simultaneously because the same inappropriate design is selected for all components, or they are tested using the same deficient procedure. This failure analysis process may be continued for all components and their related subfunctions.

The main results from the analysis, which are the root causes and the coupling factors, may be listed in a simplified cause-defense matrix, as illustrated in Table 2.

### 5.5. Task 5: implement defense measures

Implementation of CCF defense measures is important to prevent future occurrences of similar failures. In the nuclear industry, cause-defense matrices are used for detailed assessment of defenses (NUREG/CR-5460, 1990; Paula et al., 1991). In the cause-defense matrices, a set of predefined defenses are considered for each root cause and coupling factor. Several types of defenses are covered, like design related improvements, procedure related improvements, and physical barriers. The expected impact of all defense alternatives are evaluated, and used to rank their efficiency. In the nuclear power industry, the impact analysis is also used to estimate the rate of occurrence of CCFs, as input to the reliability models (e.g., see Mosleh, Parry, & Zikria, 1994). In the proposed CCF defense approach, it is recommended to apply a simplified cause-defence matrix, where simplified means that impact analysis is limited to a smaller selection of defense options.

The CCF defense approach applies the simplified cause-defense matrix in combination with a set of generic defense options, see Tables 2 and 3. The generic defense options have been adapted from NUREG/CR-5460 (1990) and Parry (1991). This list may be used in group discussions to suggest application specific defenses. The defense strategies “new procedure” and “improved quality control” may, for example, be used to derive the more specific defense strategy “regular quality checks of hydraulics”.

It should be noted that the list of generic defense options does not include staggering of staff and staggered testing, even if these measures defend against CCFs (Summers & Raney, 1999). Offshore oil and gas installations are often scarcely manned, and staggered testing may be unrealistic to implement. In addition, it may be more complex to coordinate and more time consuming. However, in other applications staggered testing and staggering of staff may be relevant and should then be added to the list.

Each plant specific defense is evaluated with respect to protection impact (the ability to protect against future occurrences) and cost impact. The protection impact is evaluated qualitatively, as either high (H) or low (L), an approach which is also used in the more extensive cause-

Table 3
Generic defense options

| | |
|---|---|
| Administrative control | Improved preparation<br>Improved coordination<br>Improved responsibilities<br>Improved feedback of experience<br>Improved safety culture<br>Improved training<br>Improved quality control |
| Documentation | Improved drawings<br>Improved functional description |
| Procedures | New procedure<br>Improved procedure text (clarification, added scope or information)<br>Improved quality control of restoration<br>Improved test tools and calibration |
| Monitoring and surveillance | New alarm or alert. Implementation must follow IEC 61508 (1998)/61511 (2003)<br>New condition or logic sequence |
| Physical barriers | Improved physical support or fastening<br>Improved physical protection |
| Hardware or software modifications of SIS | Modifications requiring design changes. Redesign following IEC 61508 (1998)/61511 (2003) |

defense matrices for the nuclear industry (but with other symbols). The cost impact may be evaluated qualitatively (high (H), medium (M) or low (L)) or quantitatively (based on a cost estimate). If the costs are considered quantitatively, the cost impact may include design and installation costs or the life cycle costs. For each selected defense, it should be indicated if the root cause (R), the coupling factor (C) or both are affected. The information may be useful for assessing the estimated impact on reliability parameters, for example, the $\beta$-factor (in case the $\beta$-factor model is selected) or the dangerous failure rate. At the current stage, the CCF defense approach does not recommend how the reliability parameters should be updated.

### 5.6. Task 6: validation and continuous improvements

Systematic failures that may lead to CCFs, are not always captures through execution and follow-up of function testing and inspection. According to Summers and Raney (1999), the most critical cause of CCFs during SIS design and implementation is an erroneous or incomplete safety requirement specification. If, for example, an inadequate fire protection is specified, the detectors may fail to detect a real fire. The similar argument may be relevant for the operational phase; if the work processes, procedures, tools and competence are inappropriate for avoidance, identification and follow-up of CCFs, they may not provide the intended protection against CCFs. Validating all work tasks at regular intervals with respect to how they comply with the new approach may capture weaknesses and lead to continuous improvement. It may also be relevant to evaluate the effect of implemented defenses, either qualitatively or quantitatively.

The CCF defense approach suggests two new validation activities: (1) task analysis of function testing and inspection execution, and (2) use of a new validation checklist. The task analysis is suitable for capturing the causes of human interaction failures (Kirwan & Ainsworth, 1992), and the selected approach builds on operational sequence diagrams OSD as illustrated in Fig. 4. One may choose to concentrate on those work processes that are related to SIS components where CCFs or CCF causes have been experienced. The new validation checklist builds on the SIS life cycle checklists proposed by Summers and Raney (1999). Many oil and gas companies perform regular audits of, for example, SIS follow-up and performance. Some of the questions suggested for the validation checklist may therefore be covered by existing audit procedures.

Checklist questions for validation:

(1) Are requirements for the safety function covered by the function test or inspection procedure(s)?
(2) Are all disciplines involved in SIS testing, inspection, maintenance and follow-up familiar with the concept of CCFs?
(3) Are dangerous undetected failure modes known and sufficiently catered for in the function test and inspection procedures?
(4) Are the test limitations (compared to the real demand conditions) known?
(5) Are all redundant channels of the safety function covered by the function test or inspection procedures?
(6) Are failures introduced during function testing and inspection captured, analyzed and used to improve the associated procedures?
(7) Are failures detected upon real demands analyzed to verify that they would have been detected during a function test or inspection?
(8) Are changes in operating or environmental conditions captured and analyzed for necessary modifications to the SIS or related procedures?
(9) Are the calibration and test tools suitable and maintained according to the vendor recommendations?
(10) Are personnel using the calibration and test tools familiar with their application?
(11) Are procedure deficiencies communicated to the responsible persons and followed up?
(12) Are the diagnostic alarms followed up within the specified mean time to restoration?
(13) Are CCF systematically identified and analyzed, and defenses implemented to prevent their recurrence?

Questions given the answer “no” indicate a potential weakness in the defense against CCFs, and should be discussed to determine corrective actions.

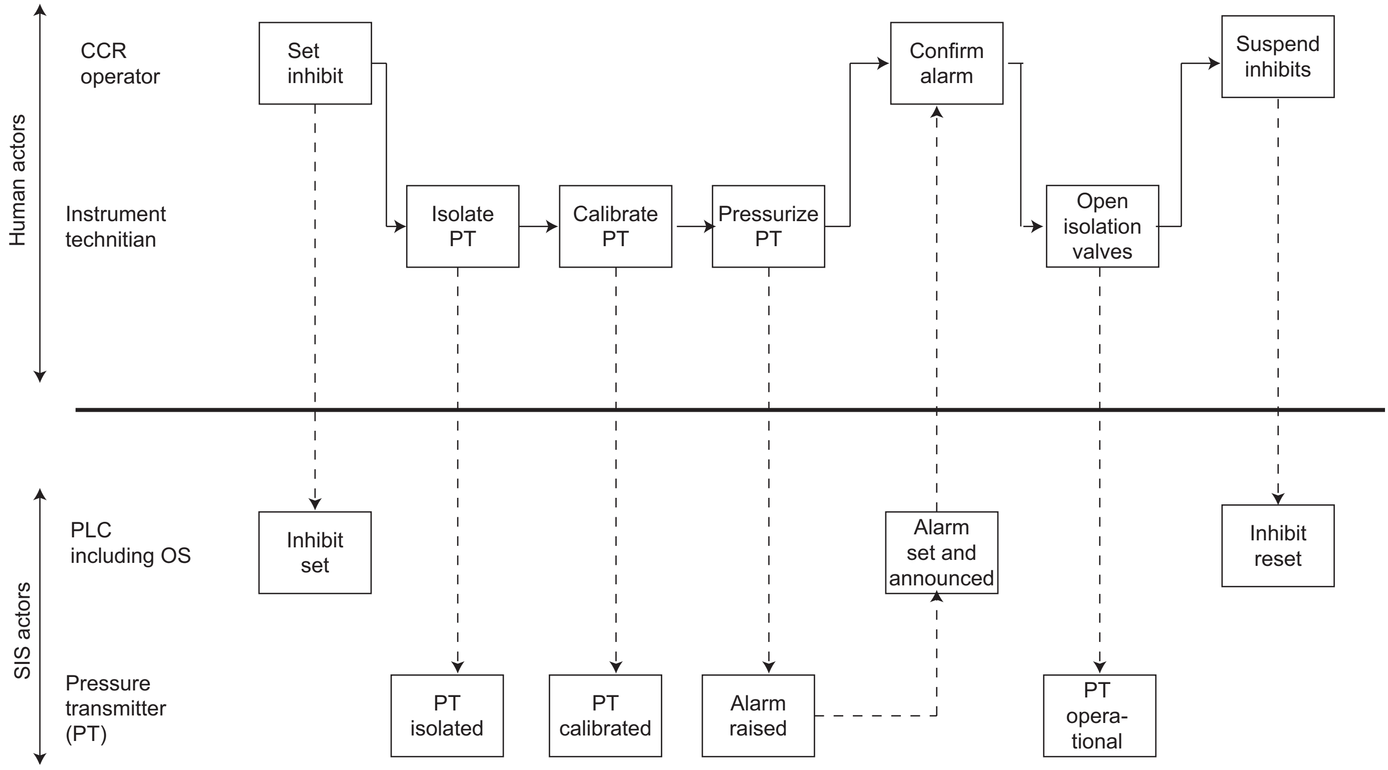


Fig. 4. OSD for function testing of pressure transmitters.

## 6. Discussion

The proposed CCF defense approach is based on a set of checklists and is supported by influence diagrams, task analyses, and simplified cause-defense matrices. The oil and gas industry is familiar with checklists that are used to initiate discussions on focus areas and identify deviations from regulations and engineering standards. One example is the crisis intervention and operability analysis (CRIOP) methodology that uses checklists to verify the design of offshore control centers (Johnsen et al., 2004).

Several important features related to the development of efficient checklists are discussed by Summers and Raney (1999), Summers, Raney, and Dejmek (1999), and Walker (1997). The questions must be relevant (so that they provide information on factors that are relevant to CCFs), complete (cover all relevant aspects of CCFs), specific (so that the attainable response is obtained), repeatable (so that the user gives the same answer when the question is repeated under similar circumstances) and reproducible (meaning that different users give the same answer under similar circumstances).

The CCF defense approach recommends that analyses of root causes and coupling factors are based on influence diagrams. Influence diagrams are suitable for qualitative as well as quantitative analyses (e.g., see Jensen, 2001). Methods like fault tree analysis, the modified FMEA analysis tool (Childs & Mosleh, 1999) and the failure classification sheets used in the nuclear power industry (Mosleh et al., 1994) may also be applied. Influence diagrams are, however, preferred since they give a simple illustration that is easy to grasp by practitioners. Cooper et al. (1993) recommend to skip the analysis of root causes, and rather focus on common failure mechanisms (which captures coupling factors). Their argument is that failure descriptions often lack sufficient information to determine the root causes, that the root causes may be interpreted differently by different people, and that the root causes are not as relevant for selecting efficient defenses against CCFs as the common failure mechanisms. In our approach, we have maintained the attention to defense tactics against root causes. However, if adequate failure descriptions are not available, one may limit the attention to the coupling factors.

A simplified cause-defense matrix has been selected rather than the more extensive version used in the nuclear power industry (Paula, 1990). To perform very detailed analysis of defense measures and their impact may not be realistic in the oil and gas industry that (at the current stage) does not use this information to estimate the CCF failure rates.

Task analysis may be used to verify that all relevant CCF causes are catered for in the checklists and procedures (e.g., see Davoudian, Wu, & Apostolakis, 1994). Task analysis is a method where the sequence of tasks, the role of the various actors and their way of communicating are analyzed. There are several approaches to task analysis (e.g., see Hendrick & Benner, 1987; Kirwan & Ainsworth, 1992). The concept of OSD has been selected for the CCF defense approach, since it is an intuitive way of visualizing the communication between various actors, both humans and technology. The OSD is organized similar to a sequential timed events plotting (STEP), an approach that has proved to be efficient in similar applications (Sintef, 1998, 2003).

The current version of the CCF defense approach does not relate the efficiency of defenses to the reliability parameters. Several approaches may be considered for future extensions. One alternative is to wait and see if the failure reports indicate a reduced failure rate. Another alternative is to take credit for the expected effect, by estimating a new failure rate or a new $\beta$-factor. However, it may be difficult to determine if the reduction is due to a certain defense measure or to other factors. The failure rate may be updated following the approach, for example, by Vatn (2006) or Sintef (2006). To update the $\beta$-factor, the PDS method (Sintef, 2006), the betaplus method Smith and Simpson (2005), IEC 61508 (1998) $\beta$-factor checklists or the checklists developed by Humphreys (1987) may be applied.

Other effects from using the CCF defense approach that may be difficult to measure quantitatively is the increased awareness to the causes and effects of CCFs. Increased awareness may improve the detection of CCFs during execution and follow-up of function testing and inspection, and give more attention to how human interaction related failures may be avoided. The importance of maintaining independence between safety functions and redundant components may also be more evident to all actors working with SIS operation, maintenance, and follow-up.

## 7. Conclusions and ideas for further work

The CCF defense approach presents a practical implementation of defenses during the operational phase of oil and gas installations. It builds on generic and recognized methodologies combined with related research results and experience from other industry sectors. To our knowledge, a similar approach has not been developed, and may therefore be a valuable contribution for SIS follow-up. The approach has yet not been tested in real applications, but this type of testing will be performed and reported later.

A main limitation of the current version of the CCF defense approach is the lack of quantitative means to indicate any trends in the status of CCF defenses in the operational phase. This is therefore an important area for future research. There are several other ideas for further work. One obvious issue is to test the checklists and tools in the oil and gas industry, and analyze feedback for further improvements of the methodology. Another area is to consider alternative analytical techniques, for example, for analyzing the root causes and coupling factors. The recommendation by ISO 14224 (2006) to collect data on CCFs may also represent a challenge for the oil and gas industry data, and it may be important to develop common approaches to classification of CCFs. A last issue is to analyze new operational concepts and technology and how they may introduce new CCF causes. In the future, one may expect extensive use of automated function testing and new ways of human interaction that may introduce new stresses to technology as well as to humans and organizations.

## Acknowledgments

We would like to acknowledge the RAMS group at the Department of Production and Quality Engineering at NTNU for valuable comments during development of this paper. We would also like to thank the anonymous referees for suggestions to improve the presentation of the paper.

## References

Childs, J. A., & Mosleh, A. (1999). A modified FMEA tool to use in identifying and addressing common cause failure risks in industry. In *Annual reliability and maintainability symposium*, Washington, DC.

Cooper, S. E., Lofgren, E. V., Samanta, P. K., & Wong, S.-M. (1993). Dependent failure analysis of NPP data bases. *Nuclear Engineering and Design*, *142*, 137–153.

Davoudian, K., Wu, J.-S., & Apostolakis, G. (1994). Incorporating organizational factors into risk assessment through the analysis of work processes. *Reliability Engineering and System Safety*, *45*(1–2), 85–105.

Edwards, G. T., & Watson, I. A. (1979). *A study of common-mode failures*. Technical Report, UKAEA-SRD- R 146.

Hauge, S., Hokstad, P. R., Herrera, I., Onshus, T., & Langseth, H. (2004). *The impact of common cause failures in safety systems*. Technical Report STF38 F04410 (restricted), Sintef, Trondheim, Norway.

Hauge, S., Onshus, T., Øien, K., Grøtan, T. O., Holmstrøm, S., & Lundteigen, M. A. (2006) *Uavhengighet av sikkerhetssystemer offshore—status og utfordringer*. Technical Report STF50 A06011, SINTEF, Trondheim, Norway (in Norwegian).

Hellstrøm, P., Johanson, G., & Bento, J.-P. (2004). Dependency defence—How to protect against dependent failures. In *PSAM 7/ESREL*, Berlin, Berlin: Springer.

Hendrick, K., & Benner, L. (1987). *Investigating accidents with STEP*. New York: Marcel Dekker.

Hirschberg, S. (1991). Experiences from dependent failure analysis in nordic countries. *Reliability Engineering and System Safety*, *34*(3), 355–388.

HSE (2002). *Principles for proof testing of safety instrumented systems in the chemical industry* (*prepared by ABB Ltd for the HSE*). Technical Report 428/2002, Health and Safety Executive.

Humphreys, P., & Jenkins, A. M. (1991). Dependent failures developments. *Reliability Engineering and System Safety*, *34*(3), 417–427.

Humphreys, R. A. (1987). Assigning a numerical value to the beta factor common cause evaluation. In *Reliability'87: Proceedings of the sixth conference*, (pp. 2C/5/1–2C/5/8), Birmingham, UK.

IEC 61508. (1998). *Functional safety of electrical/electronic/programmable electronic safety-related systems*. Part 1: General requirements. International Electrotechnical Commission, Geneva, 1998.

IEC 61511 (2003). *Functional safety—safety instrumented systems for the process industry*. Part 1: Framework, definitions, system, hardware and software requirements. International Electrotechnical Commission, Geneva, 2003.

ISO 14224 (2006). *Petroleum, petrochemical and natural gas industries—collection and exchange of reliability and maintenance data for equipment*. International Standardization Organization, Geneva, 2006.

Jensen, F. V. (2001). *Bayesian networks and decision graphs*. New York: Springer.

Johanson, G., Hellstrøm, P., Mankamo, T., Bento, J. P., Knochenhauer, M., & Pörn, K. (2003). *Dependency defence and dependency analysis guidance—Volume 2: Appendix 3-18 How to analyse and protect against dependent failures. Summary report of the Nordic Working group on Common Cause Failure Analysis*. Swedish Nuclear Inspectorate (SKI).

Johnsen, S. O., Bjørkli, C., Steiro, T., Fartum, F., Haukenes, H., Ramberg, J., et al. (2004). *CRIOP: A scenario method for crisis intervention and operability analysis*. Technical Report STF38 A03424, Sintef, Trondheim, Norway.

Johnsen, S. O., Lundteigen, M. A., Fartun, H., & Monsen, J. (2005). Identification and reduction of risk in remote operations of offshore oil and gas installations. In *ESREL'05* (pp. 957–964). Balkema.

Kirwan, B., & Ainsworth, L. K. (1992). *A guide to task analysis*. London: Taylor & Francis.

Langseth, H., Haugen, K., & Sandtorv, H. A. (1998). Analysis of OREDA data for maintenance optimisation. *Reliability Engineering and System Safety*, *60*(2), 103–110.

Lundteigen, M. A., & Rausand, M. (2007). The effect of partial stroke testing on the reliability of safety valves. In *ESREL'07*, Stavanger, Norway.

Mosleh, A., Parry, G. W., & Zikria, A. F. (1994). An approach to the analysis of common cause failure data for plant-specific application. *Nuclear Engineering and Design*, *150*(1), 25–47.

NEA (2004). *ICDE Project Report: Collection and analysis of common-cause failure of emergency diesel generators*. Number NEA/CSNI/R(2000)20. Nuclear Energy Agency.

NEA (2002). *ICDE Project Report: Collection and analysis of common-cause failures of safety and relief valves*. Number NEA/CSNI/R(2002)19. Nuclear Energy Agency.

NEA (2003). *ICDE Project Report: Collection and analysis of common-cause failures of check valves*. Number NEA/CSNI/R(2003)15. Nuclear Energy Agency.

NEA (2004). *International common-cause failure data exchange*. ICDE general coding guideline – technical note. Number NEA/CSNI/R(2004)4. Nuclear Energy Agency.

NUREG/CR-5460 (1990). *A cause-defense approach to the understanding and analysis of common cause failures*. Nuclear Regulatory Commission, Washington, DC.

NUREG/CR-5485 (1998). *Guidelines on modeling common-cause failures in probabilistic risk assessment*. Nuclear Regulatory Commission, Washington, DC.

OLF-070 (2004). *Application of IEC61508 and IEC61511 in the Norwegian Petroleum Industry*. The Norwegian Oil Industry Association.

OREDA (2002). *OREDA reliability data*. OREDA Participants, Available from: Det Norske Veritas, NO 1322 Høvik, Norway, (4th ed.).

Parry, G. W. (1991). Common cause failure analysis: a critique and some suggestions. *Reliability Engineering and System Safety*, *34*, 309–326.

Paula, H. M. (1990). Data base features that are needed to support common-cause failure analysis and prevention. An analyst's perspective. *Nuclear Safety*, *31*(2), 159–173.

Paula, H. M., Campbell, D. J., & Rasmuson, D. M. (1991). Qualitative cause-defense matrices; engineering tools to support the analysis and prevention of common cause failures. *Reliability Engineering and System Safety*, *34*(3), 389–415.

Pyy, P., Laakso, K., & Reiman, L. (1997). *A study of human errors related to NPP maintenance activities*. IEEE Sixth annual human factors meeting (pp. 12–23).

Rausand, M., & Høyland, A. (2004). *System reliability theory; models, statistical methods and applications* (2nd ed.). New York: Wiley.

Sandtorv, H. A., Hokstad, P. R., & Thompson, D. W. (1996). Practical experiences with a data collection project: The OREDA project. *Reliability Engineering and System Safety*, *51*(2), 159–167.

Sintef (1998). *Methods for safety analysis in railway systems*. Technical Report STF48 A98426, Sintef, Trondheim, Norway.

Sintef (2003). *Morgendagens HMS-analyser for vurdering av tekniske og organisatoriske endringer*. Technical Report STF38 A02423, Sintef, Trondheim, Norway (in Norwegian).

Sintef (2006). *Reliability prediction methods for safety instrumented systems—PDS method handbook*. SINTEF, Trondheim, Norway.

Sklet, S. (2006). Safety barriers: Definition classification and performance. *Journal of Loss Prevention in the Process Industries*, *19*(5), 494–506.

Smith, A. M., & Watson, I. A. (1980). Common cause failures—a dilemma in perspective. *Reliability Engineering*, *1*(2), 127–142.

Smith, D. J., & Simpson, K. G. L. (2005). *Functional safety—A straightforward guide to applying the IEC 61508 and related standards*. Burlington, UK: Elsevier.

Summers, A. E., & Raney, G. (1999). Common cause and common sense, designing failure out of your safety instrumented system (SIS). *ISA Transactions*, *38*, 291–299.

Summers, A., & Zachary, B. (2000). Partial-stroke testing of block valves. *Control Engineering*, *47*(12), 87–89.

Summers, A. E., Raney, G., & Dejmek, K. A. (1999). Safeguard safety instrumented systems. *Chemical Engineering Progress*, *95*(11), 85–90.

Vatn, J. (2006). Procedures for updating test intervals based on experience data. In *ESReDa Conference*, Trondheim, Norway.

Walker, A. J. (1997). Quality management applied to the development of a national checklist for ISO 9001 audits for software. In *Proceedings of the IEEE international software engineering standards symposium*, Walnut Creek, USA. IEEE.

Watson, I. A., & Edwards, G. T. (1979). Common-mode failures in redundancy systems. *Nuclear Technology*, *46*(2), 183–191.

# Article 3

Spurious activation of safety instrumented systems in the oil and gas industry: Basic concepts and formulas
*Reliability Engineering and System Safety*, Volume 93, p. 1208–1217, 2008

Available online at www.sciencedirect.com

ScienceDirect

ELSEVIER

Reliability Engineering and System Safety 93 (2008) 1208–1217

RELIABILITY ENGINEERING & SYSTEM SAFETY

www.elsevier.com/locate/ress

# Spurious activation of safety instrumented systems in the oil and gas industry: Basic concepts and formulas

Mary Ann Lundteigen*, Marvin Rausand

*Department of Production and Quality Engineering, The Norwegian University of Science and Technology, 7491 Trondheim, Norway*

Received 11 June 2007; received in revised form 17 July 2007; accepted 22 July 2007
Available online 2 August 2007

**Abstract**

Spurious activation of safety instrumented systems in the oil and gas industry may lead to production loss, stress on affected components and systems, and hazards during system restoration. This article defines and clarifies concepts related to spurious activation. A clear distinction is made between spurious operation, spurious trip, and spurious shutdown. The causes and effects of spurious activation are discussed and related to the concepts used in IEC 61508, IEC 61511, and OREDA. A new set of formulas for calculating the spurious activation rate is presented, and compared with formulas that are frequently used in the oil and gas industry. The new approach is illustrated in a simple case study.

*Keywords:* Spurious trip; Spurious activation; Spurious operation; Safety instrumented system; False process demand

## 1. Introduction

Safety instrumented systems (SIS) are used in the oil and gas industry to detect hazardous events, and to perform required safety actions to maintain—or bring the process back to—a safe state. The safety functions implemented into a SIS are called safety instrumented functions (SIF). A SIS comprises input elements (e.g., sensors), logic solvers (e.g., programmable electronic solver [PLC]), and final elements (e.g., safety valves, circuit breakers, alarms). The overall objective of SIS design, implementation, and follow-up is to ensure that the SIS is able to perform the intended safety functions if specific process demands should occur.

Spurious activation of the SIS may lead to a partial or full process shutdown. The spurious activation may be due to false process demands or SIS element failures. A false process demand is a demand that is erroneously treated as a real process demand, for example, a stray ray of sunlight that is mistakenly read as a fire by a flame detector. In the oil and gas industry, it is important to reduce the number of spurious activations to (i) avoid unnecessary production loss, (ii) reduce the risk related to stresses caused by the spurious activation, and (iii) avoid hazards during unscheduled system restoration and restart.

The main focus of the IEC 61508 [1] and the IEC 61511 [2] is to ensure that the SIS is able to perform on demand. Limited focus is given to spurious activations, their causes and effects, and how to estimate the rate of spurious activations. IEC 61508 has no requirements related to spurious activations, while IEC 61511 requires that a maximum *spurious trip rate* (STR) is specified, but the standard does not provide any definition of a spurious trip or guidance on how the rate should be estimated.

To estimate the STR, the oil and gas industry often uses the formulas presented in [3–6]. When comparing these formulas, it is evident that there is no unique interpretation of the concept of spurious trip. While the PDS[1] method [5] defines a spurious trip as a spurious *activation* of a single SIS element or of a SIF, ANSI/ISA 84.01 [7] refers to a spurious trip as a non-intended process shutdown. As a result, the concept of spurious trip is rather confusing and it is difficult to compare the STR in different applications.

*Corresponding author. Tel.: +47 73597101; fax: +47 73597117.
*E-mail address:* mary.a.lundteigen@ntnu.no (M.A. Lundteigen).

[1] PDS is the Norwegian abbreviation of “reliability of computer-based safety systems”.

0951-8320/$ - see front matter © 2007 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ress.2007.07.004

The objectives of this article are to (i) define and discuss terms and concepts related to spurious activation of a SIS, (ii) clarify the spurious activation causes, and (iii) establish a set of formulas for calculating the rate of spurious activations and to compare them with the formulas provided by [4,5].

The article is organized as follows: In Section 2, the main concepts of spurious activation are defined and discussed. The causes of spurious activation are discussed in Section 3 in light of the spurious activation concepts proposed in Section 2 using an influence diagram. Here, we also address the relationship between spurious activation and dangerous detected (DD) failures. Section 4 gives an overview of failure modes and discusses how spurious activations may be classified in this respect. A set of formulas are established in Section 5, and a case study gives a brief comparison with some of the alternative approaches used in the oil and gas industry today. Finally, some concluding remarks are given in Section 6.

## 2. Main concepts of spurious activation

Spurious activation is known under several different names in the literature, for example, spurious operation (SO), spurious trip, spurious stop, nuisance trip, spurious actuation, spurious initiation, false trip, and premature closure (PC) [4,8–11]. In this article, spurious activation is used as a collective term. *Spurious* indicates that the cause of activation is improper, false, or non-genuine, while *activation* indicates that there is some type of transition from one state to another.

There are three main types of spurious activation: (1) spurious activation of individual SIS elements, (2) spurious activation of a SIS (i.e., of a SIF), and (3) spurious shutdown of the process. Using the same concept to describe all three types may lead to misunderstanding and confusion. A spurious activation of, for example, a single gas detector in a 2-out-of-3 (2oo3) voted configuration of detectors will not lead to a spurious activation of the SIF, and a spurious activation of a SIF leading to start-up of a fire pump will not necessarily disturb the process.

To distinguish between the different types of spurious activation, we suggest the following terms and definitions:

- *Spurious operation*: A SO is an activation of a SIS element without the presence of a specified process demand. Examples comprise: (i) a false signal about high level from a level transmitter due to an internal failure of the transmitter, or (ii) a PC of a spring loaded, hydraulically operated, fail-safe-close safety valve due to leakage in the hydraulic circuit, and (iii) a high level alarm from a level transmitter without the liquid level having exceeded the upper limit, due to failure to distinguish the foam from the real level of the liquid in the separator.
- *Spurious trip*: A spurious trip is activation of one or more SIS elements such that the SIS performs a SIF without the presence of a specified process demand. Examples comprise: (i) two flame detectors in a 2oo3 configuration give false signal about fire, causing the final elements of the SIF to be activated, and (ii) one out of two shutdown valves in a 1oo2 configuration of final elements closes prematurely due to an internal failure.
- *Spurious shutdown*: A spurious shutdown is a partial or full process shutdown without the presence of a specified process demand.

All the three terms are used in the literature, but unfortunately, with ambiguous meanings. In ISO 14224 [11] and OREDA [8], the offshore reliability data acquisition project [8,12], the term SO is close to our definition, but they also give spurious trip the same meaning as SO. The term spurious trip is, for example, used for unexpected shutdowns of machinery.

## 3. Causes of spurious activation

In Fig. 1, the main causes of spurious activation are identified and illustrated in an influence diagram. SO, spurious trip, and spurious shutdown are shown as performance nodes (rounded rectangles), since their rates of occurrence are performance quantities that we want to minimize in order to reduce the production loss. The chance nodes (circles) represent the factors that influence the rates of spurious activation. We are not able to control these factors directly, but we may influence them indirectly through a set of decisions. A decision may be to select an element with a higher reliability than specified. Another decision may be to invest in more training and higher personnel competence in order to reduce human errors during operation and maintenance. Relevant decisions are illustrated in the figure as decision nodes (rectangles). The arrows indicate the relationships between decisions, factors, and performance measures.

Fig. 1 also illustrates the links between the three types of spurious activation: a SO (in the following referred to as SO-failure) may be one of several causes of a spurious trip, and a spurious trip may be one of several causes of a spurious shutdown. The dashed arrows in Fig. 1 indicate that the link is present under certain conditions, for example, for a specific hardware configuration.

### 3.1. Causes of SO

There are two main causes of SO of a SIS element:

(1) An internal failure of the element (or its supporting equipment) leads to a SO.
(2) The input element responds to a false demand.

SO-failures due to internal failures are often considered as *safe failures* since they do not impede the SIS from performing on a demand. However, all safe failures are not leading to SO, and it is therefore necessary to study the

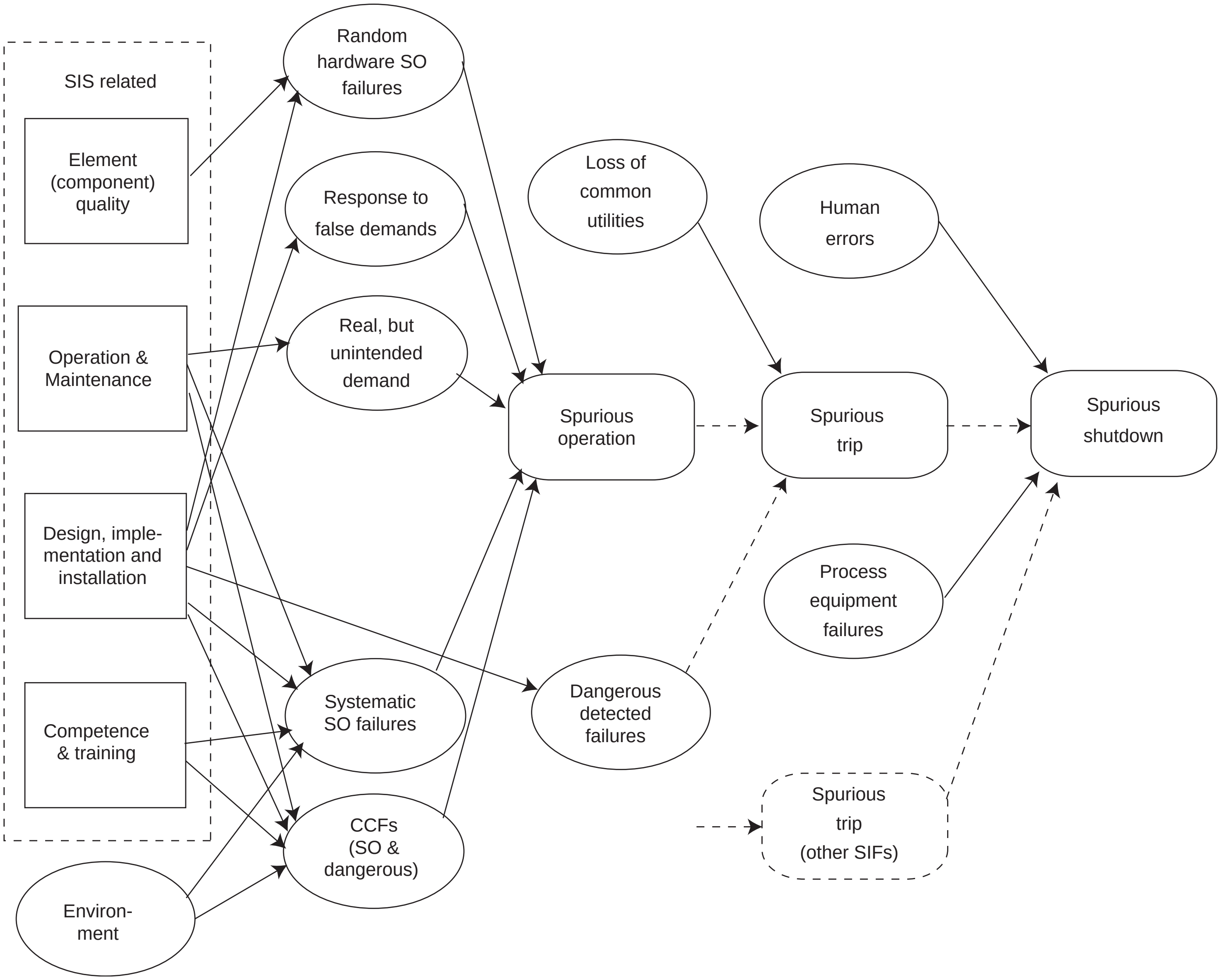

SIS related
Element (component) quality
Operation & Maintenance
Design, implementation and installation
Competence & training
Environment
Random hardware SO failures
Response to false demands
Real, but unintended demand
Systematic SO failures
CCFs (SO & dangerous)
Loss of common utilities
Dangerous detected failures
Human errors
Process equipment failures
Spurious operation
Spurious trip
Spurious shutdown
Spurious trip (other SIFs)

Fig. 1. Decisions and factors influencing spurious activation.

safe failure modes for each element to determine which ones are relevant for SO. An internal leakage in the v alve actuator of a fail-safe-close safety valve may, for example, lead to a SO, while a failure of a valve position indicator (limit switch) will not. In the following, we are using SO-failures to describe the safe failure modes that lead to a SO of the essential (safety) function of the element.

The IEC standards [1,2] distinguish between two categories of safe failures: safe *random hardware* failures and safe *systematic* failures. The safe random hardware failures are mainly due to normal degradation, while the safe systematic failures are due to causes like design error, procedure deficiency, or excessive environmental exposure that may only be removed by modifying the design, implementation, installation, operation or maintenance processes, tools or procedures. We therefore distinguish between random hardware SO-failures and systematic SO-failures in Fig. 1.

The element design and the material selection influence the rate of random hardware SO-failures. This is illustrated by an arrow from 'element quality' to 'random hardware SO-failures' in Fig. 1. A particular material may, for example, withstand high temperature and high pressure conditions better than another material, and a sensor principle used for a level transmitter may be more vulnerable to a specific operating condition than another.

As indicated in Fig. 1, operation and maintenance procedures, tools, and work processes, design, implementation and installation procedures, competence and training, and environmental exposure may influence the likelihood of systematic failures.

The IEC standards [1,2] consider systematic failures as unpredictable failures and therefore the rates of these failures do not need to be quantified. However, PDS [5] suggests a quantification method where the contribution from systematic failures is included.

Verification, validation, and testing may reduce the rate of the occurrence of systematic failures. Verification means to check and confirm (e.g., by testing or review) that the implemented design meets the specifications, while validation means to also assess the adequacy of selected design and implementation approaches and tools. In the operational phase, the rate of systematic failures may be reduced by verification and validation of, for example, function testing, visual inspection procedures, and work processes. Competence and training initiatives are important to reduce human errors during function tests. The environmental conditions influence the occurrence of systematic failures if the conditions are outside the design envelope. However, in most cases it is not possible to influence the environmental conditions. The contribution from the environment is therefore illustrated by a chance node in Fig. 1.

A common cause failure (CCF) occurs when two or more elements fail due to a shared cause. In the current context, we are not only interested in the dangerous CCFs that are included in the PFD calculations. As illustrated in Fig. 1, it is also necessary to consider CCFs that lead to SO of two or more elements. The spurious CCFs do not have the same root causes and coupling factors as the dangerous CCFs. Two safety valves may, for example, fail to close (FTC) on demand due to scaling, while scaling will never lead to SO of the same valves. A leakage in a common hydraulic supply system for two (fail-safe-close) safety valves may lead to SO and may not impede the safety valves from closing. IEC 61508 [1] recommends that dangerous CCFs are modeled by a beta-factor model, and part 6 of the standard includes a procedure that can be used to estimate a plant specific value of the parameter $\beta$ for *dangerous* CCFs. Since the dangerous CCFs are different in nature from the spurious CCFs, the procedure in part 6 of [1] is not suitable for estimating the parameter $\beta^{SO}$ for spurious CCFs. However, the same type of defences against coupling factors (e.g., reduce similarities in design, installation or procedures) apply to spurious, as well dangerous CCFs.

False demands are important contributors to SO of SIS elements. A false demand often shares some characteristics (e.g., visual appearance and composition) with a real process demand, and it may therefore be difficult for the input element to distinguish the two. A stray ray of sunlight may, for example, look like a small flame from certain angles, and a flame detector may therefore erroneously read it as a flame.

It may not be possible to reduce the occurrence of false demands, but we may influence how the input elements respond to them. It may, for example, not be possible to remove sunlight or alter the density of foam, but we may select elements that are designed to better distinguish between false and real process demands, or we may relocate the elements to make them less vulnerable to false demands.

Some false demands are man-made, which means that we are able to influence how often they occur by improving operation and maintenance procedures and work processes. If we, for example, want to avoid flame detectors from responding to welding, we must ensure that the necessary inhibits are set, alternatively that the flame detectors are covered so that they do no 'see' the welding flame. This is illustrated by an arrow from 'operation and maintenance' to the chance node 'real, but unintended demand' in Fig. 1.

### 3.2. *Causes of spurious trips*

One of the main contributors to spurious trips is evidently SO of SIS elements. SO may lead to a spurious trip if the number of activated elements corresponds to the number of elements needed to perform the safety function. The selected hardware configuration therefore determines whether or not a SO leads to a spurious trip. This 'conditional' influence is illustrated by dashed arrows in Fig. 1.

There are several other causes of spurious trips, for example:

- Loss of utilities, like pneumatic, hydraulic or power supply: Loss of utilities may directly lead to spurious trip if the SIF is designed fail-safe (which is the typical situation on oil and gas installations).
- DD failures: In some cases, the SIS may be designed to spuriously activate a SIF if the presence of DD failures are impeding the SIF from functioning on demand. The IEC standards [1,2] require this performance if the elements have not been restored within the specified mean time to restoration. A 2oo3 configuration is still able to act if a single dangerous detected failure is present. If two DD failures are present, the SIF is unable to respond to a real process demand, and the time the SIS is in such a condition should be minimized. This spurious trip may be activated automatically or manually. If the spurious trip causes a process shutdown, the shutdown will usually be more controlled/smooth than a spurious trip of the two previous types.

A SIF may also trip due to a human error during, for example, function testing. We have chosen to relate such events to the SO level (through the safe systematic failures and safe CCFs), since the human errors are affecting elements rather than the function.

### 3.3. *Causes of spurious shutdowns*

A spurious trip will usually, but not always, lead to a spurious shutdown of the process. If the SIF does not interact directly (or indirectly by activating other SIFs) with the process, the process may not be disturbed upon a spurious trip. A dashed arrow is therefore used to indicate that a spurious trip may (but not always) lead to a spurious shutdown. Fig. 1 also indicates (by dashed arrows and nodes) that different types of SIFs may lead to process shutdowns.

A spurious shutdown may also be caused by a spurious closure/stop of non-SIS equipment that interacts with the process, like control valves and pumps. A spurious closure of a control valve or a spurious stop of a pump may be due to element internal failures, human errors or automatic control system errors. In Fig. 1, we have illustrated non-SIS element failures and automatic control system failures by the chance node 'process equipment failures,' and human errors as the chance node 'human errors.'

## 4. Classification of failure modes

Fig. 2 illustrates how the various failure modes contribute to spurious trips. The failure modes are classified based on a combination of the schemes used by OREDA and the IEC standards [1,2].

OREDA [8] distinguishes between *critical*, *degraded*, and *incipient* failures. A critical failure is a failure that is sudden and causes a cessation of one or more fundamental functions, where cessation implies that the function is impeded, lost, unavailable or outside the specified limits. It should be noted that a critical failure in OREDA is not the same as a dangerous failure in the IEC standards [1,2]. Unlike the IEC 61508 and the IEC 61511, OREDA does not relate the failure categories to the consequences of failures.

OREDA defines a degraded failure as a failure that may compromise one or several functions without immediately affecting the main or fundamental functions. If a degraded failure is not corrected, it may develop into a critical failure. An incipient failure is an imperfection of the element state or condition that may, if not corrected, lead to a degraded failure and in some cases also to a critical failure. Often, it is difficult to distinguish degraded from incipient failures, and the two categories are consequently considered as one group. The IEC standards [1,2] do not define degraded/incipient failure categories, but in many cases safe failures, other than SO-failures, may be considered as degraded/incipient failures.

Failure modes may be studied on the element level as well as on the SIF level. In Fig. 2 we have focused on the element level. Different failure categories are relevant for different types of SIS elements, and in Fig. 2 we have used terms that apply to fail-safe-close safety valves. OREDA defines several failure modes as critical for safety valves, for example, FTC, delayed operation (DOP), and leakage in closed position (LCP). PC and SO are also considered critical failure modes by OREDA, since the main function of the valve is unavailable. A valve with longer closing time than expected, but where the closing time is still below the upper time constraint may be considered to have a degraded/incipient failure mode.

As discussed in Section 3, only the critical failure modes corresponding to DD and safe (S) failures are relevant when estimating the STR. The 'conditional' relationships between SO, DD failures, and spurious trips are indicated with a dashed arrow, in the same way as in Fig. 1. It should be noted that IEC 61508 and IEC 61511 distinguish between safe detected (SD) and safe undetected (SU) failures. An SO-failure may be considered as an SU-failure as well as an SD-failure. If a SO does not lead to a spurious trip, for example, a single SIS element raising an alarm in a 2oo3 configuration, we may define the SO-failure as SD since the failure is detected before the SIF is executed. However, if the SO-failure leads to a spurious trip, for example, when a valve spuriously closes in a 1oo2 configuration, we may classify the failure as SU since the failure is detected *after* the SIF has been executed.

## 5. New formulas for the STR

We define the STR as the mean number of spurious activations of the SIF per time unit. There are three main causes of spurious trips (of a SIS):

(1) SO, caused by:
- Internal failures of one or more of the SIS elements. The number of elements that have to fail to give a spurious trip depends on the SIS configuration.

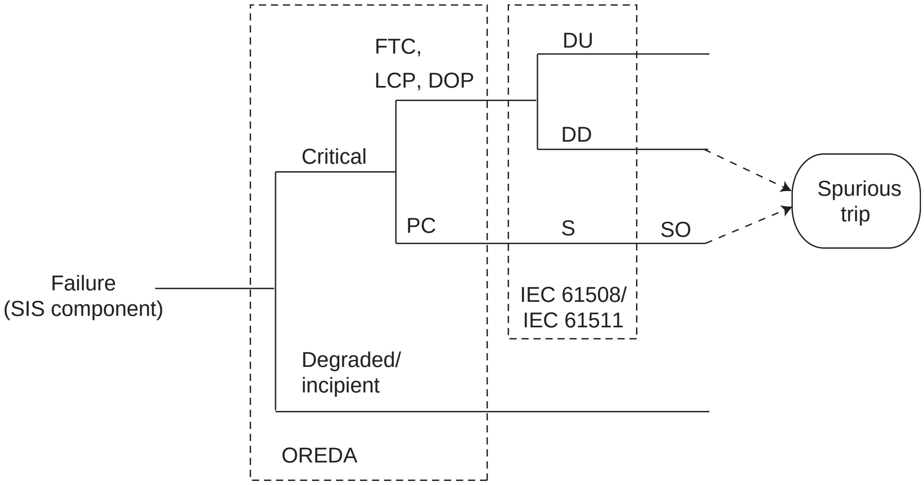


Fig. 2. Classification of failure modes.
]

- False demands. There are two main types of false demands: (a) Demands that are not real, but which share some properties or characteristics with the real demands, and (b) Demands that are real, but where the response should have been prohibited, for example, when welding has not been covered from the flame detectors.

  False demands of type (a) can only be prevented by a redesign of the system. False demands of type (b) are mainly caused by human errors or inadequate procedures, and can therefore be more easily prevented.

(2) DD failures. Whether or not one or more DD-failures will result in a spurious trip of the SIS, depends on the SIS configuration and the operating philosophy.

(3) Loss of utilities. The SIS is often designed so that the safe state of the process is obtained when the SIS is de-energized or upon loss of hydraulic or pneumatic power (so-called fail-safe design).

We discuss the causes of spurious trips separately. In this article, the term $k$oo$n$ is always used with respect to *function*. A $k$oo$n$ is functioning if at least $k$ of the $n$ elements are functioning. A $k$oo$n$ will therefore fail if at least $(n-k+1)$ of the $n$ elements fail.

### 5.1. Spurious operation

#### 5.1.1. Internal failures

Let $\lambda_{\mathrm{SO},j}$ denote the rate of SOs of a SIS element of type $j$. First, consider a 1oo$n$ configuration (i.e., a parallel structure) of $n$ *independent* elements of the same type $j$. Any SO-failure of an element in the 1oo$n$ configuration will give a spurious output from the system. If the 1oo$n$ configuration is in series with the rest of the SIS, for example, as input or final elements, any SO-failure will give a spurious trip. The STR due to internal failures of a 1oo$n$ configuration of elements of type $j$ is therefore

$$\mathrm{STR}_{1,j} = n\lambda_{\mathrm{SO},j}. \tag{1}$$

If the elements are exposed to CCFs that can be modeled by a beta-factor model such that the rate of CCFs is $\beta_j^{\mathrm{SO}}\lambda_{\mathrm{SO},j}$, the rate of spurious trips caused by the 1oo$n$ configuration is

$$\begin{aligned}\mathrm{STR}_{1,j} &= n(1-\beta_j^{\mathrm{SO}})\lambda_{\mathrm{SO},j} + \beta_j^{\mathrm{SO}}\lambda_{\mathrm{SO},j} \\ &= n\lambda_{\mathrm{SO},j} - (n-1)\beta_j^{\mathrm{SO}}\lambda_{\mathrm{SO},j}.\end{aligned} \tag{2}$$

When modeled by a beta-factor model, a 1oo$n$ structure of dependent elements has a lower STR than a structure of $n$ independent elements. This fact is easy to explain, but may be considered to be a 'strange' behavior of the beta-factor model.

Now, consider a $k$oo$n$ configuration of elements of type $j$, where $n \geqslant k \geqslant 2$. If we use the beta-factor model, the SO-failures of each element may be split into independent failures (i.e., with multiplicity 1) and CCFs (i.e., with multiplicity $n$). If a CCF occurs, with rate $\beta_j^{\mathrm{SO}}\lambda_{\mathrm{SO},j}$, a spurious trip will occur.

Independent SO-failures can also lead to a spurious trip. The first independent SO-failure will occur with rate $n(1-\beta_j^{\mathrm{SO}})\lambda_{\mathrm{SO},j}$. This failure is assumed to be revealed immediately (e.g., by a local alarm), and a repair action is initiated to bring the element back to a functioning state. The mean restoration time for an element of type $j$ is $\mathrm{MDT}_j$. To get a spurious trip, at least $(k-1)$ of the other $(n-1)$ elements must have an SO-failure before the restoration action of the first element is finished. This may be described as a binomial situation: (i) we have $(n-1)$ independent elements, (ii) each element will either survive the interval $\mathrm{MDT}_j$ without a SO-failure or not survive the interval, and (iii) the probability that an element will have a SO-failure in the restoration interval is $p = 1 - \mathrm{e}^{-(1-\beta_j^{\mathrm{SO}})\lambda_{\mathrm{SO},j}\mathrm{MDT}_j} \approx (1-\beta_j^{\mathrm{SO}})\lambda_{\mathrm{SO},j}\mathrm{MDT}_j$. The number $M$ of SO-failures that occur in the restoration interval will therefore have a binomial distribution $(n-1, p)$.

The STR of a $k$oo$n$ configuration of elements of type $j$ due to internal failures is

$$\begin{aligned}\mathrm{STR}_{1,j}^{k\mathrm{oo}n} &= n(1-\beta_j^{\mathrm{SO}})\lambda_{\mathrm{SO},j}\Pr(M \geqslant k-1) + \beta_j^{\mathrm{SO}}\lambda_{\mathrm{SO},j} \\ &\approx n(1-\beta_j^{\mathrm{SO}})\lambda_{\mathrm{SO},j}\left[\sum_{m=k-1}^{n-1}\binom{n-1}{m}p^m(1-p)^{n-1-m}\right] \\ &\quad + \beta_j^{\mathrm{SO}}\lambda_{\mathrm{SO},j},\end{aligned} \tag{3}$$

where $p = (1-\beta_j^{\mathrm{SO}})\lambda_{\mathrm{SO},j}\mathrm{MDT}_j$.

Formula (3) is correct for $k = 2$ but will slightly underestimate the STR for $k \geqslant 3$. To have a spurious trip, additional, independent SO-failures have to occur while the initial failure is repaired. These failures will also have restoration times that may extend beyond the initial restoration time, but these restoration times will generally be shorter than $\mathrm{MDT}_j$ since the repair personnel is already on site. The error caused by the approximation is considered to be negligible, because of the remote probability of having more than one additional, independent SO-failure in the short interval of length $\mathrm{MDT}_j$.

The beta factor $\beta_j^{\mathrm{SO}}$ and the restoration time $\mathrm{MDT}_j$ may obviously be different for different types of elements. The index $j$ is used to fit Eqs. (2) and (3) to the relevant types of elements. When several types of elements are used in the same configuration, we need to use a more comprehensive approach, e.g., as described in [13].

#### 5.1.2. False demands

Let $\lambda_{\mathrm{F}}$ be the rate of false demands of type (a), and let $\lambda_{\mathrm{SF}}$ be the rate of false demands of type (b). The IEC standards [1,2] define failures caused by false demands of type (b) and we have therefore chosen to use the subscript SF for this rate. When a false demand occurs, the SIS will treat this demand as a real demand and carry out its safety function. It may be situations where the false demand is only detected by at most $(k-1)$ elements in a $k$oo$n$ configuration of input elements and therefore will not initiate the SIF. To be on the conservative side, the STR of a SIS caused by false demands is estimated by

$$\mathrm{STR}_{2,j} = (\lambda_{\mathrm{F}} + \lambda_{\mathrm{SF}})(1 - \mathrm{PFD}). \tag{4}$$

The PFD of the SIF is usually so small that $(1 - \mathrm{PFD})$ can be omitted from Eq. (5).

Historical databases like OREDA do not provide estimates for $\lambda_{\mathrm{F}}$ and $\lambda_{\mathrm{SF}}$, but other sources may provide insight into how frequent such events occur. Some oil companies record non-intended incidents that have led to hazardous situations or production losses. By reviewing these records, it may be possible to estimate $\lambda_{\mathrm{SF}}$ for the SIF. Information management systems (IMS) are sometimes installed to record the number of process shutdowns and system trips. By reviewing the events recorded in the IMS, it may be possible to estimate $\lambda_{\mathrm{F}}$.

### 5.2. *DD failures*

Let $\lambda_{\mathrm{DD},j}$ denote the rate of DD-failures for elements of type $j$. When a DD-failure is revealed, a repair action is initiated to restore the function. The mean restoration time is denoted $\mathrm{MDT}_j^*$. This restoration time may, or may not, be equal to the restoration time $\mathrm{MDT}_j$ for SO-failures. A reason for a difference may be different priorities of the two types of failure.

DD-failures may be independent failures or CCFs. We will, also in this case, use a beta-factor model for the CCFs with parameter $\beta_j^{\mathrm{DD}}$. If a CCF of DD-failures occur, with rate $\beta_j^{\mathrm{DD}}\lambda_{\mathrm{DD},j}$, the system is not able to perform its safety function, and the system will be stopped. Several references [4,6] treat this stop as a spurious trip.

Consider a $k$oo$n$ configuration of elements of type $j$. In the following we assume an operating strategy where the SIF is spuriously tripped as soon as at least $(n-k+1)$ dangerous failures are detected. DD CCFs (with multiplicity $n$) will always lead to spurious trips. We will now consider the independent DD-failures (i.e., with multiplicity 1). The first independent DD-failure will occur with rate $n(1-\beta_j^{\mathrm{DD}})\lambda_{\mathrm{DD},j}$. The failure is assumed to be revealed almost immediately and a repair action is initiated. To have a spurious trip, at least $(n-k)$ of the remaining $(n-1)$ elements must get a DD-failure before the restoration of the first DD-failure is finished. In the same way as for SO-failures, this can be treated as a binomial situation where the number $M^*$ of DD-failures in the interval of length $\mathrm{MDT}_j^*$ is binomially distributed $(n-1, p^*)$, where $p^* = 1 - \mathrm{e}^{-(1-\beta_j^{\mathrm{DD}})\lambda_{\mathrm{DD},j}\mathrm{MDT}_j^*} \approx (1-\beta_j^{\mathrm{DD}})\lambda_{\mathrm{DD},j}\mathrm{MDT}_j^*$.

The STR of a $k$oo$n$ configuration of elements of type $j$ due to DD-failures is

$$\begin{aligned}\mathrm{STR}_{3,j}^{koon} &= n(1-\beta_j^{\mathrm{DD}})\lambda_{\mathrm{DD},j}\Pr(M^* \geqslant n-k) + \beta_j^{\mathrm{DD}}\lambda_{\mathrm{DD},j}\\ &\approx n(1-\beta_j^{\mathrm{DD}})\lambda_{\mathrm{DD},j}\left[\sum_{m=n-k}^{n-1}\binom{n-1}{m}(p^*)^m\right.\\ &\qquad\left.\times(1-p^*)^{n-1-m}\right] + \beta_j^{\mathrm{DD}}\lambda_{\mathrm{DD},j},\end{aligned} \tag{5}$$

where $p = (1-\beta_j^{\mathrm{DD}})\lambda_{\mathrm{DD},j}\mathrm{MDT}_j^*$.

Formulas (3) and (5) do not take into account degraded operation, for example, that the SIS upon a single SO-failure or a single DD-failure in a 2oo3 configuration may be reconfigured to a 1oo2 configuration. Degraded operation is used to allow for delayed repair without compromising the reliability of the SIS. The PDS method suggests formulas for degraded operation when calculating PFD. A similar approach may be selected for modeling spurious trips in degraded mode. Markov methods may also be used to derive formulas for degraded operation.

### 5.3. *Loss of utilities*

A utility loss (UL) may directly lead to a spurious trip when we assume a fail-safe design of the SIS. The STR due to ULs associated with elements of type $j$ is therefore

$$\mathrm{STR}_{4,j} = \lambda_{\mathrm{UL},j}. \tag{6}$$

The rate of ULs is not found in historical databases like OREDA. The occurrence of ULs strongly depends on the actual plant, for example, the number of redundant power supplies, the power supply capacities, and the pneumatic/hydraulic supply capacities. By investigating the failure reports from a specific plant, one may identify failure records associated with utility failures and use these as basis for estimating the frequency of ULs.

### 5.4. *Simplified formulas*

The total STR, $\mathrm{STR}_T$, is now found by adding the contributions from the above categories and for all groups of elements.

In Table 1, the new formulas are summarized for some selected configurations together with the formulas provided by [4,5]. The following assumptions and simplifications are made:

- The contributions from false demands, non-intended demands, and systematic failures will in most cases be negligible and are therefore omitted from the formulas in Table 1.
- The contribution from independent failures occurring during the MDT (alternatively MDT*) has been omitted since their contribution in most cases will be negligible compared to the contribution from CCFs.
- ISA [4] and PDS [5] use the 'conventional' (dangerous) $\beta$-factor, which we have denoted $\beta^{\mathrm{D}}$.
- ISA [4] includes all safe failures in their formulas. To compare the formulas, we assume that $\lambda_{\mathrm{S}}$ is equal to $\lambda_{\mathrm{SO}}$.

For 1oo$n$ configurations, the contribution from independent failures is included. For $k$oo$n$ ($k \geqslant 2$) configurations, the contribution from independent failures is negligible compared to the contribution from the CCFs. In the simplified formulas, the first part of formulas (3) and (5) may therefore be omitted. Having assumed that a CCF will affect all channels simultaneously, the new approach

Table 1
STR formulas (approximations)

| Configuration | Approach | | |
|---|---|---|---|
| | New | PDS [5] | ISA [4] |
| 1oo1 | $\lambda_{SO}+\lambda_{DD}$ | $\lambda_{SO}$ | $\lambda_{S}+\lambda_{DD}$ |
| 1oo2 | $(2-\beta^{SO})\lambda_{SO}+\beta^{DD}\lambda_{DD}$ | $2\lambda_{SO}$ | $2(\lambda_{S}+\lambda_{DD})+\beta^{D}(\lambda_{S}+\lambda_{DD})$ |
| 1oo3 | $(3-2\beta^{SO})\lambda_{SO}+\beta^{DD}\lambda_{DD}$ | $3\lambda_{SO}$ | $3(\lambda_{S}+\lambda_{DD})+\beta^{D}(\lambda_{S}+\lambda_{DD})$ |
| 2oo3 | $\beta^{SO}\lambda_{SO}+\beta^{DD}\lambda_{DD}$ | $2.4\beta^{D}\lambda_{SO}$ | $\beta^{D}(\lambda_{S}+\lambda_{DD})$ |
| 2oo4 | $\beta^{SO}\lambda_{SO}+\beta^{DD}\lambda_{DD}$ | $4\beta^{D}\lambda_{SO}$ | $\beta^{D}(\lambda_{S}+\lambda_{DD})$ |

suggests the same formulas for *koon* ($k \geqslant 2$) configurations, as for the 2oo3 and 2oo4 in Table 1. ISA has made the same assumption, while the PDS uses configuration factors to cater for CCFs in configurations other than 1oo2.

PDS [5] does not use the standard beta-factor model for CCF modeling, but a specially designed model called the multiple beta-factor model (MBF). The contribution of CCFs in a *koon* configuration is estimated as $C_{koon}\beta$, where $\beta$ is the fraction of CCFs among two components and $C_{koon}$ is a correction factor for *koon* configurations. The $\beta$ used in the PDS method is therefore different from the $\beta$ used in the beta-factor model. For 2oo3 and 2oo4 the correction factors are 2.4 and 4.0, respectively, as seen in Table 1.

As long as $\lambda_{SO}$ and $\lambda_{DD}$, as well as $\beta^{SO}$ and $\beta^{DD}$, are in the same order of magnitude, the formulas provide nearly the same results. However, when their order of magnitude starts to deviate, the formulas provide different results. This is demonstrated in a brief case study below.

### 5.5. Case study

In the following, the STR is calculated using the formulas in Table 1, when we assume that $\lambda_{DD} = 1 \times 10^{-6}$ (hours)$^{-1}$ and that $\beta_{DD} = 2\%$. Calculations are performed for the following cases:

(1) $\beta^{SO} \approx \beta^{DD}$ and $\lambda_{SO} \approx \lambda_{DD}$,
(2) $\beta^{SO}$ is 5 times larger than $\beta^{DD}$ (and $\lambda_{SO} \approx \lambda_{DD}$),
(3) $\lambda_{SO}$ is 2 times larger than $\lambda_{DD}$ (and $\beta^{SO}$ is still 5 times larger than $\beta^{DD}$).

The resulting STRs for case 1 are shown in Table 2. For a 1oo1 configuration, the ISA formula provides the same result as the new formulas (since they consider both DD failures and SO failures). This is also the situation for 2oo3 and 2oo4 configurations. The PDS method provides a lower STR since PSD only considers the SO failures.

In cases 2 and 3, the STRs calculated by the new formulas deviate from the rates calculated by the ISA and the PDS method. The magnitude of deviations is influenced by the fraction of $\beta^{SO}$ to the $\beta^{DD}$ and the fraction of $\lambda_{SO}$ to the $\lambda_{DD}$. This is illustrated in Tables 3 and 4.

Table 2
Spurious trip rates for case 1

| Configuration | New | PDS [5] | ISA [4] |
|---|---|---|---|
| 1oo1 | 2.00E − 6 | 1.00E − 6 | 2.00E − 6 |
| 1oo2 | 2.00E − 6 | 2.00E − 6 | 4.04E − 6 |
| 1oo3 | 2.98E − 6 | 3.00E − 6 | 6.04E − 6 |
| 2oo3 | 4.00E − 8 | 4.80E − 8 | 4.00E − 8 |
| 2oo4 | 4.00E − 8 | 8.00E − 8 | 4.00E − 8 |

Table 3
Spurious trip rates for case 2

| Configuration | New | PDS [5] | ISA [4] |
|---|---|---|---|
| 1oo1 | 2.00E − 6 | 1.00E − 6 | 2.00E − 6 |
| 1oo2 | 1.92E − 6 | 2.00E − 6 | 4.04E − 6 |
| 1oo3 | 2.82E − 6 | 3.00E − 6 | 6.04E − 6 |
| 2oo3 | 1.20E − 7 | 4.80E − 8 | 4.00E − 8 |
| 2oo4 | 1.20E − 7 | 8.00E − 8 | 4.00E − 8 |

Table 4
Spurious trip rates for case 3

| Configuration | New | PDS [5] | ISA [4] |
|---|---|---|---|
| 1oo1 | 3.00E − 6 | 2.00E − 6 | 3.00E − 6 |
| 1oo2 | 3.82E − 6 | 4.00E − 6 | 6.06E − 6 |
| 1oo3 | 5.62E − 6 | 6.00E − 6 | 9.06E − 6 |
| 2oo3 | 2.20E − 7 | 9.60E − 8 | 6.00E − 8 |
| 2oo4 | 2.20E − 7 | 1.60E − 7 | 6.00E − 8 |

For some configurations, like the 2oo3 configuration in case 1 and the 2oo4 configuration in case 3, the STRs calculated by the PDS method are close to the rates calculated by the new formulas. This is more due to coincidence than logic reasoning, since the formulas include different types of parameters that are not related to each other. Common for all methods is that the STR is low for configurations where $k \geqslant 2$.

## 6. Discussion and conclusions

The oil and gas industry seeks to reduce the number of spurious activations. As a means to understand the causes of spurious activation and their related effects, new definitions have been proposed. The new definitions distinguish between SO (on component level), spurious trip (on SIF level), and spurious shutdown (considering the production availability aspect).

New formulas have been established based on the new definitions of spurious trips. The main advantages of the new formulas are that (i) they are generic and may be used to any *k*oo*n* configuration, (ii) they capture the most important causes of spurious trips identified in Fig. 1, (iii) they cater for the different ways dangerous and SO-failures contribute to the STR, and (iv) they distinguish between $\beta^{\mathrm{SO}}$ and $\beta^{\mathrm{D}}$.

The new formulas have been compared with other formulas that are frequently used in the oil and gas industry [4,5]. Even though the formulas may, at first glance, seem quite different, they do not produce very different results. When the results deviate, this may be explained as follows:

- PDS [5] only considers the SO-failures, and not the DD-failures.
- ISA [4] applies the same philosophy for DD-failures as for SO-failures, which means that they assume a spurious trip in case the number of DD-failures is the same as the number of failures required to spuriously activate the SIF. Our formulas are based on a different philosophy for these two categories of failures, and we believe that this is a more realistic approach.
- The PDS method applies a configuration factor to 'calibrate' the contribution of CCFs (SO and dangerous) to the selected configuration. The standard beta-factor model suggested in IEC 61508 [1] and used as basis for the formulas in [4] and in our approach, assumes that if a CCF occurs, all the voted elements fail. However, when the STR is compared for a 2oo3 and a 2oo4 configuration (where one would expect a difference between the approaches by PDS and ISA), the results are rather similar. It should, however, be noted that PDS [5] uses a slightly different definition of $\beta$.
- ISA [4] and PDS [5] do not distinguish between $\beta^{\mathrm{SO}}$ and the $\beta^{\mathrm{DD}}$. We believe that they should be considered as two separate parameters, due to their different nature.

It should further be noted that the MDT (of SO-failures as well as DD-failures) in most cases has a negligible influence on the STR. The reason is that the MDT comes into account in the case of multiple, independent failures that have a very low probability of occurrence.

There are other approaches for calculating the STR, for example, as proposed by Lu and Jiang [14], Andrews and Bartlett [15] and Cho and Jiang [16]. Lu and Jiang [14] suggest an approach that is similar to our approach since they treat the number of SOs as a binomial random variable. However, their focus is to assess spurious activation under different maintenance strategies, and they do not include other failures than independent SO failures. Andrews and Bartlett [15] use a branching search algorithm to model the contribution from spurious activation which may be used to *k*oo*n* configurations. Their algorithm focuses on the optimal selection of *k* and *n* (in a *k*oo*n* configuration) that leads to minimum costs and a system performing within preset constraints (like the maximum rate of spurious trips). Cho and Jiang [16] suggest using a Markov model to estimate the STR. For small systems, a Markov model may be a good alternative to our approach. However, for larger systems, the state transition diagrams get complex and difficult to handle. Cho and Jiang [16] do not consider the contribution from CCFs.

One may argue against introducing a new parameter $\beta^{\mathrm{SO}}$ in addition to the $\beta^{\mathrm{D}}$, particularly since it is already difficult to collect data and estimate $\beta^{\mathrm{D}}$. However, the distinction may still be important when it comes to understanding the underlaying causes. Defending against CCFs that may lead to dangerous failures of the SIF may be performed by other means than defending against failures that may lead to spurious activation. For example, implementing means to reduce the occurrence of loss of utilities (e.g., air supply or power supply) may lead to a reduced number of spurious trips, while it does not affect (at least directly) the occurrence of dangerous failures.

An important area for future research may be to get more insight into the causes of SOs and spurious trips, and how safety and availability may be balanced. In many industry sectors, the fail-safe state is not well defined and a spurious trip or a spurious shutdown may lead to hazardous situations. With more subsea processing and longer transportation distances of three phase fluids, the oil and gas industry is challenged with higher availability on their process control and safety systems.

## References

[1] IEC 61508. Functional safety of electrical/electronic/programmable electronic safety-related systems. Geneva: International Electrotechnical Commission; 1998.

[2] IEC 61511. Functional safety—safety instrumented systems for the process industry. Geneva: International Electrotechnical Commission; 2003.

[3] Summers AE. Viewpoint on ISA TR84.0.02—simplified methods and fault tree analysis. ISA Trans 2000;39(2):125–131.

[4] ISATR 84.00.02. ISA-TR84.00.02-2002-Part 4: safety instrumented functions (SIF)—safety integrity level (SIL) evaluation techniques part 4: determining the SIL of a SIF via Markov analysis. Technical Report, Research Triangle Park, NC: The Instrumentation, Systems, and Automation Society; 2002.

[5] SINTEF. Reliability prediction methods for safety instrumented systems, PDS method handbook, 2006 ed. SINTEF; 2006.

[6] Smith DJ, Simpson KGL. Functional safety—a straightforward guide to applying the IEC 61508 and related standards. Burlington, UK: Elsevier; 2005.

[7] ANSI/ISA. ANSI/ISA-84.01-1996: application of safety instrumented systems for the process industries. Technical Report,

Research Triangle Park, NC: American National Standard Institute; 1996.

[8] OREDA. OREDA Reliability Data. OREDA Participants, 4th ed., Available from: Det Norske Veritas, NO 1322 Høvik, Norway; 2002.

[9] IEC 61513. Nuclear power plants—instrumentation and control for systems important to safety—general requirements for systems. Geneva: International Electrotechnical Commission; 2001.

[10] IEC TR 61838. Nuclear power plants—instrumentation and control functions important for safety—use of probabilistic safety assessment for the classification. Geneva: International Electrotechnical Commission; 2001.

[11] ISO 14224. Petroleum, petrochemical and natural gas industries—collection and exchange of reliability and maintenance data for equipment. Geneva: International Standards Organization; 2006.

[12] Sandtorv AH, Hokstad P, Thompson DW. Practical experience with a data collection project: the OREDA project. Reliab Eng Syst Safety 1996;51(2):159–67.

[13] Rausand M, Høyland A. System reliability theory; models, statistical methods, and applications. 2nd ed. New York: Wiley; 2004.

[14] Lu L, Jiang J. Analysis of on-line maintenance strategies for k-out-of-n standby safety systems. Reliab Eng Syst Safety 2007;92: 144–55.

[15] Andrews JD, Bartlett LM. A branching search approach to safety system design optimisation. Reliab Eng Syst Safety 2005;87: 23–30.

[16] Cho S, Jiang J. Analysis of surveillance test interval by Markov process for SDS1 in CANDU nuclear power plants. Reliab Eng Syst Safety 2006, in press, doi: 10.1016/j.ress.2006.10.007.

# Article 4

Partial stroke testing of process shutdown valves: How to determine the test coverage
*Journal of Loss Prevention in the Process Industries*, Volume 21, p. 579–588, 2008

Contents lists available at ScienceDirect

Journal of Loss Prevention in the Process Industries

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

# Partial stroke testing of process shutdown valves: How to determine the test coverage

Mary Ann Lundteigen *, Marvin Rausand

*Department of Production and Quality Engineering, Norwegian University of Science and Technology, S.P. Andersens v. 5, NO 7491 Trondheim, Norway*

ARTICLE INFO

*Article history:*
Received 14 February 2008
Received in revised form
23 April 2008
Accepted 23 April 2008

*Keywords:*
Partial stroke testing
Safety instrumented system
PST coverage
Functional testing
High integrity pressure protection system

ABSTRACT

Partial stroke testing (PST) has recently been introduced as a semi-automatic means to test process shutdown valves. Normally, this type of testing does not disturb the process and can detect many of the failures that traditionally have been revealed only by functional testing. The fraction of all dangerous failures that are detected by PST is called the PST coverage and is decisive for the effectiveness of the PST. So far, limited guidance on how to determine the PST coverage has been given. This paper discusses the application and limitations of PST and suggests a new procedure for how to determine the PST coverage factor.

## 1. Introduction

Process shutdown valves are normally operated in a so-called *low demand mode of operation* (IEC 61508, 1998). This means that the valves are kept idle in open position for long periods and are designed to close and keep tight in case a process demand should occur. The valves usually have hydraulic or pneumatic *fail-safe close* actuators. Failures may occur while in open position and may cause the valve to "fail to close" or to "leak in closed position" in a demand situation. Such failures may remain for a long period and are called dangerous undetected (DU) failures (IEC 61508, 1998). *Functional testing* is required to reveal potential DU failures and involves full stroke operation and leakage testing. The process needs to be shut down during the functional test—if no bypass of the valve is available. In recent years, *partial stroke testing* (PST) has been introduced as a supplement to functional testing (Ali & Goble, 2004; ISA-TR 84.00.03, 2002; Summers & Zachary, 2000). PST means to partially close a valve, and then return it to the initial position. The valve movement is so small that the impact on the process flow or pressure is negligible, but the valve movement may still be sufficient to reveal several types of dangerous failures. PST may be suitable for processes where a small value movement does not cause disturbances that may lead to process shutdowns. For such processes, it may be economically viable to run PST more frequently than functional testing.

Process shutdown valves are often used as final elements in safety instrumented systems (SIS). These systems are important protection layers in process plants, and comprise input elements (e.g., pressure transmitters (PT), gas detectors), logic solvers (e.g., relay based logic, programmable logic controllers), and final elements (e.g., valves, circuit breakers). A SIS may perform one or more safety instrumented functions (SIF). The international standards IEC 61508 and IEC 61511 give safety life cycle requirements to the SIS, and use safety integrity level (SIL) as a measure of SIS reliability. To comply to a SIL, it is necessary to (i) implement various measures to avoid, reveal, and control failures that may be introduced during the SIS safety life cycle, ranging from the initial specification, to design, implementation, operation, maintenance, modifications, and finally decommissioning, (ii) select hardware architecture according to the specified architectural constraints, and (iii) demonstrate by calculations that the SIS reliability meets the specified reliability targets. The IEC standards use the probability of failure on demand (PFD) as a measure of SIS reliability.

The increased reliability that is gained by introducing PST may be used to improve safety and/or to reduce cost (Lundteigen & Rausand, 2007). Safety is improved if PST is added without changing the interval between the periodic functional tests. Cost is reduced if the reliability gained is used to extend the functional test interval. The reliability gained is influenced by the PST *coverage*, that is, the fraction of DU failures that are detected by the PST. While several authors have discussed how to take credit for PST in reliability calculations (Ali, 2004; Ali & Goble, 2004; Knegtering, 2004; McCrea-Steele, 2005; Summers & Zachary,

* Corresponding author. Tel.: +47 73 59 7101; fax: +47 73 59 7117.
*E-mail address:* mary.a.lundteigen@ntnu.no (M.A. Lundteigen).

0950-4230/$ - see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jlp.2008.04.007

2000), minor guidance has been given on how to determine the PST coverage factor. Lundteigen and Rausand (2007) show that past data indicate quite different PST coverage, and ISA-TR 84.00.03 and Goble and Cheddie (2005) suggest using FMEA to determine the PST coverage.

The objective of this paper is to develop a procedure for how to determine the PST coverage, taking into account plant specific conditions, valve design, and historical data on valve performance.

The paper is organized as follows: Section 2 discusses some typical implementation approaches for PST. A case study is introduced to illustrate how PST may be implemented for a SIS application. Section 3 discusses the main attributes of PST and relates PST to other testing strategies. In Section 4, formulas for determining the reliability effects of PST are presented. Section 5 discusses the positive and negative effects of introducing PST, which at the present time are not catered for in the basic formulas. In Section 6, a new procedure for how to determine the PST coverage is presented and discussed. We conclude in Section 7 with a brief discussion of the new approach and give some recommendations for further work.

## 2. PST implementation approaches

PST is introduced to detect, without disturbing the process, failures that otherwise require functional tests. To what extent the PST can detect failures, depends on how the PST is implemented. PST can be implemented in various ways (Ali & Goble, 2004; Ali & Jero, 2003; ISA-TR 84.00.03, 2002; Summers & Zachary, 2000, 2002). Two variants are illustrated in Fig. 1: (i) a PST that is integrated with the SIS, and (ii) a separate vendor PST package.

In Fig. 1(i), the hardware and software necessary to perform the PST are implemented into the SIS logic solver. When PST is initiated based on a manual request, the logic solver deactivates its outputs for a certain period of time (typically a few seconds). The deactivated outputs cause the solenoid operated valve to start depressurizing the shutdown valve, and the shutdown valve starts to move towards the fail safe (closed) position. Just as the valve has started to move, the logic solver outputs are re-energized, and the safety valve returns to normal (open) position. The test results may be monitored manually from the operator stations, by verifying that the valve travels to the requested position and returns to the normal state when the test is completed. In some cases, an automatically generated alarm may be activated, if the valve fails to move, or to return to its initial position.

The vendor PST packages perform the same type of test sequence, but the hardware and software are implemented into separate systems. Some vendors interface the existing solenoid operated valve, while others install a separate solenoid for testing purposes (see Fig. 1(ii)). The vendor supplied PST package may automatically generate the PST at regular intervals. In many cases, the control room operators want to be in control with the actual timing of the PST, and manual activation may therefore be preferred.

The SIS implemented PST is able to test a larger part of the SIF than the vendor packages, since the test includes all components from the logic solver output cards to the shutdown valve. On the other hand, the vendor PST packages often include additional sensors or positioning devices that may collect more information on the valve condition (Ali & Goble, 2004; ISA-TR 84.00.03, 2002; Summers & Zachary, 2004), and may, as such, obtain higher PST coverage for the valve.

### 2.1. Case study

We illustrate a PST implementation by a high integrity pressure protection system (HIPPS) that is installed on a subsea

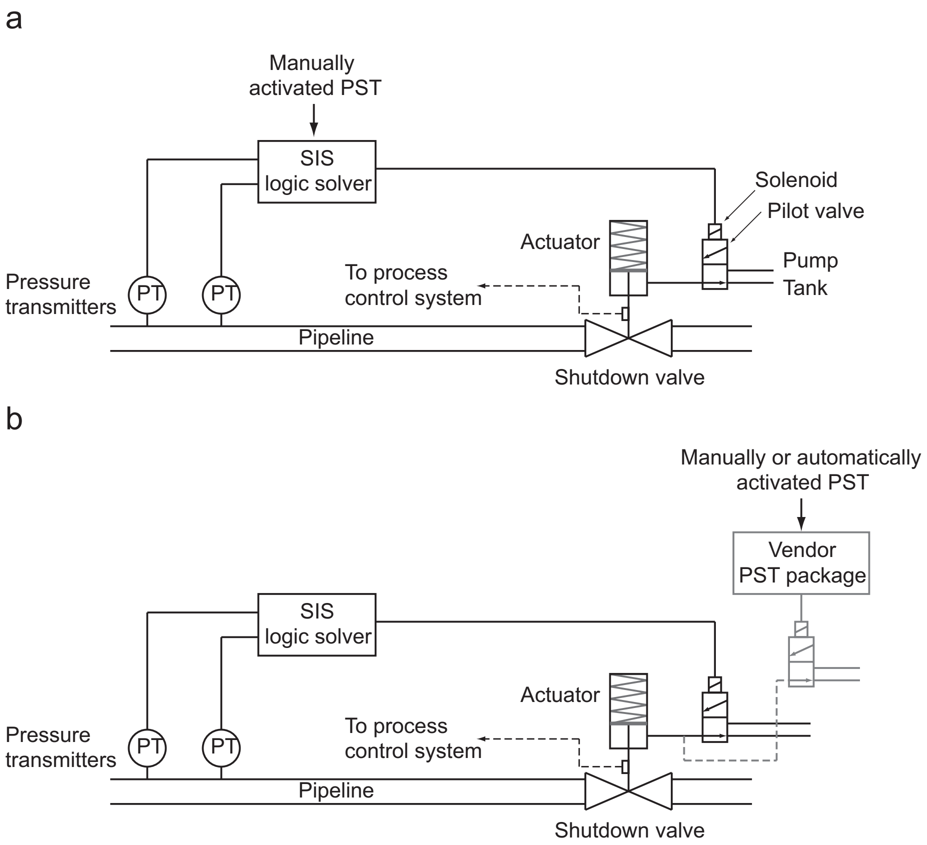


**Fig. 1.** Two different PST concepts: (i) integrated with the SIS and (ii) through an additional vendor PST package.

oil/gas pipeline to avoid loss of containment (Summers & Zachary, 2004). The HIPPS is installed to detect if the pipeline pressure exceeds a specified set pressure, and close dedicated valves to avoid further pressure build-up that may cause pipeline rupture (Aarø, Lund, & Onshus, 1995; Lund, Onshus, & Aarø, 1995; Onshus, Aarø, & Lund, 1995; Summers, 2003; Summers & Zachary, 2004). The potential pressure build-up may arise from well shut-in pressure (i.e., the maximum wellhead pressure), or from a sudden pipeline blockage, for example a spurious closure of a downstream valve. A HIPPS typically comprises PTs, logic solver(s), solenoid operated hydraulic control valve(s), and shutdown valves.

In the case study, we consider the subsea HIPPS that is installed in the Kristin subsea oil/gas field in the North Sea (Bak, Sirevaag, & Stokke, 2006). The HIPPS and its PST implementation is used to demonstrate how to determine the PST coverage.

In the Kristin field, there are six HIPPSs that are installed to protect subsea pipelines that are rated 330 bar against the well shut-in pressure of 740 bar. Each HIPPS comprises four PTs, one solid state logic solver, two solenoid operated hydraulic control valves (HCV), and two shutdown gate valves with hydraulic fail-safe actuators.

The pipelines are used to transport a mixture of water, condensate, and hydrocarbon gases. The gate valves are designed for the well shut-in pressure and for temperatures in the range from −33 to 175 °C (Bak et al., 2006). Each HIPPS arrangement is installed on a dedicated HIPPS manifold as illustrated in Fig. 2, where the gate valves are marked with a circle.

The four PTs have set-point at 280 bar and are voted 2oo4, meaning that two transmitters must detect a high pressure to initiate valve closure (Rausand & Høyland, 2004). The two gate valves are installed in series and voted 1oo2, meaning that closure of one of the valves is sufficient to stop further pressure build-up. Each of the two gate valves are operated by a HCV. When high pressure is detected, the logic solver deactivates the signal to the HCVs, causing the HCVs to depressurize the gate valve actuators. Upon loss of hydraulic pressure in the gate valve actuators, the gate valves close.

The functional safety requirements for the HIPPS are to (1) close at least one of the two gate valves within 12 seconds, and (2) not leak above a specified limit (Bak et al., 2006). The SIS implemented PST is selected to perform PST every second month, while functional testing is performed once a year. This means that hardware and software are added to the logic solver to handle a PST. Upon a request by the control room operators, the logic solver starts a timer and keeps the outputs deactivated until the timer is reset. The timer is set to 2 s. The PST is considered a success if the operators observe that signals from the valve position indicator show that the valve starts to move and then returns to the open position.

## 3. Test aspects

IEC 61508 and IEC 61511 distinguish between two main types of SIS related tests in the operating phase; (1) diagnostic tests that automatically identify and report certain types of failures and failure causes, and (2) functional tests that are performed to reveal all dangerous SIS failures, so that the SIS may be restored to its design functionality after the test (CCPS, 2007; IEC 61511, 2003). The hardware and software necessary to implement the diagnostic test are sometimes referred to as diagnostics (CCPS, 2007). The diagnostics may be an integral part of a SIS component, or added as separate software and hardware.

We distinguish between diagnostic testing and functional testing based on their differences with respect to (ANSI/ISA 84.01, 1996; IEC 61511, 2003; ISA-TR 84.00.03, 2002):

- Being automatic:
  - A diagnostic test is usually fully automatic.
  - A functional test often requires human interaction during preparation (e.g., setting inhibits and overrides), execution (e.g., to initiate the test), and restoration (e.g., to suspend the inhibits and overrides).
- Effect on production:
  - A diagnostic test does not require process shutdown.
  - A functional test normally requires process shutdown since operation of most final elements interfere with the process.
- The time to detection of a dangerous failure:
  - A diagnostic test is run frequently, typically in the range of every millisecond and up to every few hours, and may therefore detect dangerous failures shortly after they occur. Dangerous failures that are detected by diagnostics are called dangerous detected (DD) failures.
  - A functional test is performed less frequently, typically ranging from every few months to every few years, and a dangerous failure may therefore be present (and hidden) for a longer period of time.
- Degree of detection:
  - A diagnostic test intends to detect failures without causing process disturbances, and the degree of detection expresses to what extent failures are revealed by this approach.

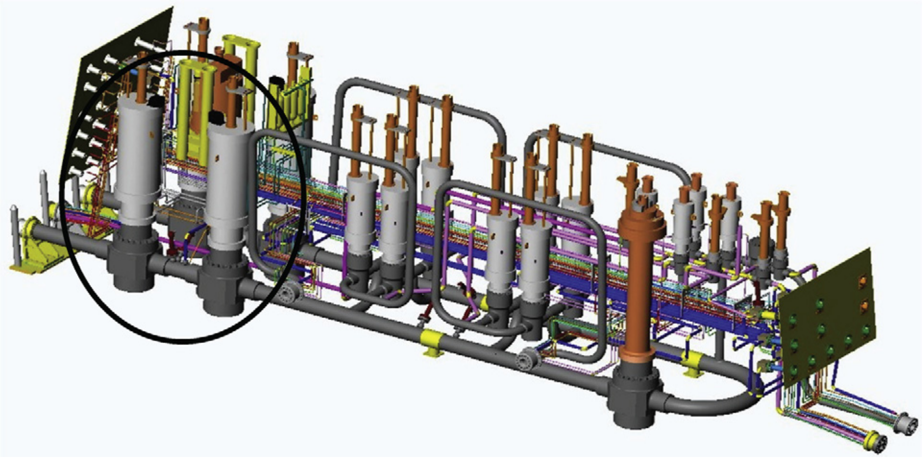


**Fig. 2.** Illustration of a HIPPS manifold at the Kristin subsea oil/gas field (Bak et al., 2006).

    Programmable logic solvers may run a high number of integrity, sequence, and run-time checks without affecting production, and may, as a result, reveal more failures than what would be found during a functional test. For other components, like valves and circuit breakers, it may be impossible to achieve a high degree of detection without fully operating the components.
  - A functional test is often intended to reveal *all* failures. However, the degree of detection is influenced by operational factors. One factor is to what extent the test conditions reflect the real demand conditions. Another aspect is to what extent operation and maintenance personnel are capable of revealing failures and avoid introducing new failures. Here, the quality of procedures, tools, and training is of importance.
- State of the SIS after the test:
  - A diagnostic test reports failures automatically, and, in some cases, forces an automated transition of the SIS to the safe state. However, the repair may not necessarily restore the component to an as good as new condition. A re-alignment of a line gas detector that has been reported out of focus is, for example, not always supplemented by a calibration check.
  - Functional tests are often aimed at restoring the SIS to an as good as new (or design) condition. However, again the state of the SIS relies on how well operational and maintenance personnel are able to reveal, correct, and avoid introducing failures.

ANSI/ISA 84.01 and ISA-TR 84.00.03 relate functional testing to safety instrumented functions (SIF) rather than to individual SIS components, but they recognize that functional testing for practical reasons is often split into subtests. As a result, we may distinguish between functional testing on three levels; (1) of the SIF, which ISA-TR 84.00.03 refers to as a complete functional test, (2) of a subsystem, for example, the configuration of input elements or output elements, and (3) of a single SIS component, for example a process shutdown valve. As opposed to the complete functional tests, the functional tests on subsystem and component level are incomplete.

A test that can be performed without process disturbance while the process is operational is called an *online* test (ISA-TR 84.00.03, 2002; Rausand & Høyland, 2004). A diagnostic test is therefore an online test. Some functional tests may also be performed online. One example is functional testing of input elements, where input elements can be isolated during the test. For online functional testing of final elements, it is necessary to have a full bypass available so that the process can remain undisturbed during the test.

A test that reveals all dangerous failures and where the SIS after the test is restored to an as good as new condition, is called a *perfect* test (Mostia, 2002; ANSI/ISA 84.01, 1996). In reliability calculations, it is usually assumed that functional tests are perfect tests, but there are several reasons to why a functional test is not perfect in practice. One reason may be inadequate preparation, execution, and restoration, which may introduce new failures or leave existing failures unrevealed. Another reason is that a functional test is performed under test conditions rather than demand conditions. To test a SIF under real demand conditions, for example, slam shutting a valve in a high pressure and high flowrate oil/gas pipeline, may lead to hammer effects that may damage the valve and the pipeline. Instead, the shutdown function is tested when the flow has been stopped by some choke device or a less critical valve (ISA-TR 84.00.03, 2002).

There are several ways to include the aspect of imperfect testing when the PFD is calculated. One way is to add a certain probability $p$ to the PFD that caters for the DU failures that remain after a functional test (e.g., see SINTEF, 2006); another approach is to assume that the functional test is not capable of detecting all dangerous failure causes, and consider the remaining undetected failures as undetected during the SIS lifetime (Rausand & Høyland, 2004).

A PST is obviously an imperfect test, since a fraction of the failures may remain unrevealed after the test. PST may also be considered an incomplete functional test, since it tests only a part of the SIF. PST shares some properties of a diagnostic test, for example that it is fully or partially automatic and that it detects a fraction of the dangerous failures without disturbing the process. The question is, however, whether or not PST should be used as a means to improve the safe failure fraction (SFF). The SFF is the fraction of the rate of "safe" failures to the total failure rate, where "safe" failures include failures that are safe by definition plus dangerous detected (DD) failures which are detected by diagnostic testing. The SFF is used by IEC 61508 and IEC 61511 to determine the architectural constraints, and a high SFF generally allows for less hardware redundancy. Different authors have different views on whether or not failures that are detected by PST should be considered DD failures. Some authors argue that PST may be used to improve the SFF (Ali & Goble, 2004; Knegtering, 2004) provided that the requirements of being a diagnostic test are fulfilled, while others claim that PST is not performed frequently enough to meet the intentions of being a diagnostic test (Lundteigen & Rausand, 2008, 2007; Velten-Philipp & Houtermans, 2006) What is meant by frequently enough is often the core of the dispute. Some claim that a PST interval of a magnitude less than the expected demand rate is frequently enough to consider the timing aspect of a diagnostic test as fulfilled. However, if the number of demands per year is less than one, we may end up by allowing diagnostic test intervals of weeks and months. We believe that intervals of this length do not meet the intentions of how frequent diagnostic tests should be run, and we do therefore not recommend that PST is introduced as a means to improve the SFF. But again, this is an issue for further discussion within the industry.

## 4. Reliability effects of introducing PST

The fraction of DU failures that are detected by PST among all DU failures is called the PST *coverage*, and is defined as

$$\theta_{\mathrm{PST}} = \frac{\lambda_{\mathrm{DU,PST}}}{\lambda_{\mathrm{DU}}} \tag{1}$$

where $\lambda_{\mathrm{DU,PST}}$ is the rate of DU failures that can be detected by PST and $\lambda_{\mathrm{DU}}$ is the total rate of DU failures.

The PST coverage may also be expressed as the conditional probability

$$\theta_{\mathrm{PST}} = \Pr(\text{Detect DU failure by PST}|\text{DU failure is present}) \tag{2}$$

The PST coverage for shutdown valves is often considered to be in the range of 60–70% (Summers & Zachary, 2000; Lundteigen & Rausand, 2007). The value of $\theta_{\mathrm{PST}}$ for a specific application should be determined based on plant specific conditions, such as valve type, functional requirements, and operational and environmental conditions. This is further discussed in Section 5.

When PST is not implemented, the average PFD of the shutdown valve is approximately the sum of the average PFD for functional testing ($\mathrm{PFD}_{\mathrm{FT}}$) and the average PFD for diagnostic testing ($\mathrm{PFD}_{\mathrm{DT}}$):

$$\mathrm{PFD} \approx \mathrm{PFD}_{\mathrm{FT}} + \mathrm{PFD}_{\mathrm{DT}} \approx \frac{\lambda_{\mathrm{DU}} \cdot \tau_{\mathrm{FT}}}{2} + \frac{\lambda_{\mathrm{DD}} \cdot \tau_{\mathrm{DT}}}{2} \tag{3}$$

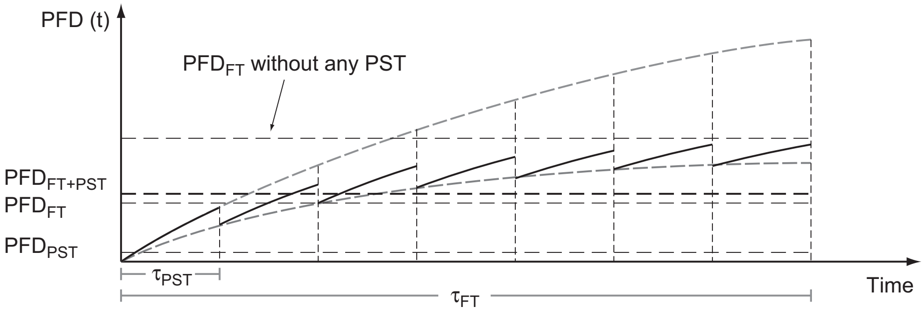


**Fig. 3.** PST contribution to PFD.

where $\tau_{FT}$ is the functional test interval and $\tau_{DT}$ is the diagnostic test interval. The diagnostic test interval is generally very short, and $PFD_{DT}$ is therefore negligible. It is here assumed that the functional test comprises necessary activities to reveal and correct *all* failures, and that the valve may be considered as good as new after the test/repair (Rausand & Høyland, 2004).

Since PST can detect only a fraction, $\theta_{PST}$, of the DU failures, the probability of failure on demand may be expressed as (Houtermans, Rouvroye, & Karydas, 2004; Knegtering, 2004; Lundteigen & Rausand, 2007; McCrea-Steele, 2005; Summers & Zachary, 2000):

$$\begin{aligned} PFD &\approx PFD_{FT} + PFD_{PST} \\ &\approx (1-\theta_{PST}) \cdot \frac{\lambda_{DU}\tau_{FT}}{2} + \theta_{PST} \cdot \frac{\lambda_{DU}\tau_{PST}}{2} \end{aligned} \tag{4}$$

where $\tau_{PST}$ is the PST interval. The PFD *with* and *without* taking PST into account are illustrated in Fig. 3.

The PFD is reduced when PST is introduced, since a fraction of the DU failures are revealed and corrected within a shorter time interval after they occur, than by functional testing. Thus, if the functional test interval is kept unchanged, the SIF reliability is improved.

## 5. Pros and cons of introducing PST

PST is a supplement rather than a means to eliminate the need for functional testing (Summers & Zachary, 2000; Nuis, 2005). The reliability improvement that is obtained by introducing PST may be used in two ways:

(1) *To improve safety*: PST is added to the initially scheduled functional tests. This leads to a reduction in the calculated PFD. With a lower PFD, the safety improves.
(2) *To reduce costs*: The potential reliability improvement is used to extend the interval between functional tests so that the calculated PFD is kept unchanged. As a result, the operating and maintenance costs may be reduced as less man-hours and fewer scheduled production stops are required.

The reliability improvement is influenced by two factors; the PST coverage and the PST interval. The PST interval is a decision variable which is entirely up to the end user to follow up, while the PST coverage must be estimated based on a number of assumptions. The assumptions related to the PST coverage should be made for the plant specific application rather than for an average valve performance (ISA-TR 84.00.03, 2002; Goble & Cheddie, 2005). The factors that may influence the PST coverage are, for example:

- *Valve design*: Different types of valves may have different failure properties. One type of valve may, for example, have more failures related to leakage in closed position than another type of valve where most failures are caused by a stuck stem. For the first valve, we expect a lower PST coverage than for the latter. The failure properties may be derived from an FMEA analysis. The FMEA analysis may be provided by or performed in close collaboration with the valve vendor.
- *Functional requirements*: PST is not able to verify all types of functional requirements. A PST reveals whether or not a valve starts to move, but is not able to verify that the valve will continue to a fully closed position and that it keeps tight in this position. ISA-TR 84.00.03 cautions that PST does not detect failures associated with tight shutoff, as for example leakage in closed position. The specified valve closing time may also impact the PST coverage. For valves where 2–3 s closing time is specified, one may obtain less information about the valve failures and performance deviations than for valves with longer closing times (Nuis, 2005).
- *PST technology*: The PST technology may affect which and to what extent failures are detected. While a SIS implemented PST with simple readback of the valve position signal may detect that a valve fails to start closing, a more advanced PST technology solution with additional sensors may indicate if other failures are present by analyzing performance deviations (in e.g., valve's speed of response) (Ali, 2004; Ali & Goble, 2004). ISA-TR 84.00.03 emphasizes that readback of position signal should confirm that the requested position has been reached. To simply verify that the limit switches have left and returned to their end position is not always considered a valid test.
- *Operational and environmental conditions*: Some operational and environmental conditions may lead to obstructions and build-up in the path towards the valve end position. Concern has been raised that build-up is more likely for valves that are moved to a fixed intermediate position (ISA-TR 84.00.03, 2002). While a stuck valve may be detected by the PST, other obstructions or build-up that impede the valve from reaching the end position, are not identified. If the operating or environmental conditions are likely to cause build-up or obstructions, (e.g., multi-phase flow, seawater flow), one may expect a lower PST coverage than if the valve is operated in a clean (e.g., gas) environment. ISA-TR 84.00.03 cautions the use of PST for valves in unclean environment where, for example, dirt, polymerization products, deposition, crystallization, corrosive chemicals are present.

Based on the discussion above, PST seems most suited to detect that a valve is stuck and does not start to move. To what extent other dangerous failures may be detected, is influenced by the features of the selected PST technology. The PST coverage is not only influenced by what the PST technology is *able* to detect. It is just as important to consider how frequent these dangerous failures occur compared to the occurrence of other dangerous failures. Here, the functional requirements, the valve design, and the documented valve performance must be considered.

Introducing PST may influence the reliability of the SIS in other ways than through the PST coverage. Soft seated valves are more vulnerable to wear when the valve is moved to the end position (Summers & Zachary, 2000). If PST is used to extend the time between functional tests, this may increase the expected lifetime of the valve seat. As a result, less failures may be experienced with this particular failure cause. PST may also provide additional information about the valve condition, like valve signatures, which may be used for earlier detection of performance deviations (Ali, 2004; Ali & Goble, 2004). Finally, automatic tests like PST require less human interaction which may lead to less systematic failures.

PST may also have unwanted effects. The risk of more spurious valve closures has been discussed by several authors (Ali & Goble, 2004; McCrea-Steele, 2005; Mostia Jr., 2003; Summers & Zachary, 2000). Even if spurious closure is normally considered as a safe failure, it may introduce other hazardous events at the plant due to, for example, water hammer effects (Langeron, Barros, Grall, & Berenguer, 2007; Signoret, 2007).

Another concern is that more frequent stroking leads to more wear on components, for example, on the valve stem and the stem seals. This may lead to failures like valve leakages. Since valve leakages are normally not detected by PST, such failures may be hidden for a longer period of time if the PST is used to extend the intervals between functional testing.

## 6. New procedure for determining the PST coverage

This section presents a new procedure for determining the PST coverage in a specific application. In Section 5, we identified factors that influence the PST coverage. The new procedure suggests *how* these factors can be taken into account. The procedure is set up for the initial design phase, but may also be used to update the estimate of the PST coverage in the operational phase.

An important assumption is that the PST coverage is a property of individual SIS components rather than for a group of components, and should therefore be determined at this level.

We may express Eq. (2) as

$$\theta_{\mathrm{PST}} = \frac{\Pr(\text{Detect DU failure by PST} \cap \text{DU failure is present}))}{\Pr(\text{DU failure is present})} \tag{5}$$

Let $\mathrm{FM}_1, \mathrm{FM}_2, \ldots, \mathrm{FM}_n$ be the relevant DU failure modes. Typical DU failure modes for a shutdown valve are: fail to close, delayed operation, and leakage in closed position, but there may also be several more failure modes in specific applications. Even if it is possible that two or more of these failure modes can be present at the same time, the likelihood of such an event is very small. We can therefore assume the failure modes to be mutually exclusive, and we can therefore write (5) as

$$\theta_{\mathrm{PST}} \approx \sum_{i=1}^{n} \frac{\Pr(\text{Detect } \mathrm{FM}_i | \mathrm{FM}_i \text{ is present}) \cdot \Pr(\mathrm{FM}_i \text{ is present})}{\Pr(\text{DU failure is present})} \tag{6}$$

Analogous to (1) we define

$$\theta_{\mathrm{FM},i} = \Pr(\text{Detect } \mathrm{FM}_i | \mathrm{FM}_i \text{ is present}) \tag{7}$$

to be the PST coverage of the DU failure mode $\mathrm{FM}_i$, for $i = 1, 2, \ldots, n$.

The fraction

$$w_i = \frac{\Pr(\mathrm{FM}_i \text{ is present})}{\Pr(\text{DU failure is present})} \tag{8}$$

is the fraction of $\mathrm{FM}_i$ failures among all DU failures, for $i = 1, 2, \ldots, n$.

The PST coverage can therefore be expressed as

$$\theta_{\mathrm{PST}} = \sum_{i=1}^{n} \theta_{\mathrm{FM},i} \cdot w_i \tag{9}$$

We suggest that the PST coverage per failure mode is determined in two sub-steps, since successful detection of a failure mode relies on two factors: (i) the failure mode must be *revealable* during a partial stroke operation, and (ii) it is important that the test results are reliable, such that the announced results reflect the valve condition. We refer to factor (i) as revealability (per failure mode), and factor (ii) as the PST reliability (per failure mode). This means that

$$\theta_{\mathrm{FM},i} = \mathrm{PST}_{\mathrm{Rev},i} \cdot \mathrm{PST}_{\mathrm{Rel},i} \tag{10}$$

where $\mathrm{PST}_{\mathrm{Rev},i}$ denotes the revealability of failure mode $i$ by PST, and $\mathrm{PST}_{\mathrm{Rel},i}$ is the PST reliability of failure mode $i$.

The revealability may be determined by expert judgment, while we suggest that the PST reliability is assessed based on a checklist. The details on how they are determined are further discussed in the procedure steps.

The procedure comprises six steps. The Kristin subsea HIPPS that was introduced in Section 2, is used to illustrate the procedure. The main focus is the HIPPS shutdown valves. The procedure builds on recognized techniques like FMEA (e.g., see Rausand & Høyland, 2004) and the use of checklists (Johnsen et al., 2004; Summers & Raney, 1999; Summers, Raney, & Dejmek, 1999; Walker, 1997). FMEA is a powerful tool to increase the knowledge of system behavior upon failures, while checklists may be used to give credit to desired behavior. Both methods are widely used in the oil and gas industry. The procedure also makes use of historical data, for example collected through the OREDA projects (OREDA, 1997, 2002). The procedure should, to the extent that is practical, be performed by a group of persons with relevant competence on the equipment, the operation, and safety issues.

*Step* 1: *Get familiar with the PST and its implementation.*

The objective of this step is to collect relevant information on the PST implementation and the application specific conditions, including:

(1) Which SIS components that are operated during a PST.
(2) The functional safety requirements of the SIS components, like valve closing time and maximum allowed leakage in closed position.
(3) How PST is initiated and controlled by dedicated hardware and software.
(4) The PST interface to the SIS and other systems, like the process control system.
(5) The operational and environmental conditions under which the SIF operates, including fluid characteristics, temperature, and pressure.

For the Kristin HIPPS, the PST implementation approach is illustrated in the upper section of Fig. 1. The additional information requested in this step is covered in Section 3.

*Step* 2: *Analyze the PST hardware and software.*

The objective of this step is to identify and analyze how PST hardware and software failures affect the PST execution and the SIS itself. This analysis provides an important basis to later answer the checklist questions, and should be performed in close collaboration between the end users and the valve vendors. The review may be time consuming, but nevertheless important to gain insight to the functionality of the PST, the PST interaction with the SIS, and the consequences of PST failures. The analysis gives insight to constraints and potential secondary effects of using PST.

We suggest an FMEA-style analysis is used to identify and assess the potential PST hardware and software failures. It is possible to use a top down or bottom up approach to FMEA. The top down approach starts with a list of functions, and may be an appropriate approach if the PST hardware and software have not been decided. The bottom up approach is illustrated in Table 1. The starting point is to list all PST related components and their functions in an FMEA worksheet, which for the case of Kristin HIPPS may be as shown in Table 1.

The FMEA worksheet may be extended by more columns, for example on how to detect the PST hardware and software failures. As seen from the analysis, the confidence of the PST test results is highly influenced by the reliability of the position indicators. The reliability of the position indicators is therefore important to consider when we calculate the PST reliability.

*Step* 3: *Determine the PST reliability*.

The PST reliability is a measure of the PST hardware and software ability to provide reliable and useful test results, within the scope of the test. A checklist is proposed for calculating the PST reliability. Each question gives credit to the preferred behavior, and have an effect on the reliability and usefulness of the test results. In addition, the questions are weighted according to their importance. Weight 1 is used as credit for questions that reflect recommended practice, weight 5 is used for highly recommended practice, and weight 10 represents mandatory practice. In this context, we use mandatory for those questions that reflect requirements in SIS related standards, highly recommended for questions that address behavior recognized by guidelines and/or several authors, and recommended for other issues which may have an effect on the PST reliability.

The PST reliability is scaled from 0.5 to 1.0. If all questions are given the answer "no", the PST reliability is 0.5, meaning that a failure, if present, has a 50% chance of being useful and correctly announced to the operators. In the case where all questions are given the answer "yes," the PST reliability is 1.0, meaning that we fully rely on the PST hardware and software's ability to announce useful and reliable information about a failure.

For each question, the corresponding credit to the PST reliability is calculated by the following formulas:

$$\text{Credit when ``yes''} = \frac{\text{Weight of question}}{\text{Sum of all weights}} \cdot 1.0 \tag{11}$$

$$\text{Credit when ``no''} = \frac{\text{Weight of question}}{\text{Sum of all weights}} \cdot 0.5 \tag{12}$$

The authors realize that the questions and their weights are issues that should be further discussed, but they may represent a good starting point. It is also important that the questions are generic, and reflect the commonly accepted issues of importance. If a user or vendor introduces a number of new questions, they may be able to reduce the contribution of the generic questions.

The questions and the corresponding weights are shown in Table 2. The table may be an integral part of an FMEA worksheet. In the table, some assumptions have been made regarding the Kristin HIPPS implementation. These assumptions have not been fully verified, and are only used to illustrate the application of the checklist. Ideally, the checklist should be applied for each dangerous undetected failure mode. In this example, we have only used the checklist once, which means that a *common* PST reliability has been assumed for all the failure modes.

Question 1 addresses the need for establishing criteria for successful execution of PST. The question is given weight 10, since defining fail/pass criteria is required by IEC 61508 and IEC 61511. Question 2 calls for application specific analysis, rather than generically selected PST coverage per failure mode. Such a plant specific analysis is the intention of the IEC standards and is also recommended by ISA-TR00.03-2002. We therefore suggest weight 10 for this question.

Question 3 asks for analysis of PST related failures and how they impact the PST execution and the SIS. IEC 61508 and IEC 61511 require that systems interfacing the SIS do not have a negative impact on the execution of the SIF. We therefore consider such analysis as mandatory by the standards, and weight 10 is suggested.

Concerns have been raised to the secondary effects of PST. Introducing PST may lead to more frequent operation of some components (e.g., solenoid operated valves) and less frequent operation of others (e.g., full stroke operation of valves). Question 4 addresses the need for analysis of potential negative effects on the SIS reliability. The issue has been addressed by ISA-TR 84.00.03, but the need to analyze secondary effects of testing is not addressed in IEC 61508 and IEC 61511. We therefore suggest weight 5. ISA-TR 84.00.03 expresses some concerns that may be relevant to consider. If the fluid running through the valve contains corrosive chemicals, dirt, polymerization products, or particles that may deposit or crystallize, a more in depth analysis should be performed to consider the gain and impact of PST.

It is often recommended to use position indicators to measure the actual valve movement, rather than just verifying that the

**Table 1**
Simplified FMEA for PST hardware and software

| Description of component | | | Failure and the failure effects | | |
|---|---|---|---|---|---|
| Component | Type | Function | Failure mode | Effect on PST | Effect on SIS |
| Test initiator | SW | To initiate a PST | Fail to initiate | No execution of PST | None |
| Timer | SW | Deactivate output according to timer setpoint | Fail to start | No execution of PST | None |
| | | | Fail to reset | Valve not returned to initial position | Spurious valve closure |
| Position indicators | HW | Measure valve position | No signal | PST may be executed, but valve position indicator does not show that the valve moves. | Repair must be initiated to correct position indicators.<br>Visual inspection of valve position may have to be inspected by ROV[a] |
| | | | Wrong signal | May fail to announce the correct valve position | SIS may be left with undiscovered failures. |

[a] Remotely operated vehicle.

**Table 2**
Checklist to determine the PST reliability

| No | Question | Answer | Weight | Credit |
|---|---|---|---|---|
| 1 | Have success criteria for the partial stroke test been clearly defined? | Y | 10 | 0.14 |
| 2 | Has an FMEA been performed to identify the SIS failure modes, and to what extent the failure modes can be detected during a partial valve operation? | Y | 10 | 0.14 |
| 3 | Have potential failures of the PST hardware and software been identified and analyzed? | N | 10 | 0.07 |
| 4 | Have potential secondary effects of PST on the reliability of valve, actuator and control devices (e.g., solenoid operated valves) been analyzed? | N | 5 | 0.04 |
| 5 | Is the actual stem movement measured (in %), as opposed to just verifying that the valves leaves and returns to the initial position? | Y | 5 | 0.07 |
| 6 | Is additional instrumentation installed, and is it capable of providing more insight to failure causes? | N | 1 | 0.01 |
| 7 | Is the PST hardware and software regularly inspected and tested (or otherwise verified)? | Y | 5 | 0.07 |
| 8 | Is the feedback from PST recorded and further analyzed? | Y | 10 | 0.14 |
| 9 | If short closure time is required: Has it been analyzed if the PST is able to provide useful information? | Y | 10 | 0.14 |
| 10 | Are means implemented to verify that the position indicators are reliable? | Y | 5 | 0.07 |
| | | Sum: | 71 | 0.89 |

valve leaves and returns to the initial position (ISA-TR 84.00.03,2002). Question 5 has been included to address this particular issue. The need for actual valve movement will be most important in cases where the valve movement is not confirmed by visual inspection or pressure readings. We have assigned weight 5 to this question, but it might be argued that weight 10 would also be applicable since ISA-TR 84.00.03 so clearly states the importance of this issue.

Question 6 gives some credit to additional instrumentation installed to measure and analyze for example the valve's speed of response, torque and hydraulic or pneumatic supply and return pressures. These may be features provided by vendor packages. Despite their ability to provide additional information about the valve condition, the vendor packages are not a necessary means to verify that the valve is able to partially move.

Question 7 recognizes the need to verify that the PST software and hardware continue to perform as specified. The IEC standards do not specifically address regular verification of PST and diagnostics hardware and software. The need for regular confirmation of the PST hardware and software ability to perform as intended may be analogue to the adopted practice of regular calibration and inspection of tools used for functional testing. As a result, we assign weight 5 to the question.

Question 8 concerns the need to record and analyze the PST test results. Failure reporting and analysis are required by IEC 61508 and IEC 61511. The question has therefore been given weight 10.

Some authors indicate that PST is not suitable for valves that have a very short closing time (e.g., 1–3 s). In this case, the valve may be unable to move at all during the short time available for the PST. Question 9 addresses this issue. The question is given weight 5, as authors indicate that this may reduce the reliability gain of introducing PST (Nuis, 2005; ISA-TR 84.00.02, 2002).

Question 10 addresses position indicators and to what extent it is being verified that they provide reliable readings. The reliability of position indicators is important for the validity of PST results, as indicated in the FMEA analysis in Step 3. We therefore give weight 5 for this question.

**Table 3**
Failure modes weights and PST revealability

| Failure mode | Refinement | Revealability factor (%) |
|---|---|---|
| | Sub failure modes | |
| Fail to close | Fail to start moving | 100 |
| | Starts, but does not reach end position | 0 |
| Delayed operation | Delayed start | 100 |
| | Starts, but uses too long closing time | 70 |
| Leakage in closed position | Minor leakage | 0 |
| | Major leakage | 0 |

With the answers suggested for Kristin HIPPS, which in this case are based on our assumptions of the actual implementation, we obtain a PST reliability of 0.89.

*Step* 4: *Determine the revealability* (*per failure mode*).

Table 3 shows columns that may be added to the FMEA worksheet for the purpose of including the revealability. The analysis considers the dangerous failure modes: fail to close, delayed operation, and leakage in closed position. A refinement of the failure modes may give a better basis for deciding whether or not the failure mode may be revealed by a partial stroke operation. It should be noted that we refine the failure modes rather than the failure causes as PST (in most cases) is unable to identify failure causes.

If we believe that the sub failure mode is fully observable during a partial movement, we assign 100% to the revealability. If it is not observable at all, we assign a value 0%. If we believe that the failure mode may be revealable with a certain probability, for example 70%, we use this value as the revealability. Table 3 lists the revealabilities that are suggested for the dangerous failure modes.

As seen in Table 3, the failure mode "fail to close" may be further split into the sub failure modes "fail to start moving" and "starts (to move), but does not reach end position." It is evident that the first one may be detected just as well by a partial stroke

**Table 4**
Failure modes weights and PST revealability

| Failure mode | Weight (%) | Refinement | | Resulting weight (%) |
|---|---|---|---|---|
| | | Sub failure modes | Split (%) | |
| Fail to close | 40 | Fail to start moving | 80 | 32 |
| | | Starts, but does not reach end position | 20 | 8 |
| Delayed operation | 40 | Delayed start | 40 | 16 |
| | | Too long travel time | 60 | 24 |
| Leakage in closed position | 20 | Minor leakage | 60 | 12 |
| | | Major leakage | 40 | 8 |

as by a full stroke, while the latter requires a full stroke operation to be detected.

*Step* 5: *Determine the failure mode weights*.

The failure mode weight $w_i$ in Eq. (8) may be determined by expert judgement or analysis of historical failure data. The latter approach is discussed by Lundteigen and Rausand (2007). The failure mode weights may be included in the FMEA worksheet directly, or as separate failure rates as shown by Goble and Cheddie (2005). Since we consider the revealability at the sub failure mode level, we must also assign failure mode weights accordingly. The allocation of failure mode weights down to the sub failure modes may be based on a more in depth analysis of historical data. OREDA (1997, 2002) provide some underlaying details of failures, but in many cases it is necessary to also study the failure records that where used to construct the data. The distribution of weights that is shown in Table 4 is just for illustration.

*Step* 6: *Determine the PST coverage*.

The PST coverage can now be determined by using Eq. (9). With the assumptions made for the PST of the Kristin HIPPS valves, we end up with a PST coverage of 65%.

## 7. Discussion and concluding remarks

The reliability that may be gained by introducing PST is influenced by two factors; (i) the PST coverage, and (ii) the PST interval. The PST coverage is partly a design parameter (e.g., valve design, PST hardware and software), and partly an operational parameter (e.g., operational and environmental conditions). While vendors may influence the PST coverage by selecting valve design and PST hardware and software in accordance with the specified operational and environmental conditions, the frequency by which the PST is executed is a decision that relies on the end user alone.

To determine the reliability gain of introducing PST, it is necessary for vendors and end users to collaborate. The valve manufacturer knows how the valve is designed and the PST vendor or supplier understands the features of the PST hardware and software. This knowledge must be combined with the end users' insight into maintenance and testing strategies and operational and environmental conditions. The new procedure suggests a framework that requires a joint effort from end users and valve vendors to estimate the PST coverage for a particular valve application.

So, what is gained by using our new procedure? Is it worthwhile using this effort to estimate a PST coverage that often ends up between 60% and 70%? We believe that the main advantage of this procedure is not only the final result, but the *process* of getting there. The process increases the awareness to which factors that may influence the PST coverage. It is evident that some factors are revealable, but not controllable, for example the failure mode weights, which are properties of the SIS components. Other factors may be controlled, like the factors we address in the PST reliability checklist. PST contributes to earlier detection of failures, and less frequent failures may be experienced when PST is applied, due to the secondary effects discussed in Section 5.

We hope that this procedure also demonstrates some of the pitfalls of introducing PST. PST becomes false comfort if the PST coverage is estimated from false premises. We may install the PST hardware and software, but refrain from implementing adequate follow-up of PST results. We may use PST to save operation and maintenance costs, but fail to consider the secondary effects of extending the intervals between full stroke testing. Our procedure asks for certain steps and analysis which may lead to a higher confidence in the selected PST coverage, and where to put focus in order to maintain the confidence throughout the operation phase. We therefore propose that the PST reliability checklist is used in the design phase as well as in the operation and maintenance phases.

The main disadvantages of the new procedure may be related to the practical implementation. First, the checklist questions may be used to make erroneous improvements to the PST coverage, particularly if the implementation of the checklist questions does not correspond to how PST is performed in the operational phase. It is therefore necessary to review the checklist questions during the operational phase and verify that the PST continues to meet the initially estimated coverage. Second, the procedure also requires that the end user spends more time on understanding PST hardware and software than what is normally done. One may question if this is realistic and if the PST hardware and software may be too complex to understand for others than the valve or PST vendor. On the other hand, the responsibility still lays on the end user, and the PST hardware and software should not be so complex that the end user is unable to verify the PST functionality under normal and failure conditions.

Further research may be necessary to develop a generic and widely accepted checklist for the PST reliability, similar to what has been done for the checklist on the determination of the beta factors in IEC 61508. Also the secondary effects of PST should be analyzed further and supported by data collection. At the present time, databases like OREDA do not suggest a separate classification for failures that are detected by PST. Without this type of classification, it may be difficult to use historical data to confirm to what extent PST is able to reveal DU failures.

## Acknowledgements

The authors acknowledge Halvor Stokke at StatoilHydro and Lars Bak at Lilleaker Consulting AS for giving us insight in the practical implementation of partial stroke testing at the Kristin field on the Norwegian Continental Shelf. We would also like to thank the reviewers of this paper for well-considered and useful inputs and comments.

## References

Aarø, R., Lund, B. F., & Onshus, T. (1995). Subsea HIPPS design procedure (Paper OTC 7829). In *Offshore technology conference* (*OTC*) *proceedings*, Houston, TX.

Ali, R. (2004). Problems, concerns and possible solutions for testing (and diagnostics coverage) of final control element of SIF loops. *Technical papers of ISA*, *454*, 995–1002.

Ali, R., & Goble, W. (2004). Smart positioners to predict health of ESD valves. In *Proceedings of the annual symposium on instrumentation for the process industries* (pp. 29–37), Exida, Sellersville, PA.

Ali, R., & Jero, L. (2003). Reliability and asset management: Smart positioners in safety instrumented systems. *Petroleum Technology Quarterly*, *8*(1), 137–140.

ANSI/ISA 84.01 (1996). *Application of safety instrumented systems for the process industries*. Research Triangle Park, NC: The Instrumentation, Systems and Automation Society (ISA).

Bak, L., Sirevaag, R., & Stokke, H. (2006). Experience with the HPHT subsea HIPPS on Kristin. In *Deep offshore technology—conference and Exhibition*, 28–30 November 2006, Houston, TX.

CCPS (2007). *Guidelines for safe and reliable instrumented protective systems*. Hoboken, New Jersey: Wiley and Center for Chemical Process Safety, AIChE.

Goble, W. M., & Cheddie, H. (2005). *Safety instrumented systems verification: Practical probabilistic calculations*. Research Triangle Park, NC: The Instrumentation, Systems and Automation Society (ISA).

Houtermans, I. J. M., Rouvroye, J. L., & Karydas, D. M. (2004). Risk reduction through partial stroke testing. In *Probabilistic safety assessment and management* (*PSAM7-ESREL'04*). Springer.

IEC 61508 (1998). *Functional safety of electrical/electronic/programmable electronic safety-related systems*. Geneva: International Electrotechnical Commission.

IEC 61511 (2003). *Functional safety—safety instrumented systems for the process industry*. Geneva: International Electrotechnical Commission.

ISA-TR 84.00.02 (2002). Safety instrumented functions SIF—safety integrity level (SIL) evaluation techniques Part 4: Determining the SIL of a SIF via Markov Analysis. Technical report, The Instrumentation, Systems, and Automation Society, Research Triangle Park, NC.

ISA-TR 84.00.03 (2002). Guidance for Testing of Process Sector Safety Instrumented Functions (SIF) Implemented as or within Safety Instrumented Systems (SIS). Technical report, The Instrumentation, Systems, and Automation Society, Research Triangle Park, NC.

Johnsen, S. O., Bjørkli, C., Steiro, T., Fartum, F., Haukenes, H., & Ramberg, J. (2004). CRIOP: A scenario method for crisis intervention and operability analysis. *Technical Report STF38 A03424*, SINTEF, Trondheim, Norway.

Knegtering, B. (2004). Safety-PLC's striking role for partial valve stroke testing. *Technical Papers of ISA*, *454*, 563–572.

Langeron, Y., Barros, A., Grall, A., & Berenguer, C. (2007). Safe failures impact on safety instrumented systems. In T. Aven, & J. Vinnem (Eds.), *Risk, reliability, and societal safety* (pp. 641–648). Taylor & Francis.

Lund, B. F., Onshus, T. E., & Aarø, R. (1995). HIPPS concepts for subsea field scenario (Paper OTC 7830). In *Offshore technology conference* (*OTC*) *Proceedings*, Houston, TX.

Lundteigen, M. A., & Rausand, M. (2007). The effect of partial stroke testing on the reliability of safety valves. In T. Aven, & J. Vinnem (Eds.), *Risk, reliability and societal safety*. Taylor & Francis.

Lundteigen, M. A. & Rausand, M. (2008). Architectural constraints in IEC 61508: Do they have the intended effect? *Submitted for publication*.

McCrea-Steele, R. (2005). Partial stroke testing implementing for the right reasons. In *Technical Papers of ISA*, vol. 459 (pp. 229–238). Research Triangle Park, NC.

Mostia, B., Jr. (2003). Partial stroke testing simple or not? *Control (Chicago, Ill)*, *16*(11), 63–69.

Mostia, W. L. (2002). Testing of SIS valves. Technical report, http://www.sipi61508.com/ciks/mostia2.pdf.

Nuis, W.-J. (2005). Partial stroking on fast acting applications. In *Proceedings from the TÜV Rheinland group's symposium*, June 9th, Cleveland, OH, USA.

Onshus, T. E., Aarø, R., & Lund, B. F. (1995). HIPPS applications and acceptance criteria Paper OTC 7828. In *Offshore technology conference* (*OTC*) *proceedings*, Houston, TX.

OREDA (1997). *OREDA reliability data* (3rd ed.). Available from: Det Norske Veritas, NO 1322 Høvik, Norway: OREDA Participants.

OREDA (2002). *OREDA reliability data* (4th ed.). Available from: Det Norske Veritas, NO 1322 Høvik, Norway: OREDA Participants.

Rausand, M., & Høyland, A. (2004). *System reliability theory: Models, statistical methods, and applications* (2nd ed.). Hoboken, New Jersey: Wiley.

Signoret, J.-P. (2007). High integrity pressure protection systems (HIPPS)—making SIL calculations effective. *Exploration and production—oil and gas review* (*OTC edition*) (pp. 14–17).

SINTEF (2006). *Reliability prediction methods for safety instrumented systems*, *PDS method handbook*. Trondheim, Norway: SINTEF.

Summers, A. E. (2003). Flare reduction with high integrity protection systems (HIPS). In *ISA technical papers*, volume 438, Research Triangle Park, NC. The Instrumentation, Systems, and Automation Society (ISA).

Summers, A., & Raney, G. (1999). Common cause and common sense, designing failure out of your safety instrumented systems (SIS). *ISA Transactions*, *38*(3), 291–299.

Summers, A., Raney, G., & Dejmek, K. (1999). Safeguard safety instrumented systems. *Chemical Engineering Progress*, *95*(11), 85–90.

Summers, A., & Zachary, B. (2000). Partial-stroke testing of safety block valves. *Control Engineering*, *47*(12), 87–89.

Summers, A., & Zachary, B. (2002). Improve facility SIS performance and reliability. *Hydrocarbon Processing*, *81*, 71–74.

Summers, A. & Zachary, B. (2004). High integrity protection systems. In *Proceedings of the annual symposium on instrumentation for the process industries*, vol. 488, pp. 49–59.

Velten-Philipp, W., & Houtermans, M. (2006). The effect of diagnostic and periodic proof testing on the availability of programmable safety systems. *WSEAS Transactions on Systems*, *5*(8), 1861–1867.

Walker, A. (1997). Quality management applied to the development of a national checklist for ISO 9001 audits for software. In *Proceedings of the IEEE international software engineering standards symposium* (pp. 6–14).

# Article 5

Architectural constraints: Do they have the intended effect? *Reliability Engineering and System Safety*, Volume 94, o. 520–525, 2009

Reliability Engineering and System Safety 94 (2009) 520–525

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

# Architectural constraints in IEC 61508: Do they have the intended effect?

Mary Ann Lundteigen [*], Marvin Rausand

*Department of Production and Quality Engineering, Norwegian University of Science and Technology, S. P. Andersens v. 5, NO 7491 Trondheim, Norway*

ARTICLE INFO

*Article history:*
Received 19 November 2007
Received in revised form
19 May 2008
Accepted 14 June 2008
Available online 18 June 2008

*Keywords:*
Safety instrumented system
Hardware fault tolerance
Safe failure fraction
Systematic failure
Probability of failure on demand

ABSTRACT

The standards IEC 61508 and IEC 61511 employ architectural constraints to avoid that quantitative assessments alone are used to determine the hardware layout of safety instrumented systems (SIS). This article discusses the role of the architectural constraints, and particularly the safe failure fraction (SFF) as a design parameter to determine the hardware fault tolerance (HFT) and the redundancy level for SIS. The discussion is based on examples from the offshore oil and gas industry, but should be relevant for all applications of SIS. The article concludes that architectural constraints may be required to compensate for systematic failures, but the architectural constraints should not be determined based on the SFF. The SFF is considered to be an unnecessary concept.

## 1. Introduction

Safety instrumented systems (SIS) are important protection layers in the process industry. A SIS comprises input elements (e.g., pressure transmitters (PTs), gas detectors), logic solvers (e.g., relay based logic, programmable logic controllers), and final elements (e.g., valves, circuit breakers). A SIS is used to detect the onset of hazardous events (e.g., gas leakages, high pressures) and/or to mitigate their consequences to humans, the environment, and material assets. A simplified SIS is illustrated in Fig. 1, where a shutdown valve is installed to stop the flow in the pipeline when high pressure is detected by the PTs. The international standards IEC 61508 [1] and IEC 61511 [2] require that reliability targets for the SIS are defined and demonstrated. The reliability targets are assigned to each safety instrumented function (SIF) that is implemented into the SIS. The IEC standards use safety integrity level (SIL) as a measure for reliability.

Compliance to a SIL must be demonstrated by quantitative and qualitative assessments. The quantitative assessment includes estimating the SIS reliability. For a SIS operating on demand, which is often the case when the SIS is used as an independent protection layer in addition to the process control system, the *average* probability of failure on demand (PFD) is calculated [1,2]. The qualitative assessment verifies that all requirements related to work processes, tools, and procedures are fulfilled in each phase of the SIS life cycle.

The PFD does not cover all aspects that may cause SIS failure, and the calculated PFD may therefore indicate a better performance than will be experienced in the operating phase. Based on this argument, the IEC standards [1,2] have included a set of additional requirements to achieve a sufficiently robust architecture. These requirements are referred to as *architectural constraints*, and their intention is to have one (or more) additional channels that can activate the SIF in case of a fault within the SIS. The architectural constraints prevent SIS designers and system integrators from selecting architecture based on PFD calculations alone, and the requirements may therefore be seen as restrictions in the freedom to choose hardware architecture.

For each part of the SIS, the architectural constraints are expressed by the hardware fault tolerance (HFT), which again is determined by the type of the components (type A or B), the safe failure fraction (SFF), and the specified SIL. The SFF is the proportion of "safe" failures among all failures and the HFT expresses the number of faults that can be tolerated before a SIS is unable to perform the SIF. A "safe" failure is either a failure that is safe by design, or a dangerous failure that is immediately detected and corrected. The IEC standards [1,2] define a safe failure as a failure that does not have the potential to put the SIS in a hazardous or fail-to-function state. A dangerous failure is a failure that can prevent the SIS from performing a specific SIF, but when detected soon after its occurrence, for example, by online diagnostics, the failure is considered to be "safe" since the operators are notified and given the opportunity to implement compensating measures and necessary repairs. In some cases, the SIS may automatically respond to a dangerous detected failure as if it were a true demand, for example, causing shutdown of a process section or the whole plant.

[*] Corresponding author. Tel.: +47 73 59 7101; fax: +47 73 59 7117.
*E-mail address:* mary.a.lundteigen@ntnu.no (M.A. Lundteigen).

0951-8320/$ - see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ress.2008.06.003

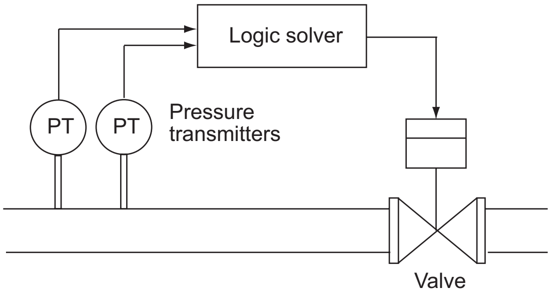


**Fig. 1.** Illustration of a SIS.

The architectural constraints are sometimes interpreted as a mistrust to the quantitative reliability analysis. Reliability experts frequently debate whether or not the architectural constraints are necessary, and if the SFF–HFT–SIL relationship is well-founded. It is particularly the suitability of the SFF that has been questioned [3–5].

The objectives of this article are to (i) provide more insight into the architectural constraints and how the HFT is determined from the type of components and the SFF, (ii) discuss and illustrate by case studies the non-intended effects of a high SFF, and (iii) decide whether or not SFF and HFT are useful concepts related to SIFs.

The article is organized as follows: The rationale for introducing the architectural constraints and for relating the architectural constraints to the SFF is discussed in Section 2. Whether or not a high SFF implies a high safety level is discussed in Section 3. The main characteristics and properties of the SFF are further analyzed and discussed in Section 4 based on two simple case studies. In Section 5, we discuss whether the concept of architectural constraints is really needed. In Section 6, we conclude and discuss the findings of the article and present some ideas for future work.

## 2. Hardware fault tolerance and safe failure fraction

The HFT gives restrictions to hardware architecture [6–8]. If HFT = 1 is specified, the selected configuration must tolerate one failure without affecting the SIF. Configurations that provide HFT = 1, are, for example, 1oo2, 2oo3, and 3oo4, where a *k*oo*n* system is functioning if at least *k* out of *n* components are functioning. The HFT needed to comply with a specified SIL is determined by the component type and the SFF.

SFF is a property of a component or component group. The IEC standards [1,2] define SFF as the proportion of "safe" failures among all component failures

$$\mathrm{SFF} = \frac{\lambda_{\mathrm{S}} + \lambda_{\mathrm{DD}}}{\lambda_{\mathrm{S}} + \lambda_{\mathrm{DD}} + \lambda_{\mathrm{DU}}} \tag{1}$$

where $\lambda_{\mathrm{S}}$ is the rate of safe failures, $\lambda_{\mathrm{DD}}$ is the rate of dangerous detected (DD) failures, and $\lambda_{\mathrm{DU}}$ is the rate of dangerous undetected (DU) failures of a component.

An alternative representation of (1) is to express SFF as a conditional probability:

$$\mathrm{SFF} = \Pr(\text{The failure is ``safe''} \mid \text{A component failure occurs}) \tag{2}$$

Hence, we may interpret SFF as a measure of the inherent safeness of a component, that is, to what extent the component responds in a safe way when a failure occurs.

The second parameter that is used to determine the HFT, is the component type. IEC 61508 [1] distinguishes between type A and type B components. A type A component is characterized by: (i) all failure modes are well defined, (ii) the behavior of the component under fault conditions is well known, and (iii) field data are dependable and able to confirm the failure rates that are claimed. The last criterion is often referred to as "proven in use." A type B component does not fulfill one or more of these criteria. IEC 61511 [2] uses a slightly different classification, and distinguishes between programmable electronic (PE) logic solvers on one side and non-PE-logic solvers/field devices on the other side. In practice, PE-logic solvers are classified as type B according to IEC 61508, while non-PE-logic solvers may fulfil the criteria for type A. Field devices may in some cases be type A and in other cases type B, depending on how many advanced (and programmable) features they have.

**Table 1**
SFF–HFT–SIL relationship in IEC 61508

| SFF | 0 | 1 | 2 |
|---|---|---|---|
| *HFT requirements* (*type A*) | | | |
| <60% | SIL1 | SIL2 | SIL3 |
| 60–90% | SIL2 | SIL3 | SIL4 |
| 90–99% | SIL3 | SIL4 | SIL4 |
| >99% | SIL3 | SIL4 | SIL4 |
| *HFT requirements* (*type B*) | | | |
| <60% | – | SIL1 | SIL2 |
| 60–90% | SIL1 | SIL2 | SIL3 |
| 90–99% | SIL2 | SIL3 | SIL4 |
| >99% | SIL3 | SIL4 | SIL4 |

IEC 61508 [1] provides separate SFF–HFT–SIL relationships for type A and type B components, see Table 1. To our knowledge, the SFF–HFT–SIL relationship is not theoretically founded, but based on a previous concept of a diagnostic (DC)–HFT–SIL relationship [8]. In the table, the SFF is split into four intervals; below 60%, between 60% and 90%, between 90% and 99%, and above 99%. Similarly, IEC 61511 [2] suggests two separate tables, one table for non-PE-logic solvers/field devices and one table for PE-logic solvers, to reflect sector specific categories of components. The main differences between the approach taken in IEC 61508 and IEC 61511, are [3,9]:

- IEC 61511 does not treat SIL 4 systems; in this case the standard refers to IEC 61508.
- IEC 61511 does not give additional credit for SFF above 99%, whereas IEC 61508 does.
- In IEC 61511, the HFT table for non-PE-logic solvers/field devices is independent of the SFF. It is assumed that such devices, when built for safety applications, have SFF in the area of 60–90%. The HFT–SIL relationship proposed for non-PE-logic solvers/field devices corresponds to the HFT–SIL relationship for PE-logic solvers with SFF between 60% and 90%.
- IEC 61511 allows a reduction in HFT by one for non-PE-logic solvers/field devices if certain conditions, for example being proven in use, are met. Having fulfilled these conditions, the HFT–SIL relationship corresponds to the HFT–SIL relationship for type A components in IEC 61508, provided that the SFF is between 60% and 90%.
- IEC 61511 suggests increasing the HFT by one for non-PE-logic solvers/field devices, if the dominant failure mode is DU rather than safe or DD. In other words, if the SFF is below 50%, which may be the case for an "energize to trip" device, it is required to increase HFT by one. In this situation, IEC 61511 requires higher HFT than IEC 61508 for devices that fulfil the criteria of being type A and with SFF <60%.

It is therefore not a one-to-one relationship between the HFT tables in IEC 61508 and IEC 61511, but in most cases, we will end up with the same requirement for HFT for the same SFF and SIL.

In this article, we focus on the IEC 61508 approach, as this is adopted by many oil and gas companies and also by OLF-070 [10]. From Table 1, we note that:

- Components of type B require a higher HFT than components of type A, for the same SIL and SFF.
- The required HFT increases when the SFF decreases.
- The required HFT increases with increasing SIL.

For configurations of different types of components, for example, PTs and level transmitters, it is not possible to use the HFT tables directly, since the components may have different SFF. Instead, IEC 61508 [1] suggests that the achievable SIL is first determined for the individual components. A set of rules is then used to find the achievable SIL for the total configuration. These rules, which we refer to as merging rules, are further explained in [3].

## 3. Does high SFF indicate safe design?

As seen from Table 1, SFF is a crucial parameter when selecting hardware architecture as required by IEC 61508. Configurations based on components with SFF >90% may require a lower HFT than for components with SFF of, for example, 75%. We may therefore deduce that components with high SFF are preferred to a similar components with low SFF. But does a high SFF indicate safe design?

Reliability experts, system integrators, and end users have questioned the suitability of SFF as an indicator of a safe design. Some concerns that have been raised, are:

- "*Safe*" *failures are not always positive for safety*. The SFF is based on the assumption that the SIS response to safe and DD-failures is safe, for the SIS as well as for the plant. However, the SIS response may sometimes induce new hazardous events [4,5]. Langeron et al. [11] argue that safe failures may evolve into dangerous failures, and therefore that the SFF is not an indicator of a safe design. A spurious closure of a shutdown valve may, for example, lead to water hammer effects that can deteriorate the valve and also affect a number of other components. Operators may lose confidence in the SIS if there are frequent alarms caused by "safe" SIS failures. There are several examples where operators have bypassed safety functions that have caused frequent alarms or process disturbances. In addition, human errors during repair and restoration of the SIS may introduce new failures.
- *The SFF may credit unneeded hardware*. The SFF gives credit to a high rate of "safe" failures, and for producers it is a business advantage to claim a high SFF. With a high SFF, components may be used in configurations with low HFT, which means lower cost for the customers.

  At present, the IEC standards [1,2] give little guidance to what type of safe failures to include in the SFF calculations. As a result, producers may use different approaches when calculating the SFF. Some include all types of safe failures, while others include only those failures that are relevant for the performance of the SIF (e.g., spurious operation failures). The PDS method [12] suggests that failures of non-critical components are omitted, which at least prevent these failures from being included with the purpose of increasing the SFF. This approach is supported by CCPS [6], which also poses additional constraints on the calculations by suggesting that only DD-failures that automatically lead to a safe state of the process are considered in the calculations.
- *Sometimes the SFF is only calculated for parts of the components*. IEC 61508 [1] covers electrical, electronic, and PE components, and as a result, producers may sometimes calculate SFF for this part of the component, and assume that the mechanical part is functioning perfectly. In this case, the SFF may not reflect the performance of the component as a whole [13].
- *If the PFD is affected by uncertain reliability data, then so is the calculated SFF*. The architectural constraints are meant to compensate for the uncertainty in the PFD estimate. However, if the reliability data that are used to find the PFD are uncertain, the data used to calculate the SFF are usually even more uncertain. Experience from the OREDA project has clearly shown that safe failures get less attention than dangerous failures in the data collection [14].

Despite these concerns, it is sometimes claimed that the SFF is "good for safety", since safe failures and DD-failures that lead to activation of final elements may act as functional tests. However, the reliability gain from this additional testing may be counteracted by the reliability loss due to stress during spurious activations.

## 4. SFF characteristics

The characteristics of the SFF become more clear if we rewrite Eq. (1), such that

$$\mathrm{SFF} = \frac{\lambda_{\mathrm{S}}}{\lambda_{\mathrm{tot}}} + \mathrm{DC}\frac{\lambda_{\mathrm{D}}}{\lambda_{\mathrm{tot}}} \tag{3}$$

where $\lambda_{\mathrm{tot}} = \lambda_{\mathrm{S}} + \lambda_{\mathrm{DD}} + \lambda_{\mathrm{DU}}$, $\lambda_{\mathrm{D}} = \lambda_{\mathrm{DD}} + \lambda_{\mathrm{DU}}$, and DC is the diagnostic coverage (of dangerous failures) defined by $\mathrm{DC} = \lambda_{\mathrm{DD}}/(\lambda_{\mathrm{DD}} + \lambda_{\mathrm{DU}})$.

From Eq. (3), some characteristics of the SFF become evident:

(1) Two components with the same total failure rate and the same SFF do not necessarily have the same properties. One component may have a higher rate of safe failures (compared to the total failure rate) than the other, while the the other component has a higher DC.
(2) The SFF is a relative number and components with the same SFF–DC relationship may therefore have quite different properties. A component with a high rate of safe failures and a high total failure rate, may have the same SFF as another component with lower failure rates.

As a result, the SFF does not necessarily indicate whether or not a component has a safe design. If a high SFF is obtained by a high rate of safe- and/or DD-failures, these failures may create a higher rate of hazardous events, as indicated in Section 2. The ambiguity of the SFF is further illustrated in two case studies.

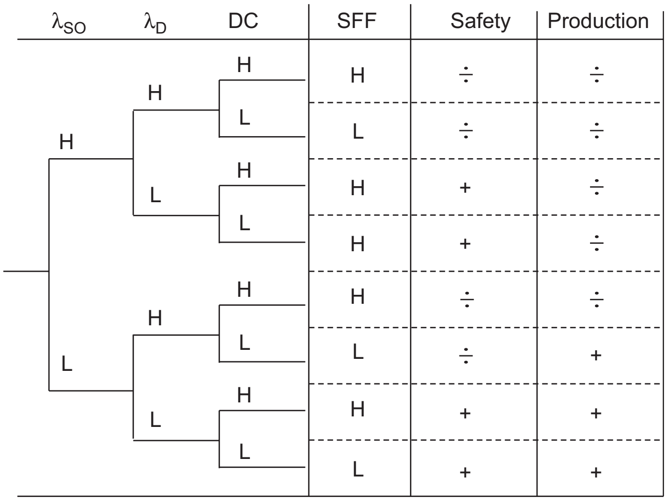
### 4.1. Case studies

Two case studies have been designed to illustrate that:

(i) the SFF may have ambiguous effects on safety and production availability;
(ii) the SFF may favor unsafe design of components.

*Case study I*: *SFF versus safety and production availability*. In this case study, we study how the various properties of a single component can affect safety and production availability. The following component properties are used to illustrate the effects:

- the initial failure rates for safe and dangerous failures are equal to $1 \times 10^{-6}$ failures per hour;



| $\lambda_{SO}$ | $\lambda_D$ | DC | SFF | Safety | Production |
|---|---|---|---|---|---|
| H | H | H | H | ÷ | ÷ |
| | | L | L | ÷ | ÷ |
| | L | H | H | + | ÷ |
| | | L | H | + | ÷ |
| L | H | H | H | ÷ | ÷ |
| | | L | L | ÷ | + |
| | L | H | H | + | + |
| | | L | L | + | + |

**Fig. 2.** The effect of high and low failure rates on safety and production availability.

- a high (H) failure rate that is 10 times the initial failure rate;
- a low (L) failure rate that is a tenth of the initial failure rate;
- a high DC equal to 90%;
- a low DC equal to 10%;
- the functional test interval is 1 year.

The tree structure in Fig. 2 shows how the SFF, the safety, and the production availability are affected by high and low values of $\lambda_S$, $\lambda_D$, and DC, respectively. We assume that the production availability is influenced by the spurious trip rate (STR) of the component. For a single component, the STR is given by [15,16]

$$\text{STR} \approx \lambda_{SO} + \lambda_{DD} \tag{4}$$

where $\lambda_{SO}$ is the rate of spurious operation failures [15]. In this case study, we assume that all safe failures give a spurious operation, such that $\lambda_{SO} = \lambda_S$. In addition, we assume that the system is configured such that a trip occurs when a DD-failure is detected [15,16], but other operating philosophies may also be selected [12,15,16].

It is further assumed that safety is measured by the average PFD, which for a single component is [17]

$$\text{PFD} \approx (1 - \text{DC}) \times \frac{\lambda_D \tau}{2} = \frac{\lambda_{DU} \tau}{2} \tag{5}$$

where $\tau$ is the functional test interval. The formula is valid when the component is restored to an "as good as new" condition after each functional test, the test and repair times are negligible compared to the length of the functional test interval, and when safe- and DD-failures are detected immediately and restored within a short time compared to the functional test interval. The PFD is seen to decrease when the dangerous failure rate decreases and/or when the DC, increases. Eq. (5) does not take into account any potential, secondary effects on safety from safe- and DD-failures.

The SFF is calculated from Eq. (1). With the suggested input data, the SFF is either below 60% or above 90%. In Fig. 2, an SFF below 60% is marked as low (L) and above 90% as high (H). We assume that $1 \times 10^{-3}$ is the PFD target for the component, and classify an average PFD below this target as positive for safety (+), and above this target as negative for safety (−). Similarly, we assume that a high rate of safe failures and/or a high rate of DD-failures corresponds to a high STR which is negative for the production availability (−). With the given input data, this means that an STR above $9.1 \times 10^{-6}$ failures per hour is considered as negative for the production availability, and an STR below this rate is considered as positive.

As seen from Fig. 2, a high SFF often has a positive effect on safety, but in some cases, when a high SFF has been derived from high failure rates, the safety may suffer. A high SFF may be both positive and negative for production availability, depending on the magnitude of the rates of safe- and DD-failures. From this simple example, it is evident that the SFF has ambiguous effects on safety and production availability.

*Case study II*: *SFF versus safe design*. The unintended effects of the SFF become even more evident if we take the producer's perspective and decide to improve the SFF of a certain type of component. In this case study, the producer may choose between the following strategies:

(1) The component is redesigned so that internal sub-component failures lead to a safe, rather than a dangerous component failure. In many cases, reduction of the rate of dangerous failures corresponds to a comparable increase in the rate of spurious operation failures (e.g., by installing a spring return so that a solenoid valve automatically goes to the specified safe position upon loss of power).
(2) The component is designed with more reliable sub-components, so that the rates of safe as well as dangerous failures decrease (e.g., by improving a valve actuator with more robust spring materials and better protection against leakage).
(3) The component is redesigned with less reliable sub-components so that the rate of spurious operations increases, while we assume that the rate of dangerous failures remains unchanged (e.g., by reducing the seal quality of a fail-safe valve actuator such that we get more frequent hydraulic leakages).
(4) The producer adds new hardware and software to the current design to detect a fraction of the previously undetectable dangerous failures, such that the DC increases (e.g., by adding an online sonic leak detection system to a valve).
(5) The component is redesigned to make it less vulnerable to spurious operation. We may assume a lower rate of spurious operation, while the rate of dangerous failures remain unchanged (e.g., by improving a valve actuator so that less frequent leakages may be expected).

In Table 2, the effects of these five design changes are shown with respect to "good engineering practice" and SFF. Good engineering practice may be considered as design in accordance with relevant standards and regulations with the purpose of preventing hazardous events [18]. For components used in a SIS application, good engineering practice is a means to ensure safe and reliable components.

The case study shows that some improvements that are in accordance with good engineering practice, for example, cases 2 and 5, have no, or a negative effect on the SFF. This means that the SFF does not encourage such design changes. The case study also shows that modifications leading to a worse design, for example, as shown in case 3, is given credit through a higher SFF. For cases 1 and 4, the SFF responds as expected, that is, the SFF increases when the improvements are in line with good engineering practice.

One may question if there is a logical reasoning behind the relationship between SFF and HFT. HFT is a measure of the *robustness* against component failures, that is, the ability of the SIF to be activated in the presence of dangerous failures in one or more channels. Linking *safe* failures to architecture robustness does not seem reasonable, since the safe failures do not have the potential to prevent the SIF from performing its function. In fact,

**Table 2**
The effect of design modifications on the SFF

| | Good engineering practice? | Effect on the SFF |
|---|---|---|
| Case 1 | Yes. As long as the total failure rate is not increased. | Increases |
| Case 2 | Yes. The valve is expected to be more reliable with respect to dangerous as well as safe failures. | No effect |
| Case 3 | No. The valve will cause more spurious trips, which is not the intention of the standards. | Increases |
| Case 4 | Yes and no. Increasing the DC may also increase the complexity, and potentially introduce new dangerous failure modes. On the other hand, if these aspects are catered for, a higher DC improves safety. | Increases |
| Case 5 | Yes. The valve will cause less process disturbances. | Decreases |

the safe failures may cause the SIF to be activated when this is not intended. Thus, we may claim that there is no well-founded reason for reducing the HFT if the high SFF is based on a high fraction of safe failures.

## 5. Do we need the architectural constraints at all?

The rationale for introducing the architectural constraints is to "*achieve a sufficiently robust architecture, taking into account the level of subsystem complexity*" [1,2]. The underlying concern is that quantitative assessments alone may underestimate the reliability, and as a result, lead to selection of unsafe architectures. The IEC standards [1,2] assume that the reliability increases with increasing HFT. But does the architectural constraints lead to more reliable architectures?

One immediate effect of increasing the HFT is that the STR increases [15]. As mentioned in Section 3, more frequent spurious trips may have a negative effect on safety, due to the secondary effects from process disturbances, like stress on affected physical components as well as on the personnel. The correlation between HFT and reliability improvements may be further questioned in cases where:

- *The SIF is likely to fail due to common cause failures* (*CCF*) *rather than independent failures*. Higher HFT makes the SIF less vulnerable to independent (random) dangerous failures. However, if redundant components share the same or similar design principles, follow-up, or are exposed to same operational and environmental conditions, one may experience that two or more components fail simultaneously. These CCFs [19–21] will reduce the reliability benefit from increasing the HFT.
- *The reliability model is incomplete*. HFT is considered for those components that have been identified to have an effect on the SIS's ability to perform the SIF and, consequently, are included in the reliability model. If the SIS is complex, have complex interactions with other systems, or if we have not put enough effort into understanding the complete SIF loop, we may fail to capture all relevant components. If some of these unidentified components alone may cause failure of the SIF, a higher HFT of the identified components may not lead to a more reliable system.

An additional concern when increasing the HFT is that we add complexity and potentially new vulnerabilities to the SIS. As a result, we may experience that the reliability is reduced rather than increased by raising the HFT.

One argument that may support a higher HFT, at least at first glance, is the potential for systematic failures. Systematic failures are safe and dangerous failures caused by design errors, implementation errors, installation errors, and operation and maintenance related errors. Systematic failures also embrace software failures, and failures that are due to the selection of inappropriate hardware for the current environmental conditions. The IEC standards [1,2] recommend that systematic failures are omitted in the PFD calculations, since they do not have the same predictable characteristics as random hardware failures. HFT can therefore be a means to compensate for systematic failures. Operational experience indicates that a significant fraction of SIS failures are systematic rather than random hardware failures [1,2,12,17]. Some reliability databases, like OREDA [14], therefore include systematic failures in their failure rate predictions. Other reliability databases cover only random hardware failures. This is, for example, the case for MIL-HDBK-217F [22], where the data come from controlled laboratory testing.

The robustness against systematic failures from raising the HFT may not be as high as expected. First of all, the systematic failures may be safe as well as dangerous, which means that the frequency of process disturbances increases with increasing HFT. Secondly, the causes of systematic failures often share the properties of CCF causes [20], and a systematic failure is therefore likely to affect several components rather than a single component. As discussed above, a higher HFT has a limited effect on the reliability of the SIF if a considerable fraction of the failures are due to CCFs.

## 6. Discussion and further work

According to the IEC standards [1,2], the SIS hardware architecture must be selected so that (i) the calculated reliability meets the specified SIL, and (ii) the HFT is according to the architectural constraints. In some cases, the architectural constraints call for higher HFT than is necessary based on the reliability calculations. End users and system integrators have therefore questioned the need for architectural constraints, and whether architectural constraints lead to safer design. Their concern has been addressed and discussed in this article.

The architectural constraints specify a minimum HFT for each subsystem (input elements, logic solver, final elements) based on the SIL target, the component type, and the SFF. The IEC standards use the SFF as a measure of inherent safeness of components, and allow lower HFT for configurations of components with high SFF. This article has critically examined the properties of the SFF in two case studies, and investigated if a high SFF necessarily leads to a safe design. Based on the case studies, we conclude that:

- The SFF is not an adequate indicator of a component's reliability properties. Two components with the same SFF may have quite different characteristics with respect to rate of spurious operations, rate of dangerous failures, and DC.
- A high SFF does not always indicate a safe component, in the same way as a low SFF is not always synonymous with an unsafe component. The SFF may give credit (in terms of increased SFF) to unsafe designs as well as punishment (in terms of unchanged or decreased SFF) for safe designs.

We have argued that reliability models and reliability data may fail to capture all failures of a SIF. One example is that reliability calculations often omit the contribution from systematic failures.

In fact, IEC 61508 suggests that these failures should not be included in reliability calculations, and argue for other means to identify and prevent such failures, for example, use of checklists. The increasing use of PE-logic solvers and smart field devices, will inevitably lead to more failures with systematic causes, introduced during design, construction, and sometimes also during operation, maintenance, and modifications. Adding more HFT to such functions may increase the robustness against systematic failures, but will also increase the system complexity.

A project has recently been initiated to study the relationship between the SFF and the PFD, using Markov methods [23]. It may be useful to explore the results from this project, to gain more insight into the effects of high and low SFF.

More research should be devoted to treat systematic failures in reliability assessments. New methods to predict and analyze systematic failures should be developed. A first steps in this development has been taken by the PDS project [12]. In a new method, the contribution from software failures represents a major challenge. Hardware functions are increasingly being replaced by software implemented functions, to allow new and more flexible technical solutions and to save costs. The cost of writing software code once is lower than the cost of having hardware in all systems. As mainly hardware components are catered for in reliability calculations, it is a need to clarify how the contribution from systematic failures may affect the reliability of SIS.

As a supplement to the architectural constraints, we believe that more attention should be directed to the construction of reliability models, and the system and functional analyses on which the models are based. With more complex features of SIS components it is important to analyze the functionality of each SIS component, rather than assuming a certain behavior, and also to take into account their interactions. Such a qualitative analysis gives two benefits: improved reliability models and improved insight into the SIS functionality.

## Acknowledgments

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

## References

[1] IEC 61508. Functional safety of electrical/electronic/programmable electronic safety-related systems. International Electrotechnical Commission; Geneva: 1998.

[2] IEC 61511. Functional safety—safety instrumented systems for the process industry. International Electrotechnical Commission; Geneva: 2003.

[3] Lundteigen MA, Rausand M. Assessment of hardware safety integrity. In: Proceedings of the 30th ESReDA seminar hosted by SINTEF, Trondheim, Norway, June 7–8, Ispra, Italy: ESReDA, European Commission, Joint Research Centre; 2006. p. 185–98.

[4] Innal F, Dutuit Y, Rauzy A, Signoret J-P. An attempt to understand better and apply some recommendations of IEC 61508 standard. In: Langseth H, Cojazzi G, editors. Proceedings of the 30th ESReDA seminar hosted by SINTEF, Trondheim, Norway, June 7–8, Ispra, Italy. ESReDA, European Commission, Joint Research Centre; 2006. p. 1–16.

[5] Signoret J-P. High integrity pressure protection systems (HIPPS)—making SIL calculations effective. Exploration and Production—oil and gas review (OTC edition). p. 14–7.

[6] CCPS. Guidelines for safe and reliable instrumented protective systems. Hoboken, NJ: Wiley & Center for Chemical Process Safety; 2007.

[7] Goble W, Cheddie H. Safety instrumented systems verification: practical probabilistic calculations. Instrumentation, Systems, and Automation Society. NC: Research Triangle Park; 2005.

[8] Smith DJ, Simpson KGL. Functional safety—a straightforward guide to applying the IEC 61508 and related standards. Burlington, U.K.: Elsevier; 2005.

[9] Van Beurden I, Van Beurden-Amkreutz R. What does proven in use imply? In: Technical papers of ISA, vol. 454. NC, ISA: Research Triangle Park; 2004. p. 1125–39.

[10] OLF-070. Application of IEC 61508 and IEC 61511 in the Norwegian petroleum industry. Technical report, The Norwegian Oil Industry Association, Stavanger, Norway; 2004.

[11] Langeron Y, Barros A, Grall A, Berenguer C. Safe failures impact on safety instrumented systems. In: Aven T, Vinnem J, editors. Risk, reliability, and societal safety, vol. 1. London: Taylor & Francis; 2007. p. 641–8.

[12] Sintef. Reliability prediction methods for safety instrumented systems, PDS method handbook. Trondheim, Norway: Sintef; 2006.

[13] SIS expert answers 5 key user questions. ⟨http://www.flowcontrolnetwork.com⟩; 2006.

[14] OREDA. Offshore reliability data. Det Norske Veritas, Høvik, Norway, OREDA Participants, 4th ed.; 2002.

[15] Lundteigen MA, Rausand M. Spurious activation of safety instrumented systems in the oil and gas industry: basic concepts and formulas. Reliab Eng Syst Saf 2008;93(8):1208–17.

[16] ISA-TR84.00.02. Safety instrumented functions (SIF)—safety integrity level (SIL) evaluation techniques part 4: determining the SIL of a SIF via Markov analysis. Research Triangle Park, NC: The Instrumentation, Systems, and Automation Society; 2002.

[17] Rausand M, Høyland A. System reliability theory; models, statistical methods, and applications. 2nd ed. Hoboken, NJ: Wiley; 2004.

[18] Summers AE. IEC 61511 and the capital project process; a protective management system approach. J Hazardous Mater 2006;130:28–32.

[19] Hokstad P, Rausand M. Common cause failures: status and trends. In: Misra KB, editor. Handbook of performability engineering. London: Springer; 2008 [chapter 39].

[20] Lundteigen MA, Rausand M. Common cause failures in safety instrumented systems on oil and gas installations: implementing defense measures through function testing. J Loss Prev Process Ind 2007;20(3):218–29.

[21] Summers AE, Raney G. Common cause and common sense—designing failure out of your SIS. ISA TECH/EXPO Technol Update Conf Proc 1998;2(6):39–48.

[22] MIL-HDBK-217F. Reliability prediction of electronic equipment. Technical Report, U.S. Department of Defense, Washington, DC; 1991.

[23] Munkeby E. Effect of safe failures on the reliability of safety instrumented systems. Master's thesis, Norwegian University of Science and Technology (NTNU), Trondheim, Norway; 2008.

# Article 6

Reliability assessment of safety instrumented systems in the oil and gas industry: A practical approach and a case study

*Submitted to International Journal of Reliability, Quality and Safety Engineering (IJRQSE)*

# Reliability assessment of safety instrumented systems in the oil and gas industry: A practical approach and a case study

Mary Ann Lundteigen and Marvin Rausand
Department of Production and Quality Engineering,
The Norwegian University of Science and Technology,
NO 7491 Trondheim, Norway

**Abstract**

This article presents a practical approach to reliability assessment of a complex safety instrumented system that is susceptible to common cause failures. The approach is based on fault tree analysis where the common cause failures are included by post-processing the minimal cut sets. The approach is illustrated by a case study of a safety instrumented function of a workover control system that is used during maintenance interventions into subsea oil and gas wells. The case study shows that the approach is well suited for identifying potential failures in complex systems and for including design engineers in the verification of the reliability analyses. Unlike many software tools for fault tree analysis, the approach gives conservative estimates for reliability. The suggested approach represents a useful extension to current reliability analysis methods.

## 1 Introduction

Many oil and gas installations rely on safety instrumented systems (SISs) to respond to hazardous events and mitigate their consequences to humans, the environment, and material assets. Reliability targets are often assigned to each safety instrumented function (SIF) that is performed by a SIS and detailed reliability analyses are carried out to prove compliance to these targets. If the specified target is not met, the analyses should help the design engineers to make improvements to the SIS. Such improvements may be related to physical design changes, changes to the voting logic, improved diagnostic test routines, protection against common cause failures (CCFs), and so forth. An important objective is therefore that the reliability analyses are possible to comprehend by design engineers who are usually not trained in reliability engineering. If the system is already in operation, the analyses should also be comprehensible for operators and maintenance personnel such that the analyses can help them to get an increased awareness to potential failure combinations.

The authors have recently carried out an industry project to determine the reliability of a SIF that is performed by a well workover system. The workover system is used for maintenance interventions into subsea oil and/or gas wells, and the purpose of the SIF is to stop flow from the well when demanded by the operator.

A reliability target for the SIF is usually set according to IEC 61508 and IEC 61511, two widely accepted standards in the oil and gas industry. These standards use safety integrity as a measure of reliability and distinguish between four safety integrity levels (SILs), where SIL 1 is the lowest (least reliable) level and SIL 4 is the highest (most reliable) level. For a SIS in a so-called *low demand* mode of operation [13] that is subject to periodic testing, the reliability target is expressed by the average probability of failure on demand (PFD). For the SIF in this project, the target SIL 2 was specified.

To verify compliance to, for example, SIL 2, one needs to demonstrate by reliability analysis that the PFD is less than $1 \cdot 10^{-2}$. IEC 61508 and IEC 61511 suggest the use of fault tree analysis (FTA), reliability block diagrams (RBD), or Markov methods for this analysis. Methods like Petri Net and Monte Carlo simulations are also sometimes used [2, 3]. The effect of CCFs must be taken care of in the analysis.

The calculations are usually based on approximation formulas, and it is therefore essential that these approximations are *conservative*, such that the "true" PFD is less than the computed PFD. A problem here is that several software tools use non-conservative approximations for systems of periodically tested components.

The objective of this article is to suggest a practical approach for reliability assessment of a low demand, periodically tested, complex SIS that is susceptible to various types of CCFs. The approach must produce a conservative estimate of the system's PFD and be easy to comprehend by practitioners who are not trained in reliability engineering.

The suggested approach is illustrated for the SIF "shut in well flow by the lower riser package upon demand" that is performed by the subsea well workover system mentioned above. For confidentially reasons, the system is slightly altered and anonymized. Additional analyses are required to verify compliance to a SIL, but this article only considers the requirements related to the PFD.

The main focus of this article is the analysis approach. Reliability data that were used in the project, are not included in the article.

The article is organized as follows; Section 2 discusses alternative modeling and calculation approaches, and gives the main arguments for selecting FTA. In Section 3, the approach for making conservative estimation of the PFD is presented as a stepwise procedure. The case study in Section 4 illustrates the application of the approach. Sections 5 and 6 make some final comments and ideas for further work.

# 2 Background for the approach

## 2.1 Selection of modeling approach

Both RBD and FTA are applicable methods for analyzing the reliability of a complex SIF. An RBD often resembles the physical structure of the SIS, and the sequence of the functional blocks in the RBD may be set up to be similar to the sequence the SIS components are activated. When establishing an RBD, we think in terms of functions: "How can this function be achieved?" This may be a strength, but is also a weakness, since it is easy to forget functions that are installed (or should be installed) to protect the main system functions in specific fault situations. Unlike the physical structure, an RBD may include the same component in different sections of the model. This may be confusing for persons who are not familiar with reliability modeling.

When constructing a fault tree, our mindset is different, and we focus on how a function may fail rather than how the function may be achieved [26, 14, 5, 10]. This failure oriented approach is considered more comprehensive and complete than RBD [26] since it is easier to identify failures that are not directly linked to a component function. A fault tree (with only AND and OR gates) can always be transferred to an RBD and visa versa. When the model is established, the two approaches give the same result. Even so, fault trees are easier to understand for persons who are not familiar with reliability analysis, due to the intuitive and structured approach when establishing the fault tree.

An RBD and a fault tree provide a "static picture" of a system function and fault, respectively, and can not easily be used to model systems that are switching between different operational modes or systems with complex maintenance procedures. For such systems, Markov methods are more suitable [15, 26, 6]. For systems with a high number of components, the Markov models will be very large and the multitude of fault states, operational modes, and maintenance modes can be difficult to comprehend by practitioners.

For the current SIF, the reliability analysis was restricted to a single operational mode, the intervention mode. It was further considered to be important to involve design engineers, operators, and maintenance personnel in the analysis to verify the model, increase their awareness of critical failure combinations, and to give them a background to implement design changes and/or modified operational procedures that will improve the system reliability.

Based on these arguments, FTA was found to be the most appropriate modeling approach for the reliability assessment of the SIF.

## 2.2 PFD calculation

Assume that a fault tree for a specified TOP event has been constructed and that $m$ minimal cut sets $\{\mathrm{MC}_1, \mathrm{MC}_2, \ldots, \mathrm{MC}_m\}$ have been identified. This case study is restricted to the technical features of the workover system, and all the basic events in the fault tree are therefore related to technical component failures. In the following, we will therefore refer to the *components* of a cut set rather than the basic events of the cut set.

Let $\mathrm{PFD}_{j,i}$ denote the (average) probability of failure on demand of component $i$ in minimal cut set $j$, for $j = 1, 2, \ldots, m$. Minimal cut $j$ of order $m_j$ is a 1-out-of-$m_j$:G structure, and will only fail when all its $m_j$ components are in a failed state at the same time. To simplify the notation, the cut parallel structure of a minimal cut set is called a *minimal cut*. When all the components in the cut set are independent, the probability of failure on demand of minimal cut $j$ is usually calculated by

$$\mathrm{PFD}_{\mathrm{MC}_j} \approx \prod_{i=1}^{m_j} \mathrm{PFD}_{j,i} \tag{1}$$

Equation (1) is used by many software tools for FTA, but does not give an accurate result [3]. This is due to the well-known Schwartz' inequality saying that "the average of a product is not equal to the product of averages". Equation (1) is therefore an approximation, and the approximation is *non-conservative*.

The average $\mathrm{PFD}_{j,i}$ for a single component that is periodically tested may be calculated as [26]

$$\mathrm{PFD}_{j,i} = \frac{1}{\tau} \int_0^{\tau} \big(1 - \exp(-\lambda_{\mathrm{DU},j,i} \cdot t\big)\, dt \quad \lessapprox \quad \frac{\lambda_{\mathrm{DU},j,i} \cdot \tau}{2} \tag{2}$$

where $\lambda_{\mathrm{DU},j,i}$ is the rate of dangerous undetected (DU) failures of component $i$ in minimal cut $j$, and $\tau$ is the functional test interval. A dangerous (D) failure is a failure that may prevent the execution of a safety function, and when it is also classified as undetected (U), the failure can only be revealed by a functional test or a demand. In this article, all components are covered by the same functional test, and the index $i$ is therefore omitted for the functional test interval $\tau$.

Equation (2) gives a conservative approximation [26] and the approximation is generally considered to be adequate when:

- $\lambda_{\mathrm{DU},j,i} \cdot \tau$ is "small" (i.e., $< 10^{-2}$). For higher values, the approximation might be too conservative.

- The operation is stopped when a DU failure is revealed and not restarted until the failure has been repaired. This means that the function of the component is not demanded while the component is being repaired.

- The functional test is perfect, which means that all DU failures are revealed during the test.

If the operation continues while the component is being repaired such that demands for the component may occur, the unavailability due to the repair downtime must be added to (2). This contribution is approximately $\lambda_{\mathrm{DU},j,i} \cdot \mathrm{MTTR}_{j,i}$, where $\mathrm{MTTR}_{j,i}$ is the mean time required to repair (or restore) a DU failure of component $i$ in minimal cut $j$.

Non-perfect test conditions may be accounted for by introducing a test coverage factor C. This means that a fraction (1 − C) of the DU-failures, remains unrevealed by the test and the unavailability due to these failures must be added to (2) to obtain the actual $\mathrm{PFD}_{\mathrm{MC}_j}$.

Consider a minimal cut $j$ with $m_j$ *independent* components with test interval $\tau$. The $\mathrm{PFD}_{\mathrm{MC}_j}$ of this minimal cut is

$$\begin{aligned}
\mathrm{PFD}_{\mathrm{MC}_j} &= \frac{1}{\tau}\int_0^{\tau} \prod_{i=1}^{m_j} \left(1 - \exp(-\lambda_{\mathrm{DU},j,i} \cdot t\right) dt \\
&\lessapprox \frac{1}{\tau}\int_0^{\tau} \prod_{i=1}^{m_j} \left(\lambda_{\mathrm{DU},j,i} \cdot t\right) dt = \frac{\left(\prod_{i=1}^{m_j} \lambda_{\mathrm{DU},j,i}\right) \cdot \tau^{m_j}}{m_j + 1} \\
&= \frac{\left(\bar{\lambda}_{\mathrm{DU},j} \cdot \tau\right)^{m_j}}{m_j + 1}
\end{aligned} \tag{3}$$

where

$$\bar{\lambda}_{\mathrm{DU},j} = \left(\prod_{i=1}^{m_j} \lambda_{\mathrm{DU},j,i}\right)^{\frac{1}{m_j}} \tag{4}$$

is the *geometric mean* of the $m_j$ DU-failure rates $\lambda_{\mathrm{DU},j,1}, \lambda_{\mathrm{DU},j,2}, \ldots, \lambda_{\mathrm{DU},j,m_j}$.

For a minimal cut $j$ of two independent components with failure rates $\lambda_{\mathrm{DU},j,1}$ and $\lambda_{\mathrm{DU},j,2}$, the average $\mathrm{PFD}_{\mathrm{MC}_j}$ is from (3):

$$\mathrm{PFD}_{\mathrm{MC}_j} \lessapprox \frac{\lambda_{\mathrm{DU},j,1} \cdot \lambda_{\mathrm{DU},j,2} \cdot \tau^2}{3} \tag{5}$$

By combining (1) and (2), we get $\mathrm{PFD}_{\mathrm{MC}_j} \approx \lambda_{\mathrm{DU},j,1} \cdot \lambda_{\mathrm{DU},j,2} \cdot \tau^2/4$ which is a nonconservative approximation. Software tools for FTA that use this approach will therefore get a PFD for this cut set that is around 25% lower than the correct value. This percentage increases with the order $m_j$ of the minimal cut.

The "correct" approximation (3) for a minimal cut of order $m_j$ is obtained by multiplying the result obtained from (1) and (2) by the correction factor

$$\frac{2^{m_j}}{m_j+1} \tag{6}$$

For a minimal cut set of order 2, this corresponds to a correction factor of 4/3.

### 2.3 Modeling of CCFs

CCFs may be modeled explicitly as separate events in the fault tree, or implicitly, by post-processing the minimal cut sets [7, 11, 18, 35, 33]. For systems with several types of common causes, the explicit approach may lead to large fault trees that are difficult to interpret. In addition, it may be easy to overlook, or make incorrect inclusion of, events that are dependent, but located in different branches of the fault tree.

With the implicit approach, the fault tree is kept simple and the CCFs are identified from the minimal cut sets.

IEC 61508 and IEC 61511 recommend the beta-factor model for including CCFs in the calculations. This model assigns a fraction, $\beta$ of the failures of a component to be CCF, and assumes that when a CCF occurs, *all* components in that group will fail due to the same cause. The associated formulas for calculating the PFD are presented in, for example [15, 26, 29].

In practise, we may expect to have CCFs where *not all* redundant components fail. This means that the effect of a CCF may be different for different voted configurations, such as 1-out-of-3:G and 2-out-of-3:G. The PDS method [28, 27] uses a correction factor to adjust the CCF rate for such configurations. In this article, the standard beta-factor model is used, since it gives adequate results, is easy to understand, and the parameter $\beta$ is easy to interpret.

## 3 Stepwise Procedure

This section presents the approach that was developed to analyze the well workover system. The approach has eight steps, each of which represents a stage where an intermediate result may be discussed with design engineers, operators, and maintenance personnel.

### Step 1: System familiarization

System familiarization is always an important part of a reliability analysis. The starting point is to list the SIFs, and to describe the operational modes and conditions where a SIF response may be required. Relevant operational modes may be normal operation, test modes, and contingency modes induced by failures, faults, or operator errors [26].

System familiarization then continues with a review of documentation that describes each SIF, like topology drawings, loop drawings for pneumatic, hydraulic, and electrical hook-up, cause and effects diagrams, and operation manuals. The outcome of the review should describe: The criteria for successful SIF execution, which components that are operated to achieve the SIF, and how these components may fail due to normal degradation, design failures, misuse, or excessive stresses from operations or the environment.

### Step 2: TOP event definition

Based on the system familiarization and description of the SIF, the next task is to define and delimit the TOP event of the fault tree. The TOP event is the non-fulfillment of the SIF, and must be thoroughly discussed with the design engineers to ensure that all participants have a common understanding of the event. The description of the TOP event should answer the following questions [26]: (i) *What* is the TOP event? What is really happening when the TOP event occurs? (ii) *Where* does the TOP event occur? and (iii) *When* does the TOP event occur – during what operation?

The same type of event may occur in more than one operational mode, for example, during start-up and during normal operation. TOP events for these operational modes must be analyzed separately.

### Step 3: Fault tree construction

A fault tree for the TOP event is then constructed in close cooperation with the design engineers and operators.

Fault tree construction is described in several guidelines [18, 14, 12]. The guidelines should be carefully adhered to and a suitable software tool for FTA should be selected. For the analysis of the workover system, CARA FaultTree [32] was used.

### Step 4: Identification and verification of minimal cut sets

Most software tools for FTA have efficient algorithms that can find the minimal cut sets.

The minimal cuts are used as basis for thorough discussions with design engineers and operators. The review is important in order to verify that the fault tree reflects the current design, in the documentation as well as the physical installation, and that the reliability analysts and the personnel designing or working with the system share a common understanding of how the system may fail.

The same component can be a member of several minimal cuts. This means that the minimal cuts become dependent even when the components are independent. The effect on the calculations is discussed in step 7.

### Step 5: Identification of common cause component groups

For each minimal cut, say $\mathrm{MC}_j$, we must determine whether the components of the cut set are independent or dependent. Components that are dependent and share the *same* common failure cause, are included in the *same* common cause component group $\mathrm{CG}_{j,\nu}$, for $j = 1,2,\dots,m$, and $\nu = 1,2,\dots,r_j$, where $r_j$ is the number of different common cause component groups in minimal cut $\mathrm{MC}_j$. To each $\mathrm{CG}_{j,\nu}$, we may assign a corresponding beta factor, $\beta_{j,\nu}$. The index $\nu$ may be omitted when the minimal cut includes a single common cause component group.

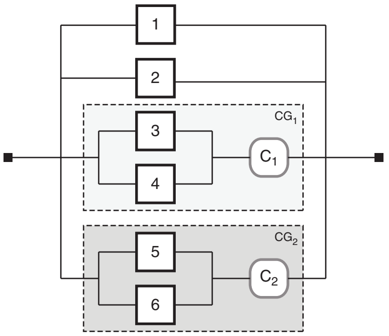


Figure 1: Minimal cut with two common cause component groups

A minimal cut of order six is illustrated in Fig. 1 as an RBD with two common cause component groups, CG$_1$ and CG$_2$, each with two components. The CCF is included as a virtual component in series with the parallel structure comprising the components of the common cause component group [26].

The remaining components, $\mathrm{H}_j = \mathrm{MC}_j \setminus \left(\bigcup_{v=1}^{r_j} \mathrm{CG}_{j,v}\right)$, are the components in MC$_j$ that are considered to be independent. We denote the order of H$_j$ by $k_j^{(I)}$ and the order of CG$_{j,v}$ by $k_{j,v}^{(C)}$. The components in H$_j$ have failure rates $\lambda_{\mathrm{DU,i}}^{(I)}$ for $i = 1,2,\ldots,k_j^{(I)}$ and the components in CG$_{j,v}$ have $\lambda_{\mathrm{DU},j,v,\ell}$ for $v = 1,2,\ldots,r_j$ and $\ell = 1,2,\ldots,k_{j,v}^{(C)}$. For the minimal cut in Fig. 1, $k^{(I)} = 2$, $r = 2$, $k_1^{(C)} = 2$, and $k_2^{(C)} = 2$.

To determine whether or not the components are dependent, we start by looking for common root causes and coupling factors of the various components of the minimal cuts. A root cause is a basic cause of a component failure (e.g., a corrosive environment), while a coupling factor explains why several components are affected by the same root cause (e.g., same design specification, same materials, same environmental exposure).

Several guidelines and checklists for identification of coupling factors and root causes have been developed [1, 4, 30, 31, 25, 24, 19, 20, 17, 8]. Some authors also address various ways to automate the identification and inclusion of CCFs in fault tree analysis, see for example [37, 36, 7, 23, 35, 34, 38, 40, 39]. To analyze potential CCFs within a minimal cut, we first ask if coupling factors are present, and then assess the potential root causes to decide if a CCF is likely to occur.

## Step 6: Determine $\beta_{j,v}$ for CG$_{j,v}$

The beta factor $\beta_{j,v}$ for common cause component group CG$_{j,v}$ should preferably be determined based on plant specific conditions. Checklists have been developed for this purpose, for example in part 6 of IEC 61508, and in [29, 9, 28].

Another approach is to determine a generic $\beta$ based on data bases like OREDA [22] or by expert judgments. OLF 070 [21], a guideline developed by the Norwegian oil and gas industry to support the application of IEC 61508 and IEC 61511, has selected this approach.

## Step 7: Determine $\text{PFD}_{\text{MC}_j}$ for $j = 1, 2, \ldots, m$

Two important assumptions were made for (2) in section 2: That the functional test is perfect and that the operation is stopped while a DU failure is being repaired. This step should start by confirming the validity of these assumptions.

It is therefore important to clarify with design engineers and operators if *all* components are operated during the functional test, to what extent the functional test is capable of revealing *all* DU failures, and if the operation is stopped once a dangerous failure is revealed. If any of these conditions are not according to the assumptions, it is necessary to consider the options that were presented in section 2. In our approach, it is assumed that the assumptions of (2) are valid.

For a minimal cut of order $m_j$, i.e., a 1-out-of-$m_j$:G structure, the approach for calculating the $\text{PFD}_{\text{MC}_j}$ is influenced by:

1. The order $m_j$ of the minimal cut
2. Whether or not the components of the minimal cut are identical
3. Whether or not the components of the minimal cut are dependent
4. Whether or not the components of the minimal cut are tested simultaneously

Based on the factors above, we get the following equations for calculating the average $\text{PFD}_{\text{MC}_j}$ of minimal cut $j$.

**Alternative 1: Independent components**
Consider a minimal cut with $m_j$ independent components with DU failure rates $\lambda_{\text{DU},j,1}, \lambda_{\text{DU},j,2}, \ldots, \lambda_{\text{DU},j,m_j}$ and assume that all the components are tested at the same time with test interval $\tau$. In this case, (3) and (4) apply directly.

**Alternative 2: Identical and dependent components**
Consider a minimal cut with $m_j$ identical and dependent components with DU failure rate $\lambda_{\text{DU},j}$ and beta factor $\beta_j$. Assume that all the components of the minimal cut are tested simultaneously with test interval $\tau$. The PFD for this structure, $\text{PFD}_{\text{MC}_j}$, then becomes [26]:

$$\text{PFD}_{\text{MC}_j} \lessapprox \frac{\left((1-\beta_j)\lambda_{\text{DU},j} \cdot \tau\right)^{m_j}}{m_j + 1} + \frac{\beta_j \lambda_{\text{DU},j} \cdot \tau}{2} \tag{7}$$

**Alternative 3: Non-identical and dependent components**
In some cases, the components of a minimal cut are non-identical but still vulnerable to the same common cause of failure. One example is that vibration may lead to failure of two different types of sensors. Generally, this beta factor should be smaller than for identical components, as "diverse redundancy" gives a lower degree of dependency or coupling [28].

Some care must be taken when calculating the contribution from CCFs with the beta factor model. Some authors have proposed that the beta factor is a fraction of the geometric mean of the failure rates of the components [8]. This approach may be adequate when the component failure rates are similar, but may lead to a CCF rate that is higher than the lowest component failure rate when the failure rates are different.

To overcome this problem, we define the beta factor to be a fraction of the *lowest* component failure rate as this rate limits how often a parallel structure of components fails simultaneously.

Consider a minimal cut $\mathrm{MC}_j$ where all components are dependent and non-identical such that they belong to the same common cause component group with $\beta_j$. In this case, the $\mathrm{PFD}_{\mathrm{MC}_j}$ becomes:

$$\begin{aligned}\mathrm{PFD}_{\mathrm{MC}_j} \quad \approx \quad & \frac{\left[\left(1-\beta_j\right)\bar{\lambda}_{\mathrm{DU},j}\cdot\tau\right]^{m_j}}{m_j+1} \\ & +\beta_j\cdot\lambda_{\mathrm{DU},j}^{\min}\cdot\frac{\tau}{2}\end{aligned} \tag{8}$$

where

$$\lambda_{\mathrm{DU},j}^{\min}=\min_{i\in\mathrm{MC}_j}\{\lambda_{\mathrm{DU},j,i}\} \tag{9}$$

is the lowest DU failure rate in $\mathrm{MC}_j$.

**Alternative 4: More complex minimal cuts**

A minimal cut may have more than one common cause component group or include independent as well as dependent components. In this case, it is not possible to apply (7) and (8) directly.

The proposed approach may be illustrated by using Fig. 1 as basis. The minimal cut in Fig. 1 has "virtual" cut sets of order 4, 5, and 6. For a general cut set, the lowest order is $k_j^{(I)}+r_j$. Since we assume that the common cause component groups within a minimal cut are independent, we can now find the probability of failure on demand, $\mathrm{PFD}_{\mathrm{MC}_j}$ for minimal cut $j$ by using formulas similar to (3) for each of the "virtual" minimal cuts sets in $\mathrm{MC}_j$. For the virtual cut with the lowest order, the PFD is

$$\mathrm{PFD}_{\mathrm{MC}_j}^{(1)}\approx\frac{\left(\prod_{i=1}^{k_j^{(I)}}\lambda_{j,i}^{(I)}\cdot\prod_{v=1}^{r_j}\beta_{j,v}\cdot\lambda_{\mathrm{DU},j}^{\min,v}\right)\tau^{k_j^{(I)}+r_j}}{k_j^{(I)}+r_j+1} \tag{10}$$

where $\lambda_{\mathrm{DU},j}^{\min,v}$ is the lowest DU failure rate in $\mathrm{CG}_{j,v}$ in minimal cut $\mathrm{MC}_j$.

For the virtual cut with the lowest order in Fig. 1, $\{1,2,\mathrm{C}_1,\mathrm{C}_2\}$, the PFD becomes (the index $j$ has been omitted)

$$\mathrm{PFD}_{\mathrm{MC}}^{(1)}\approx\frac{\left(\lambda_1^{(I)}\lambda_2^{(I)}\beta_1\beta_2\lambda_{\mathrm{DU}}^{\min,1}\lambda_{\mathrm{DU}}^{\min,2}\right)\tau^4}{5} \tag{11}$$

The PFD of the other virtual cuts can be found in a similar way. Consider the virtual minimal cut $\{1,2,3,4,\mathrm{C}_2\}$ in Fig. 1. Here, the PFD becomes

$$\mathrm{PFD}_{\mathrm{MC}}^{(2)}\approx\frac{\left(\lambda_{\mathrm{DU},1}^{(I)}\cdot\lambda_{\mathrm{DU},2}^{(I)}(1-\beta_1)^2\lambda_{\mathrm{DU},1,1}\lambda_{\mathrm{DU},1,2}\beta_2\lambda_{\mathrm{DU}}^{\min,2}\right)\tau^5}{6} \tag{12}$$

For the virtual cut $\{1,2,C_1,5,6\}$, the PFD is

$$\text{PFD}_{\text{MC}}^{(3)} \approx \frac{\left(\lambda_{\text{DU},1}^{(I)} \cdot \lambda_{\text{DU},2}^{(I)}(1-\beta_2)^2\lambda_{\text{DU},2,1}\lambda_{\text{DU},2,2}\beta_1\lambda_{\text{DU}}^{\text{min},1}\right)\tau^5}{6} \tag{13}$$

Consider the virtual minimal cut of order 6, $\{1,2,3,4,5,6\}$. Here, the PFD becomes:

$$\text{PFD}_{\text{MC}}^{(4)} \approx \frac{\left(\lambda_{\text{DU},1}^{(I)} \cdot \lambda_{\text{DU},2}^{(I)}(1-\beta_1)^2\lambda_{\text{DU},1,1}\lambda_{\text{DU},1,2}(1-\beta_2)^2\lambda_{\text{DU},2,1}\lambda_{\text{DU},2,2}\right)\tau^6}{7} \tag{14}$$

Since (12), (13), and (14) have a higher order than (11), their PFD will usually be small compared to $\text{PFD}_{\text{MC}}^{(1)}$. In many applications, we can therefore omit these virtual cuts.

The $\text{PFD}_j$ of a minimal cut $j$ can be calculated by the "upper bound approximation" formula which is available in most software tools for FTA.

$$\text{PFD}_{\text{MC}_j} \approx 1 - \prod_{\text{All``virtual''cuts } k}\left(1-\text{PFD}_{\text{MC}_j}^{(k)}\right) \tag{15}$$

This approximation formula is slightly conservative, and this may compensate for omitting higher order virtual cuts.

**Non-simultaneous testing** The four alternatives assume that all components are tested at the same time. This assumption is valid for most SIFs in the oil and gas industry, and was valid for the case study. Components that are tested at different times and with different test intervals will give more complex formulas. To calculate the PFD, we can use the same approach as the one derived for staggered testing in [26]. The approach is straightforward, but the calculation will, in most cases, require the use of a computer.

## Step 8: Calculate system $\text{PFD}_{\text{SIF}}$

The $\text{PFD}_{\text{SIF}}$ can now be found by using the "upper bound approximation" on the minimal cuts $\text{MC}_1, \text{MC}_2, \ldots, \text{MC}_m$.

$$\text{PFD}_{\text{SIF}} \lessapprox 1 - \prod_{j=1}^{m}\left(1-\text{PFD}_{\text{MC}_j}\right) \tag{16}$$

**Dependency between minimal cuts** So far, we have not discussed dependency between minimal cuts. There are two main reasons why the minimal cuts may be dependent. One reason is that the same component may be a member of more than one minimal cut. The corresponding minimal cuts will therefore be (positively) dependent even when all the components are independent. The other reason is that different components that are members of different minimal cut sets may be exposed to the same CCF. In both cases, the minimal cut sets will have a positive dependency that can be described by so-called *associated variables*. This type of dependency is thoroughly discussed in [26], where it is also shown that the approximation in (16) is conservative also in this case.

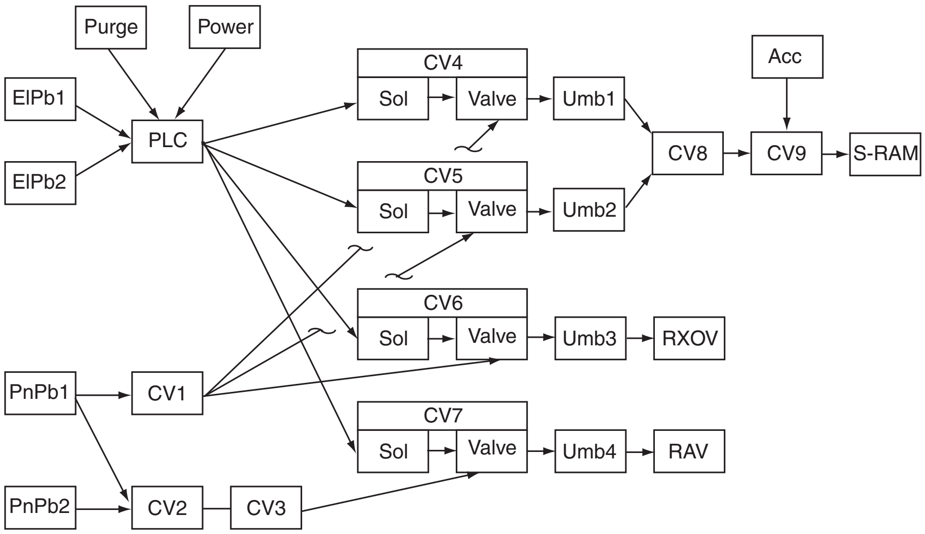


Figure 2: Simplified functional block diagram of the isolation function

# 4 Application of the approach

This section describes how the suggested approach was applied to the SIF that is performed by the workover system. We assume that all components are periodically tested and that the functional tests are perfect in the sense that all failures are revealed by the test. All failure rates are assumed to be constant and demands for the SIF are assumed to occur so seldom that we can consider the system to be a low demand system [13].

## Description of the SIF

During a workover intervention, a workover riser is connected to the subsea wellhead. The lower riser package that is attached to the lower end of the riser includes a number of valves that are operated by the workover control system.

The SIF analyzed in the case study was “*to shut in the well flow by the lower riser package upon a demand during intervention mode*”.

The shear ram and at least one of the riser annulus valve and the riser cross over valve in the lower riser package must close to achieve successful shut in of well. When the shear ram is operated, it will also cut any wires that are in the production tubing.

## Step 1: System familiarization

The simplified functional block diagram in Fig. 2 was developed based on a detailed review of drawings and documentation of the workover system.

The following components are used to implement the function (Notation used in Fig. 2 is shown in parentheses):

- A shear ram (S-RAM) used to cut the wireline string and isolate the well.

- Equipment used to activate the shear ram including a shuttle valve (CV8), subsea mounted hydraulic accumulators (Acc), and a subsea mounted control valve (CV9).
- A riser annulus valve (RAV) and a riser crossover valve (RXOV) that are installed in the annulus bore lines.
- Umbilical lines, two lines for operating the shear ram (Umb1 and Umb2) and one line for each of the two valves RXOV (Umb3) and RAV (Umb4).
- A hydraulic power unit.
- An electrical power supply (Power). The electric power is supplied from the oil and gas installation or rig. In addition, there is a dedicated un-interruptible power supply.
- Air supply from the rig or platform (Purge) that is used to supply control pressure and maintain overpressure in the workover container and the programmable logic controller (PLC) cabinet.
- Equipment for electrical activation of emergency function, including:
  - Two push-buttons for electrical activation (ElPb1 and ElPb2)
  - One PLC
  - Four pulse operated hydraulic control valves, two of which operate the shear ram (CV4 and CV5), one that operates the RXOV (CV6) and one that operates the RAV (CV7).
- Equipment for pneumatic activation of emergency function, including:
  - Two push-buttons for pneumatic activation (PnPb1 and PnPb2)
  - Two pneumatic operated hydraulic control valves (CV1 and CV3)
  - One pneumatically operated pneumatic control valve (CV2)

The isolation at the lower riser package is successful when: (1) the shear ram closes and (2) one of the two valves RAV or RXOV closes. The RAV and RXOV are kept in open position as long as their actuators are pressurized, and will automatically close when their actuators are depressurized. The shear ram starts to close when the subsea mounted control valve (CV9) is depressurized. The shuttle valve (CV8) merges the two umbilical lines to a single line to the control valve. When the control valve (CV9) is depressurized, it switches over and allows the hydraulic accumulators to pressurize the shear ram actuators that operates the two knives. The shear ram including knives and knife actuators are referred to as one unit (S-RAM).

Unrestricted return of hydraulic fluids from the S-RAM, the RAV, and the RXOV and back to the rig or platform is important. As the same umbilical lines are used for supply and return of hydraulics, it is important to avoid any sharp bends on the umbilicals. The RAV and RXOV are operated by separate umbilicals, while the shear-ram has two umbilicals available.

The electrical push-buttons (ElPb1 and ElPb2) as well as the pneumatic push-buttons (PnPb1 and PnPb2) are voted 1-out-of-2:G, which means that the emergency function is initiated (electrically or pneumatically) upon pressing one of the two push-buttons. The PLC reads the electrical push-button signals and sends a pulse signal to the pulse operated valves (CV4, CV5, CV6, CV7). These valves are split into two parts in Fig. 2, the solenoid (sol) part and the hydraulic (hydr) valve part. The reason is that the valve part is a common component for pneumatic as well as electrical initiation of workover isolation, since the hydraulic return in both cases must pass through this valve. To operate the shear-ram, it is necessary that either CV4 or CV5 functions. The pulse operated valves are not able to switch and start depressurizing the hydraulic lines upon loss of communication with the PLC. This means that they are not fail-safe. Loss of electric power to the PLC may therefore prevent electric activation of the emergency function.

Upon pressing one of the two pneumatic push-buttons, the pilot lines to the pneumatic operated valves CV1 and CV2 are depressurized. Upon loss of pilot signal, the pneumatic operated valve CV1 starts to depressurize hydraulic supply to the shear-ram and the RXOV. The hydraulic return must pass through the pulse operated valves (CV4, CV5, and CV6), and a restriction through these valves may prevent successful depressurization upon electric as well as pneumatic activation. The second pneumatic operated valve, CV2, depressurizes the pilot line to the pneumatic operated valve CV3. Upon loss of pilot signal, CV3 starts to depressurize the hydraulic supply to the RAV. Also in this case, the hydraulic return must pass through CV7. A restriction in the valve part of CV7 may therefore prevent successful depressurization upon electrical as well as pneumatic activation.

The PLC is installed in an environment that may contain hydrocarbon gases. The PLC panel and the container unit are therefore protected by overpressure. Upon loss of overpressure in the PLC cabinet, the PLC shuts down. Loss of overpressure may therefore lead to unsuccessful electrical activation of the emergency function.

### Step 2: Definition of TOP event

Based on system familiarization, the following TOP event for the fault tree was formulated: *"Fail to shut in the well flow by the lower riser package upon a demand during intervention mode"*.

### Step 3: Fault tree construction

The top structure of the fault tree in Fig. 3 was established and shows how failures of the main elements, the shear ram, the RXOV, and/or the RAV, may lead to the TOP event.

The next level of the fault tree, i.e., the fault trees associated with the shear ram failure, the RXOV failure, and the RAV failure are shown in Figs. 4, 5, and 6, respectively. The fault trees were all constructed in close cooperation with a design engineer, and also verified with operators in field to check that the documentation corresponded to the physical installation.

The basic events of the fault trees are named according to the physical components, but they only represent the dangerous failure modes of the components.

### Step 4: Identification of minimal cut sets

The minimal cut sets that are listed in Table 1 were generated using CARA FaultTree [32]. Many FTA software tools have a default cut off criterion for listing minimal cut sets – based on the order of the cut set. When components may be dependent, it is

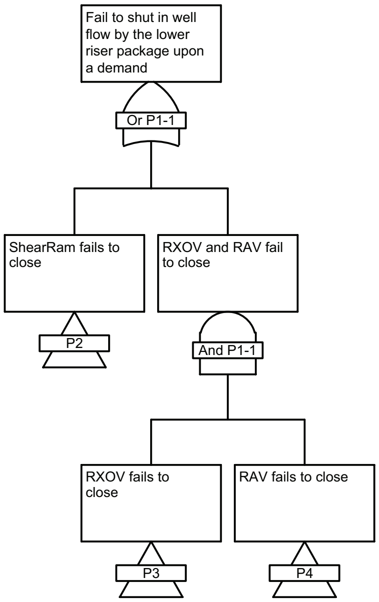

Fail to shut in well flow by the lower riser package upon a demand
Or P1-1
ShearRam fails to close
RXOV and RAV fail to close
P2
And P1-1
RXOV fails to close
RAV fails to close
P3
P4

Figure 3: Top structure of fault tree for the workover isolation function

Table 1: Minimal cut sets (MCS)

| No | Components | No | Components | No | Components |
|---|---|---|---|---|---|
| 1 | S-RAM | 25 | CV5-sol,P**nPb1,PnPb2** | 49 | RXOV,CV7-sol,CV3 |
| 2 | Acc | 26 | PLC,**PnPb1,PnPb2** | 50 | PLC,RXOV,CV2 |
| 3 | CV9 | 27 | Purge,**PnPb1,PnPb2** | 51 | PLC,RXOV,CV3 |
| 4 | CV8 | 28 | Power,**PnPb1,PnPb2** | 52 | Purge,RXOV,CV2 |
| 5 | **Umb1,Umb2** | 29 | Umb3,CV7-sol,CV2 | 53 | Purge,RXOV,CV3 |
| 6 | Umb1,CV5-hydr | 30 | Umb3,CV7-sol,CV3 | 54 | Power,RXOV,CV2 |
| 7 | CV4-hydr,Umb2 | 31 | PLC,Umb3,CV2 | 55 | Power,RXOV,CV3 |
| 8 | **CV4-hydr,CV5-hydr** | 32 | PLC,Umb3,CV3 | 56 | **ElPB1,ElPb2**,Umb3,CV2 |
| 9 | CV4-sol,CV1 | 33 | Purge,Umb3,CV2 | 57 | {**ElPB1,ElPb2**},{**PnPb1,PnPb2**} |
| 10 | CV5-sol,CV1 | 34 | Purge,Umb3,CV3 | 58 | **ElPB1,ElPb2**,Umb3,CV3 |
| 11 | PLC,CV1 | 35 | Power,Umb3,CV2 | 59 | **PnPb1,PnPb2**,Umb3,Cv7-sol |
| 12 | Purge,CV1 | 36 | Power,Umb3,CV3 | 60 | **ElPB1,ElPb2**,CV6-hydr,CV2 |
| 13 | Power,CV1 | 37 | CV6-hydr,CV7-sol,CV2 | 61 | **ElPB1,ElPb2**,CV6-hydr,CV3 |
| 14 | **Umb3,Umb4** | 38 | CV6-hydr,CV7-sol,CV3 | 62 | **PnPb1,PnPb2**,CV6-hydr,Cv7-sol |
| 15 | Umb3,CV7-hydr | 39 | PLC,CV6-hydr,CV2 | 63 | **PnPb1,PnPb2**,CV6-sol,Umb4 |
| 16 | Umb3,RAV | 40 | PLC,CV6-hydr, CV3 | 64 | **PnPb1,PnPb2**,CV6-sol,CV7-hydr |
| 17 | CV6-hydr,Umb4 | 41 | Purge,CV6-hydr, CV2 | 65 | {**PnPb1,PnPb2**},{**Cv6-sol,Cv7-sol**} |
| 18 | **CV6-hydr,CV7-hydr** | 42 | Purge,CV6-hydr, CV3 | 66 | **PnPb1,PnPb2**,CV6-sol,RAV |
| 19 | CV6-hydr,RAV | 43 | Power,CV6-hydr, CV2 | 67 | CV1,**CV6-sol,CV7-sol**,CV2 |
| 20 | RXOV,Umb4 | 44 | Power,CV6-hydr, CV3 | 68 | CV1,**CV6-sol,CV7-sol**,CV3 |
| 21 | RXOV,CV7-hydr | 45 | CV1, CV6-sol,Umb4 | 69 | **ElPB1,ElPb2**,RXOV,CV2 |
| 22 | **RXOV,RAV** | 46 | CV1,CV6-sol,CV7-hydr | 70 | **ElPB1,ElPb2**,RXOV,CV3 |
| 23 | **ElPB1,ElPb2**,CV1 | 47 | CV1,CV6-sol,RAV | 71 | **PnPb1,PnPb2**,RXOV,CV7-sol |
| 24 | CV4-sol,**PnPb1,PnPb2** | 48 | RXOV,CV7-sol,CV2 | | |

important to review *all* minimal cut sets, as a CCF reduces the order of the minimal cut set.

The minimal cut sets were reviewed together with the design engineer and op-

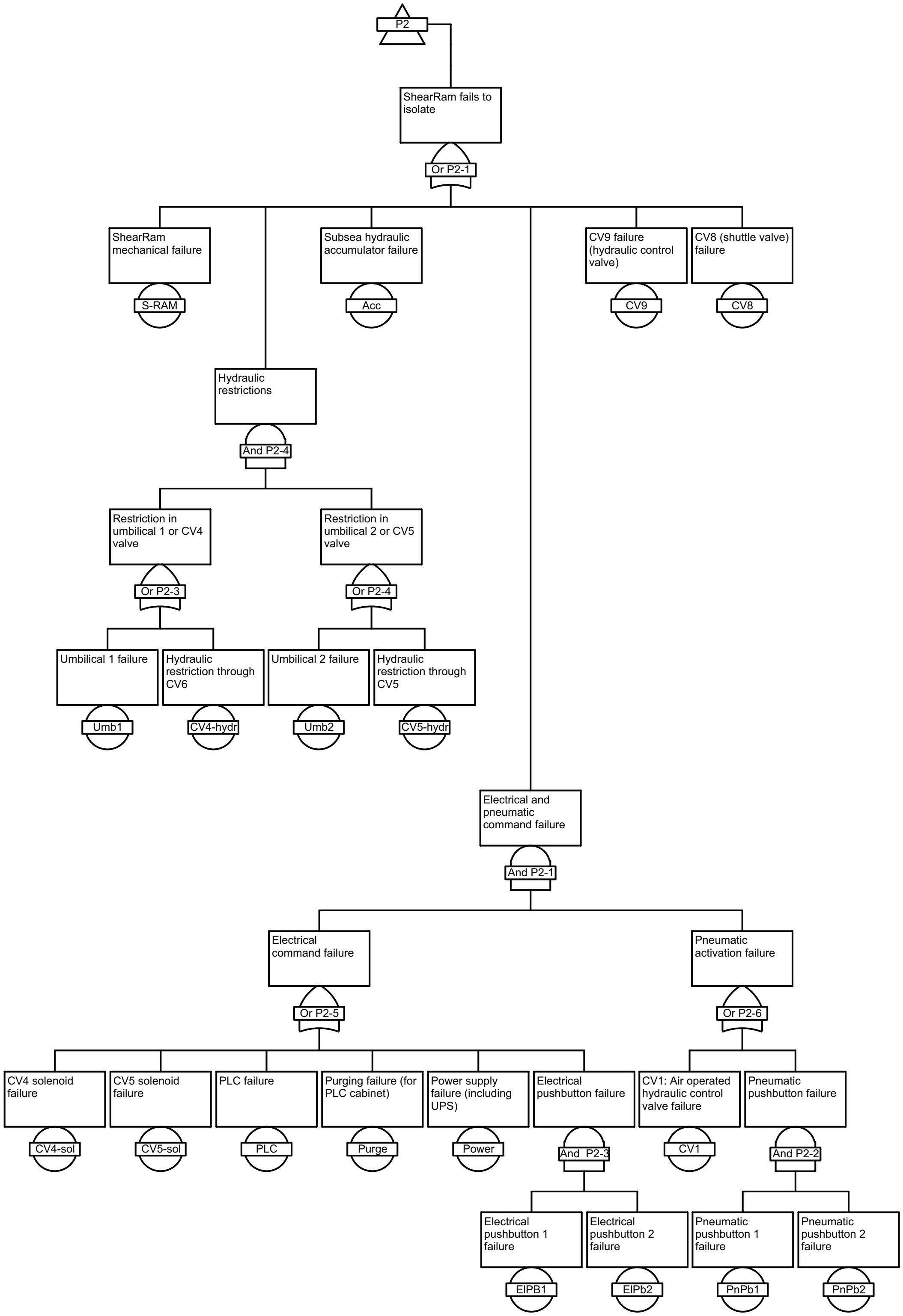

P2
ShearRam fails to isolate
Or P2-1
ShearRam mechanical failure
S-RAM
Subsea hydraulic accumulator failure
Acc
CV9 failure (hydraulic control valve)
CV9
CV8 (shuttle valve) failure
CV8
Hydraulic restrictions
And P2-4
Restriction in umbilical 1 or CV4 valve
Or P2-3
Restriction in umbilical 2 or CV5 valve
Or P2-4
Umbilical 1 failure
Umb1
Hydraulic restriction through CV6
CV4-hydr
Umbilical 2 failure
Umb2
Hydraulic restriction through CV5
CV5-hydr
Electrical and pneumatic command failure
And P2-1
Electrical command failure
Or P2-5
Pneumatic activation failure
Or P2-6
CV4 solenoid failure
CV4-sol
CV5 solenoid failure
CV5-sol
PLC failure
PLC
Purging failure (for PLC cabinet)
Purge
Power supply failure (including UPS)
Power
Electrical pushbutton failure
And P2-3
CV1: Air operated hydraulic control valve failure
CV1
Pneumatic pushbutton failure
And P2-2
Electrical pushbutton 1 failure
ElPB1
Electrical pushbutton 2 failure
ElPb2
Pneumatic pushbutton 1 failure
PnPb1
Pneumatic pushbutton 2 failure
PnPb2

Figure 4: Fault tree for activation of shear ram (P2)

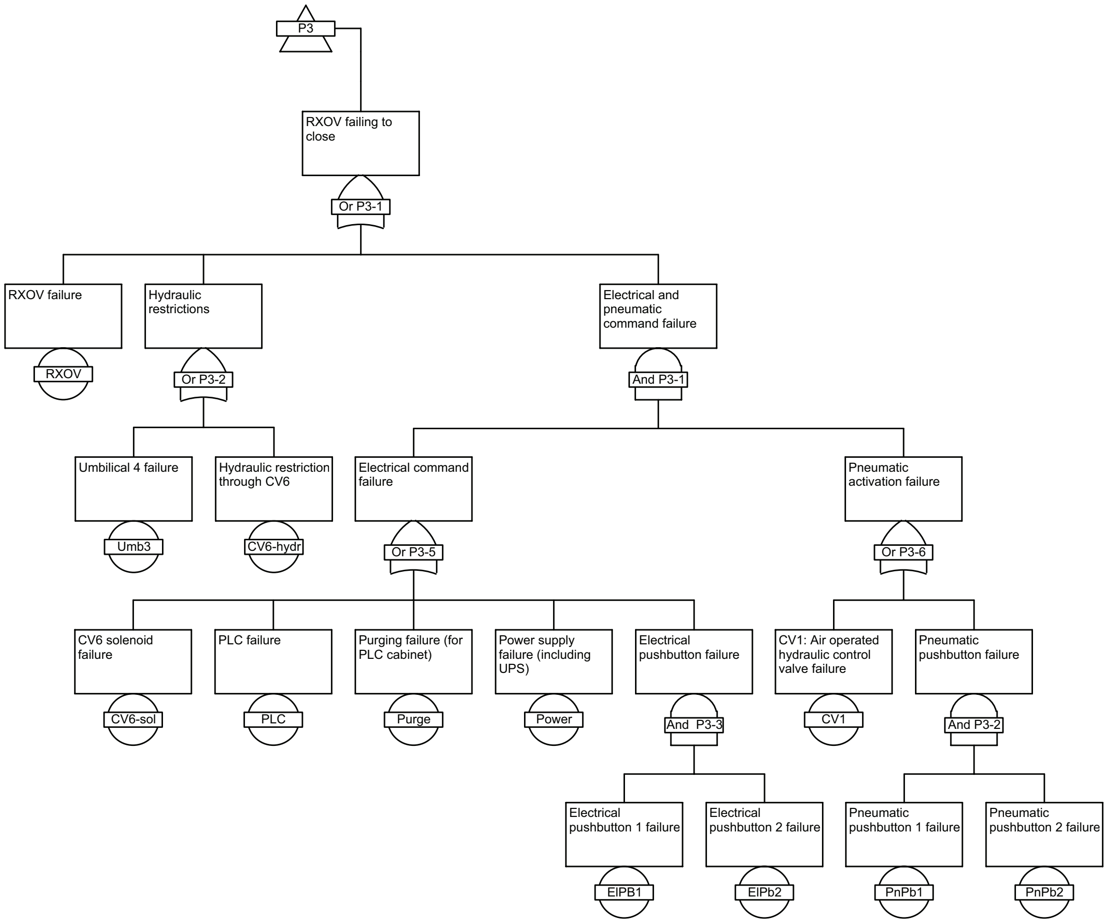

P3
RXOV failing to close
Or P3-1
RXOV failure
RXOV
Hydraulic restrictions
Or P3-2
Electrical and pneumatic command failure
And P3-1
Umbilical 4 failure
Umb3
Hydraulic restriction through CV6
CV6-hydr
Electrical command failure
Or P3-5
Pneumatic activation failure
Or P3-6
CV6 solenoid failure
CV6-sol
PLC failure
PLC
Purging failure (for PLC cabinet)
Purge
Power supply failure (including UPS)
Power
Electrical pushbutton failure
And P3-3
CV1: Air operated hydraulic control valve failure
CV1
Pneumatic pushbutton failure
And P3-2
Electrical pushbutton 1 failure
ElPB1
Electrical pushbutton 2 failure
ElPb2
Pneumatic pushbutton 1 failure
PnPb1
Pneumatic pushbutton 2 failure
PnPb2

Figure 5: Fault tree for activation of RXOV (P3)

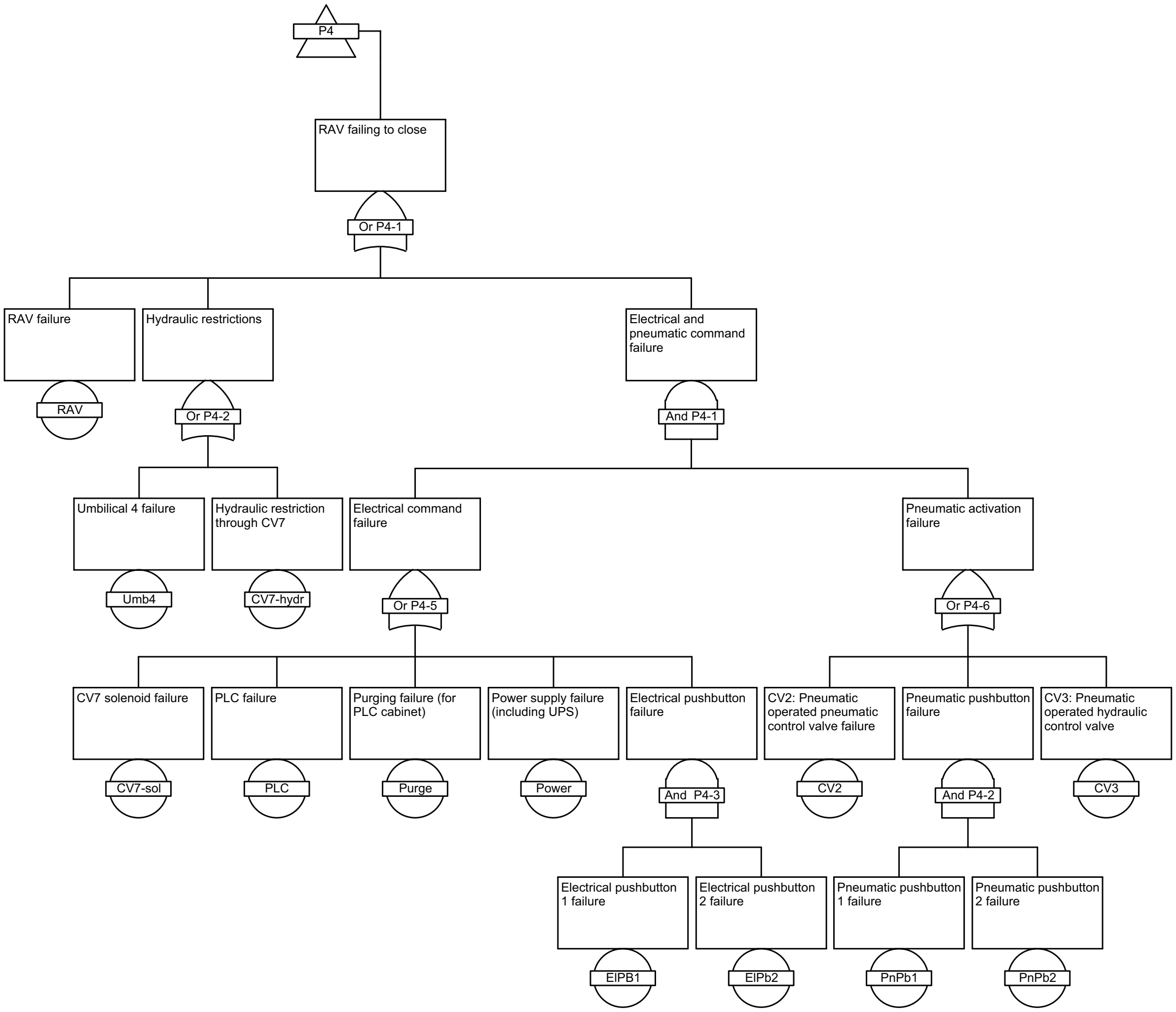

P4
RAV failing to close
Or P4-1
RAV failure
Hydraulic restrictions
Electrical and pneumatic command failure
RAV
Or P4-2
And P4-1
Umbilical 4 failure
Hydraulic restriction through CV7
Electrical command failure
Pneumatic activation failure
Umb4
CV7-hydr
Or P4-5
Or P4-6
CV7 solenoid failure
PLC failure
Purging failure (for PLC cabinet)
Power supply failure (including UPS)
Electrical pushbutton failure
CV2: Pneumatic operated pneumatic control valve failure
Pneumatic pushbutton failure
CV3: Pneumatic operated hydraulic control valve
CV7-sol
PLC
Purge
Power
And P4-3
CV2
And P4-2
CV3
Electrical pushbutton 1 failure
Electrical pushbutton 2 failure
Pneumatic pushbutton 1 failure
Pneumatic pushbutton 2 failure
ElPB1
ElPb2
PnPb1
PnPb2

Figure 6: Fault tree for activation of RAV (P4)

erators to verify that the failure combinations of the fault tree corresponded to their understanding of how the system may fail.

## Step 5: Identification of Common Cause Component Groups

The minimal cut sets were reviewed to identify components that may fail due to a common cause. In the analysis, we mainly focused on the coupling factor "similar or same design". Components that share the same (potential) cause of failure were included in the same common cause component group.

The identified common cause component groups are shown in bold in Table 1. Where two common cause component groups are present within the same minimal cut set, they are put within separate brackets. For example, minimal cut set 57 has two common cause component groups; $\mathrm{CG}_{57,1}$ = {ElPb1, ElPb2} and $\mathrm{CG}_{57,2}$ = {PnPb1, PnPb2}.

## Step 6: Determination of $\beta_{j,v}$

We used OLF 070 [21] as basis for selecting $\beta_{j,v}$ values. For many field devices, a $\beta$ of 5% is suggested. This value was therefore used if no other information was available that would indicate a higher or lower $\beta$.

One exception was for the pulse-operated valves, where $\beta$ was set equal to 10%. A careful review of reported failures for these components indicated some potential design weaknesses, and we therefore assumed that these valves might be more vulnerable to CCF than indicated by the generic data.

Using minimal cut set 65 as illustration, this means that $\beta_{65,1}$ was set equal to 5% and and $\beta_{65,2}$ equal to 10%.

## Step 7: Calculate PFD$_j$

For each minimal cut set $j$ we calculated $\mathrm{PFD}_{\mathrm{MC}_j}$. In the following, some of the resulting equations are illustrated, using minimal cut sets 1, 5, 16, 27, and 57 as examples.

### Equation for minimal cut 1:

Minimal cut 1, {S-RAM}, has only one component. By using (3), with $m_j = 1$, and $\lambda_{\mathrm{DU},1} = \lambda_{\mathrm{DU,S-RAM}}$, the $\mathrm{PFD}_{\mathrm{MC}_1}$ is

$$\mathrm{PFD}_{\mathrm{MC}_1} \approx \frac{\lambda_{\mathrm{DU,S-RAM}} \cdot \tau}{2} \tag{17}$$

### Equation for minimal cut 5:

Minimal cut 5, {Umb1, Umb2}, has two components involving two umbilicals of the same type with the same failure rate, $\lambda_{\mathrm{DU,Umb}}$. Both components are therefore included in the same common cause component group, $\mathrm{CG}_5$: {Umb1, Umb2} with $\beta_5$ and $k_5^{(C)} = 2$. By using (7), the $\mathrm{PFD}_{\mathrm{MC}_5}$ is

$$\text{PFD}_{\text{MC}_5} \approx \frac{\left[(1-\beta_5)\lambda_{\text{DU,Umb}} \cdot \tau\right]^2}{3} + \frac{\beta_5 \lambda_{\text{DU,Umb}} \cdot \tau}{2} \tag{18}$$

**Equation for minimal cut 16:**

Minimal cut 16, {Umb3, RAV}, has two different components, umbilical 3 and RAV with different failure rates, $\lambda_{\text{DU,Umb}}$ and $\lambda_{\text{DU,RAV}}$, and we assume that they will not fail due to CCF. By using (3), the $\text{PFD}_{\text{MC}_{16}}$ is

$$\text{PFD}_{\text{MC}_{16}} \approx \frac{\lambda_{\text{DU,Umb}}\lambda_{\text{DU,RAV}} \cdot \tau^2}{3} \tag{19}$$

**Equations for minimal cut 27:**

Minimal cut 27, {Purge,PnPb1,PnPb2}, has three components involving two pneumatic push buttons and the purge system. We assume that the push buttons may fail due to CCF, such that $\text{CG}_{27}$ become {PnPb1,PnPb2} with $\beta_{27}$, and that the purge system is independent of PnPb1 and PnPb2.

By using (10) – (14) with $k_{27}^{(I)} = 1$, $r_{27} = 1$, $\lambda_{\text{DU},27} = \lambda_{\text{DU,Purge}}$ and $\lambda_{\text{DU},27,1}^{(C)} = \lambda_{\text{DU},27,2}^{(C)} = \lambda_{\text{DU,PnPb}}$, the PFD of the virtual cuts is

$$\text{PFD}_{\text{MC}_{27}}^{1} \approx \frac{\lambda_{\text{DU,Purge}} \cdot \beta_{27}\lambda_{\text{DU,PnPb}} \cdot \tau^2}{3} \tag{20}$$

$$\text{PFD}_{\text{MC}_{27}}^{2} \approx \frac{\lambda_{\text{DU,Purge}}(1-\beta_{27})^2\lambda_{\text{DU,PnPb}}^2 \cdot \tau^3}{4} \tag{21}$$

$\text{PFD}_{\text{MC}_{27}}$ is found by inserting (20) and (21) into (15).

**Equations for minimal cut 57:**

Minimal cut 57, {ElPb1, ElPb2, PnPb1, PnPb2}, has four components involving two electrical and two pneumatic push buttons. The components are dependent, but assigned to two different common cause component groups, $\text{CG}_{57,1}$: {ElPB1, ElPb2} with $\beta_{57,1}$ and $\text{CG}_{57,2}$: {PnPb1, PnPb2} with $\beta_{57,2}$ since electrical push buttons and pneumatic push buttons are based on different design principles.

By using (10) – (14) with $k_{57}^{(I)} = 0$, $k_{57,1}^{(C)} = 2$, $k_{57,2}^{(C)} = 2$, $r_{57} = 2$, $\lambda_{\text{DU},57,1,1} = \lambda_{\text{DU},57,1,2} = \lambda_{\text{DU,ElPb}}$, and $\lambda_{\text{DU},57,2,1} = \lambda_{\text{DU},57,2,2} = \lambda_{\text{DU,PnPb}}$, the PFD of the virtual cuts is

$$\text{PFD}_{\text{MC}_{57}}^{1} \approx \frac{\beta_{57,1}\lambda_{\text{DU,ElPb}}\beta_{57,2}\lambda_{\text{DU,PnPb}} \cdot \tau^2}{3} \tag{22}$$

$$\text{PFD}_{\text{MC}_{57}}^{2a} \approx \frac{(1-\beta_{57,1})^2\lambda_{\text{DU,ElPb}}^2\beta_{57,2}\lambda_{\text{DU,PnPb}} \cdot \tau^3}{4} \tag{23}$$

$$\text{PFD}_{\text{MC}_{57}}^{2b} \approx \frac{\beta_{57,1}\lambda_{\text{DU,ElPb}}(1-\beta_{57,2})^2\lambda_{\text{DU,PnPb}}^2 \cdot \tau^3}{4} \tag{24}$$

$$\mathrm{PFD}^{3}_{\mathrm{MC}_{57}} \approx \frac{(1-\beta_{57,1})^2\lambda^2_{\mathrm{DU,ElPb}}(1-\beta_{57,2})^2\lambda^2_{\mathrm{DU,PnPb}}\cdot\tau^4}{5} \tag{25}$$

$\mathrm{PFD}_{\mathrm{MC}_{57}}$ is found by inserting (22) – (25) into (15).

In this case study, we have not found situations where it is likely to have CCFs among different components and (8) was therefore not used.

### Step 8: Calculate $\mathrm{PFD}_{\mathrm{SIF}}$

The calculations for all minimal cuts were done in Excel. The result indicated that the $\mathrm{PFD}_{\mathrm{SIF}}$ was greater than $1\cdot 10^{-2}$, and therefore not in accordance with the SIL 2 requirement. The main contributor to $\mathrm{PFD}_{\mathrm{SIF}}$ was the shear ram, and its associated components (control valve and accumulator). Based on this information, improvements have been suggested to the current design of these components. While this workover system has only one shear ram, newer systems often include more than one cutting facility.

## 5 Discussion and Concluding Remarks

We have presented a practical approach for reliability assessment of a complex SIS, and demonstrated its application on the SIF "*Shut in the well flow by the lower riser package upon a demand during intervention mode*" that is implemented for a subsea well workover system.

The assessment is done according to IEC 61508 and IEC 61511 and is based on fault tree analysis where CCFs are included by post-processing the minimal cut sets. Fault tree analysis is preferred because of two main reasons: (i) The failure-oriented approach of FTA will lead to a more complete identification of failure causes, and (ii) the fault tree construction process and the resulting fault tree are easy to comprehend by practitioners who have not been trained in reliability engineering, but whose knowledge is important for verifying the reliability model.

To verify that the PFD of a SIF meets a SIL requirement, it is essential to use conservative approximations when such approximations are required. Many software tools for FTA use non-conservative approximations for systems that are subject to periodic testing. Our approach applies (slightly) conservative approximation formulas to provide estimates of the PFD.

We have introduced a new approach for treating CCFs among non-identical components. Instead of defining $\beta$ as a fraction of the geometric mean, which in some cases may lead to a rate of CCFs that is unrealistically high, we suggest that $\beta$ is determined as a fraction of the lowest failure rate of the components in the minimal cut.

The approach does not include all aspects that are necessary to demonstrate compliance to the SIL 2 requirements. Additional measures would be to verify the SIF against the requirements for architectural constraints and the requirements for control and avoidance of systematic failures and software failures [13, 16, 17].

The main disadvantage of the suggested approach is the manual effort that is needed once the minimal cut sets have been identified. However, some of these efforts may be automated by implementing the steps into a suitable software tool.

# 6 Further work

In the suggested approach, we assume that all components are tested simultaneously and with the same functional test interval. This may not always be the case for SIS components, and an area of further work may be to extend the approach with new equations for components that are tested at different times. The approach is straightforward, but the calculation may be rather complex and will require the use of a computer.

A second area of further work is to consider "outer" dependencies [28]. An "outer" dependency is a dependency that may exist among two or more CCFs [28]. We have disregarded the possibility of having dependencies between two or more common cause component groups within the same minimal cut set, but the approach would benefit from being further developed with this as an option.

In our approach, we consider the minimal cuts one by one. Each minimal cut is a 1-out-of-$n$:G structure. For the case study, this approach is sufficient, but it will not be satisfactory for systems with $k$-out-of-$n$:G structures where $k \geq 2$. The main challenge is to include CCFs in a proper way. According to the beta-factor model, we should add the CCF as a single virtual component in series with the $k$-out-of-$n$:G structure [13, 26, 28]. When generating minimal cut sets for a $k$-out-of-$n$:G with $k \geq 2$, we obtain $\binom{n}{n-k+1}$ minimal cut sets. With the approach described in this article, we add the virtual CCF-component to each of these $\binom{n}{n-k+1}$ cut sets, and will, for this reason, obtain a result that is more conservative than the result obtained by the beta-factor model. One potential way to solve this problem is to model $k$-out-of-$n$:G with $k \geq 2$ as one component, and use the equations developed for $k$-out-of-$n$:G configurations [13, 28]. Another alternative is to identify, for example by a search algorithm, those minimal cut sets that represent configurations that are voted $k$-out-of-$n$:G with $k \geq 2$, and then add the contribution from CCFs only once for these minimal cut sets.

## Acknowledgements

The authors acknowledge Per Magne Bjørnetun at Multicontrol and StatoilHydro for giving us insight in the practical implementation of workover control systems.

## References

[1] Burdick, G. (1977). COMCAN - a computer code for common-cause analysis. *IEEE Transactions on Reliability*, R-26:100–102.

[2] Dutuit, Y., Innal, F., Rauzy, A., and Signoret, J.-P. (2008a). Probabilistic assessments in relationship with safety integrity levels by using fault trees. *Reliability Engineering and System Safety*, 93(12):1867–1876.

[3] Dutuit, Y., Innal, F., Rauzy, A., and Signoret, J.-P. (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(3):371–379.

[4] Edwards, G. T. and Watson, I. A. (1979). *A study of common-mode failures*. UKAEA SRD R 146, Warrington, UK.

[5] Evans, R. A. (2002). Editorial: Fault-trees and cause-consequence charts. *IEEE Transactions on Reliability*, 51(1):1.

[6] Goble, W. M. and Cheddie, H. L. (2005). *Safety instrumented systems verification.* The Instrumentation, Systems, and Automation Society, Research Triangle Park, NC.

[7] Heising, C. and Luciani, D. (1987). Application of a computerized methodology for performing common cause failure analysis: The Mocus-Bacfire Beta Factor (MOBB) code. *Reliability Engineering*, 17(3):193–210.

[8] Hokstad, P. and Rausand, M. (2008). Common cause failure modeling: Status and trends. In Misra, K. B., editor, *Handbook of Performability Engineering*, chapter 39. Springer-Verlag, London.

[9] Humphreys, R. A. (1987). Assigning a numerical value to the beta factor for common cause evaluation. In *Reliability'87: Proceedings of the Sixth Conference*, pages 2C/5/1–2C/5/8, Birmingham, UK.

[10] Hurdle, E.E., B. L. M. and Andrews, J. (2008). System fault diagnostics using fault tree analysis. *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, 221(1):43–55.

[11] IAEA (1992). *Procedures for conducting common cause failure analysis in probabilistic safety assessments*. International Atomic Energy Agency, Vienna, Austria.

[12] IEC 61025 (2006). *Fault tree analysis (FTA)*. International Electrotechnical Commission, Geneva.

[13] IEC 61508 (1998). *Functional safety of electrical/electronic/programmable electronic safety-related systems*. International Electrotechnical Commission, Geneva.

[14] ISA TR 84.00.02 (2002a). *ISA-TR84.00.02-2002-Part 3: Safety Instrumented Functions (SIF) - Safety Integrity Level (SIL) Evaluation Techniques Part 4: Determining the SIL of a SIF via Falt Tree Analysis*. The Instrumentation, Systems, and Automation Society, Research Triangle Park, NC.

[15] ISA TR 84.00.02 (2002b). *Safety Instrumented Functions (SIF) - Safety Integrity Level (SIL) Evaluation Techniques. Parts 1-5.* The Instrumentation, Systems, and Automation society, Research Triangle Park, NC.

[16] Lundteigen, M. A. and Rausand, M. (2006). Assessment of hardware safety integrity. In *Proceedings of the 30th ESReDA seminar*, pages 185–198. European Commission, Joint Research Centre, Ispra, Italy.

[17] 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(3):218–229.

[18] NASA (2002). *Fault tree handbook with areaspace applications.* NASA Headquarters, Washington, DC.

[19] NEA (2004). *International common-cause failure data exchange*. Number NEA/CSNI/R(2004). Nuclear Energy Agency, Issy-les-Moulineaux, France.

[20] NUREG/CR-5460 (1990). *A cause-defense approach to the understanding and analysis of common cause failures.* Nuclear Regulatory Commission, Washington, DC.

[21] OLF 070 (2004). *Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry*. Oljeindustriens landsforening (OLF), Stavanger, Norway.

[22] OREDA (2002). *OREDA Reliability Data*. OREDA Participants, Available from: Det Norske Veritas, NO 1322 Høvik, Norway, 4rd edition.

[23] Park, B. and Cho, N. (1992). Development of a computer code for common cause failure analysis. *Journal of the Korean Nuclear Society*, 24:14–29.

[24] Parry, G. W. (1991). Common cause failure analysis: A critique and some suggestions. *Reliability Engineering and System Safety*, 34:309–326.

[25] Paula, H. M., Campbell, D. J., and Rasmuson, D. M. (1991). Qualitative cause-defense matrices; Engineering tools to support the analysis and prevention of common cause failures. *Reliability Engineering and System Safety*, 34(3):389–415.

[26] Rausand, M. and Høyland, A. (2004). *System Reliability Theory: Models, Statistical Methods, and Applications*. Wiley, Hoboken, NJ.

[27] SINTEF (2006a). *Reliability data for safety instrumented systems – PDS Data Handbook*. SINTEF, Trondheim, Norway.

[28] SINTEF (2006b). *Reliability prediction methods for safety instrumented systems – PDS Method Handbook*. SINTEF, Trondheim, Norway.

[29] Smith, D. J. and Simpson, K. G. L. (2004). *Functional Safety: A straightforward guide to applying IEC 61508 and related standards*. Elsevier: Butterworth Heinemann, Oxford, 2nd edition.

[30] Summers, A., Ford, K., and Raney, G. (1999). Estimation and evaluation of common cause failures in SIS. *Chemical Engineering Progress*.

[31] 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.

[32] Sydvest. CARA-FaultTree: Software tool for fault tree analysis. http://www.sydvest.com/Products/Cara/.

[33] Tang, Z. and Dugan, J. (2004). An integrated method for incorporating common cause failures in system analysis. In *Annual Reliability and Maintainability Symposium. 2004 Proceedings*, pages 610–14. Institute of Electrical and Electronics Engineers Inc., Piscataway, NJ.

[34] Tang, Z., Xu, H., and Dugan, J. B. (2005). Reliability analysis of phased mission systems with common cause failures. In *Proceedings - Annual Reliability and Maintainability Symposium*, volume 2005, pages 313–318. Institute of Electrical and Electronics Engineers Inc., Piscataway, NJ.

[35] Vrbanic, I., Kosutic, I., Vukovic, I., and Simic, Z. (2003). Presentation of common cause failures in fault tree structure of Krsko PSA: An historical overview. In *International Conference - Nuclear Energy for New Europe, Proceedings*, pages 445–452. Nuclear Society of Slovenia, Ljubljana,Slovenia.

[36] Wagner, D., Cate, C., and Fussel, J. (1977). Common cause failure analysis methodology for complex systems. In *Nuclear systems reliability engineering and risk assessment*. Society of industrial and applied mathematics, Philladelphia, PA.

[37] Worrell, R. and Burdick, G. (1976). Qualitative analysis in reliability and safety studies. *IEEE Transactions on Reliability*, R-25:164–170.

[38] Xing, L. (2005). Reliability modeling and analysis of complex hierarchical systems. *International Journal of Reliability, Quality and Safety Engineering*, 12:477–492.

[39] Xing, L. (2007). Effective component importance analysis of complex hierarchical systems. *International Journal of Reliability, Quality and Safety Engineering*, 14:459–478.

[40] Xing, L., Meshkat, L., and Donohue, S. (2007). Reliability analysis of hierarchical computer-based systems subject to common-cause failures. *Reliability Engineering and System Safety*, 92(3):351–359.

# Article 7

Development of safety instrumented systems – RAMS engineering and management from a producer perspective
*Submitted to Reliability Engineering and System Safety*

# Development of safety instrumented systems – RAMS engineering and management from a producer perspective

Mary Ann Lundteigen[1], Marvin Rausand and, Ingrid Bouwer Utne

*Department of Production and Quality Engineering, Norwegian University of Science and Technology, S. P. Andersens v. 5, NO 7491 Trondheim, Norway*

## Abstract

This article outlines a new approach to reliability, availability, maintainability, and safety (RAMS) engineering and management. The new approach covers all phases of the new product development process and is aimed at producers of complex products like safety instrumented systems (SIS). The article discusses main RAMS requirements to a SIS and presents these requirements in a holistic perspective. The approach is based on a new life cycle model for product development and integrates this model into the safety life cycle of IEC 61508. A high integrity pressure protection system (HIPPS) for a deep-water oil and gas application is used to illustrate the approach.

*Key words:* Reliability, Product development, Safety instrumented systems, RAMS management, System life cycle, IEC 61508

## 1. Introduction

Safety instrumented systems (SIS) are used in many industry sectors to reduce the risk to human lives, environment, and material assets. A SIS is installed to detect and respond to the onset of hazardous events by the use of electrical, electronic, or programmable electronic (E/E/PE) technology. In cars, the airbag systems and the anti-lock braking systems (ABS) are two examples of SIS applications. When a sensor detects that the car collides, the airbag is activated. The ABS prevents the wheels from locking during heavy braking, so that the driver can maintain control of the car. In the process industry, SIS are used to stop flow and isolate electrical equipment upon detected high pressures, high temperatures, fires, and gas leakages. One such SIS application is the high integrity pressure protection system (HIPPS) which is used to prevent over-pressure in vessels and pipelines.

We may split a SIS into three main sub-systems; input elements (e.g., sensors, transmitters, push buttons), logic solvers (e.g., programmable logic controllers, relay based logic), and final elements (e.g., safety valves, circuit breakers). To be defined as a SIS, at least one element must be based on E/E/PE technology.

Producers of SIS components and complete SIS applications must comply with a number of requirements, such as customer requirements, corporate requirements, regulatory requirements, and technical requirements [11, 38]. Regulatory requirements give overall requirements for what the SIS shall do and how well it shall perform for

*Email addresses:* mary.a.lundteigen@ntnu.no (Mary Ann Lundteigen)

[1] Corresponding author: Mary Ann Lundteigen

a particular industry application. In addition, regulatory requirements may address product safety, that is how the product must be designed to avoid risk to those operating or maintaining the product. Customer requirements may reflect many aspects of the regulatory requirements as it is in the interest of the customer to develop safe and reliable products. However, customers may add requirements for operation availability, maintainability, and maintenance support. Corporate requirements reflect the producer's own objectives, policy, and business goals. Technical requirements may be addressed in all the previous categories of requirements, or identified during the detailing of SIS design and development. Many of these requirements are related to the reliability, availability, maintainability, and safety (RAMS) aspects of the SIS.

For design and operation of SIS, many national authorities make reference to the IEC 61508 [20], or its sector specific implementations as recommended practise. It is therefore important that the SIS producers adapt key requirements from these standards for their product development. Examples of sector specific standards that build on the IEC 61508 are the IEC 61511[21] (process industry), IEC 62061[23] (machinery control systems), IEC 61513 [22] (nuclear power plants), and IEC 60601[19] (medical equipment). An IEC standard is also being developed for the car industry.

IEC 61508 and some of the related standards use the safety life cycle approach as framework for structuring SIS requirements. The safety life cycle splits SIS specification, design, construction, and operation into 16 phases, starting with the initial concept evaluation and ending up with decommissioning and disposal. In IEC 61508, SIS design and construction are mainly addressed in phase 9 of the safety life cycle. For SIS producers, it may be advantageous to use this framework as basis for their product development. Unfortunately, phase 9 is not very detailed on the product development phases as seen from the producer's perspective. In addition, producers must have a holistic approach to the specification and adoption of RAMS requirements, so that also customer requirements, corporate requirements, and technical requirements are sufficiently accounted for.

Many authors address product development models and product development challenges [42, 4, 37, 28, 8, 14, 15, 38]. Product development is viewed from different angles; producer perspective, consumer perspective, or a combination of the two. Unfortunately, none of the models seem to take a holistic approach to the specification and adoption of RAMS requirements, which is an important aspect of SIS development. Papadopoulos & McDermid [42] compare three safety standards, including IEC 61508, and specify a new safety process for system development which fit into the framework of the standards. However, maintainability, availability (in terms of operability) and product safety are not discussed. The product development model proposed by Jackson et al. [28], addresses reliability, availability, and maintainability, but has limited focus on safety related requirements. Murthy et al. [38] suggest a life cycle framework for decision making regarding product reliability, and indicate that the model may be suited for a large range of applications, including SIS development.

The main incentive for writing this article is that product development in IEC 61508 (primarily phase 9) can benefit from being structured according to the model by Murthy et al. [38]. The article presents and discusses the new model from the perspective of a SIS producer, and suggests how producers may account for RAMS in their product development. To illustrate the application of the new model, we describe the design and development of a HIPPS.

The HIPPS is an example of a custom-built product. Custom-built products are products manufactured to a specific request from a customer, and include specialized defense and industrial products [38]. Another category is standard products. Standard products are manufactured in anticipation of a subsequent demand. Standard products include all non-durable (short life) products and durable (long life) products and most commercial and industrial products. This may be a new version of a programmable logic controller or a new type of pressure transmitter. Standard products and custom-built products may be produced in small as well as large quantities. However, a HIPPS is usually tailored made for one particular target application, for example an offshore oil and gas installation.

The first part of the article discusses important concepts regarding RAMS engineering and management and SIS, before presenting the safety life cycle of the IEC 61508. The main part of the article describes the model of Murthy et al. [38] and important RAMS activities when developing SIS. The article concludes that the development process of SIS can benefit from implementing the model of Murthy et al. [38], because it represents a holistic and structured approach focussing on RAMS performance rather than safety alone as in the IEC 61508.

## 2. RAMS Requirements

Good product quality influences business success through satisfied customers, improved market share, and higher productivity [5]. For producers of SIS or SIS components, the most important dimensions of product quality are; reliability, availability, safety, and maintainability. A producer must therefore identify and ensure proper adoption of all relevant RAMS requirements.

We may split RAMS requirements into the following main categories, as illustrated in Fig. 1:

- Functional safety and safety integrity requirements
- Product safety requirements
- Operation availability requirements
- Maintainability and maintenance support requirements

The producer must develop a RAMS specification where all the relevant requirements are included. This specification may be an extension of the SIS safety requirement specification (SRS) that is defined in IEC 61508. In the following sub sections, we briefly discuss some main aspects of the four categories.

### *2.1. Functional Safety and Safety Integrity*

Functional safety and safety integrity are key concepts in IEC 61508 for describing the desired performance of a SIS. Functional safety concerns the overall safety of a plant or a system, but may be detailed down to the required functionality of the SIS. The required SIS functions are deduced from a hazard and risk analysis of the plant or system, that is called equipment under control (EUC) by [20]. Safety integrity is used to describe how well the SIS must perform and is therefore a measure of SIS reliability. Safety integrity is defined as the probability that the SIS is able to perform the required safety functions under all the stated conditions and within a stated period of time [20].

IEC 61508 distinguishes between four safety integrity levels (SIL), where SIL 1 is the lowest level and SIL 4 is the highest. To comply with a SIL, it is necessary to demonstrate that each safety instrumented function (SIF) that is implemented by the SIS, is within the specified reliability range, and that a number of measures have been implemented to avoid, reveal, and control random hardware failures, software failures, and systematic failures. 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 [20].

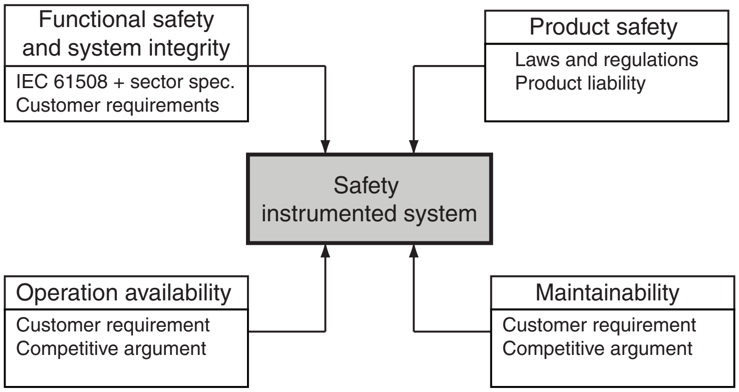


Figure 1: RAMS aspects of a SIS

For custom-built products, the customer usually specifies the SIFs and their associated SIL. For standard products, the producer must themselves identify these requirements. In some cases, the producer may use similar products on the market as reference. In other cases, they must start with the EUC and from that point identify the required functionality and reliability.

IEC 61508 classifies SIS as either operating on demand or in high demand mode. Demand is here a request that requires response by the SIS. On demand systems (also called low demand systems) are passive during normal operation, and typically experience less than one demand per year. Here, a separate system is used for plant or system control during normal operation. As the SIS is normally passive, a SIS failure may not have an immediate effect. Dangerous failures of a low demand SIS are only manifested when a demand occurs. This is, for example, the case for an airbag system with a “fail to activate” failure mode.

A high demand SIS experiences demands frequently, typically several times per year. In some cases, the high demand systems are operated almost continuously. Most control functions of a high demand SIS have direct effect on safety, and a failure may lead to an immediate hazardous event. The ABS in a car or in an airplane is an example of a SIS that operates in a high demand mode, since heavy braking occurs rather frequently. If the ABS fails to operate, this may lead to immediate harm.

Separate reliability measures and ranges are required for on demand and high demand systems. For on demand systems, IEC 61508 uses the (average) probability of failure on demand (PFD) as a measure of reliability, whereas the probability of a dangerous failure per hour (PFH) is used for high demand systems. The reliability or availability may be calculated based on a reliability model, for example a reliability block diagram, a fault tree, a Markov transition diagram, or a Petri net [43]. Some reliability models are more suitable for including maintenance and testing strategies than others [43, 25, 45].

IEC 61508 recognizes that all failures are not safety-critical. The standard distinguishes between:

- *Dangerous failures*: i.e., failures that may prevent execution of a safety function, and where the safety function will be unavailable until the failure is detected and corrected.

- *Safe failures*: i.e., failures that do not prevent the execution of the safety function, or otherwise do not cause a hazardous situation. A spurious (non-intended) activation of a safety function is sometimes defined as a safe failure. A safe failure does usually not affect the availability of the safety function, but the EUC may be unavailable for some time.

The failure classification is important to consider when calculating the PFH or the PFD. In addition, the failure classification is important for calculating the safe failure fraction (SFF) [31, 30, 35]. This parameter is used to determine the architectural constraints for the hardware configuration. The architectural constraints define minimum hardware fault tolerance of a configuration, or the number of dangerous failures to be tolerated before the SIS is unable to perform a SIF. To determine if a failure is safe or dangerous, it is necessary to assess the application specific conditions. A spurious activation is, for example, not always safe, such as an airbag on the driver's side that is activated while driving a car.

The SIS reliability is also influenced by the (potential) presence of common cause failures (CCF) [20, 43, 47, 46, 16]. A CCF is a failure that affects two or more components (close to) simultaneously due to a shared cause [20, 21], and may reduce the effect of hardware fault tolerance [33]. IEC 61508 and related standards require that measures are taken to avoid CCF during all phases of SIS development. All measures that concern avoidance of systematic and software failures have a positive effect on avoidance of CCF [32].

Most SIS in the process industry are operating on demand. The diagnostic coverage of dangerous failure, is along with the length of the functional test intervals, the factors that highly influence the PFD. The diagnostic coverage is defined as the fraction of dangerous failures detected by online diagnostic systems to the total number of dangerous failures [20, 31]. Some components have comprehensive diagnostic features, like smart transmitters and PE logic solvers, while other components, like shutdown valves, have just a few of these features.

### *2.2. Product Safety Requirements*

Producers must take reasonable care regarding the safety performance of their products, related to all types of intended use and foreseeable misuse of the product. Product safety requirements are mainly given in laws, regulations, and standards, or stated by customers of specialized products.

For custom-built products, safety requirements are often included in the overall requirements from the customer. Obligations to fulfill safety requirements in laws, regulations, and standards are often explicitly stated in the requirement documents.

For standard products, the producer has to identify all relevant safety requirements and integrate these into the development process.

For products developed for the European market, the producer must document compliance to the product safety directives, for example GPSD [13]. One example is equipment used in areas with explosive atmospheres, that must comply to ATEX 94/9/EC [2] or similar standards. Another example is electrical systems, for example power distribution systems and electrical apparatus. They must be designed in accordance with directives on electromagnetic compatibility.

Product hazards may arise from failures (e.g., spurious activation of an airbag) or from design features of the product (e.g., sharp edges, toxic materials). Product hazard and risk analyses have to be integrated into the product development process to minimize the risk related to such hazards [27].

### *2.3. Operation Availability*

Operation availability may be defined as the fraction of time a system is able to perform the intended functions [43].

Unintended operation of the SIS may lead to reduced operation availability. A spurious closure of a HIPPS valve may lead to shutdown of the plant or at least a process section. Testing and maintenance are other activities that may affect operation availability. If the ABS system in a car indicates a failure, the driver has to take the car to the workshop. If a HIPPS valve has an external leakage, it may be necessary to shut down the EUC to perform necessary repair.

When the product is custom-built, the customer may provide operation availability targets for the SIS. For standard products, operation availability may be specified based on competitive arguments. Lack of adequate availability may lead to product recall, lawsuits, or loss of market share and reputation. It is therefore important for the producer to analyze the product and demonstrate its ability to meet the specified operation availability targets.

NORSOK Z-016 [39] is a Norwegian standard for the oil and gas industry on production availability. The standard suggests a framework for determination and follow-up of production availability. This standard is currently being used as a basis for development of an ISO standard on the same topic.

### *2.4. Maintainability and Maintenance Support*

Maintainability and maintenance support are features of the SIS that become evident once the product is put into operation. Maintainability is a design feature that describes the ease by which an item can be maintained or repaired [18]. Testability is a similar concept that describes the ease and speed by which an item can be tested. A subsea HIPPS valve is sometimes welded to the pipeline, and to repair such a valve is a complicated and time-consuming operation. The maintainability of the valve is therefore rather low. The testability is also low, as the EUC must be shut down while performing a full stroke operation of the HIPPS valves.

Maintenance support is the ability of a maintenance organization, under given conditions, to provide upon demand, the resources required to maintain an item, under a given maintenance policy [18]. Dedicated test and maintenance tools are often developed as part of the total product delivery. For subsea systems, the test and maintenance tools may sometimes be more complex and more expensive than the products they are associated to.

The producer must consider maintainability when selecting hardware and software design, and prepare for maintenance support. In some cases, the producer may be responsible for product maintenance, for example overhaul, and must establish the necessary resources and facilities for maintenance support.

## 3. RAMS Performance and Management

Successful products perform very close to its desired performance. In our context, performance is related to the RAMS properties of a product, and measured relatively to the RAMS specification.

We may distinguish between the desired RAMS performance, the predicted RAMS performance, and the actual RAMS performance. Usually, the *desired RAMS performance* emanates from RAMS requirements that were discussed in Section 2. A successful product has a very narrow gap between the desired performance and the *actual RAMS performance*. The actual RAMS performance is demonstrated when the SIS or the SIS component is released to market and installed at the particular target application. The actual performance is not linked to the product properties alone, but is also influenced by its development process, operation and maintenance; important elements of the product life cycle.

Moving from customer needs and a desired RAMS performance to a satisfactory actual RAMS performance, involves a design process ensuring that all relevant product requirements are specified and evaluated. During the design and construction process, we may estimate the product's performance by analysis, simulation, testing, and so on. This estimate may be referred to as the *predicted RAMS performance*, and may be split into four categories of analyses corresponding to the requirements illustrated in Fig. 1.

To ensure proper employment of RAMS requirements during product development, the producer must establish a RAMS management system. RAMS management may be defined as a process which supports [24]:

- Definition of RAMS requirements
- Assessment and control of threats to RAMS
- Planning and implementation of RAMS tasks
- Achievement of compliance to RAMS requirements
- On-going monitoring, during the life cycle, of compliance.

An important part of the RAMS management system is the management of functional safety. Management of functional safety is used in IEC 61508 to describe management and technical activities which are necessary to achieve the specified functional safety. From the producer perspective, management of functional safety should describe all activities required to design and construct a SIS according to the specified functional safety and safety integrity requirements. Such activities may be design reviews, probabilistic reliability analysis, failure modes and effects analysis (FMEA), various types of testing of software and hardware, and assessment of procedures, work practises and tools with respect to IEC 61508 or related requirements.

To the list of management of functional safety activities, it is necessary to add operation availability analysis, maintainability analysis, and maintenance support analysis.

## 4. Product Development

IEC 61508 and related standards use the safety life cycle as a framework to structure requirements. The safety life cycle is a sequence of phases, each containing a number of tasks, covering the total life of a system. For producers, it may be important to align their product development with the relevant phases of the safety life cycle model. In this Section, we first introduce the main phases of the safety life cycle, and then suggest how the safety life cycle may be merged with the model of Murthy et al. [38].

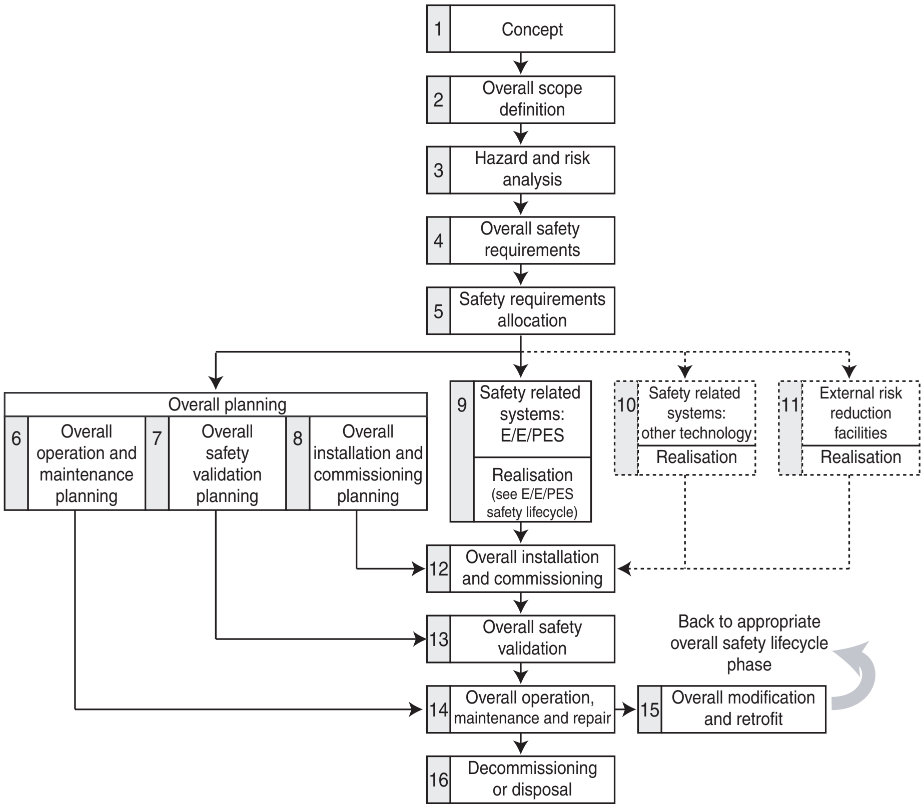

1 Concept
2 Overall scope definition
3 Hazard and risk analysis
4 Overall safety requirements
5 Safety requirements allocation
Overall planning
6 Overall operation and maintenance planning
7 Overall safety validation planning
8 Overall installation and commissioning planning
9 Safety related systems: E/E/PES
Realisation (see E/E/PES safety lifecycle)
10 Safety related systems: other technology
Realisation
11 External risk reduction facilities
Realisation
12 Overall installation and commissioning
13 Overall safety validation
14 Overall operation, maintenance and repair
15 Overall modification and retrofit
Back to appropriate overall safety lifecycle phase
16 Decommissioning or disposal

Figure 2: The safety life cycle of IEC 61508 [20]

### *4.1. The Safety Life Cycle in IEC 61508*

IEC 61508 splits the safety life cycle into 16 phases as shown in Fig. 2.

The safety life cycle starts with the definition of the EUC, and continues with the identification of the EUC related hazards and risk. The hazard and risk analysis is used to specify safety functions. Based on tools and methods provided by the standard, the necessary risk reduction that is to be provided by the safety functions are defined. The safety functions may be realized by SIS (E/E/PE technology), other technology or other risk reduction facilities. The realization of the two latter categories of safety systems is not covered by the standard.

Parallel to the realization of the SIS, the standard requires planning and preparation for the subsequent phases of overall installation, commissioning, validation, operation, and maintenance. In this context, overall means that *all* safety systems are considered.

In the operation and maintenance phase, IEC 61508 focuses on how to operate and maintain the SIS in accordance with the functional safety and safety integrity requirements. This includes failure recording and analysis.

The SIS modification phase addresses necessary analyses of minor and major modifications of the SIS. IEC 61508 requires that all modifications are carefully analyzed with respect to their impact on the EUC, the EUC risk, the SIS hardware and software, and the operation and maintenance procedures, tools, and practises. The impact analysis should suggest the return to an appropriate safety life cycle phase for implementation.

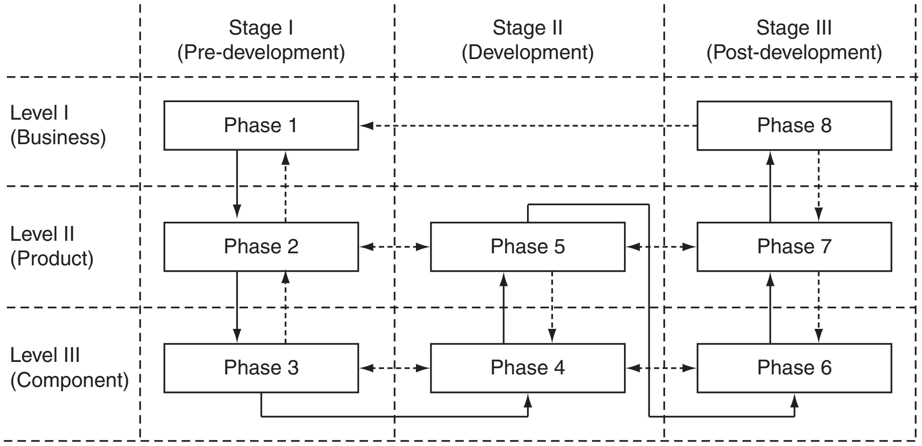


Figure 3: Product life cycle model, from the perspective of a producer [38]

The safety life cycle embraces SIS design and construction as well as SIS operation. This means that all phases may not be relevant from the producer's perspective. The producer's responsibility is often restricted to SIS realization (phase 9), but in some cases, the producer may be involved in the overall system integration, installation, commissioning, and safety validation. Some producers may also be involved in product follow-up and modifications. In fact, within some industry sectors it is a trend that product performance is purchased instead of being inherent in products. This means that the producer is responsible for the product use (or operation), and must also ensure adequate maintenance and repair.

For custom-built products, the customer may wish to be more involved in the product development phase. The customer may want to participate in design reviews and witness product testing. Development of standard products may be without any external involvement at all, or the producer may decide to involve intended users at certain stages during the product development.

### *4.2. New Life Cycle Model for Product Development*

Murthy et al. [38] have recently developed a new model to assist producers in accomplishing the desired product performance. The model consists of three stages (pre-development, development, and post-development), three levels (business, product, and component), and eight phases, shown in Fig. 3.

The three stages and levels are:

- Stage I (Pre-development): This stage is concerned with a non-physical (or abstract) conceptualization of the product with increasing level of detail.

- Stage II (Development): This stage deals with the physical embodiment of the product through research and development and prototyping.

- Stage III (Post-development): This stage is concerned with the remainder of the product life cycle (e.g., production, sale, use) subsequent to the new product development.

- Level I (Business level): This level is concerned with linking the business objectives for a new product to desired product attributes.

- Level II (Product level): This level links product attributes to product characteristics (the distinction between attributes and characteristics are described in [38]). The product is treated as a black-box.

- Level III (Component level): This level is concerned with linking product characteristics to lower level product characteristics, at an increasing level of detail.

Based on these stages and levels, the model outlines eight phases of product development. The model portrays its phases as being sequential, but the necessity of iteration is illustrated by the arrows between phases.

The main advantage of this product development model is the split between product specification, pre-qualification, final construction, product use, and overall product evaluation. The model describes the process of linking business objectives for a new product to desired product attributes and components. A successful design process, from gathering of user needs to the transformation of requirements into an optimal product design solution, is based on effective decision making in an overall business perspective. Hence, the model of Murthy et al. [38] represent a more holistic approach to development of SIS.

In the next section, we describe the content of the eight phases of the new model, and how RAMS performance can be sufficiently catered for in the development process of a new SIS.

## 5. RAMS Management in the Product Life Cycle

The previous parts of the article have discussed general challenges when developing a SIS. In the following, we will demonstrate how the product development model by Murthy et al. [38] may be used for development of a SIS, taking into account RAMS aspects and the main requirements for product development in IEC 61508. To illustrate this implementation, we use a the development of a HIPPS as an example. A HIPPS may be implemented in several ways, see for example [3, 34, 50].

A HIPPS is a custom-built product, where the main functionality is specified by the customer. A HIPPS is used to protect against overpressure in pipelines or vessels that are not designed for the maximum pressure that may arise from e.g., well shut-ins (i.e., the maximum wellhead pressure) and sudden downstream blockage (e.g., spurious closure of a downstream valve). The HIPPS monitors the pressure in the oil or gas pipeline, and if the pressure exceeds a pre-determined level, dedicated valves are closed to avoid further pressure build-up that may cause pipeline rupture.

A HIPPS comprises pressure transmitters, logic solver(s), solenoid-operated hydraulic control valves, and fast-closing shutdown valves. The main components are illustrated in Fig. 4. For illustration, we have included a single logic solver, a single shutdown valve, and two pressure transmitters voted 1-out-of-2, meaning that one transmitter must detect a high pressure to initiate valve closure [43]. In a real situation, there may be more than two pressure transmitters to detect high pressures and more than two shutdown valves available to stop flow. However, for this case study, the focus is on the development process and not to present an actual HIPPS configuration.

Regarding the development of the HIPPS, we assume that the customer is an oil company. We further assume that the HIPPS producer does not develop hardware and software themselves, but are responsible for the integration of HIPPS hardware and software that are supplied by subcontractors. The initial phases of the safety life cycle of IEC 61508 are performed by the customer, including concept evaluation, overall

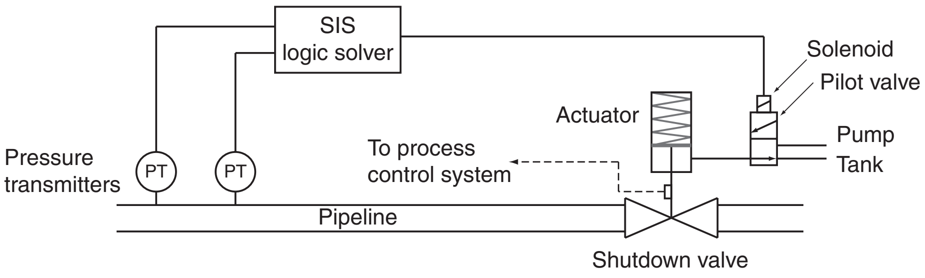


Figure 4: Simplified illustration of the HIPPS

scope definition, hazard and risk analysis, and requirements specification and allocation. Based on this analysis, the customer orders the HIPPS from the producer, who then becomes involved in the realization part (phase 9, Fig. 2) of the safety life cycle. In this case study, we assume that a SIL 3 target has been set for the HIPPS.

The remainder of this section discusses the HIPPS development process for the producer in line with the models of Murthy et al. [38] and IEC 61508, but with focus on the RAMS-related activities in the various phases.

*Phase 1.* involves identifying the need for a new product or the need for modifications of an existing product in accordance with business objectives and strategies of the company and the customer needs for the product. A key aspect of phase 1 for standard products is the product definition. The product must fulfil business objectives as well as customer requirements. Customer requirements may not be given explicitly, and market and competitive analysis may be required to capture the customer expectations of product performance [38].

The need for the HIPPS and several RAMS requirements are already pre-determined when the development process starts. The risk analysis performed by the customer has lead to a SIL requirement for the HIPPS, which puts constraints to the solution space for the producer. Thus, phase 1 of the model implies a process at two levels for the producer; (1) their overall business strategy regarding which type of products and services they will develop, and (2) the development of this particular HIPPS. The main activities in phase 1 consist of sorting out and making agreements with the customer about the delivery, which in this case is the HIPPS.

The HIPPS is subject to several RAMS requirements, and during phase 1 it is important to establish and enforce overall strategies and frameworks for the management of RAMS during product development. One task is to develop a *RAMS policy*, which states the management commitments to RAMS principles, and outlines the main strategy for achieving RAMS policy. The overall RAMS policy should be rooted at the business level, constituting an umbrella for all development activities. Regarding the HIPPS, the specific RAMS activities emanate from the overall policy, but the extent and content of the activities may vary from one project to another. With reference to the discussions in Section 3, RAMS management reflect the main principles of management of functional safety in IEC 61508.

The RAMS management activities should be listed in a *RAMS management plan*, containing overall product development guidelines, verification, and validation activities, being adjusted depending on the product to be developed. In short, a RAMS management plan describes all RAMS related activities in each product life cycle phase, it identifies persons, departments, and organizations responsible for the different phases and tasks of product development. Further, the plan identifies competence requirements and training of personnel involved in product development, and makes reference to company procedures, tools, and methods for product development. References to other governing documents, for example standards, such as the IEC 61508 [20], directives, such as the GPSD [13], regulations, and guidelines, should also be included, as well as requirements to documentation in each phase of the product life cycle.

To take advantage of previous product development processes and experiences, a *critical items and hazard list* should be established, in which failures and hazards related to similar products are recorded and evaluated. This list can be used as a starting point to identify and evaluate potential hazards in the design of the HIPPS, and should also be part of the RAMS management plan. *Verification* and *validation* are important activities in all phases of the project development process, and these activities should be planned for and rooted in the RAMS management plan.

Verification and validation have slightly different meaning [14, 15, 48]. Verification may be understood as an activity in which the deliverables from any stage (e.g., product life cycle phase) are compared to the specifications developed in the previous stages [48]. Verification activities may for example be design and documentation reviews, FMECA, HAZOP, and testing. For software verification, the V-model may apply [20]. Validation may be defined as the confirmation that a product meets the specification and that it is appropriate for the intended use. In an initial phase, validation is performed *prior* to detailed design to gain confidence in that the product concept will satisfy the desired performance [14]. Later in the development process, at the stage where the product has been constructed and is ready for start-up or release to market, validation is conducted to prove that the HIPPS works as intended [48].

Validation activities may be included in what IEC 61508 refers to as *functional safety assessments (FSA)*. However, the scope of an FSA goes beyond validation. An FSA should also examine to what extent procedures, tools, methods, and design principles meet the requirements of IEC 61508, or its sector or application specific implementations. If these product development tools and procedures have previously been approved according to IEC 61508 (or similar), an FSA may verify if they are followed.

Establishment of *RAMS controlling documents* is necessary if not already available. Controlling documents should include procedures, work processes, tools, and methods that address RAMS aspects and the requirements for functional safety according to IEC 61508 or its related standards if they apply. For the HIPPS development, the procedures, tools, and methods must be aligned with the requirements for SIL 3. Some work process requirements prevail regardless of the specified SIL, whereas other requirements are “SIL-dependent”. IEC 61508 includes a number of tables that concern identification, avoidance, and control of random hardware failures, software failures, and systematic failures, where each requirement is defined as mandatory, highly recommended, recommended, or not recommended depending on the SIL. The documentation should address the handling of ; (1) non-conformities, deviations, and recommendations from verification, validation, and testing activities, and (2) management of change, including authorities for approving and follow-up of product modifications.

The RAMS policy, the RAMS management plan, and controlling documents are the overall framework for the HIPPS development. More specific documents tailor-made for each project, is the *RAMS specification* of desired product performance for reliability/availability, maintainability and safety. For custom-built products, such as the HIPPS, the RAMS specification may be deduced from the customer safety requirement specification (SRS). The SRS is used by IEC 61508 as the overall specification of functional safety and safety integrity requirements. For standard products, the RAMS specification is developed by the producer. The RAMS specification should have a dual focus on performance requirements and design constraints, and ensure that they reflect the intended use, support, testing and maintenance. Regarding the HIPPS, the producer will have to negotiate and come to terms with the customer about RAMS requirements.

*Phase 2.* is, along with phase 3, the most important phases from a producer's perspective. Based on the overall RAMS requirements determined in phase 1, the product characteristics are decided in phase 2. The objectives of phase 2 are to transform the desired performance from phase 1 into a physical product, with sub-systems and components, and to develop a preliminary product design which may be used as basis for comparing the predicted performance with desired RAMS performance. The characteristics are technical in nature, and should consider the desired performance as well as the possible misuse of the product.

The SIL requirement influences how phases 3 and 4 are executed. First, the required SIL affects the work processes, which should be reflected in the controlling documents. Second, the required SIL influences the selection of software language, programming tools, and programming methods. Third, the required SIL influences the selection of hardware architecture and hardware components. Here, reliability analysis must be performed to verify if the proposed product design is able to meet the specified SIL.

The main RAMS activities in phase 2 are to:

- Detail the RAMS requirements into product characteristics. For the HIPPS, it is important to review of IEC 61508, or its sector/application specific implementations, to identify additional requirements that concern hardware and software characteristics (architecture, diagnostic features, behavior upon fault conditions).
- Develop a preliminary product description, of the system, its sub-systems, and components.
- Communicate and enforce work procedures that ensure product design in accordance with IEC 61508 or its sector specific implementation.
- Conduct design reviews, one or several depending on the complexity of the product, should be carried out to assess how well the design at a given point in time reflects the desired product performance. In general, the results from the design review document justify design decisions [6, 17].
- Perform reliability analyses, for example:
  - Establish top-level functional model and carry out functional analysis.
  - List all assumptions made for the reliability assessment.
  - Perform top-down FMEA [43], of the product and its foreseeable misuse
  - Establish preliminary reliability model (e.g., by reliability block diagram, fault tree, or Markov model) [43] and make a preliminary reliability prediction. For the HIPPS, this means to calculate the PFD based on an initially selected testing strategy and component failure rates.
  - Allocate reliability targets to sub-systems (e.g., reliability apportionment of PFD requirements, for example 35% to input elements, 15% to logic

solvers, and 50% to final elements). This allocation is important as reliability of components and subsystems must be specified in contracts with subcontractors.

  - Verify the hardware architecture against the architectural constraints [33]
  - Propose modifications and follow-up based on the results from the reliability assessment and the FMEA.
  - Perform human reliability analysis [12, 29], if human errors may have a major impact on the product reliability. In case of the HIPPS, the system is installed subsea and rarely subject to direct human activities. However, maintenance operations performed by remotely operated vehicles (ROV) are controlled by humans, and such activities may be considered for analysis.

- Perform operability analysis. For the HIPPS, this means to predict how the HIPPS related spurious activations, testing activities, and maintenance activities affect operability due.
- Perform maintainability analysis. In case of the HIPPS, this means to analyze if the product has sufficient inherent features that facilitate maintenance and testing according to the specified requirements.
- Perform product safety analysis. Since the HIPPS is a system that is installed subsea, it has limited potential to cause damage to humans. However, the HIPPS may affect the environment if the valves or piping leak, and the causes and effects of such events should be analyzed.
- Assess if there are *new* conflicts arisen between the functional safety and safety integrity, product safety, operability, and maintainability, and decide how to handle them. In case of the HIPPS, a SIL requirement may imply that two shutdown valves have to be installed. Having two valves, may reduce the operability due to more (potential) spurious activations, testing, and maintenance. One means to compensate for the reduced operability may be to introduce partial stroke testing [32, 35, 49].
- Update the RAMS specification based on the description of product characteristics and the results from the reliability, operability, product safety, and maintainability analyses.
- Initiate planning for product testing, product installation and commissioning (alternatively, market release).
- Update the critical items and hazard list, based on findings from the reliability, operability, product safety, and maintainability analysis.
- Perform an FSA with focus on the RAMS specification and its completeness according to the identified product requirements, the RAMS management plan and the RAMS policy.
- Update the product RAMS specification as a requirement for the next phase.
- Decide whether or not the RAMS performance is adequate to proceed to the next phase.

*Phase 3.* involves detail design of product, placement of orders for components to be purchased, and preparation of initial product construction and testing. All functions identified in phase 2 are transformed into a *(product) design specification* describing the individual components and their relevant properties [38]. The design specification is used as basis for the specification of components to be purchased. This is the start of product development for subcontractors, and may involve new technology development.

In case of the HIPPS, we may assume that all components are available on the market, but that some additional challenges may be expected due to high temperature and high pressure conditions.

RAMS activities in phase 3 are to:

- Develop product design specifications for components (including new developments) to be purchased from subcontractors. It is important that the specifications address desired features for diagnostics and component behavior upon fault conditions. In case of the HIPPS, the producer needs to purchase pressure transmitters, logic solvers, valves, and piping/cables. In addition, the producer must specify and prepare for interfaces with other systems, for example the process control system and other SIS, for status presentation and alarm notifications.
- Follow-up of subcontractors, and verify that the components achieve the desired RAMS performance.
- Follow-up and control product safety design features (e.g., sharp edges, gaps) of components and assemblies and assure that these do not cause unnecessary hazards. For the HIPPS, the focus of product safety may be on the avoidance of environmental hazards.
- Update the reliability analysis, operability and maintainability analyses from phase 2, with new information on component failure rates and characteristics.
- Maintain and update the critical items and hazard list.
- Perform design review at intermediate stages of the detailed design. In the case of the HIPPS, the producer may perform internal design reviews as well as participating in design reviews performed by subcontractors. Design reviews should focus on the intended use as well as foreseeable misuse.
- Develop plans for assembling of components that need pre-quantification before the final product is constructed. In case of the HIPPS, one may want to build a test facility to test the shutdown valves, to verify that the valves are able to close within the specified time and with the specified pressure drop.
- Update the *product design specification* as a requirement for the next phase.
- Develop initial versions of operation (user) and maintenance manuals and instructions.
- Perform safety analyses of scheduled activities in phases 4 and 5 that may expose humans or environment to risk, for example activities related to construction, installation, and testing.
- Start preparing for maintenance support, that is the development of testing aids, support services and so on.

- Assess hazards related to product disposal. Some products may contain materials and substances hazardous to human health and environment, and thus, disposal, dismantling and recycling should be planned for during the development process [51].
- Decide whether or not the RAMS performance is adequate to proceed to the next phase.

Phases 4, 5, and 6 will be different for products that are developed in high numbers than for a one of a kind product.

*Phase 4.* and phase 5 constitute the first stage of product qualification. The main objectives of phase 4 are to build one or more prototypes and test them in a controlled environment against the desired performance. For products to be produced in high numbers, the prototype may be a complete product. For a one of a kind product, the prototype may be the construction of some selected subsystems that require further testing before the final construction of the product is started. When the prototype involves new technology, it is important to adhere to procedures and guidelines on qualification of new technology, for example as in [10].

The process of prototype development starts at the component level, before continuing with all subsystem levels until the product as a whole is finally reached [38]. In case of the HIPPS, phase 4 may include construction, integration, and testing of logic solver hardware and software, including input/output cards, drivers, and communication. Or as mentioned in phase 3, to install and test the shutdown valves in a test facility.

The main RAMS activities in phase 4 are to:

- Verify that the specified procedures, work practises, and tools are adhered to so that systematic failures are avoided, revealed and followed up.
- Perform function testing of prototype components, taking into account reliability, maintainability and operability requirements. The function testing should also address behavior upon fault conditions and foreseeable misuse.
- Update the product safety analysis to find out if new hazards have been introduced.
- Perform various type of reliability testing, for example stress testing or accelerated testing to reveal if the product can lead to problems in over-stress situations.
- Document the qualification of new technology according to relevant guidelines and procedures, for example as in [10].
- Update and follow up of the critical items and hazard list.
- Update product documentation and product description
- Review and update the reliability and operability analyses with new information and data.
- Prepare operational testing, including establishment of system for customer feedback on product performance.
- Decide whether or not the RAMS performance is adequate to proceed to the next phase.

The testing done in phase 4 is limited, because it is most often carried out in controlled conditions, such as in a laboratory. Thus, the RAMS performance is reflected through the predicted performance of the product. When developing custom built products, produced in very few numbers, the costs for complete product tests may be unreasonable. Then the RAMS characteristics or procedures are tested, for example, by use of engineering analyses, analogy, laboratory test, functional mockups, or model simulation [51]. In such cases, phase 4 is the last phase before the production starts in phase 6 [38].

For standard products, often a prototype of the product is released to a limited number of potential customers. This occurs in phase 5.

*Phase 5.* consists of operational testing, which means in some cases that selected customers keep a log of the relevant information about how the product works. This information is used to assess field safety performance and to make design changes, if necessary. Influence from factors like the usage intensity and the operating environment may reveal additional hazards, contributing to a more complete picture of the actual product field performance. For some products, like cars, the products are tested in in a wide span of environments to reveal hazards and operational problems.

The main RAMS-related activities in phase 5 are to:

- Perform operational testing under various operational and environmental conditions.
- Record and classify all non-conformities, and allocate responsibilities for their follow-up.
- Analyze customer feedback on product performance.
- Update and follow up critical items and hazard list.
- Decide whether or not the RAMS performance is adequate to start producing the product.

Since there will be no temporary HIPPS installed subsea, it is not relevant to talk about operational testing of a prototype in its true environment. However, some operational testing may still be performed under similar operational conditions. If components are to keep tight under exposure of high temperatures and high pressures, they may be tested under such conditions while submerged in a basin/pool.

The final qualification of the product may be a factory acceptance test (FAT). When the product is custom-built, the customer may witness the test and make the formal approval of the prototype based on test results.

*Phase 6.* covers the physical production of the product. This may imply large scale production which is often the case for standard products, or the final construction of a single product at the target application, which is often the case for a custom-built product. The production process has to be adapted so that the product achieves the desired performance. This means that the production process must not introduce new failures or have any other negative impact on reliability, safety, operability, or maintainability characteristics of the product. When the production process is fine tuned, the full scale production of the product can start [38].

To ensure that the actual performance of the product matches the desired performance, quality assurance is important. An effective quality control system is considered from the early design phases, and covers all parts of the production process [44]. Product batches are tested to eliminate defects, assembly errors, and early failures. If, during testing, a significant number of items are found not to conform with the desired safety standards, the root causes should be found. Root causes may be related to component quality or to the production process, and corrective action should be taken [1].

Acceptance testing is used to test raw materials, parts and components when received from suppliers to decide if the items are acceptable or not with respect to product performance requirements [6]. Specialized and complex products may be subject to a series of tests before they are delivered to the customer [38].

RAMS-related tasks in this phase are:

- Ensure quality control or product samples and production process. In the case of the HIPPS, quality control should focus on verification of construction, installation, and commissioning. Focus should also be directed to the avoidance of construction, installation and commissioning errors.
- For large scale production; Do conformance checking of product samples to weed out non-conforming items.
- Perform safety analyses of scheduled activities in phase 7 that may expose humans or environment to risk, for example activities related to operation, cleaning, testing, maintenance, and disposal.
- Update and finalize operator (user) and maintenance instruction manuals.
- Update and finalize maintenance support preparation.

In case of the HIPPS, this phase concerns the final construction, installation, and commissioning of the system at site. The phase concludes with the site acceptance test (SAT), which is witnessed by the customer.

*Phase 7.* marks the start of the product life cycle for the customer, because this is when the product is put into operation. The phase can be divided into several sub-phases, which according to ISO 12100 [26] consists of:

- Transport, assembly, and installation (at site or at the final destination)
- Commissioning
- Use of the product, including:
  - Setting, teaching/programming or process changeover
  - Operation
  - Cleaning
  - Fault finding
  - Maintenance
  - Repair/overhaul
  - Testing

- De-commissioning, dismantling, and related to safety; disposal.

Phase 7 is when the product's RAMS performance, that should be integrated from early on in the product development process, is challenged and tested in the field. A safe and reliable product reflects a development process in which RAMS requirements have been taken seriously. In this phase, the RAMS activities for the producer of the HIPPS include:

- Data collection and evaluation of the product performance (data from customers and possibly distributors).
- Regular inspection, function testing and maintenance.
- Making decisions regarding "adequate" RAMS performance (and possible actions if adjustments and improvements are required).
- Updating critical items list, the hazard list and RAMS controlling documents.
- Sharing information with users and possibly distributors regarding unrevealed failures.

Customer feedback is necessary to attain input data for customer satisfaction measurements and product improvements [36]. Brombacher [7] points out that actual field reliability performance should be considered in product development processes, to improve the quality of reliability predictions. Still, it may be difficult to get systematic feedback from customers. Regarding the HIPPS, where performance monitoring is required by the IEC 61508 and regulatory authorities, the customer may see the benefit of cooperating so that sufficient statistical significance may be obtained for the data. In the oil and gas industry, reliability data are collected and published through the Offshore reliability data (OREDA) handbooks [40, 41].

*Phase 8.* concludes the product development. Here, the producer assesses the HIPPS delivery from an overall business perspective. Costs, such as warranty expenses, profits from sale, and business consequences like product recalls, bad reputation, and liabilities due to inadequate RAMS performance, should be evaluated [38]. These analyses are enabled by assessing the collected data about RAMS performance and the expenses regarding reported failures and customer complaints. The main outcome of phase 8 should be to gain organizational learning and insights that are valuable for the development of the next product generation [9].

Phase 7 and 8 occur more or less parallel in time, but at different levels. Phase 7 encompasses the activities carried out by the responsible engineering and development team. The business level involves strategic marketing and management decisions based on results from phase 7.

## 6. Concluding Remarks

In this article we have integrated RAMS aspects into the model of Murthy et al. [38], and argued that the approach fits into the framework of safety life cycle of IEC 61508 [20]. The safety life cycle covers the development of a SIS, including all phases from "cradle to grave". The approach has similarities to other system development processes, such as the systems engineering process in which a need is identified and analyzed, before designing, solving the problem, verifying and testing the chosen solution [6, 52]. For each phase in the safety life cycle, activities and recommendations for achieving functional safety are described, addressing not only a single system, but several that may be included in the EUC.

A SIS, such as the HIPPS, is not only subject to functional safety requirements, as is the focus of IEC 61508. The technological progress leads to systems performing an increasing number of tasks, and as a consequence, our activities are getting more dependent on the ability of the systems to deliver the expected services. This means that, like any other product, a successful SIS has to possess sufficient quality features, related to reliability, availability, and maintainability performance, along with safety. By using the model of Murthy et al. [38], we achieve a more holistic development process of a SIS, focussing not only on safety performance, but placing equal importance on RAM requirements, as well. Besides the RAMS performance, there may be other attributes subject to trade-offs in the requirement specification process, for example, costs, usability, and aesthetics, depending on type of product or system. In the HIPPS example, these do not play a prominent part of the development process. For consumer products, such as cars, these attributes have to be addressed more explicitly.

## 7. Further work

The focus in this article is mostly on custom-built products, like the HIPPS, but it would be useful to describe how the model could be applied in a development process of a standard consumer product. Originally, the model was developed to help producers' specify reliability performance of a product. However, whether the model may be suitable for improving the RAMS performance from a customer's perspective, should be further exploited.

## References

[1] Andersen, B. & Fagerhaug, T. (2006). *Root cause analysis: simplified tools and techniques*. Milwaukee, Wis.: ASQ Quality Press.

[2] ATEX 94/9/EC (1994). *Directive 94/9/EC of the European Parliament and of the council of 23 March 1994 on equipment and protective systems intended for use in potentially explosive atmospheres (ATEX)*. Brussels, Belgium: European Union.

[3] Bak, L., Sirevaag, R., & Stokke, H. (2006). Experience with the HPHT subsea HIPPS on Kristin. In *Deep Offshore Technology - Conference and Exibition*, 28.-30.November 2006, Houston, Texas.

[4] Berden, T., Brombacher, A., & Sander, P. (2000). The building bricks of product quality: an overview of some basic concepts and principles. *International Journal of Production Economics*, *67*(1), 3 – 15.

[5] Bergman, B. & Klefsjö, B. (1994). *Quality: from customer needs to customer satisfaction*. Lund, Sweden: Studentlitteratur.

[6] Blanchard, B. S. & Fabrycky, W. J. (1998). *Systems engineering and analysis*. Upper Saddle River, NJ: Prentice Hall.

[7] Brombacher, A. C. (1999). Maturity index on reliability: covering non-technical aspects of iec 61508 reliability certification. *Reliability Engineering and System Safety*, *66*, 109–210.

[8] den Ouden, H., Yuan, L., Sonnemans, P., & Brombacher, A. (2006). Quality and reliability problems from a consumer's perspective: an increasing problem overlooked by businesses? *Quality and Reliability Engineering International*, *22*(7), 821 – 38.

[9] Dhudsia, V. (1992). Guidelines for equipment reliability. Technical report, SEMATECH.

[10] DNV RP A203 (2001). *Qualification procedures for new technology*. Det Norske Veritas (DNV).

[11] Gershenson, J. K. & Stauffer, L. A. (1999). A taxonomy for design requirements from corporate customers. *Research in Engineering Design*, *11*, 103–115.

[12] Gertman, D. I. & Blackman, H. S. (1993). *Human reliability and safety analysis data handbook*. New York: John Wiley & Sons, Inc.

[13] GPSD (2001). *Directive 2001/95/EC of 3 December 2001 on general product safety*. Brussels, Belgium: Official Journal of the European Communities.

[14] Grady, J. O. (2006). *System requirements analysis*. Amsterdam: Elsevier Academic Press.

[15] Grady, J. O. (2007). *System verification*. Amsterdam: Elsevier Academic Press.

[16] Hokstad, P. & Rausand, M. (2008). Common cause failure modeling: status and trends. In K. B. Misra (Ed.), *Handbook of Performability Engineering* chapter 39. London: Springer-Verlag.

[17] IEC 61160 (2005). *Design review*. Geneva: International Electrotechnical Commission.

[18] IEC 60300 (2003). *Dependability management*. Geneva: International Electrotechnical Commission.

[19] IEC 60601-1 (2005). *Medical electrical equipment - part 1: general requirements for basic safety and essential performance*. Geneva: International Electrotechnical Commission.

[20] IEC 61508 (1998). *Functional safety of electrical/electronic/programmable electronic safety-related systems*. Geneva: International Electrotechnical Commission.

[21] IEC 61511 (2003). *Functional safety - safety instrumented systems for the process industry*. Geneva: International Electrotechnical Commission.

[22] IEC 61513 (2004). *Nuclear power plants - instrumentation and control for systems important to safety - general requirements for systems*. Geneva: International Electrotechnical Commission.

[23] IEC 62061 (2005). *Safety of machinery - functional safety of safety-related electrical, electronic and programmable electronic control systems*. Geneva: International Electrotechnical Commission.

[24] IEC 62278 (2002). *Railway applications - specification and demonstration of reliability, availability, maintainability and safety (RAMS)*. Geneva: International Electrotechnical Commission.

[25] ISA TR 84.00.02 (2002). *Safety instrumented functions (SIF) - safety integrity level (SIL) evaluation techniques. Parts 1-5*. Research Triangle Park, NC: The Instrumentation, Systems, and Automation Society.

[26] ISO 12100-1 (2003). *Safety of machinery - basic concepts, general principles for design - part 1:Basic terminology, methodology.* Geneva: International Organization for Standardization.

[27] ISO 14121-1 (2007). *Safety of machinery - risk assessment - part 1: principles*. Geneva: International Organization for Standardization.

[28] Jackson, Y., Tabbagh, P., Gibson, P., & Seglie, E. (2005). The new Department of Defense (DoD) guide for achieving and assessing RAM. volume 2005, (pp. 1 – 7)., Alexandria, VA, United States.

[29] Kirwan, B. (1994). *A guide to practical human reliability assessment*. London: Taylor &Francis Ltd.

[30] Langeron, Y., Barros, A., Grall, A., & Berenguer, C. (2007). Safe failures impact on safety instrumented systems. In T. Aven & J. Vinnem (Eds.), *Risk, Reliability, and Societal Safety*, volume 1 (pp. 641–648). London: Taylor & Francis.

[31] Lundteigen, M. A. & Rausand, M. (2006). Assessment of hardware safety integrity. In *Proceedings of the 30th ESReDA seminar hosted by SINTEF, Trondheim, Norway, June 7-8*, (pp. 185–198)., Ispra, Italy. ESReDA, European Commission, Joint Research Centre.

[32] Lundteigen, M. A. & 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*(3), 218–229.

[33] Lundteigen, M. A. & Rausand, M. (2008a). Architectural constraints in IEC 61508: do they have the intended effect? *Reliability Engineering and System Safety, (Accepted for publication)*.

[34] Lundteigen, M. A. & Rausand, M. (2008b). Partial stroke testing of process shutdown valves: how to determine the test coverage. *Journal of Loss Prevention in the Process Industries, (Accepted for publication)*.

[35] Lundteigen, M. A. & 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.

[36] Markeset, T. & Kumar, U. (2003). Integration of RAMS and risk analysis in product design and development work processes. *Journal of Quality in Maintenance Engineering*, *9 (4)*, 393–410.

[37] Minderhoud, S. & Fraser, P. (2005). Shifting paradigms of product development in fast and dynamic markets. *Reliability Engineering and System Safety*, *88*(2), 127 – 135.

[38] Murthy, D. N. P., Østerås, T., & Rausand, M. (2008). *Product reliability: specification and performance*. London: Springer.

[39] NORSOK Z-016 (1998). *Regularity management and reliability technology*. Oslo, Norway: Pronorm.

[40] OREDA (1997). *OREDA reliability data* (3rd ed.). Available from: Det Norske Veritas, NO 1322 Høvik, Norway: OREDA Participants.

[41] OREDA (2002). *OREDA reliability data* (4rd ed.). Available from: Det Norske Veritas, NO 1322 Høvik, Norway: OREDA Participants.

[42] Papadopoulos, Y. & McDermid, J. A. (1999). The potential for a generic approach to certification of safety critical systems in the transportation sector. *Reliability Engineering and System Safety*, *63*, 47–66.

[43] Rausand, M. & Høyland, A. (2004). *System reliability theory: models, statistical methods, and applications* (2nd ed.). Hoboken, NJ: Wiley.

[44] Ridley, J. & Pearce, D. (2002). *Safety with machinery*. Oxford: Butterworth-Heinemann.

[45] Rouvroye, J. L. & Brombacher, A. C. (1999). New quantitative safety standards: different techniques, different results? *Reliability Engineering and System Safety*, *66*, 121–125.

[46] Sintef (2006). *Reliability prediction methods for safety instrumented systems, PDS method handbook*. Trondheim, Norway: Sintef.

[47] Smith, D. J. & Simpson, K. G. L. (2005). *Functional safety – a straightforward guide to applying the IEC 61508 and related standards*. Burlington, U.K.: Elsevier.

[48] Summers, A. (2003). Differences between IEC 61511 and ISA 84. In *Safety Instrumented Systems for the Process Industry*, (pp. 45–54)., SIS-TECH Solutions, Houston, TX.

[49] Summers, A. & Zachary, B. (2000). Partial-stroke testing of safety block valves. *Control Engineering*, *47*(12), 87–89.

[50] Summers, A. & Zachary, B. (2004). High integrity protection systems. In *Proceedings of the Annual Symposium on Instrumentation for the Process Industries*, volume 488, (pp. 49–59).

[51] U.S. Air Force (2000). *Air force system safety handbook*. Kirtland, NM: Air Force Safety Agency.

[52] Utne, I. B. (2006). Systems engineering principles in fisheries management. *Marine Policy*, *30*(6), 624–634.

# Article 8 (conference)

The effect of partial stroke testing on the reliability of safety valves
In *Risk, Reliability and Societal Risk*, Volume 3. Taylor & Francis 2007, p. 2479-2486

Is not included due to copyright

## Article 9 (conference)

A new approach for follow-up of safety instrumented systems in the oil and gas industry
In *Safety, Reliability, and Risk Analysis: Theory, Methods and Applications*, Volume 3. CRC Press. 2008, p. 2921–2928

## Article 10 (conference)

Assessment of hardware safety integrity requirements
In *I: Reliability of Safety-Critical Systems: Proceedings of the 30th ESReDA Seminar*. European Commission, Joint Research Centre, p. 185–198, 2006

# Assessment of Hardware Safety Integrity Requirements

Mary Ann Lundteigen
Department of Production and Quality Engineering
Norwegian Institute of Science and Technology
7491 Trondheim, Norway

Marvin Rausand
Department of Production and Quality Engineering
Norwegian Institute of Science and Technology
7491 Trondheim, Norway

## Abstract

*Safety instrumented systems are installed to detect hazards and mitigate their consequences. Several international standards give requirements and guidance on how to design, operate and maintain such systems. Two relevant standards for safety instrumented systems in the process industry are the IEC 61508 and the IEC 61511. The two standards propose requirements related to how hardware architecture may be configured, also referred to as architectural constraints. The main objectives in this paper are to clarify the application of these requirements, discuss some of the related ambiguities, and propose ways to improve the requirements.*

**Keywords:** IEC 61508, IEC 61511, hardware safety integrity, architectural constraints, safe failure fraction (SFF)

## 1. Introduction

Safety instrumented systems (SIS) are used in many industrial processes to reduce the consequences of process demands on humans, the environment and material assets. Process demands may be hazardous events like, e.g., overpressure and gas leakage, requiring a response by the SIS. One important aspect of SIS is the ability to perform its intended safety functions upon demand. Measures are therefore required to obtain reliable design and implementation of SIS hardware and software.

International standards have been developed to ensure that the SIS is designed, implemented and operated according to the specified needs. The focus in this paper is on SIS applications in the process industry, and here the IEC 61508 [1] and the IEC 61511 [2] have been widely accepted. Both standards give lifecycle requirements for the SIS. IEC 61508 is a generic standard, and is often used by vendors when developing new products. IEC 61511 is a sector specific standard for the process industry based on the same concepts as IEC 61508, and focusing on the integration of certified or proven-in-use hardware and software components. Both standards use the term *safety integrity* as an expression for the ability of the SIS to perform its intended safety functions.

IEC 61508 and IEC 61511 split the safety integrity into two parts; *hardware safety integrity* and *systematic safety integrity*. Both parts are important to ensure reliable design and implementation of hardware and software. Hardware safety integrity is related to random hardware failures, while systematic safety integrity is related to systematic failures. The safety integrity is split into four discrete safety integrity levels (SIL), SIL1 to SIL4. SIL4 is the level with the most stringent requirements. To fulfill a specified SIL, the SIL requirements related to hardware safety integrity as well as systematic safety integrity must be met.

The hardware safety integrity requirements comprise two different aspects of SIS reliability; 1) the quantified evidence that the safety function is able to meet the reliability target and 2) the necessary constraints on the system architecture that ensure sufficient fault tolerance. The latter is often referred to as *architectural constraints*. In this context, constraints are a set of requirements that limits the designers' freedom on how the hardware may be configured.

Several papers discuss the application of IEC 61508 and IEC 61511 [3-12], but few papers cover the architectural constraints in a broad perspective. Several guidelines and reports on the application of IEC 61508 and IEC 61511 are available on the Internet. One such example is the OLF-070 guideline developed by the Norwegian Oil Industry Association [13]. The papers and guidelines address various aspects of how the IEC 61508 and IEC 61511 requirements should be adopted. The standards are not prescriptive, which gives room for different interpretations, and hence opens up for new methods, approaches and technology. If inadequate methods and technology are selected, they may produce solutions that are not sufficiently safe. Rouvroye and van den Blick [14] and Rouvroye and Brombacher [15] compare different qualitative and quantitative safety analysis techniques and show that they may lead to different results. They conclude that more research is required to assess which technique is most suited in different situations. Van Beurden and Van Beurden-Amkreutz [16] compare the IEC 61508 and the IEC 61511 requirements on architectural constraints, and discuss that, e.g., the standards have different definitions of *proven-in-use* components. Goble [17, 18] discusses several aspects of architectural constraints, e.g., the rationale of relating safe failure fraction (SFF) to architectural constraints and how different assumptions and estimation techniques may lead to different estimates of failure rates.

This paper focuses on the requirements related to architectural constraints. The objectives are to clarify the application of these requirements, discuss some of the related ambiguities, and propose improvements and areas of further research.

The paper is organized as follows; Section 2 discusses basic concepts related to hardware safety integrity. Section 3 gives a brief description of the quantitative part of hardware safety integrity, and a more detailed presentation of the requirements related to the architectural constraints. A four-step procedure is proposed to clarify the necessary analytical steps that determine the required hardware architecture. Section 4 discusses the ambiguities related to architectural constraints, and section 5 proposes some related improvements. Section 6 gives some final remarks, proposed improvements and conclusions.

## 2. Basic Concepts

In this section the basic concepts related to architectural constraints are discussed and clarified.

### 2.1 Safety instrumented function versus safety instrumented system

A safety instrumented function (SIF) is used to describe the safety functions implemented by instrumented technology. The SIS is the physical system implementing one or more SIFs. The SIF may be considered as a *barrier function*, while the SIS may be considered as a *barrier system* [19]. The SIF usually performs the following actions or subfunctions; detect process demands, decide what to do and act in order to bring the process back to a safe state. The configurations of physical components used to implement the subfunctions may be referred to as *subsystems*. The subsystems may comprise input elements like sensors, push buttons and switches, logic solvers like programmable electronic solvers (PLC) or hardwired logic solvers, and final elements like valves, solenoids and circuit breakers. The relationship between a SIF and a SIS is illustrated in Figure 1.

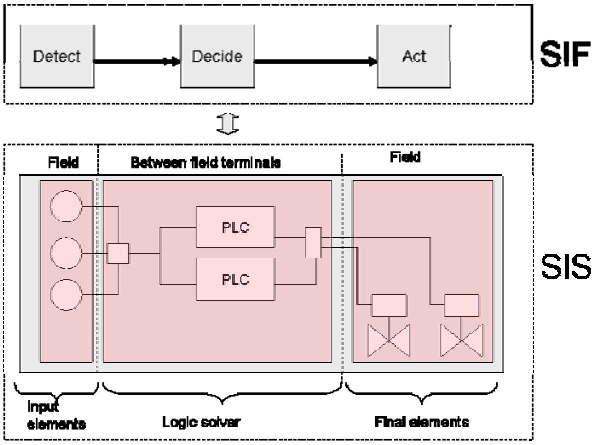


**Figure 1.** SIS versus SIF

The SIL requirements are allocated to a specific SIF. To assess the hardware safety integrity, it is therefore necessary to analyze the configurations of the hardware architecture that realizes the SIF.

### 2.2 Failure classification

Failures may be classified in many different ways [20, 21]. They may be classified according to their causes or according to their effects. IEC 61508 and IEC 61511 use both approaches. Failures classified according to their causes may be referred to as either random hardware failures or systematic failures. Failures classified according to their effects may be referred to as safe or dangerous failures. The four types of failures are in IEC 61508 and IEC 61511 described as follows:

- *Random hardware failures:* Failures occurring in random time resulting from a variety of degradation mechanisms in the hardware. Usually, only degradation mechanisms arising from conditions within the design envelope (natural conditions) are considered as random hardware failures. A constant rate of occurrence of such failures (ROCOF) is usually assumed.
- *Systematic failures:* Failures related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design, manufacturing process, operational procedures, documentation or other relevant factors. Design faults and maintenance procedure deficiencies are examples of causes that may lead to systematic failures.
- *Safe failures:* Failures that do not prevent the SIS from performing its intended safety functions. The immediate consequences of safe failures are typically spurious trips or false alarms. However, restoration of a safe failure may in some situations be hazardous.
- *Dangerous failures:* Failures that prevent the SIS from performing its intended function upon a demand.

Safe and dangerous failures may be split into two subcategories, detected and undetected. According to IEC 61508 and IEC 61511, detected failures are failures that are revealed by online (self) diagnostics. Undetected failures are only revealed during periodic proofs tests (often referred to as functional tests).

## 2.3 Safe failure fraction and hardware fault tolerance

The safe failure fraction (SFF) and the hardware fault tolerance are two important parameters related to architectural constraint. The SFF is a parameter that gives the fraction of failure rates considered as “safe” versus the total failure rates. In this context, “safe” failures comprise safe failures and dangerous failures detected by diagnostics. The dangerous detected failures are considered “safe” as it is assumed immediate follow-up and repair. It is also assumed that compensating measures are implemented to ensure that the level of safety integrity is maintained during this period. A compensating measure may be degraded operation of the SIS, which means that the SIS changes the voting of redundant channels to reflect that one component is not operational. The SIS may for example degrade a configuration voted 2oo3 to a 1oo2 upon a dangerous detected failure. Here, a KooN configuration is a configuration where K out of N channels (or redundant components) must function in order to perform the safety function.

Another interpretation of SFF is that it gives the fraction of failures not leading to a dangerous failure of the safety function [22]. The SFF is calculated from the following equation:

$$SFF = \frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_{Tot}} = \frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_S + \sum \lambda_{DD} + \sum \lambda_{DU}} \qquad (1)$$

where $\sum\lambda_S$ is the sum of safe failure rates (detected as well as undetected), $\sum\lambda_{DD}$ is the sum of dangerous detected failure rates, $\sum\lambda_{DU}$ is the sum of dangerous undetected failure rates, , and the $\sum\lambda_{Tot}$ is the sum of all failure rates. The application of the SFF is further discussed in sections 3.2 and 4.

Fault tolerance is according to IEC 61508 defined as the "ability of a functional unit to continue to perform a required function in the presence of faults or errors". The hardware fault tolerance measures the number of faults tolerated before the safety function is affected. To model the architecture, a reliability block diagram may be used. A 1oo2 and a 2oo3 system have a hardware fault tolerance equal to 1 while a 1oo3 system has a hardware fault tolerance of 2.

## 3. Hardware Safety Integrity

Some main quantitative and qualitative requirements to hardware safety integrity are listed in Table 1. The requirements are found in part 2 of IEC 61508 [23]. A brief summary of the requirements is also given by Smith and Simpson [24]. The requirements are used to determine or verify the *hardware safety integrity level* of the hardware architecture. The hardware safety integrity level corresponds to the lowest SIL obtained from using the qualitative and quantitative requirements.

**Table 1:** Hardware safety integrity requirements [23]

| | |
|---|---|
| Quantitative requirements | The probability of failure of safety functions due to random hardware failures shall be estimated so that:<br>The probability of failure of each safety function shall be equal or less than the target value<br>• The estimation should take into account the following:<br>- Hardware architecture (configuration)<br>- Dangerous detected and undetected failures<br>- Susceptibility with respect to common cause failures utilizing plant specific beta-factor<br>- Diagnostic coverage of the diagnostic test intervals<br>- Repair times for detected failures<br>- Proof test intervals (periodic functional tests)<br>- The probability of undetected failure of any data communication process |
| Qualitative requirements | Architectural constraints shall be identified. The architectural constraints limit the achievable SIL based on hardware fault tolerance and safe failure fraction (SFF) of the subsystem. |

In the following sections, the applications of these requirements are elaborated in more detail.

### 3.1 Quantitative requirements

IEC 61508 and IEC 61511 distinguish between a SIS operating in a low demand mode and in a high demand (continuous) mode. A demand is a process deviation that must be handled by the SIS. Low demand mode means that the SIS experiences a low frequency of demands, typically less than once per year. If more frequent demands are expected, typically several times a year, the SIS is operating in a high or continuous mode. The probability of SIF failure due to random hardware failures in the low demand mode is often quantified as the probability of failure on demand (PFD). It is often the average PFD within a proof test interval, and not the time dependant PFD that is being used. In the high demand mode, any dangerous undetected failure is likely to cause SIF failure. Hence, for SIS operating in the high or continuous mode it is often the frequency of dangerous failures to perform the SIF (per hour) that is calculated.

A range of PFD values is allocated to each SIL. However, it is the calculated probability of a SIF failure that should be compared to the initial risk reduction target, and not any other PFD value within the range of the corresponding SIL. This issue is also emphasized by Smith and Simpson [24].

The reliability calculations must consider all requirements addressed in Table 1. IEC 61508 proposes to use the standard β-factor model for modeling common cause failures (CCFs), while IEC 61511 lists a number of alternative approaches. The β-factor model is discussed, e.g., in Rausand and Høyland [20]. A CCF is a multiple failure affecting several or all of the redundant channels, potentially leading to failure of the safety function. A channel means here a single component or a group of components that independently perform a subfunction. In redundant systems, the contribution from CCFs is often the dominant part compared to the contribution from single failures.

The petroleum industry in Norway often apply an extended version of the standard β-factor model, referred to as the PDS method [13, 25]. The PDS method calculates the effect of CCFs between 2 or more redundant channels in KooN configurations [26, 27], and incorporates the effect on PFD from degraded operation and potential failures introduced during testing. The PDS method also describes how the contribution from systematic failures may be added. In the PDS method handbook it is argued that random hardware failures only represent a limited fraction of the actual experienced failures, and that systematic failures should be included to better predict the real performance of the SIS.

IEC 61508 states that the mean time to restoration for a given component should be calculated by adding the diagnostic test interval and the (mean) repair time of detectable failures. The diagnostic test interval may be omitted if the diagnostic tests are run close to continuously. If the diagnostic tests are run less frequently, it is important to also assess the effect of the diagnostic test interval.

### 3.2 Qualitative requirements

The qualitative requirements comprise measures necessary to determine the architectural constraints. There are two approaches to how these requirements are applied; they may be applied to specify the required architecture or applied to verify if a given architecture corresponds to a specified SIL.

The rationale for introducing architectural constraints is to "achieve a sufficiently robust architecture, taking into account the level of subsystem complexity" (IEC 61508 and IEC 61511). The statement may imply a low confidence in how complexity is captured in reliability calculations, since the requirements related to architectural constraints limit the achievable SIL regardless of the quantified result. There are several reasons why the quantified reliability may be uncertain:

- Only random hardware failures are included in the calculations
- Failure modes may have been omitted due to misinterpretations
- Only the average PFD within the proof test interval is usually calculated
- The failure data used for quantification are uncertain
- The contribution from software failures is usually not considered

Some of these limitations may be overcome by using more exact reliability calculation models, but it is not possible to remove all uncertainty like i.e. uncertainty in failure rates. It may therefore seem reasonable to have some qualitative measures that may ensure sufficient fault tolerance.

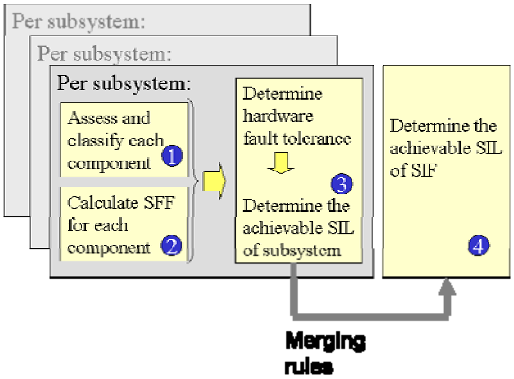

Per subsystem:
Per subsystem:
Per subsystem:
Assess and classify each component
1
Calculate SFF for each component
2
Determine hardware fault tolerance
3
Determine the achievable SIL of subsystem
Determine the achievable SIL of SIF
4
Merging rules

**Figure 2.** Four-step procedure to determine the architectural constraints

To determine the architectural constraints of a SIF, it is necessary to carry out the following analytical steps:

1) Assess and classify the subsystem components
2) Calculate the SFF for each component
3) Determine the achievable SIL of the subsystem

4) Determine the achievable SIL of the SIF

The four steps, referred to as the four-step procedure, are illustrated in Figure 2. The first three steps determine the architectural constraints for each subsystem. The forth step comprises a set of merging rules used to obtain the overall architectural constraints of the SIS components used to implement the SIF.

In the following, a more detailed description of the necessary steps is given.

*Step 1: Assess and classify the subsystem components*
IEC 61508 and IEC 61511 require that the subsystem components are assessed and classified. The objective is to assess the complexity of the component and thereby the uncertainty associated with the components' behavior. IEC 61508 uses a rather generic classification where components are classified as type A or type B. Type A components are characterized by well defined failure modes, completely determined behavior and sufficiently documented performance by field experience data. Sufficiently documented performance means to fulfill the IEC 61508 requirements for proven-in-use. Valves and solenoids are often considered as type A components. Type B components do not meet one or more of these requirements. Components having application software are often considered as type B.

IEC 61511 uses a more industry specific and straightforward classification, and defines programmable electronic logic solvers as one class and sensors, final elements and non-programmable electronic logic solvers as another class. The latter group is considered to have less complexity. The IEC 61511 classification may be used if the components are considered as proven-in-use by this standard. To be considered proven-in-use by IEC 61511, it is required to document evidence of prior performance in safety or non-safety applications. The proven-in-use requirements are further discussed by Van Beurden and Van Beurden-Amkreutz [16], who highlight the fact that IEC 61508 has straighter requirements to proven-in-use than IEC 61511.

*Step 2: Calculate the SFF*
The SFF must be determined for the components of the subsystem using equation (1). IEC 61508 and IEC 61511 assume similar components in redundant configurations; hence each subsystem is associated with one SFF value. In case the redundant components are dissimilar, it may be necessary to treat the components as independent subsystems.

One important issue when calculating the SFF is how the failures are classified. The distinction between dangerous detected and undetected failure rates seems to be ambiguous, an issue which is further discussed in section 4. At present, it is possible to increase the SFF by increasing the safe failure rates. However, this approach is probably not intended by the standards, and may not imply a good engineering practice.

The OLF-070 guideline lists generic SFF values for typical components used in the petroleum industry. The data have been derived from the PDS data handbook [28] that contains generic failure data mainly based on the offshore reliability database OREDA [29, 30]. Vendors may also provide failure rates for their components.

Regardless of data source selected, it is important to ensure that the data are valid and suitable for the application.

*Step 3: Determine the achievable SIL of the subsystem*
To determine the achievable SIL of a subsystem, it is first necessary to determine the hardware fault tolerance. The hardware fault tolerance is found by assessing the voting of the hardware architecture, as explained in section 2.3. Step 3 is repeated until all subsystems implementing the SIF have been covered.

The relationship between the achievable SIL, the hardware fault tolerance of a subsystem and the SFF is given by the hardware fault tolerance tables in IEC 61508 and IEC 61511. There are two tables in each standard, one table for each class of components, see Table 2. The two tables in IEC 61511 have been transformed so that they have a similar setup as the tables in IEC 61508. Note that the table uses the following abbreviations: Hardware fault tolerance (HFT), sensor (S), final element (FE) and programmable electronic logic solver (PE LS).

**Table 2:** Hardware fault tolerance tables in IEC61508 and IEC 61511

| | **IEC61508** | | | | | | **IEC 61511** | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **SFF** | **Type A** | | | **Type B** | | | **S, FE, non-PE LS** | | | **PE LS** | | |
| **/HFT** | **0** | **1** | **2** | **0** | **1** | **2** | **0** | **1** | **2** | **0** | **1** | **2** |
| **<60%** | SIL1 | SIL2 | SIL3 | - | SIL1 | SIL2 | Not relevant | | | - | SIL1 | SIL2 |
| **60-90%** | SIL2 | SIL3 | SIL4 | SIL1 | SIL2 | SIL3 | SIL1 | SIL2 | SIL3 | SIL1 | SIL2 | SIL3 |
| **90-99%** | SIL3 | SIL4 | SIL4 | SIL2 | SIL3 | SIL4 | Not relevant | | | SIL2 | SIL3 | Note[1] |
| **>99%** | SIL3 | SIL4 | SIL4 | SIL3 | SIL4 | SIL4 | Not relevant | | | SIL2 | SIL3 | Note[1] |

As seen from Table 2, there are differences between how IEC 61508 and IEC 61511 relate the hardware fault tolerance to SFF and SIL. This issue is also discussed by Van Beurden and Van Beurden-Amkreutz [16]:

- IEC 61511 does not treat SIL 4 systems
- IEC 61511 does not give extra credit for SFF above 99%
- In IEC 61511, the class of sensors, final elements and non-programmable electronic solvers is independent of SFF. The hardware fault tolerance versus SIL corresponds to a SFF of 60-90%.
- The IEC 61511 allows a reduction in the hardware fault tolerance by 1 for IE, FE and non-PE LS if certain conditions are met. Without this rule, the IEC 61511 would in most cases require more hardware fault tolerance than if using the IEC 61508 classification.

*Step 4: Determine the achievable SIL of the SIF*
Once the achievable SIL has been obtained for each subsystem, the next step is to develop the achievable SIL of the SIF.

[1] IEC 61511 does not relate hardware fault tolerance and SFF to SIL4 systems. For SIL4 systems it is necessary to comply with the requirements in IEC 61508.

IEC 61508 proposes a set of merging rules to be used to determine the achievable SIL of the SIF. The merging rules are rather simple; the achievable SIL for subsystems in series is restricted by the subsystem having the *lowest* SIL, while the achievable SIL for subsystems in parallel is equal to the subsystem having the *highest* SIL plus one level. The assessment of the subsystems is repeated until the overall achievable SIL by architecture is obtained. The merging rules demonstrate that lower SIL components may be used to satisfy the needs for a higher SIL function.

## 4. Ambiguity and uncertainty of architectural constraints

As previously discussed, the architectural constraints have been introduced to ensure a sufficiently robust architecture. A fundamental question to ask is why these requirements are needed. Another question is whether the requirements may be interpreted differently in a way that may lead to different results.

Quantitative risk and reliability assessments are based on the belief that reliability may be estimated and that the result has some valuable meaning for decision makers. However, such assessments are always based on various assumptions. The gap between a reliability model with its assumptions and the real world determines the uncertainty of the quantified result. Some potential sources of uncertainty are discussed in section 3.2. When the complexity of the system increases, one may expect that the uncertainty in the quantified result also increases. The principle of introducing architectural constraints may be seen as a precautionary principle [31]; if we have insufficient evidence that the safety is good enough, additional measures should be introduced. However, it is not evident if the requirements related to architectural constraints are able to capture complexity in a better way than existing quantitative approaches.

A closer look at the requirements related to architectural constraints, indicate that they open up for different interpretation that may lead to different architecture. The parameter that seems to be the most ambiguous is the SFF. The uncertainty related to classification of components seems to be associated how to comply with the IEC 61508 requirements for proven-in-use. The definition of hardware fault tolerance is rather straight forward, and the uncertainty seems to be related to how well the real SIS configurations have been captured in the architecture model (reliability block diagram).

There are at least three factors that may lead to different results when calculating the SFF. The first factor is the vague distinction between diagnostic testing and proof testing. The main uncertainty seems to be related to whether the length of the test interval should influence if the test is classified as a diagnostic test or a proof test. Today, the standards refer to diagnostic testing as online testing as well as automated tests performed continuously or periodically. It seems not clear if “automated or not” or “online or not” is the key issue? Ali and Goble [32] have proposed partial stroke testing as a means to increase the SFF, without discussing any requirements to the diagnostic test interval. Would a partial stroke testing every week versus every two months influence how we classify the test? IEC 61508 and IEC 61511 require that the diagnostic test interval shall be taken into account through the mean time to restoration when calculating the PFD, but it is not clear from the paper by Ali and Goble that this has been done.

A second factor is that the SFF may be increased by increasing the number of safe failures. At present, there is no restriction in the IEC 61508 and IEC 61511 on what to consider as safe failures as long as they are not dangerous. This means that non-essential features having no meaning for the safety function may be added as a means to increase the SFF. This is probably not the intention, and the PDS method has therefore proposed an alternative SFF where non-essential (non-critical) failure rates are excluded from the safe failure rates.

A third factor is that vendors may calculate failure rates using different assumptions. This means that failure rates stated by different vendors may not be comparable, an issue that has been discussed by Goble [33]. SFF may therefore not be a parameter which is suitable for comparison between different components.

## 5. Potential improvement of SFF

From the discussions on the ambiguity and uncertainty of architectural constraints, it seems clear that the SFF is the main parameter to question. The first question is whether or not the parameter is important at all. One perspective is to consider hardware fault tolerance as a configuration issue only, where frequency of how often the component fail or do not fail is irrelevant. In this case the SFF would be superfluous. Another perspective is to consider the diagnostics as important, and credit configurations of components with high diagnostic capabilities more than those with poor diagnostics. This approach seems to be in line with current intention in the IEC 61508 and IEC 61511. At present, more research is required to decide which alternative that is the best.

To clarify the application of SFF, the standards should define more precisely the requirements related to diagnostic test intervals, and give some guidance to when a test should be classified as a diagnostic test and when to classify it as a proof test. It should also be emphasized that only safe failures affecting the SIF (such as spurious trips or alarms) should be included in the calculation of the SFF. The latter proposal is in line with the PDS method.

An alternative approach is to replace the SFF by a new parameter. The new parameter, called diagnostic failure fraction (DFF), is really a modification of the SFF that gives some new features. The DFF is defined as:

$$DFF = \frac{\sum \lambda_{DD}}{\sum \lambda_{Tot}} = \frac{\sum \lambda_{DD}}{\sum \lambda_S + \sum \lambda_{DD} + \sum \lambda_{DU}} \qquad (2)$$

From equation (2), it is evident that the DFF only credits improvement of the components' diagnostics (increasing the DFF), while any increase in safe or dangerous undetected failures is punished (decreasing the DFF). An increase in the dangerous detected failure rate often means a corresponding decrease in the dangerous undetected failure rates. It may be desirable to disfavor safe failures since spurious trips or false alarms may have negative long term effects due to wear, hazardous situations during restoration and reduced confidence in alarms. It should be noted that the range of the DFF is different than the present range of SFF, and the hardware fault tolerance tables would need to be recalibrated.

## 6. Discussions and Conclusions

The HSI requirements have been discussed, and various aspects of the requirements related to the architectural constraints have been elaborated. A procedure that clarifies necessary analytical steps to determine architectural constraints has been proposed.

The discussion on the fundamental question “are the requirements related to architectural constraints really needed?” has not been solved, and requires further research and discussions. One approach could be to assess some typical implementations of SIFs, and evaluate in more detail how the various complexity issues are captured by the quantitative and qualitative methods.

It has been shown that SFF is a parameter that may need further clarification. It has also been discussed if the SFF should be replaced by a new parameter, DFF. Further research is required to determine if such a modification would be advantageous.

It is not always evident how requirements should be clarified or improved. Stephenson and McDermid [34] demonstrate an analytical approach for how requirements may be rewritten in a way that removes unwanted ambiguities. First, the various uncertainty elements of the existing requirements are identified, then the various interpretation of the requirements are tested adding necessary assumptions, and last the insight obtained is used to rewrite the requirements. Such a process may demonstrate necessary guidance and clarifications for future updates of the IEC 61508 and IEC 61511.

## 7. References

[1] IEC61508-1, "Functional safety of electrical/electronic/programmable electronic safety related systems - Part 1: General requirements," IEC 1998.

[2] IEC61511-1, "Functional safety - Safety instrumented systems for the process industry sector, Part 1: Framework, definitions, system, hardware and software requirements," International Electrotechnical Commission (IEC) 2003.

[3] B. Knegtering and A. C. Brombacher, "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*, vol. 66, pp. 171-175, 1999.

[4] K. A. L. Van Heel, B. Knegtering, and A. C. Brombacher, "Safety lifecycle management. A flowchart presentation of the IEC 61508 overall safety lifecycle model," *Quality and Reliability Engineering International*, vol. 15, pp. 493-500, 1999.

[5] A. C. Brombacher, "Maturity index on reliability: Covering non-technical aspects of IEC61508 reliability certification," *Reliability Engineering and System Safety*, vol. 66, pp. 109-120, 1999.

[6] S. Brown, "Overview of IEC 61508. Design of electrical/electronic/programmable electronic safety-related systems," *Computing and Control Engineering Journal*, vol. 11, 2000.

[7] K. T. Kosmowski, "Functional safety concept for hazardous systems and new challenges," *Journal of Loss Prevention in the Process Industries*, vol. 19, pp. 298-305, 2006.

[8] A. E. Summers, "Setting the standard for safety-instrumented systems," *Chemical Engineering*, vol. 107, pp. 92-94, 2000.

[9] A. Summers, "Differences between IEC 61511 and ISA 84 " presented at Safety Instrumented Systems for the Process Industry, Houston, TX, United States.

[10] A. E. Summers, "What every manager should know about the new SIS standards," presented at Technical papers of ISA: Safety Instrumented Systems for the Process Industry, Baltimore, MD, United States, May 14-16 2002, 2002.

[11] E. W. Scharpf and W. G. Goble, "State-of-the-art safety verification," *Australian Journal of Instrumentation and Control*, vol. 16, pp. 4-7, 2001.

[12] B. Hoekstra, "Safey integrity - More than hardware," *Hydrocarbon Engineering*, vol. 10, pp. 79-82, 2005.

[13] OLF-GL-070, "Application of IEC 61508 and IEC61511 in the Norwegian Petroleum Industry," 2004.

[14] J. L. Rouvroye and E. G. Van den Bliek, "Comparing safety analysis techniques," *Reliability Engineering and System Safety*, vol. 75, pp. 289-294, 2002.

[15] J. L. Rouvroye and A. C. Brombacher, "New quantitative safety standards: Different techniques, different results?," *Reliability Engineering and System Safety*, vol. 66, pp. 121-125, 1999.

[16] I. Van Beurden and R. Van Beurden-Amkreutz, "What does proven in use imply?," Houston, TX, United States, 2004.

[17] W. M. Goble, "Comparing failure rates," in *Hydrocarbon Processing*: Gulf Publ Co, Houston, TX, USA, 2001.

[18] W. M. Goble, "The safe failure fraction barrier," in *Hydrocarbon Processing*: Gulf Publ Co, Houston, TX, USA, 2001.

[19] S. Sklet, "Safety barriers: Definitions, classification and performance," *Journal of Loss Prevention in the process industries (article in press)*, 2005.

[20] M. Rausand and A. Høyland, *System Reliability Theory - Models, Statistical Methods, and Applications*, Second ed: Wiley, 2004.

[21] M. Rausand and K. Oien, "Basic concepts of failure analysis," *Reliability Engineering & System Safety*, vol. 53, pp. 73-83, 1996.

[22] IEC62061, "Functional safety of safety-related electrical, electronic and programmable electronic control systems," 2001.

[23] IEC61508-2, "Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2:Requirements for electrical/electronic/programmable electronic safety related systems," 2000.

[24] D. J. Smith and K. G. L. Simpson, *Functional safety - A straightforward guide to applying the IEC 61508 and related standards*, Second edition ed: Elsevier, 2005.

[25] SINTEF, "Reliability Prediction Methods for Safety Instrumented Systems - PDS Method Handbook, 2006 Edition," SINTEF 2006.

[26] P. Hokstad and K. Corneliussen, "Loss of safety assessment and the IEC 61508 standard," *Reliability Engineering & System Safety*, vol. 83, pp. 111-120, 2004.

[27] P. Hokstad, "Estimation of Common cause factors from systems with different channels," *IEEE Transactions on Reliability*, vol. 55, 2006.

[28] SINTEF, "Reliability Data for Safety Instrumented Systems - PDS Data Handbook, 2006 Edition," 2006.

[29] H. Langseth, K. Haugen, and H. Sandtorv, "Analysis of OREDA data for maintenance optimisation," *Reliability Engineering & System Safety*, vol. 60, pp. 103-110, 1998.

[30] H. A. Sandtorv, P. Hokstad, and D. W. Thompson, "Practical experiences with a data collection project: the OREDA project," *Reliability Engineering & System Safety*, vol. 51, pp. 159-167, 1996.

[31] J. Hoden, *Ethics and safety: "Mortal" questions for safety management*, vol. 3, 1998.

[32] R. Ali and W. Goble, "Smart positioners to predict health of ESD valves," College Station, TX, United States, 2004.

[33] W. Goble, "SIL verification," in *Hydrocarbon Processing*, 2001.

[34] Z. Stephenson and J. McDermid, "Deriving architectural flexibility requirements in safety-critical systems," *IEE Proceedings: Software*, vol. 152, pp. 143-152, 2005.

# Part III

## Supplementary information

# 4

# Safety instrumented systems

*This chapter briefly explains some frequently used concepts and terms that are used with safety instrumented systems (SISs). The main focus is SIS applications in the oil and gas industry.*

## 4.1 Key concepts

SISs are used in the oil and gas industry to detect the onset of hazardous events and/or to mitigate their consequences to humans, material assets, and the environment. A SIS belongs to the category of safety systems that uses at least some electrical, electronic, and/or programmable electronic components.

A SIS is often split into three main subsystems as illustrated in Fig. 4.1; input elements, logic solvers, and final elements. The input elements are used to *detect* the onsets of hazardous events, the logic solver for *deciding* what to do, and the final elements to *perform* according to the decision.

The SIS may perform one or more safety instrumented function (SIF). The distinction between a SIS and a SIF may be illustrated as in Fig. 4.1. Here, we assume that the SIS comprises two level transmitters (LT), two pressure transmitters (PT), one programmable logic controller (PLC), two shutdown valves, and one circuit breaker. A single SIF may use some of these components, as indicated in the figure. It should be noted that the logic solver is often a shared component for all SIFs that are implemented by the same SIS.

SIS is a term that has been widely accepted in the process industries, including the oil and gas industry, and is used by many standards and guidelines on SIS design, construction, and operation in this industry sector [39, 100]. Still, some other terms with similar meaning may be found in literature, such as instrumented protective system (IPS) and instrumented safety systems (ISS) [13]. IEC 61508, a generic standard on SIS design, construction, and operation, has adopted the term safety-related E/E/PE systems. For machinery, it is more com-

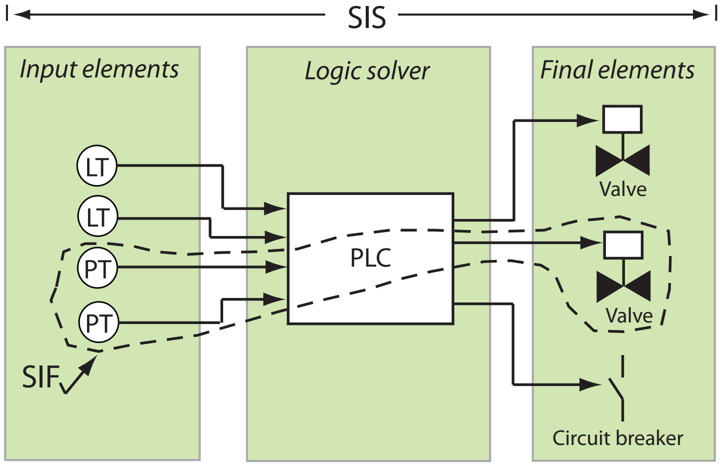


**Fig. 4.1.** The main subsystems of a SIS

mon to talk about safety-related electrical control system (SRECS) [41, 74], since control and safety functions are often combined in the same system.

A plant or an equipment to be protected may have more than one SIS. In this case, they are often given names according to their main functions. On oil and gas installations, we may, for example, find emergency shutdown systems (ESD), process shutdown systems (PSD), high integrity pressure protection systems (HIPPS), and fire and gas (F&G) detection system [100].

## 4.2 SIS technologies

Several authors give thorough descriptions of SIS technologies, see for example Smith and Simpson [116], Goble and Cheddie [24], MacDonald [73, 74], Gruhn [27], CCPS [13].

Input elements may be pneumatic or electrical push buttons, pneumatic or electrical switches, and electrical, electronic, or PE based sensors. The switches may isolate electrical circuits or depressurize hydraulic or pneumatic lines. Sensors may be used to measure current, pressure, temperature, level, concentration (e.g., of smoke and hydrocarbon gases), and radiation (e.g., from a fire). Sensors that are based on PE technology are sometimes referred to as smart sensors or smart transmitters.

The logic solvers are the SIS' "brain" and may be constructed using electrical relays, electronic components (e.g., printed circuit boards), or programmable logic controllers (PLC).

Relay based logic solvers are sometimes referred to as direct wired logic, since the input elements interact directly with the final elements via electrical relays. Printed circuit boards are sometimes called solid state logic, and have a fixed (printed) arrangement of electronic components such as resistors, capacitors, transistors, diodes, and so on.

A PLC comprises input cards, one or more central processing units (CPU), output cards, and associated cables for communication. The logic is mainly implemented by software that is downloaded to the CPU. The use of software reduces hardware costs and eases the process of doing modifications, but leads at the same time to more complex systems with the added features that come with the software.

The decision taken by the logic solver on how to act on the input signals is determined by how the signals are voted. If the input signals are voted $k$-out-of-$n$, the SIF is performed when $k$-out-of-$n$ components raise an alarm. The voting may be implemented by software, hardware, or a combination of both depending on the technology being used.

The SIS may use more than one logic solver to perform the safety functions. This approach is sometimes used in railway signaling systems, where two logic solvers have to agree on setting a green (go) signal, while it is sufficient that one out of the two logic solvers agrees on setting a red (stop) signal.

Final elements may be valves, relays, and circuit breakers capable of stopping flow and isolating electrical equipment. To improve safety and reliability, it is sometimes used more than one final element to perform the same function. In this case, the physical installation determines how the final elements are voted. If two valves are installed in the same pipeline, it is sufficient that $1$-out-of-$2$ valves closes to stop flow.

## 4.3 SIS example

We may briefly illustrate the implementation of a SIS by using a high integrity pressure protection system (HIPPS) as an example. A HIPPS is used to detect if the pipeline pressure exceeds a specified set pressure, and to close dedicated valves to avoid further pressure build-up that may cause pipeline rupture. Pressure build-up may arise from well shut-in pressure (i.e., the maximum wellhead pressure), or from a sudden pipeline blockage, for example a spurious closure of a downstream valve.

A HIPPS typically comprises PTs, logic solver(s), and valves. The main components of a HIPPS are illustrated in Fig. 4.2.

In this example, the logic solver continuously reads and compares the two PT signals with a value that corresponds to the high pressure set point. We assume that the logic solver is configured so that the shutdown valve closes when one out of the two PTs detects a high pressure.

The shutdown valve has two parts, the actuator and the valve. As indicated in Fig. 4.2, we assume that this is a gate valve, since this type is often used when

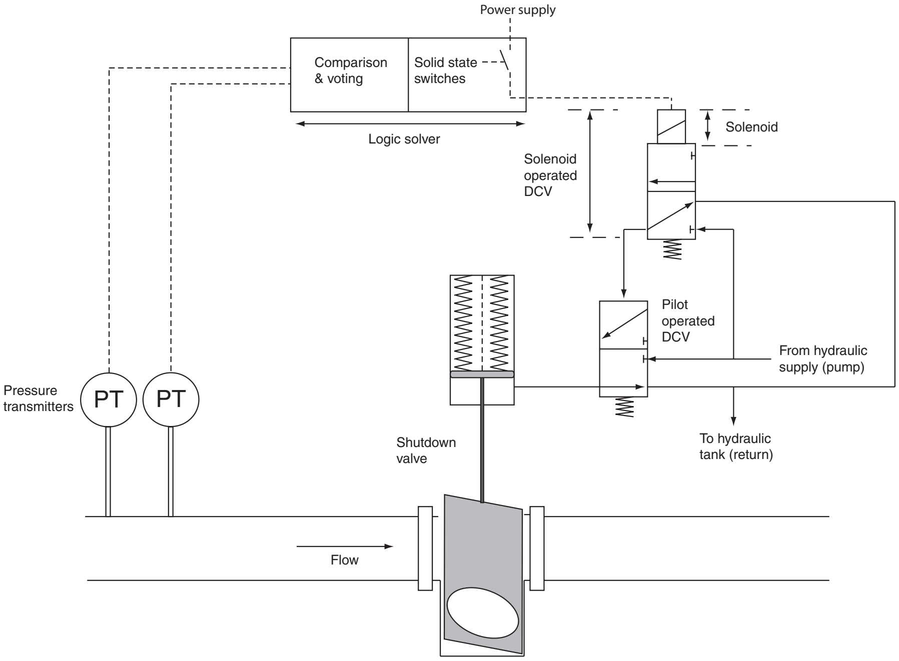


**Fig. 4.2.** SIS example

rapid closure is required. The actuator includes a spring package that forces the valve to close upon loss of hydraulic pressure. Without this spring package, the shutdown valve would be left in the last (open) position.

The shutdown valve is not operated directly by the logic solver, but via two smaller valves, a solenoid operated hydraulic directional control valve (DCV) and a pilot operated DCV, illustrated in Fig. 4.2. As for the shutdown valve, the two smaller valves have springs that force the valves to a specified position upon loss of signal.

The logic solver initiates the valve closure by isolating the power to the solenoid operated DCV. Upon loss of power, this DCV switches and depressurizes the signal line to the pilot operated DCV. It is the pilot operated DCV that controls the hydraulic flow to and from the shutdown valve. Upon loss of pilot signal, the DCV switches so that the shutdown valve actuator is depressurized.

It should be noted that a HIPPS often uses two shutdown valves instead of one and sometimes more than two PTs to achieve the desired level of safety and reliability.

## 4.4 Other related concepts

A SIS design starts with the analysis of the equipment under control (EUC). IEC 61508 [38] uses EUC as a collective term to describe an equipment, machinery, apparatus, or plant that needs some type of protection from the unwanted consequences of hazardous events. At oil and gas installations, the EUC may be a process section that contains hydrocarbon gases under high pressures and high temperatures.

The EUC is usually equipped with an EUC control system that operates the EUC in a desired manner during normal operation, start-up, and planned shutdowns [38]. In the process industries, the EUC control system is sometimes referred to as the (basic) process control system (BPCS) [39]. The EUC control system monitors EUC states, reads commands from operators, and actuates final elements so that the desired state of the EUC is achieved or maintained.

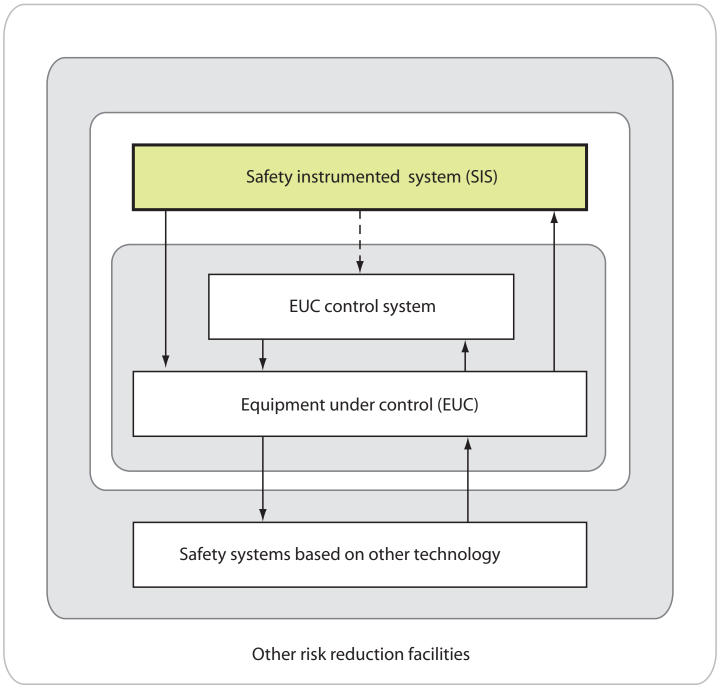

Safety instrumented system (SIS)
EUC control system
Equipment under control (EUC)
Safety systems based on other technology
Other risk reduction facilities

**Fig. 4.3.** EUC, EUC control system, and safety barriers

EUC control systems and SISs use similar types of technologies and have the same main subsystems, but they do not face the same safety and reliability requirements. The EUC control system does not need to comply to the IEC 61508 or related standards, unless safety and control are combined in the same system.

SISs are not the only means to protect of EUC from unwanted consequences. Protection may be provided by non-instrumented components and systems (e.g., pressure relief valves, rupture disks) and other risk reduction measures (e.g., fire walls, drain systems, administrative procedures) [38, 39, 115]. Some means are also inherent properties of the EUC, for example as pressure tolerances of vessels and pipelines.

The protection means that are added to the EUC and the EUC control system are sometimes referred to as protection layers [39] or safety barriers [115]. One way of illustrating the relationship between various protection layers is shown in Fig. 4.3.

When several protection means (or layer) are used, it is important to ensure that they are independent. This means that a failure on one means (or layer) does not lead to a failure of the other. Standards related to safety systems suggest various means to achieve independence, for example through technical design, physical installation, and work practises and procedures.

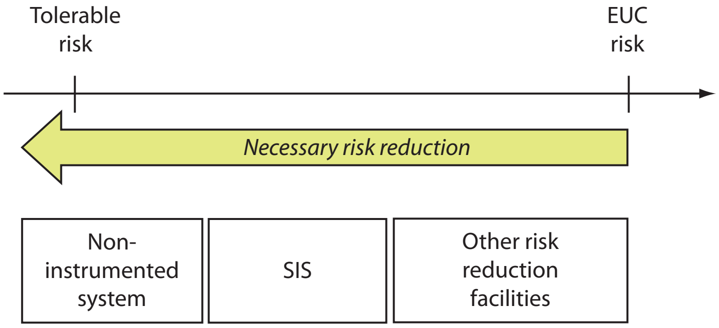


**Fig. 4.4.** EUC risk, tolerable risk, and risk reduction

For on demand safety systems, the reliability of the protection layers is determined from the necessary risk reduction. The necessary risk reduction is the difference between the EUC risk and the tolerable risk level, as illustrated in Fig. 4.4. The EUC risk is the risk arising from the EUC or its interaction with the EUC control system [38], and may be expressed as the expected number of a specified hazardous event (e.g., overpressure) per year. The tolerable risk is the risk which is accepted in a given context (for example on an oil and gas installation on the Norwegian continental shelf) based on the current values of society [39]. The tolerable risk level may be determined by authorities, guidelines, or the plant owner.

The necessary risk reduction may be allocated to one or more protection layers, as illustrated in Fig. 4.4. The risk reduction that is allocated to a SIS will be the reliability target of the associated SIF.

## 4.5 Design principles

Three important and frequently mentioned properties of SIS design are fail-safe operation, fault tolerance, and independence [116, 73, 24, 13].

A SIS that is designed for fail safe operation will, upon specified failures such as loss of power supply, operate in a way where the safe state of the EUC is maintained or achieved. On oil and gas installations, the safe state may be to stop shut down a process section or the whole plant. In this case, the SIS may use de-energize-to-trip components and fail-to-close (position) valves.

A fault tolerant system is able to function even in the presence of one (and sometimes several) failures, and may be achieved by having more than one component to perform the same function. Fault tolerance may be implemented with hardware, software, or a combination of both. The level of fault tolerance is determined by how the (software or hardware) components are voted. A $k$-out-of-$n$ voted configuration has a fault tolerance of $n - k$. This means for example that a $2$-out-of-$3$ system can tolerate one failure before the system is unable to perform its functions, whereas a $1$-out-of-$3$ system tolerates two failures.

Raising the level of fault tolerance improves the reliability, at least when we assume that the components or systems operate and fail independently of each other. In practise, the components or systems may not be independent and the fault tolerance adds more complexity and more maintenance and testing. The level of hardware fault tolerance should therefore be balanced with the need to have systems that are easy to comprehend for designers and end users and that are not too prone to design failures, installation, failures, and maintenance and testing failures. This issue is further discussed in [71].

To design for independence means, at least in the context of a SIS, that the system is designed for robustness against common cause failures (CCFs). A CCF is a failure of more than one device, function, or system due to the same cause [13]. IEC 61508 and IEC 61511 focus on two types of CCFs: CCFs of redundant components in a SIS subsystem and CCFs of SISs (or other technology systems) that are redundant in the sense that they shall provide protection against the same hazardous event.

In practise, it is difficult to avoid that some common causes of failure are present, through common design principles, technologies, physical location, and operational and environmental exposure. But we may reduce the vulnerability through functional diversity (i.e. use of totally different approaches to achieve the same result), diverse technologies (i.e. use of different types of equipment to achieve the same results), separation in physical installation, separation in common services or support systems, and separation in maintenance and testing activities (e.g., staggered testing, using different procedures) [104, 126, 67].

## 4.6 Failure classification

During SIS design, construction, and operation, it is important to avoid introducing failures, to reveal failures, and to correct failures. Failure classification systems are useful means to get more insight into why components fail and what the consequences are. In the following, we briefly discuss some of the main approaches for classifying failure causes and effects.

### Failure classification in OREDA

OREDA handbooks [101, 60] include reliability data collected from oil and gas installations. Here, failure causes are classified as either design-related, fabrication/installation-related, operation/maintenance related, or miscellaneous (not identified or covered by the other categories).

Failure effects are split into critical, degraded, and incipient. A critical failure is defined as a failure of an equipment unit which causes an immediate cessation of the ability to perform a required function. In this context, the term "required function " comprises two elements: The ability to activate on demand and the ability to maintain production when safe (no demands) [114]. This failure category therefore includes failures that may prevent the execution of a SIF as well as unintended (spurious) activation failures.

Degraded failures and incipient failures are partial failures. For degraded failures, this means that some of the functions have failed, but without ceasing the fundamental functions. A hydraulic leakage in an actuator for a fail-safe (close) valve may, for example, lead to spurious closure of the valve, but will not, while in open position, prevent the valve from closing on demand.

An incipient failure is the onset of a degraded failure, and will, if no corrective action is taken, develop into a degraded failure.

### Failure classification in IEC 61508 and IEC 61511

IEC 61508 [38] and IEC 61511 [39] distinguish between random hardware failures or systematic failures for failure causes and safe and dangerous failures for the failure effects. The relationship between all failure categories used by the IEC standards is illustrated in Fig. 4.5.

Random hardware failures are failures that are due to normal degradation, and which for this reason, may be predicted based on a failure distribution function. For safety and reliability assessments of SIS, we often assume exponentially distributed time to failure, which means that we use a constant rate of occurrence of failures ("failure rate").

Systematic failures are failures that are introduced due to design errors, implementation errors, installation errors, or operation and maintenance errors. Unlike random hardware failures, their occurrence cannot be predicted. Instead, the

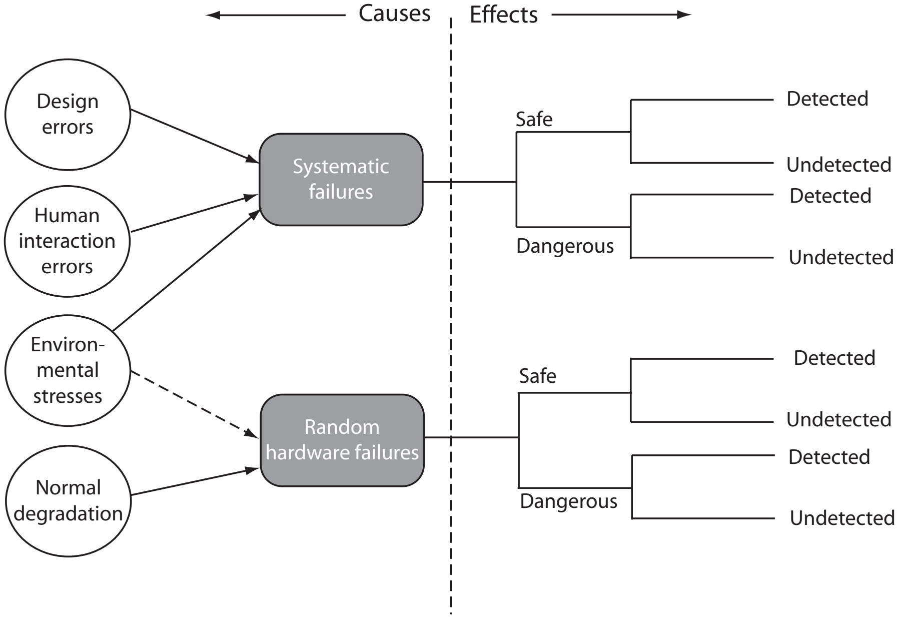


**Fig. 4.5.** Classification of failures

IEC standards suggest a number of methods and requirements for avoidance and control with systematic failures. In practise, systematic failures as well as random failures are recorded by the oil companies, and we may assume (even if it is not mathematically correct) that failure rates to some extent reflect both failure categories.

A failure type that does not fit entirely into the classification system of systematic or random hardware failures, is the CCFs. Per definition, these failures are dependent failures [108] and cannot be classified as random random hardware failure. For this reason, they should belong to the class of systematic failures. A systematic failure is, however, used to classify individual failures, while a CCF includes the failure of *more* than one component. Still, the causes of systematic failures and CCFs are similar, and defense measures against systematic failures may therefore also be efficient means to defend against CCFs.

When including CCFs in reliability calculations, we extract a fraction (e.g., $\beta$) of the random hardware failure rate and classify it as the CCF rate. This means that we indirectly give CCFs some of the same properties as the random failures, for example a constant failure rate. This is a somewhat contradicting approach, but still widely used in the industry.

IEC 61508 [38] and IEC 61511 [39] distinguish between safe and dangerous failure effects. A dangerous failure is a failure which has the potential to put the safety instrumented system in a hazardous or fail-to-function state [39], whereas a safe failure does not have this potential. A failure that prevents the valve from closing on demand is defined as a dangerous failures, while a spurious valve closure is defined as a safe failure. This may indicate that the IEC standards consider spurious activation as less safety-critical than OREDA.

Safe and dangerous failures may be further split into detected and undetected failures. A detected failure is a failure that is revealed by online diagnostics [39], and, in some cases, by operators during normal operation [114] and which is corrected or acted upon shortly after its occurrence.

Undetected failures are failures that are only revealed by a function test or upon a demand. The dangerous undetected failures are therefore of vital importance when calculating the SIS reliability as they are a main contributor to SIS unavailability.

### Other classification systems

The PDS method [114] also distinguishes between random hardware failures and systematic failures. Here, the aging (normal degradation) failures are related to random hardware failures, while environmental stresses, design failures, and (human) interaction failures are considered to be causes of systematic failures. In practise, it is often difficult to discriminate between an aging failure or a stress failure [114]. As illustrated with the dotted line in Fig. 4.5, the class of random hardware failures may sometimes include both environmental stress related failures and aging failures.

The PDS method has adopted the concept of safe and dangerous failures for classifying failure effects. In addition, they use the concept of critical and non-critical failures. The main intention with this amendment is to distinguish between the more “severe” safe failures (i.e. spurious activations) and the less severe ones (e.g., small drift in signal).

The approach taken by the PDS method has some practical benefits, particulary when calculating the safe failure fraction (SFF). The SFF is used in the IEC 61508 and IEC 61511 to determine the required level of hardware fault tolerance, and is the fraction of safe and dangerous detected failures among all failures. The use of the SFF as a design parameter has been criticized, as it may be manipulated by adding superfluous equipment with high safe failure rates [71]. By extracting the non-critical failures from the safe failure category, the ability to manipulate the SFF is reduced.

# 5

# SIS related standards and guidelines

*This chapter gives an overview of some frequently used standards and guidelines for SIS design, construction, and operation. The main focus is the oil and gas industry, but some other industry sectors are also briefly discussed.*

## 5.1 Industry practises

International standards and guidelines on SIS design and follow-up have evolved over a number of years [73, 24]. The first initiatives were taken in the 1970s as a response to a number of industry related accidents, like the explosion at the Flixborough plant in 1974 and the large chemical release from the Seveco plant in 1976. For the offshore oil and gas industry, the large accident at the Piper Alpha installation in 1988 influenced the design of safety systems onboard oil and gas installations. Results from the accident investigations led to new legislations and directives like e.g., the Occupational Safety and Health Adminstration (OSHA) Process safety management (PSM) legislation (USA), the Seveso II legislation on prevention of chemical accidents, and the Health and Safety Executive (HSE) safety case regulations.

In addition to the lessons learnt from accidents, the industry recognized that the use of new technology in SIS designs could lead to new type of SIS failures [24]. Programmable electronic controllers (PLCs) had started to replace traditional relay logics, and safety functions were implemented by software instead of by physical devices. The use of software allowed for more flexibility and reduced hardware acquisition costs.

The globalization of the process industry during the 1980s and 1990s resulted in a demand for international practises rather than national practises and guidelines [13]. The IEC 61508 titled *functional safety of electrical/electronic/ programmable electronic safety-related systems* was developed for this purpose. The standard was based on a number of recognized national standards [29, 16, 17, 102, 7, 31], and developed further to fit the purpose of being a generic standard for development of safety systems where electrical, electronic or programmable electronic devices are key elements. A key element of the IEC 61508 is to approach SIS development using a life cycle perspective. The process sector specific standard, IEC 61511, has been developed with IEC 61508 as basis, but adjusted to the concepts and technology used in the process industries.

IEC 61508 and related standards are not automatically mandatory unless they are referenced by national authority regulations. Such a reference is given in the Norwegian Petroleum Safety Authority (PSA). HSE also recognizes IEC 61508 and IEC 61511 as good engineering practise, while OSHA refers to ANSI/ISA 84.00.01 [8], the US version of IEC 61511. The Norwegian Railway Inspectorate refers to sector specific standards that build on the IEC 61508 [20, 21, 22].

### 5.1.1 Oil and gas industry

The overall requirements for equipment and systems are provided by the national authorities. In Norway, onshore and offshore oil and gas installations must adhere to the Petroleum Safety Authority (PSA) regulations. The main requirements for SIS are found in the PSA activity regulations, the management regulations, and the facility regulations. For maritime systems onboard mobile rigs and floating production storage and offloading (PFSO) vessels, the regulations provided by the Norwegian Maritime Directive apply.

In the UK, the Health and Safety Executive (HSE) is the authority for onshore and offshore oil and gas installations, while in the US, the authority is split between Occupational Safety & Health Administration (OSHA), Minerals Management Service (MMS), United States Coast Guard (USCG), and Environmental Protection Agency (EPA).

Some of the standards that are referenced by the PSA and therefore apply to the Norwegian oil and gas industry, are shown in Fig. 5.1. The standards have the following title and scope:

- ISO 10418 [55] *Petroleum and natural gas industries* - *Offshore production installations* - *Basic surface process safety systems*: This standard describes protection means for process related equipment and systems. The standard is a replacement for API RP 14C. For implementation of the safety instrumented functions, the standard makes reference to IEC 61511.
- ISO 13702 [56] *Petroleum and natural gas industries* - *Control and mitigation of fires and explosions on offshore production installations* - *Requirements and guidelines*: This standard concerns design of fire and gas detection and mitigation systems.
- IEC 61508, IEC 61511, and OLF 070 [38, 39, 100]: These standards are covered in more detail in Sections 5.3 and 5.4.
- ISO/FDIS 14224 [60] *Petroleum, petrochemical and natural gas industries* - *Collection and exchange of reliability and maintenance data for equipment*:

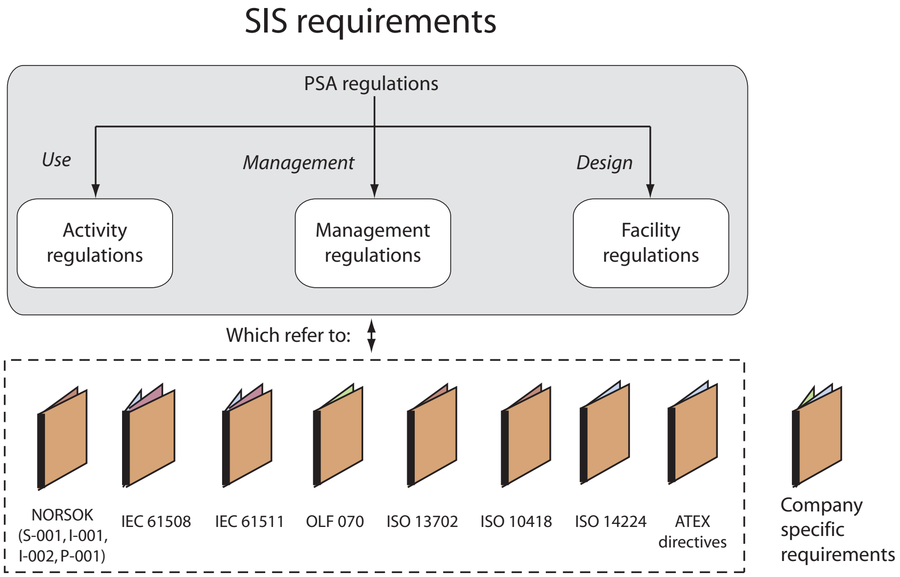


**Fig. 5.1.** Some of the standards that apply to SIS used on oil and gas installations

This standard gives guidance on failure recording and classification and is based on the approach in OREDA [101] and in NORSOK Z-008 [92].

- NORSOK S-001 [91] *Technical safety*: This standard provides the Norwegian best practise principles and requirements for design of instrumented and non-instrumented safety systems. For fire and gas detection systems, the standard supplements the requirements in ISO 13702.
- NORSOK P-001 [90] *Process design*: This standard provides the Norwegian best practise requirements for topside process piping and equipment design in general, and propose means to handle process deviations. The standard makes reference to the ISO 10418 [55].
- NORSOK I-001 [88] *Field instrumentation*: The standard provides the Norwegian best practise requirements for the selection of field sensors, hook-up details and documentation requirements.
- NORSOK I-002 [89] *Safety and automation systems* (SAS): This standard covers the Norwegian best practise requirements for programmable electronic systems used for control and safety functions. The standard does not specify which safety functions that are required, but focuses on technical design features such as human-machine interfaces, alarm and event handling, wiring and termination, management of access rights, and so on.
- ATEX directives [3, 1]: These directives give requirements for design and follow-up of equipment that has the potential to cause ignition in areas with explosive atmospheres. Further information about the ATEX directives is given in Section 5.2.1.

The NORSOK standards have been developed by as a joint effort by oil companies in Norway. The objective was to replace existing company specific standards with a common set of technical requirements, and in this way contribute to improved safety, value creation and cost efficiency. Some of the NORSOK standards have become internationally accepted and been developed further into ISO standards. One such example is the ISO 14224 standard.

As illustrated in Fig. 5.1, the company may still have additional standards and guidelines that can apply for SIS design, construction, and operation.

### 5.1.2 Nuclear industry

Numerous international guidelines and standards apply for SIS design, construction, and follow-up in the nuclear power industry, and many of them are listed in IEC 61513 [40] *Nuclear power plants* - *Instrumentation and control for systems important to safety* - *General requirements for systems*. Many of the referenced standards are published by IEC and the International Atomic Energy Agency (IAEA). IEC 61513 [40] links these standards to IEC 61508 [116].

The US Nuclear Regulatory Commission Regulation (NUREG) is the publisher of several reports that have got wide acceptance internationally. One guideline is NUREG/CR-6090 [97] on PLCs and their application in nuclear reactor systems. NUREG/CR-5485 [96] describes different approaches for treating CCFs in probabilistic risk assessments, while NUREG/CR-5460 [95] describes a cause-defense methodology for CCFs. Recently, IEC has published a new standard IEC 62340 [44] that also addresses requirement related to CCFs.

CCFs are given extensive attention in the nuclear power industry, and the Nuclear Energy Agency (NEA) has initiated the International Common Cause Data Exchange (ICDE) project to encourage collection and analysis of data related to CCF events [86]. Several reports with CCF data have been published, see for example in NEA [83, 84, 85].

### 5.1.3 Railway industry

Railway signalling systems installed in Europe have traditionally adhered to European Norms (EN). After the introduction of IEC 61508, they have been updated with references to this standard. EN 50126 is the overall approach to SIS specification design, construction, and operation, and describes the railway sector version of the overall SIS life cycle requirements. As opposed to the IEC 61508, the standard puts explicit emphasis on availability and maintainability requirements. The standard also encourages European industry inter-operability [116], meaning to ease railway traffic between European countries. An international standard IEC 62278 [42] has been developed that is based on EN 50126.

EN 50128 [21] and EN 50129 [22] give requirement for software and hardware design and construction, and have similar scope as IEC 61508, part 3 and IEC 61508, part 2. A frequently applied principle is to use redundant logic solvers with diverse software. As with EN 50126, EN 50129 and EN 50128 are now available as IEC standards, IEC 62425 [45] and IEC 62279 [43].

EN 50129 specifies a particular structure of the documentation of compliance to the EN 50128 and EN 50129, the technical safety report. The technical safety report is one section of the overall safety case that is required by EN 50126 and which describes, in all respects, how the system complies with EN 50126 and its references standards.

A railway signalling system is usually considered as a high demand (continuously operating) system, since each train passing or request for leaving a station, which may be several times a day, represents a demand.

### 5.1.4 Automobile applications

The amount of programmable devices in cars is increasing. Components that used to be pure mechanical (e.g., the gear systems, braking systems) can now be replaced by software implemented functions. The systems experience a demand each time they are activated by the driver, and control and safety functions are highly integrated. Many of these functions are therefore operating in the continuous mode.

Some differences between traditional SIS design and the safety related systems in cars, are for example [129]:

- Instead of hardware redundancy, the safety related systems in cars often use software diversity to reduce space requirements and costs.
- While a SIS in many industry sectors is one of a kind, the safety related systems for cars are reproduced in large volumes.
- While many SISs are operated by trained personnel, a car driver may have little or no competence on the systems he or her are operating.
- While SISs in many industry sectors cannot be tested under real demand conditions, it is possible to perform such testing for safety related systems in cars.

Before the Motor Industry Reliability Research Association (MISRA) published a development guideline for vehicle based software [79] in 1994, there were no national or international guidelines that applied specially to in such applications [129].

The MISRA guideline distinguishes between five integrity levels (0 to 4) [116], but does not assign quantitative reliability targets or ranges for these levels. Instead, each integrity level corresponds to a risk level and a corresponding (qualitative) acceptable failure rate.

IEC 61508 has not achieved acceptance within the automobile industry. They feel that the standard has too little focus on real-time embedded systems, that the current automotive development processes are not reflected, that too little guidance on the manufacturer/supplier relationship is provided, and that too little focus is given on product development for the mass market [129].

A sector specific standard, ISO 26262 [58], is now under development and is scheduled for publishing in 2008. The ISO 26262 will apply to SIS installed in road vehicles of class M, N and O, which by 70/156/EEC [2] is defined as cars used for the carriage of passengers, cars used for the carriage of goods, and trailers.

The ISO 26262 adopts a customer risk-based approach for determination of risk at the vehicle level and provides automotive-specific analysis methods to identify SIL requirements and for developing hardware and software according to these requirements.

Similar to the current MISRA guideline, the ISO 26262 does not assign a probabilistic target value to each SIL. ISO 26262 has therefore introduced ASIL to indicate a slightly different SIL concept than what is used in the IEC 61508.

The industry has also used another approach to integrity classification, where the integrity is split into four levels A to D. The categories A to D corresponds to ASIL 1 to ASIL 4, where C is defined in the middle range of what IEC 61508 define as SIL 2 and SIL 3. SIL 4 is not considered relevant since road vehicles do not trigger catastrophic events that would require this amount of risk reduction. The ISO 26262 recognizes that redundancy is not required to enhance reliability and safety even for ASIL 3 systems.

### 5.1.5 Civil aviation

The national authorities, which in Norway is the Civil Aviation Authority, give reference to international regulations, standards, and guidelines. For aircrafts and air traffic management in Europe, these references include standards and guidelines developed by the European Aviation Safety Agency (EASA) and the Joint Aviation Authority (JAA).

Civil aviation require global collaboration as aircrafts travel from one country to another. The international Civil Aviation Organization (ICAO) is a global forum for civil aviation and works to achieve harmonized regulations, standards, and guidelines.

## 5.2 Cross sector standards

### 5.2.1 ATEX directives

The potential presence of explosive atmospheres on plants affects the selection of SIS components. Plants that handle combustible materials may occasionally have small leakages from flanges, valves, and pipes. Explosive atmospheres are created when combustible materials like gases, vapor, and dust are mixed with oxygen. On oil and gas installations, there may occasionally be hydrocarbon gases in the wellhead and process areas, whereas explosive gases and dust may be present from time to time at chemical plants.

To cause an explosion, it is necessary to have an ignition source. Ignition sources may be high temperature surfaces, open fires, and electrical charges. Electrical equipment may have high temperature surfaces and produce arcs and sparks. When installed in areas where explosive atmospheres may be present, *all* electrical equipment must be designed or located so that they are not able to be ignition sources. Equipment that are designed to not cause ignition are sometimes referred to as explosion (ex) proof equipment [3, 34].

Standards and regulations have been developed for design and selection of ex-proof equipment. One standard is the IEC 60079 [34]. The standard comprises a number of parts, each addressing one particular implementation of explosion proof protection. Some alternative methods are:

- Oil-filled protection, where all electrical components are submerged in oil so that the mixture is too rich to produce an explosive atmosphere.
- Sand-filled protection, where all electrical components are submerged in sand, so that neither explosive gases and dust nor oxygen can get in contact with the components.
- Explosion proof protection, where all electrical components are encapsulated in a housing with flameproof joints. The housing is designed to withstand an internal explosion, and the flame proof joints prevent the transmission of explosion to the surroundings.
- Increased safety protection, where additional measures have been taken that reduce the probability of having high temperature surfaces, arcs and sparks during normal operation and specified abnormal conditions.
- Intrinsic protection, where all electrical components are designed with energy limitations so that they do not cause ignition during normal operation and some specified failure conditions.
- Overpressure protection, where one or more electrical components are encapsulated in a housing with supplied or mechanically generated overpressure.

Equipment for use in areas with explosive atmospheres and which are to be sold and used within the European market must comply to the ATEX directives. The ATEX directives are the product directive 94/9/EC [3] and the user directive 1999/92/EC [1]. The product directive addresses product design and is directed towards the electrical component manufacturers. 94/9/EC [3] describes the overall approach to product design of equipment to be used in areas with explosive gases, and is not restricted to only electrical equipment. For detailed design of electrical equipment, further reference is made by 94/9/EC [3] to the European Norms EN 50014 through EN 50028. As such, EN 50014 through EN 50028 have similar scope as IEC 60079.

The user directive focuses on the safety of workers, and describes principles for assessment of explosion risk, including classification of areas (or zones) according to their explosion risks. The user directive also addresses the selection of explosion proof design principles according to the area classification.

### 5.2.2 Machinery directive

Machinery produced for the European market must meet the requirements of ISO 13849 [57]. This ISO standard replaces the previous European Norm EN 954-1:1996 on safety of machinery. The ISO 13849 provides life cycle requirements for specification, design, implementation, construction, operation, maintenance, and modifications of control and safety systems in rotating machinery. Machinery systems have close integration of control and safety functions and operate usually in the high demand (continues) mode.

A new international standard IEC 62061 [41] for machinery that builds on the IEC 61508 has been developed. Here, the SIS is referred to as safety-related electrical control system (SRECS) to reflect the close integration of safety and control functions. The requirements in ISO 13849 are compatible with the requirements provided by IEC 62061, but uses some slightly different concepts. One example is the use of performance level instead of SIL.

## 5.3 IEC 61508

The international standard, IEC 61508 *Functional safety of electrical/ electronic/ programmable electronic (E/E/PE) safety-related systems* is the overall or “umbrella” standard for safety instrumented systems and covers multiple industries and applications [24, 116, 12].

A primary objective of the IEC 61508 standard is to serve as a guideline to help individual industries develop sector specific standards, tailored specifically for their industry but at the same time in accordance with the IEC 61508 requirements. A secondary objective is to enable the development of E/E/PE safety-related systems where related sector standards do not already exist. The IEC 61508 may also be used for to qualify new E/E/PE technology for use in safety related applications. This is one reason for why the IEC 61508 is sometimes referred to as the ‘vendors standard’.

IEC 61508 has seven parts:

Part 1: General requirements
Part 2: Requirements for E/E/PE safety-related systems
Part 3: Software requirements
Part 4: Definitions and abbreviations
Part 5: Examples of methods for the determination of safety integrity levels
Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3
Part 7: Overview of techniques and measures

The first three parts are normative parts while the remaining four parts provide informative annexes to the standard.

IEC 61508 is often referred to as a performance-based standard. This means that the standard intends to describe the required behaviour of systems and processes, rather than giving prescriptive requirements on how the systems shall be implemented. Taking into account the standards size, some users may still find the standard rather prescriptive.

Part 1 defines the overall requirements associated with safety related systems and introduces the safety life cycle to structure the requirements. Part 1 applies safety systems in general, but regarding realization of safety systems the standard is restricted to E/E/PE technologies. It describes the steps that are necessary to identify the EUC hazards and risks, to allocate the necessary risk reduction to different safety related systems, and the activities that are necessary to plan for and execute overall system integration, validation, installation, commissioning, operation, maintenance, modifications, and finally, decommissioning.

SIS design and realization are covered in part 2 and part 3. Part 2 provides requirements for hardware design and the integration of hardware and software. In addition, part 2 outlines the principles and methods for demonstrating that a SIF fulfils the specified reliability targets defined in the preceding phases.

Part 3 gives requirements for the selection, implementation, and verification of software tools, applications, and programming languages. A number of principles and recommendations related to the selection of tools, language, and development process are proposed to ensure adequate level of safety integrity.

A brief description of the remaining parts of the standard is that part 4 lists definitions and abbreviations that are used elsewhere in the standard, part 5 suggests ways to determine the SIL, part 6 is a guideline on the application of part 2 and 3, and part 7 gives specific recommendations associated with tools, methods, and approaches.

Several international organizations have developed guidelines that suit the needs of different industry sectors. Some examples are:

- IEC 61511 *Functional safety – Safety instrumented systems for the process industry*. The Instrument Society of America (ISA) has independently developed ANSI/ISA S84.01 *Application of safety instrumented systems for the process industries* that is similar to IEC 61511.

- IEC 62061 *Safety of machinery – Functional safety of electrical, electronic and programmable electronic systems*. This standard was initially developed as a European standard to support the EU Machinery Directive.
- IEC 61513 *Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems.*
- EN 50126 *Railway applications – The specification and demonstration of reliability, availability, maintainability, and safety (RAMS).*
- EN 50128 *Railway applications – Software for railway control and protection systems.*[1]
- EN 50129 *Railway applications – Safety related electronic systems for signalling.*
- IEC 60601 *Medical electrical equipment*

Some of these standards have already been mentioned, while others will be discussed later.

### 5.3.1 The safety life cycle

IEC 61508 uses the safety life cycle as a framework to structure its own requirement. The safety life cycle comprises 16 phases, as illustrated in Fig. 1.2 in part I, section 1.1.3. The initial five phases (1-5) lead up to the functional safety requirements, stating *what* the SIS is required to do, and the safety integrity requirements, stating *how well* the SIS is require to perform. These requirements may, together with the assumptions under which the requirements have been developed, be documented in a safety requirement specification (SRS). The SRS is an important document for the subsequent phases of SIS safety life cycle.

Phase 9 is the realization phase of SIS and specifies the work processes and design principles for hardware and software design and integration. Phase 9 should be performed separately for each SIS. The safety life cycle also indicates that other means may be used for risk reduction, by using other technologies (e.g., pure mechanical systems) or other risk reduction facilities (e.g., fire walls, drain systems). However, the IEC 61508 does not include requirements for how these systems should be designed and constructed.

Phases 12 and 13 outline the main activities and principles for the overall installation, commissioning, and validation. Overall means here that all safety systems that were specified in the SRS are to be considered. Validation refers to the activities that are necessary to document compliance to the requirements and assumptions in the SRS.

Parallel to the realization phase, the IEC 61508 specifies necessary planning of overall installation, commissioning, validation, and operation and maintenance. The main purpose is to ensure that adequate procedures, tools, and work

[1] EN 50126 and EN 50128 were based on earlier drafts of IEC 61508.

processes are in place to maintain the functional safety and safety integrity. Failure recording and analyses are two important activities for measuring the safety integrity. If the SIS does not perform according to the specified functional safety and safety integrity requirements, it is necessary to implement (e.g., design modifications, adjustments of functional test and inspection intervals) will have to be implemented.

Phase 15 specifies the handling of modifications. Key aspects is to analyze the impact of the proposed modifications, and determine the life cycle phase to return to for proper implementation (phases 6 to 8). In some cases, operating conditions or plant modifications may introduce new hazards and risks. In this case, it may be necessary to return to the initial phases so that any new or modified functional safety and safety integrity requirements are identified and catered for.

Phase 16 denotes the last phase of the SIS life, and covers the necessary cautions that must be taken when the SIS is decommissioned and dismantled.

### 5.3.2 Safety integrity

Safety integrity is used as a measure of how well a safety function (e.g., a SIF) shall perform. The IEC 61508 distinguishes between four safety integrity levels (SIL), where SIL 1 is the lowest (least reliable) level and SIL 4 is the highest (most reliable). For each SIL, it is specified a target range for the PFD. In addition, the SIL outlines the requirements for architectural constraints.

It is distinguished between three categories of safety integrity:

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

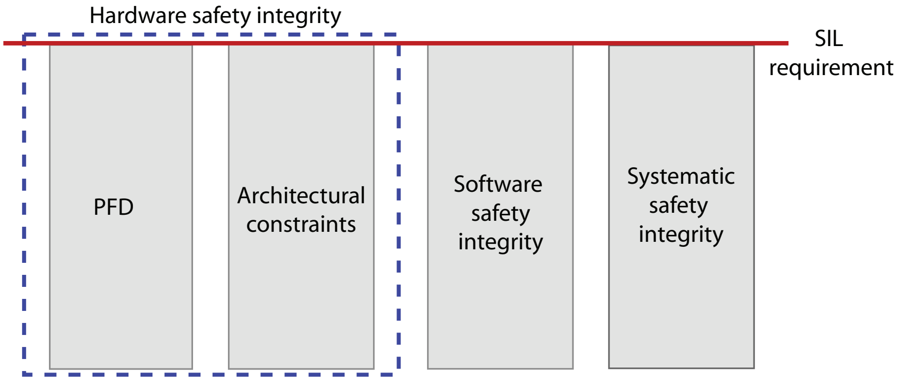

Hardware safety integrity
SIL requirement
PFD
Architectural constraints
Software safety integrity
Systematic safety integrity

**Fig. 5.2.** Illustration of safety integrity categories and SIL

Hardware safety integrity is split into two parts: One part is associated with the quantitative requirements and the other part concerns the architectural constraints. The quantitative requirements address how to calculate the probability of failure on demand (PFD) for SIS that works on demand, or alternatively the probability of a dangerous failure per hour (PFH) for continuously operating SIS. The architectural constraints are used to achieve a sufficiently robust architecture and not selecting hardware architecture based on calculations alone.

The systematic safety and software safety are handled by qualitative requirements. To achieve a specified SIL, it is necessary to select and demonstrate adequate use of the corresponding methods that are proposed for this SIL.

IEC 61508 requires that all three safety integrity categories meet the specified SIL before the SIL can be claimed for the SIF. This is illustrated in Fig. 5.2. If one of the categories fails to meet SIL 2, for example for the software, the SIF is not a SIL 2 function even if SIL 2 is supported by the reliability calculations.

## 5.4 IEC 61511

IEC 61511 is the process sector version of the IEC 61508. IEC 61511 is directed at the system level designers, integrators, and end users rather than for vendors developing new devices, and the standard is therefore sometimes referred to as the ‘end user’ standard. It follows the requirements of IEC 61508, but modifies them to suit the practical situation, concepts and terms in the process industry [73]. The IEC 61511 refers to E/E/PE safety systems as safety instrumented systems (SIS).

The standard consists of three parts:

Part 1: Framework, definitions, system, hardware and software requirements
Part 2: Guidelines for the application of IEC 61511, part 1
Part 3: Guidance for the determination of the required safety integrity levels

Part 1 and 2 have similar scope as part 1 to 3 of IEC 61508, whereas part 3 of IEC 61511 corresponds to the content of part 5 of IEC 61508. The main amendment to part 3 in IEC 61511 compared to part 5 in IEC 61508 is the layers of protection analysis (LOPA), a method that is frequently used in the process industry [123].

There are some situations where IEC 61511 directs the end users or system integrators back to IEC 61508 [117]:

- The devices is new and does not have any documented evidence for being compliant to IEC 61508 (proven-in-use).
- A device is being modified and/or used in a manner not intended by the vendor.
- A SIL 4 is specified for the SIF.

- A device is being programmed using full variability language.

A first rule of thumb is that IEC 61511 applies to SIS up to SIL 3 if the SIS is based on proven-in-use components or components that are developed and verified according to IEC 61508. In this context, proven in use means (i) that there is appropriate documented evidence of previous use, and (2) that the component is suitable for use in this particular application [39]. A second rule of thumb is that the IEC 61511 requirements apply to safety functions up to SIL 2 when off-the-shelf PLCs are being used [116].

That components are to be developed and verified according to IEC 61508 does not necessarily imply that a certification is required. However, certified bodies sometimes provide certificates after they have assessed a particular product. The certificate may indicate that the component is suitable up to a certain SIL, given some assumptions about application specific conditions such as functional test intervals and fail safe operation.

Different national organizations have developed separate guidelines on the application of IEC 61508 and IEC 61511 that take national regulations and practices into account. Some of these guidelines are:

*Guide to the application of IEC 61511 to safety instrumented systems in the UK process industries [19]:*

Representatives of the Energy Industry Council (EIC), Engineering Equipment Manufacturers and Users Association (EEMUA), United Kingdom Offshore Operators Association (UKOOA), and HSE are currently developing a guide to the application of IEC 61511 to SIS in the UK process industries. The guide discusses how the various IEC requirements should be interpreted in light of the UK regulations and practices. The guideline does not suggest the same approach as the OLF 070 with respect to minimum SIL requirements.

*ANSI/ISA-84.00.01-2004, Functional safety: Safety instrumented systems for the process industry sector (IEC 61511 mod)[8]:*

This is the recommended practice for US process industries. The pre-runner of this standard, the ANSI/ISA-84.01, *Application of safety instrumented systems for the process industries,* was used as basis for development of IEC 61508 as well as IEC 61508. Through the ANSI/ISA 84.00.01-2004, the US has adopted the IEC 61511 requirements with some exceptions. Summers [122, 117, 124, 119] discuss some of the differences. An important distinction between ANSI/ISA-84.01 / ANS/ISA-84.00.01 and IEC 61511 is the grandfather clause. The grandfather clause is derived from the OSHA 1910.119 PSM regulation, and concerns SIS installed *prior* to the issuance of the ANSI/ISA standards. The clause ask for verification that the SIS is designed, maintained, and operated in a safe manner. This means that the plant operator or owner should verify that the SIS not built according to the IEC 61508, IEC 61511 requirements, or ANSI/ISA standards is built, operated, and maintained according to recognized and generally accepted engineering practices [124, 119, 118].

*UKOOA Guidelines for instrumented protective systems [127]:*

This guideline represents an early interpretation of the IEC 61508 standard in UK. The guideline has extended the use of risk graph to also consider requirements for environment and loss of production [116].

*OLF 070 Guidelines for the application of IEC 61508 and IEC 61511 in the Norwegian petroleum industries[100]:*

The OLF 070 guideline has been developed by the Norwegian Oil Association. The objective has been to simplify the implementation of the IEC standards. The guideline does not take a full risk based approach like IEC 61508. As the Norwegian PSA requires that any new approaches to SIS design should at least be as good or better than current practices, the OLF 070 includes calculations of PFD for typical SIFs and proposes the corresponding SILs as minimum SIL requirements. The underlying assumption is that the SIFs are according to the requirements in ISO 13702 [56] and ISO 10418 [55]. The reliability calculations are preformed with the PDS method [114, 113].

*Other IEC 61508/IEC 61511 related guidelines:*

The instrumentation, systems, and automation society (ISA)[2] has developed guidelines on more specific issues related to SIS reliability assessments and SIS design, implementation, operation and maintenance, as for example:

- ISA TR 84.00.04-1 [50]: Guidelines for the implementation of ANSI/ISA-84.00.01-2004 (IEC 61511 mod).
- ISA TR 84.00.04-2 [51]: Example implementation of ANSI/ISA84.00.01-2004 (IEC 61511 mod).
- ISA TR 84.00.02 [48]: Safety Instrumented Functions (SIF) - Safety Integrity Level (SIL) Evaluation Techniques. Parts 1-5.
- ISA TR 84.00.03 [49]: Guidance for testing of process sector safety instrumented functions (SIF) implemented as or within safety instrumented systems (SIS).
- ISA TR 96.05.01 (draft) [52]: Partial stroke tesing of automated block valves.

[2] ISA has recently been given a new interpretation; The International Society of Automation.

# A

# Acronyms and Abbreviations

| | |
|---|---|
| AC | Architectural constraints |
| ABS | Anti-block breaking system |
| ALARP | As low as reasonably practicable |
| ANSI | American National Standards Institute |
| ASIL | Automobile safety integrity level |
| ATEX | ATmospheres EXplosibles (French) |
| BIP | Brukerstyrte inovasjonsprosjekter (User controlled innovation projects) |
| BPCS | Basic process control system |
| CCF | Common cause failure |
| CCPS | Center for Chemical Process Safety |
| CPU | Central processing unit |
| DC | Diagnostic coverage |
| DCV | Directional control valve |
| DD | Dangerous detected |
| DU | Dangerous undetected |
| EASA | European Aviation Safety Agency |
| EC | European Commission |
| EEMUA | Engineering Equipment Manufacturers and Users Association |
| E/E/PE | Electrical, electronic, programmable electronic |
| E/E/PES | Electrical, electronic, programmable electronic system |
| EIC | Energy Industry Council |
| EN | European Norm |
| ETA | Event tree analysis |
| EUC | Equipment under control |
| FDIS | Final draft international standard |
| FMEA | Failure modes and effects analysis |
| FMECA | Failure modes, effects, and criticality analysis |
| FMEDA | Failure modes, effects, and detectability analysis |
| FPL | Fixed programming language |

| | |
|---|---|
| FSA | Functional safety assessment |
| FTA | Fault tree analysis |
| FVL | Full variability language |
| HAZOP | Hazard and operability study |
| HFT | Hardware fault tolerance |
| HSE | Health and Safety Executive |
| HW | Hardware |
| IAEA | International Atomic Energy Agency |
| ICDE | International Common Cause Data Exchange |
| ICAO | International Civil Aviation Organization |
| IDEF | Integrated definition language |
| IE | Input element(s) |
| IEC | International Electrotechnical Committee |
| IEEE | Institute of Electrical and Electronic Engineers |
| I/O | Input/Output |
| IPS | Instrumented protective systems |
| ISA | Instrumentation, Systems, and Automation Society |
| ISO | International Organization for Standardization |
| ISS | Instrumented safety system |
| JAA | Joint Aviation Authority |
| LOPA | Layers of protection analysis |
| LS | Logic solver |
| MISRA | Motor industry reliability research association |
| MTBF | Mean time between failure |
| MTTR | Mean time to repair |
| NEA | Nuclear Energy Agency |
| NORSOK | Norsk sokkels konkurranseposisjon (Eng: Competitive position for the Norwegian continental shelf) |
| NTNU | Norwegian University of Science and Technology |
| NUREG | US Nuclear Regulatory Commission |
| OLF | Oljeindustriens landsforening (Eng: The Norwegian Oil Industry Association) |
| OREDA | Offshore Reliability Data |
| OSHA | Occupational Safety and Health Administration |
| PFD | Probability of failure on demand |
| PFH | Probability of a dangerous failure per hour |
| PLC | Programmable electronic controller |
| PSA | Petroleum Safety Authority (Norway) |
| PSM | Process safety management (legislation, OSHA) |
| PST | Partial stroke testing |
| RAMS | Reliability, availability, maintainability, and safety |
| RBD | Reliability block diagram |
| ROCOF | Rate of occurrence of failures |

| | |
|---|---|
| SAT | Site acceptance test |
| SD | Safe detected |
| 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 |
| SO | Spurious operation |
| SRCS | Safety-related electrical control system |
| SRS | Safety requirement specification (may also mean safety-related system) |
| STR | Spurious trip rate |
| SU | Safe undetected |
| SW | Software |
| UKOOA | United Kingdom Offshore Operators Association |

# B

# Glossary

**Accident:** An unintended event or sequence of events causing death, injury, environmental, or material damage [14].
*Note: In the context of event tree analysis, we may define the end events involving death, injury, environmental, or material damage as accidents.*

**Accident scenario:** An accident scenario includes an initiating event, a related sequence of subsequent events, and a resulting undesired consequence [75].
*Note: An undesired consequence corresponds to an end event involving death, injury, environmental, or material damage.*

**Actual performance:** The product performance that is experienced in field, based on observations and feedback from customers and end users (deduced from Murthy et al. [80]).
*Note: In the context of SIS, the observations may for example include the number and type of failures that are recorded.*

**Analysis (risk):** Systematic use of available information to identify hazards and to estimate the risk [54].

**Architecture:** Arrangement of hardware and/or software elements in a system, for example a SIS [39].

**Architectural constraints (AC):** Used by IEC 61508 [38] and IEC 61511 [39] to denote the requirements that restrict the freedom in selection of hardware architecture.

**Assessment (risk):** The overall process comprising a risk analysis and a risk evaluation [54].

**Automatic testing:** A test which consists of simulated process conditions to a logic solver which cause the logic solver to take specified action and signal a final control element to move to a specified position [49].
*Note: The test may be trigged automatically, for example on specified calender time, or by humans.*

**Availability:** May be defined as either:

- The ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided [33].
- A measure of reliability of repairable components or systems [108].

**Safety barrier:** Physical and/or non-physical means planned to prevent, control, or mitigate the undesired events or accidents [115].

***Note:*** *A SIS may be considered as a barrier system.*

**Basic event:** The bottom or "leaf" events of a fault tree. The limit of resolution of the fault tree [81]. Examples of basic events are component failures and human errors.

**Basic process control system (BPCS):** See **EUC control system**.

**Best estimate analysis:** Used in the context of accident analysis, and defined as analysis that [32]:

- Is free from deliberate pessimism regarding selected acceptance criteria;
- Uses a **best estimate code**;
- Includes **uncertainty analysis**.

***Note:*** *This definition can also be applied for safety and reliability assessments.*

**Best estimate code:** A **code** which [32]:

- Is free of deliberate pessimism regarding selected acceptance criteria;
- Contains a sufficiently detailed model to describe the relevant processes required to be modeled.

**Channel:** Element or group of elements that independently performs a **function**[39].

**Code:** For accident analysis in the nuclear industry, see e.g., IAEA [32], the term 'code' seems to include what we refer to as system models, input data, and calculation approach.

**Confidence level:** We may relate confidence level to confidence intervals or statistical tolerance limits [32]:

- Confidence intervals: Probability $p$ that the confidence interval to be computed from the sample will contain the true parameter value.
- Statistical tolerance limits: Probability $p$ that the limits to be computed will cover the specified proportion $\alpha$ of the population (probability content $\alpha$). The confidence level is specified to account for a possible sampling error due to the limited sample size, for example a limited number of calculations, from which the statements are obtained.

**Configuration:** Used with the same meaning as **architecture**. May be used to describe software as well as hardware.

**Conservative analysis:** Analysis leading to pessimistic results relative to a specified acceptance criterion [32].

***Note:*** *In the context of SIS, a conservative analysis may be defined as an analysis where conservative assumptions are made for the model, the data,* *and the calculation approach so that the calculated PFD most likely is higher than what we may experience once the SIS is put into operation.*

**Common cause failure (CCF):** CCF may be defined as either:

- Failure of more than one device, function, or system due to the same cause [13].
- Failure, which is the result of one or more events, causing failures of two or more separate channels in a multiple channel system, leading to system failure [38].
- Failure (or unavailable state) of more than one component due to a shared cause during the system mission [82]
- Multiple component faults that occur at the same time or that occur in a relatively small time interval and that are due to a common cause [81].

***Note:*** *The four definitions indicate some of the differences in the interpretation of what a CCF is. Some restrict the concept of CCFs to events within a single safety function, while others include CCFs between different functions. Some restrict CCFs to events that occur within the same mission time (e.g., same flight, same functional test interval), while others do not have this restriction.*

**Complex interactions:** Those of unfamiliar sequences, or unplanned and unexpected sequences, and either not visible or not immediately comprehensible [107].

**Complexity:** Not easy to understand; complicated (Oxford Dictionary).

***Note:*** *IEC 61508 [38] uses the classification of type A and B components to distinguish low complex components from those that are more complex. Here a type A component is characterized by (i) all failure modes are well defined, (ii) the behavior of the component under fault conditions is well known, and (iii) field data are dependable and able to confirm the failure rates that are claimed, while a type B component does not meet one or more of these criteria.*

**Component:** One of the parts of a system, subsystem, or device performing a specific function [39].

***Note:*** *In some situations, the IEC 61508 and IEC 61511 use "element" and "device" with the same meaning.*

**Coupling:** Coupling may be used in two different contexts; for classifying CCF causes and for classifying systems:

- In relationship with CCF causes: A coupling factor explains why several components are affected by the same root cause (e.g., inadequate material selection for several valves) [104, 105].
- In relationship with system classification: Perrow [107] uses coupling to express the degree of dependencies between system components:
  - Tight coupling means that there is no slack or buffer between two items, and what happens in one item will directly affect what happens in the other.

  - Loose coupling means that there is such slack or buffer, and the items may operate independently of each other.

**(Cumulative) distribution function:** Consider a random variable $X$. The (cumulative) distribution function of $X$ is [108]:

$$F_X(x) = \Pr(X \leq x)$$

**Construction:** Construction is sometimes used with quite different meaning, for example as:

- A process that consists of the building or assembling of infrastructure (Wikpidia).
- The analysis, design, manufacture, fabrication, placement, erection, installation, modification, inspection, or testing of a facility or activity which is subject to the regulations in this part and consulting services related to the facility or activity that are safety related (U.S. Nuclear regulatory commission regulations, title 10, Code of Federal Regulations, part 21, Reporting of defects and noncompliance).

***Note:** In the context of SIS, construction may be used to describe the assembling of hardware, the development of application software, and the integration of hardware and software.*

**Continuous mode:** The mode of operation for a SIS where a dangerous failure may lead to an immediate hazardous event [39].

***Note:** IEC 61508 uses high demand/continuous mode in the same meaning as IEC 61511 uses continuous mode. A SIS that experiences more than one demand per year or more than one demands during a period of two subsequent functional test interval, shall be considered as working in the continuous mode [38]*

**Critical failure:** Failure of an equipment unit which causes an immediate cessation of the ability to perform a required function [60].

**Dangerous failure:** Failure which has the potential to put the safety instrumented system in a hazardous or fail-to function state [39].

**Data:** A representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means [13].

***Note:** In reliability modeling and calculation, we distinguish between input and output data. Input data are the values that we assign to the model parameters, for example the failure rates. Output data are the values that we obtain from the calculations, for example the average PFD.*

*The terms generic data, predicted data, experience data, historical data, plant specific data, and field data are sometimes used. These terms may be given the following meaning:*

- *Generic data: Data that represent a property, for example the failure rate, for a group of similar components, for example pressure transmitters. Generic data may be based on experience data or predicted data.*

- *Predicted data: Data that are based on the aggregation of failure rate models for subcomponents like integrated circuits, transistors, diodes, resistors, capacitors, relays, switches, and connectors. Such failure rate models are provided by e.g., MIL-HDBK-217F [77].*
- *Experience data: Data that is based on historical performance. OREDA [101] publishes data handbooks with failure rates that are based on recorded failures in the oil and gas industry. Historical data is often used with the same meaning as experience data.*
- *Plant specific data: Experience data that are based on information collected for a specific plant. Field data is used with the same meaning as plant specific data.*

**Degraded failure:** Failure that does not cease the fundamental function(s), but compromises one or several functions [60].

**Demand mode:** Where a specified action (for example, closing of a valve) is taken in response to undesired process conditions or other demands. In the event of a dangerous failure of the safety instrumented function a potential hazard only occurs in the event of a failure in the process or the BPCS [39].
***Note:*** *IEC 61508 uses low demand mode in the same meaning as IEC 61511 uses demand mode. A rule of thumb in IEC 61508 is that that a SIS operates in the (low) demand mode if it experiences one or less demands per year or, alternatively, one or less demands during a period of two subsequent functional test interval.*

**Dependability:** Collective term used to describe the availability performance and its influencing factors: reliability performance, maintainability performance and maintenance support performance [33, 35].

**Dependent failure:** Failure whose probability cannot be expressed as the simple product of the unconditional probabilities of the individual events which caused it [38, 39].
***Note:*** *CCFs is a category of dependent failures.*

**Desired performance:** What the consumers or end user expect from a product [80].
***Note:*** *In the context of a SIS, the desired performance is stated through the functional safety (what to perform) and safety integrity requirements (how well to perform) [38, 39]. In addition, we may add other reliability, availability, maintainability, and safety (RAMS) requirements.*

**Detected:** In relation to hardware and software faults, detected by the diagnostic tests or through normal operation [39].
***Note:*** *IEC 61508 also includes failures that detected by proof tests (e.g., functional tests) into the category of detected failures, but this approach has not adopted by the process industry.*

**Deterministic method:** A deterministic method has the following features in common with probabilistic methods (deduced from [32]):

- **Code** and **transients** are identified

- **Uncertainties** are identified

  Deterministic methods does not use probability distributions for model parameters. Instead, reasonable uncertainty ranges or bounding values are specified that encompass, for example, available relevant experimental data. The statements of the uncertainty code results are deterministic, not probabilistic.

**Device:** See **component**.

**Diagnostic coverage (DC):** Ratio of the detected failure rate to the total failure rate of the component or subsystem as detected by diagnostic tests [39].

***Note:*** *Diagnostic coverage does not include any faults detected by proof tests.*

**Diagnostic test interval:** The interval between on-line tests to detect faults in a safety-related system that has a specified diagnostic coverage [38].

***Note:*** *The contribution from diagnostic tests is often negligible when calculating the PFD, provided that the diagnostic test interval is short. Currently, IEC 61508 and IEC 61511 provide little guidance on what is meant by " short".*

**Diversity:** Existence of different means performing a required function[39].

***Note:*** *Diversity is not the same as redundancy, as redundancy may be achieved by having similar/or same means performing the required function.*

**E/E/PE (safety-related) system:** System for control, protection or monitoring based on one or more programmable electrical/electronic/programmable electronic (E/E/PE) devices, including all elements of the system such as power supplies, sensors and other input devices, data highways and other communication paths, and actuators and other output devices [38].

***Note:*** *E/E/PE system corresponds to SIS in IEC 61511.*

**Electrical (logic solver):** Sometimes referred to as relay based or direct wired logic. The input elements and the final elements are connected in a common electrical circuit, so that the state of the input elements directly determines the state of the final elements.

**Element:** See **component**.

**End event:** A description an outcome of an **accident scenario** in an **event tree analysis**.

**Equipment:** See **component**.

**Equipment under control (EUC):** A collective term used to describe equipment, machinery, apparatus, or plant to be analyzed.

**Error:** Discrepancy between a computed, observed or measured value or condition and the true, specified or theoretical correct value or condition [33].

**Estimated performance:** An estimate of an objects performance, based on observations and feedback from customers (deduced from [80]).

***Note:*** *The estimated performance is based on observations and is therefore our best measure of an object's actual performance. In the context of a SIS, the estimated performance may be calculated based on for example:*

- *The number of dangerous detected and undetected dangerous failures;*
- *The functional test intervals;*

- *The number of spurious activations;*
- *The average repair times for detected and undetected failures.*

**EUC control system:** System which responds to input signals from the process and/or operator and generates output signals causing the **EUC** to operate in the desired manner [38].

***Note:*** *On an oil and gas installation and in the process industry in general, the EUC control system is the same as what is sometimes described as process control systems. Therefore, IEC 61511 uses the term basic process control system (BPCS) instead of EUC control system.*

**EUC risk:** Risk arising from the EUC or its interaction with the **EUC control system** [38].

**Evaluation (risk):** Procedure based on the risk analysis to determine whether the tolerable risk has been achieved [54].

**Event tree:** A logic tree diagram that starts from a basic initiating event and provides a systematic coverage of the time sequence of events propagating to its potential outcomes or consequences [108].

**Event tree analysis:** Identification and analysis of potential outcomes and consequences of an **initiating event**.

**External risk reduction facilities:** Measures to reduce or mitigate the risks, which are separate and distinct from the SIS [39].

***Note:*** *Such measures may be drain systems and fire walls.*

**Factory acceptance test (FAT):** The following definitions indicate when and what a FAT is about:

- The test performed for an equipment or system at the construction site (factory) before it is is moved to its final destination.
- A test conducted to determine and document equipment hardware and software operates according to its specification, covering functional, fault management, communication, support systems, and interface requirements [13].

**Fail safe:** Denotes an equipment or a system that, upon specified failures such as loss of **utilities**, will operate in a way such that the safe state of the EUC is achieved or maintained.

**Failure:** The termination of the ability of a functional unit to perform a required function [33].

**Failure cause:** The circumstances during design, manufacture or use that have led to a failure [33].

**Failure mode:** The *effect* by which a failure is observed on a failed item [108], that is in *which way* an item is no longer able to fulfill a required function.

***Note:*** *For a shutdown valve, a failure mode may be 'Not able to close on demand'. Failure modes should not be mixed with failure causes. For a valve it is not relevant to talk about 'corrosion' as a failure mode.*

**Failure rate:** The formal definition of the rate at which failures occur as a function of time and is the life distribution of a single component. If $T$ denotes the time to failure of an time, the failure rate $z(t)$ is defined as [108]:

$$z(t) = \lim_{\Delta t \to \infty} \frac{Pr(t < T \leq t + \Delta t \mid T > t)}{\Delta t}$$

***Note:*** *The failure rate may be understood as the "proneness to failure" and is for this reason sometimes called "force of mortality (FOM)" [108].*

**Fault:** The state of an item characterized by inability to perform a required function [108].

**Fault tree:** A logic diagram that displays the interrelationships between a potential critical event in a system and the causes for this event [108].

***Note:*** *Analogue terms for critical events are initiating events and hazardous events.*

**Fault tree analysis:** Two useful definitions are:

- Identification and analysis of conditions and factors that cause or may potentially cause or contribute to the occurrence of a defined top event [37].
- An analytical technique, whereby an undesired state of the system is specified (usually a state that is critical from a safety or reliability standpoint), and the system is then analyzed in the context of its environment and operation to find all realistic ways in which the undesired event (top event) can occur [81].

**Fault tolerance:** Ability of a functional unit to continue to perform a required function in the presence of faults or errors [39].

**Final element:** A SIS element that implements the physical action necessary to achieve a safe state. Builds on the definition of final element in IEC 61511 [39].

**Functional safety:** Part of the overall safety relating to the process and the basic process control system (BPCS) which depends on the correct functioning of the SIS and other protection layers [39].

**Functional safety assessment:** Investigation, based on evidence, to judge the functional safety achieved by one or more protection layers [39].

**Functional (or function) test:** Used the process industries in the same meaning as **proof test**.

**Hardware safety integrity:** Part of the safety integrity of the safety instrumented function relating to **random hardware failures** in a dangerous mode of failure [39].

**Harm:** Physical injury or damage to the health of people, either directly or indirectly, as a result of damage to property or to the environment [54].

**Hazard:** Potential source of harm [54].

***Note:*** *Hazards may lead to hazardous events in combination with some triggering event(s). Icy streets can represent a hazard, but a hazardous event does not occur before the hazard is combined with a triggering event e.g., a car starts to slide off the road.*

**Hazardous event:** Hazardous situation which may lead to harm.

*Note: In practise, we may consider an hazardous event to be an initiating event. But hazardous events may also be the undesired outcome of an event in an event tree.*

**High demand mode:** See *continuous mode*.

**Human error:** Human action or inaction that produces an unintended result [39].

***Note:*** *Unintended result may be the same as an undesired event. Human errors are sometimes also referred to as mistakes.*

**Initiating event:** The first significant deviation from the normal situation that may lead to a system failure or an accident [108].

***Note:*** *We may refer to an hazardous event as an initiating event.*

**Input element:** An element used to monitor the process and its associated equipment in order to provide input information for the logic solver. Builds on the definition of input function in IEC 61511 [39].

**Instrumented protective function (IPF):** A protective function allocated to an instrumented protective system that provides the risk reduction necessary to reduce the risk in an identified hazardous event below the owner/operator risk criteria [13].

***Note:*** *IPF has the same meaning as SIF.*

**Instrumented protection (protective) system (IPS):** Composed of separate and independent combination of sensors, logic solvers, final elements, and support systems that are designed and managed to achieve a specified risk reduction. An IPS may implement on or more instrumented protective functions (IPF) [13].

***Note:*** *IPS has the same meaning as SIS.*

**$k$-out-of-$n$:** A configuration of $n$ redundant elements, where $k$ elements must perform the required safety functions in order to perform the SIF (Slightly modified compared to the definition used in IEC 61511 [39]).

***Note:*** *This definition gives the conditions for successful performance of a subsystem. In some cases, $k$-out-of-$n$ is used to describe the conditions for system failure. To distinguish between the two types of notations, we may denote the first type as $k$-out-of-$n$:G (for good) and the latter as $k$-out-of-$n$:F (for fail).*

**Linear interactions:** Those in expected and familiar production or maintenance sequences, and those that are quite visible even if unplanned [107].

**Logic solver:** That portion of either a BPCS or SIS that performs one or more logic function(s) [39]. In practice, the logic solver reads signals from the input elements, makes decisions on how to respond to these signals, and set output signals accordingly.

**Manual test:** A test which consists of simulating process conditions using the input device to a logic solver causing the logic solver to take specified action and signal a final control element to move to a specified position [49].

***Note:*** *To this definition, we may add that the simulation process is performed by humans.*

**Minimal cut set:** A smallest combination of basic events whose occurrence results in the occurrence of the top event of a fault tree [81].

**Mode of operation:** Way in which a safety instrumented function operates [39].

***Note:*** *See also (low) demand mode and continuous/high demand mode.*

**Necessary risk reduction:** The risk reduction required to ensure that the risk is reduced to a tolerable level [39].

**Non-critical failure:** Failure of an equipment unit which does not cause an immediate cessation of the ability to perform its required function [60].

***Note:*** *Degraded failures are often considered as non-critical failures.*

**Off-line testing:** Testing performed while the process or equipment being protected is not being operated to carry out its designated function [49]

**On-line testing:** Testing performed while the process or equipment being protected is operating performing its designated function [49].

**Partial stroke testing (PST):** The following two definitins may apply:

- Confirmed movement of a block valve from the normal operating state towards the designated safe state [7].
- A test that partially closes a valve, and then returns it to the initial position [69].

**Partial testing:** Method of proof testing that checks a portion of the failures of a device, e.g., partial stroke testing of valves and simulation of input or output signals [13].

**PST coverage:** The fraction of DU failures that are detected by the PST [69]

**PST reliability:** A measure of the PST hardware and software ability to provide reliable and useful test results, within the scope of the test [69].

**Predicted performance:** An estimate of an object's performance, obtained through analysis, simulation, testing, and so on [80].

***Note:*** *In the context of a SIS, the use predicted performance to characterize the future intended performance of the SIS. As such, the predicted performance of a SIS may be documented through:*

- *Safety analysis reports*
- *Results from FAT and SAT*

**Prior use:** See *proven-in-use*.

**Probabilistic method:** A probabilistic method has the following features (deduced from IAEA [32]):

- Code and transients are identified.
- Sources of uncertainties are identified.
- The input parameters to be studied, and their associated probability distribution functions, are selected.
- The statements of the uncertainty code results are probabilistic.

**Probability density function:** Consider a random variable $X$. The probability density function $f_x(x)$ of $X$ is [108]:

$$f_X(x) = \frac{dF_x(x)}{dx} = \lim_{\Delta x \to \infty} \frac{\Pr(x < X \leq x + \Delta x)}{\Delta x}$$

**Process deviation:** A state where the plant has left its normal operating conditions.

**Process industry:** The industries involving extraction of raw materials, their transport and their transformation (conversion) into other products by means of physical, mechanical and/or chemical processes using different technologies (Wikipedia).
***Note:*** *The process industry includes petroleum extraction, treatment, refining, petrochemical, chemical and pharmaceutical industries, pulp and paper manufacturing, mining, etc. (Wikipedia).*

**Producer:** Derivative of produce, which means to make, manufacture, or create (Oxford Dictionary).
***Note:*** *Producer is often used with the same meaning as a manufacturer.*

**Proof test:** Test performed to reveal undetected faults in a safety instrumented system so that, if necessary, the system can be restored to its designed functionality [39].
***Note:*** *Periodically performed proof tests are often referred to as **functional tests**.*

**Protection layer:** Any independent mechanism that reduces risk by control, prevention, or mitigation [39].
***Note:*** *The term has a similar meaning as the term **safety barrier**.*

**Proven-in-use:** A category of components with documented evidence, based on the previous use of the component, that they are suitable for use in a safety instrumented system (deduced from IEC 61511 [39]).
***Note:*** *Prior use is a term that has similar meaning as proven-in-use.*

**Quality:** Degree to which a set of inherent characteristics fulfils requirements[59].
***Note:*** *ISO 9000 defines requirements as need or expectations that is stated, generally implied or obligatory. In the context of IEC 61508 and IEC 61511, we may consider requirements to be restricted to those that are stated.*

**Random hardware failure:** Failure, occurring at a random time, which results from a variety of degradation mechanisms in the hardware [39].

**Redundancy:** The use of multiple elements or systems to perform the same function; redundancy can be implemented by identical elements (identical redundancy) or by diverse elements (diverse redundancy) [39].
***Note: Redundancy*** *and **fault tolerance** are related terms. The fault tolerance of a redundant components are determined by how the components are voted, see the definition for $k$-out-of-$n$.*

**Risk:** Risk is often defined as the combination of the frequency of occurrence of harm and the severity of that harm [54].

***Note:*** *Kaplan [63] suggests that risk comprises three elements; the scenario (what can happen or go wrong?), the frequency (how likely is it?), and the consequences (in terms of injury, death, environmental damages, or material damages).*

**Risk acceptance criteria:** Criteria that are used to express a risk level that is considered tolerable for the activity in question [93].

**Risk analysis:** See **analysis**.

**Risk assessment:** See **assessment**.

**Risk evaluation:** See **evaluation**.

**Root cause:** A basic cause of a component failure [104, 105].

**Safe failure:** Failure which does not have the potential to put the safety instrumented system in a hazardous or fail-to-function state [39].

*Note: Spurious activations are usually considered as safe failures, as the EUC is taken to a safe state. The concept of safe failure should not be mixed with what OREDA[101, 60] defines as non-critical failures. In OREDA [101, 60], spurious activation failures are defined as critical failures as they lead to unavailability of the function or equipment.*

**Safe failure fraction (SFF):** The SFF is a property of a component or component group. The IEC standards [38, 39] define SFF as the proportion of “safe” failures among all component failures

$$\mathrm{SFF} = \frac{\lambda_{\mathrm{S}} + \lambda_{\mathrm{DD}}}{\lambda_{\mathrm{S}} + \lambda_{\mathrm{DD}} + \lambda_{\mathrm{DU}}}$$

where $\lambda_{\mathrm{S}}$ is the rate of safe failures, $\lambda_{\mathrm{DD}}$ is the rate of dangerous detected (DD) failures, and $\lambda_{\mathrm{DU}}$ is the rate of dangerous undetected (DU) failures of a component.

An alternative interpretation is that the SFF is a conditional probability [71]:

$$\mathrm{SFF} = \Pr(\text{The failure is “safe”} \mid \text{A component failure occurs})$$

Hence, we may interpret SFF as a measure of the inherent safeness of a component, that is, to what extent the component responds in a safe way when a failure occurs.

**Safe state:** State of the EUC (process) when safety is achieved [38, 39].

**Safety:** Freedom from unacceptable risk [53, 54].

**Safety analysis report (SAR):** SAR is a term introduced by OLF-070 [100] and denotes the document that describes how an equipment or a system meets the requirements of the safety requirement specification that has been allocated to the equipment or system.

***Note:*** *The SAR should include evidence of compliance of the equipment’s or system’s contribution to hardware safety integrity, software safety integrity, and systematic safety integrity.*

**Safety and reliability analysis:** Systematic use of available information to identify safety and reliability influencing factors and to predict or estimate their impact on safety and reliability (deduced from ISO-IEC Guide 51 [54].

**Safety and reliability assessment:** The overall process comprising safety and reliability analysis and safety and reliability evaluation (based on the ISO-IEC Guide 51 [54] definition of **assessment**).

**Safety and reliability evaluation:** The process using the results from the safety and reliability analysis to determine if the desired performance has been achieved.

**Safety function:** Function to be implemented by a E/E/PE safety-related system, other technology safety-related systems or external risk reduction facilities, which is intended to achieve or maintain a safe state of the EUC, in respect of a specific hazardous event [38].

**Safety instrumented control function:** Safety instrumented function with a specified SIL operating in continuous mode which is necessary to prevent a hazardous condition from arising and/or to mitigate its consequence [39]. Note: This term is analogue to the term Safety-related electrical control system (SRCES) used in the Machinery directive IEC 62061 [41].

**Safety instrumented function (SIF):** Safety function with a specified safety integrity level which is necessary to achieve functional safety and which can be either a safety instrumented protection function or a safety instrumented control function [39].

***Note:** In literature, a more common definition of a SIF is that it is a safety function that is implemented by a SIS.*

**Safety instrumented protection function:** See **instrumented protection function**.

**Safety instrumented system:** Instrumented system used to implement one or more safety instrumented functions. An SIS is composed of any combination of sensor (s), logic solver (s), and final elements(s) [39].

**Safety integrity:** Average probability of a safety instrumented system satisfactorily performing the required safety instrumented functions under all the stated conditions within a stated period of time [39].

**Safety integrity level (SIL):** Discrete level (one out of four) for specifying the safety integrity requirements of the safety instrumented functions to be allocated to the safety instrumented systems. Safety integrity level 4 has the highest level of safety integrity; safety integrity level 1 has the lowest [39].

**Safety life cycle:** Specification that contains the safety integrity requirements of the safety instrumented functions that have to be performed by the safety instrumented system(s) [39].

**Safety manual:** Manual which defines how the device, subsystem or system can be safely applied [39].

**Safety margin:** The difference in physical units, between a threshold that characterizes an acceptance criterion and the result provided by either a best estimate or a conservative calculation. In the case of best estimate calculation, the uncertainty band must be used when defining the safety margin [32].

**Safety-related electrical control system (SRCES):** Electrical control system of a machine whose failure can result in an immediate increase of the risk(s) [41].

**Safety-related system (SRS):** Designated system that both [38]:

- Implements the required safety functions necessary to achieve or maintain a safe state of the EUC; and
- Is intended to achieve, on its own or with other E/E/PE safety-related systems, other technology safety-related systems or external risk reduction facilities, the necessary safety integrity for the required safety functions.

**Safety requirement specification (SRS):** Specification that contains all the requirements of the safety instrumented functions that have to be performed by the safety instrumented systems [39].

**Scenario:** We may define a scenario as:

- A description of what can go wrong [63].
- A single or sequence of events with the potential to cause harm.

***Note:*** *In risk analysis, we often use the term accident scenario. However, the term does not seem to have a proper definition.*

**Sensitivity analysis:** Two definitions may apply:

- Quantification of the degree of impact of the uncertainty from the individual input parameters of the model on the overall model outcome (uncertainty importance analysis) [32].
- Performed in a probabilistic risk assessment (PRA) to indicate analysis inputs or elements whose value changes cause the greatest change in partial or final risk results [82].

**SIS designer:** A SIS designer may be a person that develops concepts and details on how a SIS may be built and constructed.

***Note:*** *Builds on the following definitions: (i) A designer is a person who designs something (Wikipedia), and (ii) design may be a plan (with more or less detail) for the structure and functions of an artifact, building or system (Wiktionary). A SIS designer may sometimes be referred to as a system integrator.*

**SIS manufacturer:** A SIS business engaged in manufacturing some product.

***Note:*** *This definition builds on the following definitions: (i) Manufacturer is a business engaged in manufacturing some product (Princeton), and (ii) manufacturing may be considered as fabrication, which is the act of making something (a product) from raw material (Princeton).*

**Site acceptance test (SAT):** A SAT may be defined as:

- A test performed for an equipment or system at its final destination (site) prior to start-up.
- A test conducted to determine and document that a new or modified instrumented protective system meets the design basis, is installed in accor-

dance with construction, installation, and software requirements, and is ready to start up [13].

**Software:** Software in a safety instrumented system with application, embedded or utility software functionality [39]. IEC 61511 distinguishes between three types of software program types:

- Application software: Software specific to the user application. In general, it contains logic sequences, permissives, limits and expressions that control the appropriate input, output, calculations, decisions necessary to meet the safety instrumented functional requirements. See fixed and limited variability language
- Embedded software: Software that is part of the system supplied by the manufacturer and is not accessible for modification by the end-user. Embedded software is also referred to as firmware or system software. See 3.2.81.1.3, full variability language
- Utility software: Software tools for the creation, modification, and documentation of application programs. These software tools are not required for the operation of the SIS

**Software language:** IEC 61511 [39] distinguishes between the following three languages:

- Fixed program language (FPL): In this type of language, the user is limited to adjustment of a few parameters (for example, range of the pressure transmitter, alarm levels, network addresses).
- Limited variability language (LVL): This type of language is designed to be comprehensible to process sector users, and provides the capability to combine predefined, application specific, library functions to implement the safety requirements specifications.
- Full variability language (FVL): This type of language is designed to be comprehensible to computer programmers and provides the capability to implement a wide variety of functions and applications

**Software safety integrity:** Measures that signifies the likelihood of software in a programmable electronic system achieving its safety functions under all stated conditions within a stated period of time [38].

**Spurious activation:** A collective term used to characterize an improper, false, or non-genuine transaction from one state to another. We may distinguish between the following categories of spurious activations [70]:

- Spurious operation: A spurious operation is an activation of a SIS element without the presence of a specified process demand.
- Spurious trip: A spurious trip is activation of one or more SIS elements such that the SIS performs a SIF without the presence of a specified process demand.
- Spurious shutdown: A spurious shutdown is a partial or full process shutdown without the presence of a specified process demand.

**Start-up:** The state of putting the equipment or system into operation at the final destination.

**System:** Set of elements, which interacts according to a design; an element of a system can be another system, called a subsystem, which may be a controlling system or a controlled system and may include hardware, software and human interaction [39].

**Systematic failure:** Failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or of the manufacturing process, operational procedures, documentation or other relevant factors [39].

**Systematic safety integrity:** That part of the safety integrity of safety instrumented function relating to systematic failures in a dangerous mode of failure [39].

**Tolerable risk:** Risk which is accepted in a given context based on the current values of society [39].

**Top event:** The initial event of a fault tree or success tree. Also called the undesired event in case of a fault tree [81].

**Transient:** In risk assessments in the nuclear industry, see e.g., IAEA [32], transients seem to be a state where the plant has left its normal operating conditions. A transient may therefore be interpreted as a process deviation.

**Triggering (trigger) event:** Two definitions may apply:

- An event that activates a failure, or initiates the transition to the failed state, whether or not the failure is revealed at the time the trigger event occurs [96].
- An event that in combination with one or more **hazards** may develop into an hazardous event.

**Uncertainty:** Two definitions that may apply:

- Measure of the scatter in experimental data or calculated values. It is expressed by an interval around the true mean of a parameter resulting from the inability to either measure or calculate the true value of that parameter (scatter). The uncertainty is often given as a (e.g., 95%) probability (confidence) limit or probability interval [32].
- A measure of our degree of knowledge or confidence in the calculated numerical risk results [82].

***Note:** In the context of safety and reliability assessment of SIS, we may define uncertainty as the degree of doubt in our ability to capture the relevant factors in model, the data, and/or the calculations.*

**Uncertainty analysis:** Analysis performed to evaluate the degree of knowledge or confidence in the calculated numerical risk results [82].

**Uncertainty range or bound (deterministic or probabilistic:** Depending on the uncertainty method used, the state of knowledge about an uncertain parameter is given as a ‘bounding’ range, ‘reasonable’ uncertainty range or as a probability distribution [32].

**Undesired event:** Technical failures, human errors, external events, or a combination of these occurrences that may realize potential hazards. We may consider accidents, hazardous events, initiating events, and basic events as undesired events.

**Undetected:** In relation to hardware and software faults not found by the diagnostic tests or during normal operation [39].

***Note:** This definition deviates from the one that is used in IEC 61508. However, it is the IEC 61511 version of the definition that is used in most safety and reliability assessments.*

**Utility systems:** A common term to describe pneumatic, hydraulic, and power supply systems.

***Note:** An utility system may also be called a support system.*

**Validation:** Confirmation through the provision of objective evidence that specified requirements have been met [38].

***Note:** IEC 61508 uses the term in relation with the activities of demonstrating that the deliveries from one safety life cycle phase meets the objectives and requirements set for the specific phase.*

**Verification:** Confirmation by examination and provision of objective evidence that the particular requirements for a specific intended use are fulfilled [38].

***Note:** IEC 61508 uses the term in relationship with the activities of demonstrating that the SIS under consideration, before or after installation, meets in all respect the safety requirement specification.*

# References

[1] 1999/92/EC (1999). *Directive 1999/92/EC of the European Parliament and of the Council of 16 December 1999 on minimum requirements for improving the safety and health protection of workers potentially at risk from explosive atmospheres*. European Parliament and Council of the European Union, Brussel.

[2] 70/156/EEC (1970). *Council Directive 70/156/EEC of 6 February 1970 on the approximation of laws of the member states relating to the type-approval of motor vehicles and their trailers*. European Parliament and Council of the European Union, Brussel.

[3] 94/9/EC (1994). *Directive 94/9/EC of the European Parliament and of the council of 23 March 1994 on the approximation of the laws of the Member States concerning equipment and protective systems intended for use in potentially explosive atmospheres (ATEX)*. European Parliament and Council of the European Union.

[4] Ali, R. (2004). Problems, concerns and possible solutions for testing (and diagnostics coverage) of final control element of SIF loops. *Technical Papers of ISA*, 454:995–1002.

[5] Ali, R. (2005). "Safety Life Cycle" -Implementation benefits and impact on field devices. volume 459, pages 509 – 527, Chicago, IL.

[6] 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*, pages 29–37. The Instrumentation, Systems, and Automation Society, Research Triangle Park, NC.

[7] ANSI/ISA -84.01 (1996). *Application of Safety Instrumented Systems for the Process Industries*. Instrumentation, Systems, and Automation Society, Research Triangle Parl, NC.

[8] ANSI/ISA 84.00.01 (2004). *Functional Safety: Safety Instrumented Systems for the Process Industry Sector: Framework, defintions, system, hardware and software requirements (IEC 61511-1 Mod)*. Instrumentation, Systems, and Automation Society, Research Triangle Parl, NC.

[9] Apeland, S., Aven, T., and Nilsen, T. (2002). Quantifying uncertainty under a predictive, epistemic approach to risk analysis. *Reliability Engineering and System Safety*, 75(1):93–102.

[10] Berden, T., Brombacher, A., and Sander, P. (2000). The building bricks of product quality: An overview of some basic concepts and principles. *International Journal of Production Economics*, 67(1):3 – 15.

[11] Brombacher, A. (1999). Maturity index on reliability: Covering non-technical aspects of IEC 61508 reliability certification. *Reliability Engineering and System Safety*, 66(2):109 – 20.

[12] Brown, S. (2000). Overview of IEC 61508. Design of electrical/electronic/programmable electronic safety-related systems. *Control Engineering Journal*, 11(1):6 – 12.

[13] CCPS (2007). *Guidelines for Safe and Reliable Instrumented Protective Systems*. Wiley (Center for Chemical Process Safety of AIChE), Hoboken, NJ.

[14] DEF-STD 00-56 (1996). *Safety Management Requirements for Defense Systems*. US Defence Standardization, Washington, DC.

[15] den Ouden, H., Yuan, L., Sonnemans, P., and Brombacher, A. (2006). Quality and reliability problems from a consumer's perspective: an increasing problem overlooked by businesses? *Quality and Reliability Engineering International*, 22(7):821 – 38.

[16] DIN 19250 (1994). *Grundlegende Sicherheitsbetrachtungen für MSR – Schutzeinrichtungen (Fundamental safety aspects to be considered for measurement and control equipment)*. Deutsches Institut für Normung (DIN), Berlin.

[17] DIN V VDE 801 (1990). *Grundsätze für Rechner in Systemen mit Sicherheitsaufgaben (Principles for computers in safety-related systems)*. Deutsches Institut für Normung (DIN), Berlin.

[18] Dutuit, Y., Innal, F., Rauzy, A., and Signoret, J.-P. (2008). Probabilistic assessments in relationship with safety integrity levels by using fault trees. *Reliability Engineering and System Safety*, 93(12):1867–1876.

[19] EIC, EEMUA, UKOOA, and HSE (200x). *Guide to the application of IEC 61511 to safety instrumented systems in the UK process industries (draft, not published)*. Energy Industries Council, Engineering Equipment Manufacturers and Users Association, United Kingdom Offshore Operators Association, and Health and Safety Executive.

[20] EN 50126 (1999). *Railway applications - The specification and demonstration of reliability, availability, maintainability, and safety (RAMS)*. European Standard, Brussels.

[21] EN 50128 (2001). *Railway applications - Communication, signalling and processing systems - Software for railsway control and protection systems*. European Standard, Brussels.

[22] EN 50129 (2003). *Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling*. European Standard, Brussels.

[23] Goble, W. (2005). HPIn automation safety: Implementing the new ANSI/ISA 84.01-2004 standard. *Hydrocarbon Processing*, 84(10):118.

[24] Goble, W. M. and Cheddie, H. L. (2005). *Safety instrumented systems verification*. Instrumentation, Systems, and Automation Society, Research Triangle Park, NC.

[25] Grady, J. O. (2006). *System requirements analysis*. Elsevier Academic Press, Amsterdam.

[26] Grady, J. O. (2007). *System verification*. Elsevier Academic Press, Amsterdam.

[27] Gruhn, P. (2006). *Safety Instrumented Systems: Design, analysis, and justification*. Number 2nd ed. ISA, Research Triangle Park, NC.

[28] Hauge, S. and Lundteigen, M. (2008). A new approach for follow-up of safety instrumented systems in the oil and gas industry. In *Safety, Reliability and Risk Analysis: Theory, Methods and Applications*, pages 2921–2928. CRC Press/Balkema, Leiden, The Netherlands.

[29] Hölscher, H. and Rader, J. (1984). *Mikrocomputer in der Sicherheitstechnik (Microcomputers in Safety Technology)*. Verlag TUV-Rheinland, Köln.

[30] Hokstad, P., Oien, K., and Reinertsen, R. (1998). Recommendations on the use of expert judgment in safety and reliability engineering studies. Two offshore case studies. *Reliability Engineering and System Safety*, 61(1-2):65–76.

[31] HSE (1987). *Programmable electronic systems in safety related applications*. Sheffield, U.K.

[32] IAEA (2008). *Best estimate Safety analysis for nuclear power plants: Uncertainty evaluation*. International Atomic Energy Agency (IAEA), Vienna, Austria.

[33] IEC 60050-191 (1990). *International Electrotechnical Vocabulary - Chapter 191 - Dependability and Quality of Service*. International Electrotechnical Commission, Geneva.

[34] IEC 60079 (2007). *Explosive atmospheres/Electrical apparatus for explosive gas atmospheres*. International Electrotechnical Commission, Geneva.

[35] IEC 60300 (2003). *Dependability management*. International Electrotechnical Commission, Geneva.

[36] IEC 60601-1 (2005). *Medical electrical equipment - Part 1: General requirements for basic safety and essential performance*. International Electrotechnical Commission, Geneva.

[37] IEC 61025 (1990). *Fault Tree Analysis (FTA)*. International Electrotechnical Commission, Geneva.

[38] IEC 61508 (1998). *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*. International Electrotechnical Commission, Geneva.

[39] IEC 61511 (2003). *Functional Safety - Safety Instrumented Systems for the Process Industry*. International Electrotechnical Commission, Geneva.

[40] IEC 61513 (2004). *Nuclear power plants - Instrumentation and control for systems important to safety - General requirements for systems*. International Electrotechnical Commission, Geneva.

[41] IEC 62061 (2005). *Safety of Machinery - Functional Safety of Safety-Related Electrical, Electronic and Programmable Electronic Control Systems*. International Electrotechnical Commission, Geneva.

[42] IEC 62278 (2002). *Railway applications - Specification and demonstration of reliability, availability, maintainability and safety (RAMS)*. International Electrotechnical Commission, Geneva.

[43] IEC 62279 (2002). *Railway applications - Communications, signalling, and processing systems - Software for railway control and protection systems*. International Electrotechnical Commission, Geneva.

[44] IEC 62340 (2007). *Nuclear power plants - Instrumentation and control for systems important to safety - Requirements for coping with common cause failure (CCF)*. International Electrotechnical Commission, Geneva.

[45] IEC 62425 (2002). *Railway applications - Communication signalling and processing systems - safety rleated electronic systems for signalling*. International Electrotechnical Commission, Geneva.

[46] Innal, F., Dutuit, A., and Signoret, J.-P. (2008). New insight into PFD$_{avg}$ and PFH. In *Safety, Reliability and Risk Analysis: Theory, Methods and Applications*, pages 2921–2928. CRC Press/Balkema, Leiden, The Netherlands.

[47] Innal, F., Dutuit, Y., Rauzy, A., and Signoret, J.-P. (2006). An attempt to understand better and apply some recommendations of IEC 61508 standard. In Langseth, H. and Cojazzi, G., editors, *Proceedings of the 30th ESReDA seminar*, pages 1–16. European Commission, Joint Research Centre, Ispra, Italy.

[48] ISA TR 84.00.02 (2002). *Safety Instrumented Functions (SIF) - Safety Integrity Level (SIL) Evaluation Techniques. Parts 1-5*. Instrumentation, Systems, and Automation Society, Research Triangle Park, NC.

[49] ISA TR 84.00.03 (2002). *Guidance for Testing of Process Sector Safety Instrumetned Functions (SIF) Implemented as or within Safety Instrumented Systems (SIS)*. Instrumentation, Systems, and Automation Society, Research Triangle Park, NC.

[50] ISA TR 84.00.04-1 (2005). *Guidelines for the implementation of ANSI/ISA-84.00.01-2004 (IEC 61511 Mod)*. Instrumentation, Systems, and Automation Society, Research Triangle Park, NC.

[51] ISA TR 84.00.04-2 (2005). *Part 2: Example implementation of ANSI/ISA 84.00.01-2004 (IEC 61511 mod)*. Instrumentation, Systems, and Automation Society.

[52] ISA TR 96.05.01 (draft) (2008). *Partial stroke tesing of automated block valves*. Instrumentation, Systems, and Automation Society.

[53] ISO-IEC Guide 2 (2004). *Standardization and related activities - General vocabulary*. International Standards Organization, International Electrotechnical Commission, Geneva.

[54] ISO-IEC Guide 51 (21999). *Safety aspects - Guidelines for their inclusion in standards*. International Standards Organization, International Electrotechnical Commission, Geneva.

[55] ISO 10418 (2003). *Petroleum and natural gas industries - Offshore production installations, basic surface process safety systems*. International Standards Organization.

[56] ISO 13702 (1999). *Petroleum and natural gas industries - Control and mitigation of fires and explosions on offshore production installlations - Requirements and guidelines*. International Standards Organization, Geneva.

[57] ISO 13849 (2006). *Safety of Machinery – Safety-Related Parts of Control Systems*. International Standardization Organization, Geneva.

[58] ISO 26262 (2006). *Road vehicles – Functional safety*. International Standardization Organization, Geneva.

[59] ISO 9000 (2005). *Quality management systems - Fundamentals and vocabulary*. International Standards Organization, Geneva.

[60] ISO/FDIS 14224 (2006). *Petroleum, petrochemical and natural gas industries - Collection and exchange of reliability and maintenance data for equipment*. International Standards Organization, Geneva.

[61] Jackson, Y., Tabbagh, P., Gibson, P., and Seglie, E. (2005). The new Department of Defense (DoD) guide for achieving and assessing RAM. In *Proceedings - Annual Reliability and Maintainability Symposium*, volume 2005, pages 1 – 7. Institute of Electrical and Electronics Engineers, Inc., Piscataway, NJ.

[62] Johannessen, J.-A. (2006). *Vitenskapsstrategi og vitenskapsfilosofi*. Fagbokforlaget, Bergen.

[63] Kaplan, S. (1997). Words of risk analysis. *Risk Analysis*, 17(4):407 – 417.

[64] Knegtering, B. (2004). Safety-PLC's striking role for partial valve stroke testing. *Technical Papers of ISA*, 454:563 – 572.

[65] Lundteigen, M. and Rausand, M. (2009a). A practical approach to reliability assessment of safety instrumented systems in the process industry. *Not yet submitted*.

[66] Lundteigen, M. A. and Rausand, M. (2006). Assessment of hardware safety integrity. In *Proceedings of the 30th ESReDA seminar*, pages 185–198. European Commission, Joint Research Centre, Ispra, Italy.

[67] Lundteigen, M. A. and Rausand, M. (2007a). Common cause failures in safety instrumented systems on oil and gas installations: Implementing defense measures through function testing. *Journal of Loss Prevention in the Process Industries*, 20(3):218–229.

[68] Lundteigen, M. A. and Rausand, M. (2007b). The effect of partial stroke testing on the reliability of safety valves. In *Risk, Reliability and Societal Safety*. Taylor & Francis, London, UK.

[69] 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.

[70] Lundteigen, M. A. and Rausand, M. (2008b). Spurious activation of safety instrumented systems in the oil and gas industry: basic concepts and formulas. *Reliability Engineering and System Safety*, 93:1208–1217.

[71] Lundteigen, M. A. and Rausand, M. (2009b). Architectural constraints in IEC 61508: do they have the intended effect? *Reliability Engineering and System Safety*, 94:520–525.

[72] Lundteigen, M. A. and Rausand, M. (200x). Development of safety instrumented systems – RAMS engineering and management from a producer perspective. *Submitted to Reliability Engineering and System Safety*.

[73] MacDonald, D. (2004a). *Practical industrial safety, risk assessment and shutdown systems*. Elsevier, Burlington, MA.

[74] MacDonald, D. (2004b). *Practical machinery safety*. Newnes, Oxford, UK.

[75] Mahn, J. A. (1996). Getting to necessary and sufficient - Developing accident scenarios for risk assessment. Technical report, Sandia National Laboratories, Albuquerque, NM.

[76] McCrea-Steele, R. (2005). Partial stroke testing implementing for the right reasons. In *Technical Papers of ISA*, volume 459, pages 229–238. Instrumentation, Systems, and Automation Society, Research Triangle Park, NC.

[77] MIL-HDBK-217F (1991). *Reliability Prediction of Electronic Equipment*. U.S. Department of Defense, Washington, DC.

[78] Minderhoud, S. and Fraser, P. (2005). Shifting paradigms of product development in fast and dynamic markets. *Reliability Engineering and System Safety*, 88(2):127 – 135.

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

[80] Murthy, D. N. P., Rausand, M., and Østerås, T. (2008). *Product reliability: Specification and performance*. Springer, London, UK.

[81] NASA (2002a). *Fault Tree Handbook with Aerospace Applications*. NASA Office of Safety and Mission Assurance, Washington, DC.

[82] NASA (2002b). *Probabilistic risk assessment procedures guide for NASA managers and practitioners*. NASA Office of Safety and Mission Assurance, Washington, DC.

[83] NEA (2000). *ICDE ProjectReport: Collection and analysis of common-cause failure of emergency diesel generators*. Nuclear Energy Agency, Issy-les-Moulineaux, France.

[84] NEA (2002). *ICDE Project Report: Collection and analysis of common-cause failures of safety and relief valves*. Number NEA/CSNI/R(2002)19. Nuclear Energy Agency, Issy-les-Moulineaux, France.

[85] NEA (2003). *ICDE Project Report: Collection and analysis of common-cause failures of check valves*. Number EA/CSNI/R(2003)15. Nuclear Energy Agency, Issy-les-Moulineaux, France.

[86] NEA (2004). *International common-cause failure data exchange*. Number NEA/CSNI/R(2004). Nuclear Energy Agency, Issy-les-Moulineaux, France.

[87] Nordland, O. and Lundteigen, M. A. (2007). Safety qualification of a software development environment. *International Journal of Performability Engineering*, 3(1):61–73.

[88] NORSOK I-001 (2000). *Field instrumentation (Rev. 3)*. Norwegian Technology Centre, Lysaker, Norway.

[89] NORSOK I-002 (2001). *Safety and automation systems (SAS) (Rev. 2)*. Norwegian Technology Centre, Lysaker, Norway.

[90] NORSOK P-001 (2006). *Process design (Rev. 4)*. Norwegian Technology Centre, Lysaker, Norway.

[91] NORSOK S-001 (2000). *Technical safety (Rev. 3)*. Norwegian Technology Centre, Lysaker, Norway.

[92] NORSOK Z-008 (2001). *Criticality Analysis for maintenance purposes*. Norwegian Technology Centre, Lysaker, Norway.

[93] NORSOK Z-013 (2001). *Risk and emergency prepardness analysis*. Norwegian Technology Centre, Lysaker, Norway.

[94] Norwegian Research Council (2000). *Quality in Norwegian Research. A summary of concepts, methods, and means (In Norwegian: Kvalitet i norsk forskning. En oversikt over begreper, metoder og virkemidler)*. Norwegian Research Council, Oslo, Norway.

[95] NUREG/CR-5460 (1990). *A Cause-Defense Approach to the Understanding and Analysis of Common Cause Failures*. US Nuclear Regulatory Commission, Washington, DC.

[96] NUREG/CR-5485 (1998). *Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment*. US Nuclear Regulatory Commission, Washington, DC.

[97] NUREG/CR-6090 (1993). *The Programmable Logic Controller and its Application in Nuclear Reactor Systems*. US Nuclear Regulatory Commission, Washington, DC.

[98] OECD. Organization for economic co-operation and development: Glossary of statistical terms. http://stats.oecd.org/glossary/index.htm.

[99] Oien, K. (1998). Improved quality of input data for maintenance optimization using expert judgment. *Reliability Engineering and System Safety*, 60(2):93–101.

[100] OLF-070 (2004). *Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry*. The Norwegian Oil Industry Association, Stavanger, Norway.

[101] OREDA (2002). *OREDA Reliability Data*. OREDA Participants, Available from: Det Norske Veritas, NO 1322 Høvik, Norway, 4rd edition.

[102] OSHA 1910-119 (1992). *Process safety management of highly hazardous chemicals - 1910.119*. Occupational Safety & Health Administration, Washington, DC.

[103] Papadopoulos, Y. and A. McDermid, J. (1999). The potential for a generic approach to certification of safety critical systems in the transportation sector. *Reliability Engineering and System Safety*, 63(1):47–66.

[104] Parry, G. W. (1991). Common cause failure analysis: A critique and some suggestions. *Reliability Engineering and System Safety*, 34:309–326.

[105] Paula, H. M., Campbell, D. J., and Rasmuson, D. M. (1991). Qualitative cause-defense matrices: Engineering tools to support the analysis and prevention of common cause failures. *Reliability Engineering and System Safety*, 34(3):389–415.

[106] Peres, F., Bouzaiene, L., Bocquet, J.-C., Billy, F., Lannoy, A., and Haik, P. (2007). Anticipating aging failure using feedback data and expert judgment. *Reliability Engineering and System Safety*, 92(2):200–10.

[107] Perrow, C. (1999). *Normal accidents: living with high-risk technologies*. Princeton University Press, Princeton, NJ.

[108] Rausand, M. and Høyland, A. (2004). *System Reliability Theory: Models, Statistical Methods, and Applications*. Wiley, Hoboken, NJ, 2nd edition.

[109] Redmill, F. (1998). IEC 61508 - principles and use in the management of safety. *Computing and Control Engineering Journal*, 9(5):205 – 213.

[110] Rooney, J. (2001). IEC 61508: an opportunity for reliability. In *Proceedings of the Annual Reliability and Maintainability Symposium*, pages 272–277. Institute of Electrical and Electronics Engineers, Inc., Piscataway, NJ.

[111] Signoret, J.-P. (2007). High integrity pressure protection systems (HIPPS) - Making SIL calculations effective. *Exploration and Production - oil and gas review (OTC edition)*, pages 14–17.

[112] Sinnamon, R. M. and Andrews, J. D. (1996). Fault tree analysis and binary decision diagrams. In *Proceedings of the Annual Reliability and Maintainability Symposium*, pages 215–222. Institute of Electrical and Electronics Engineers, Inc., Piscataway, NJ.

[113] SINTEF (2006a). *Reliability prediction methods for safety instrumented systems, PDS data handbook, 2006 edition*. SINTEF, Trondheim, Norway.

[114] SINTEF (2006b). *Reliability prediction methods for safety instrumented systems, PDS method handbook, 2006 edition*. SINTEF, Trondheim, Norway.

[115] Sklet, S. (2006). Safety barriers: Definition, classification, and performance. *Journal of Loss Prevention in the Process Industries*, 19(5):494–506.

[116] Smith, D. J. and Simpson, K. G. L. (2004). *Functional Safety: A straightforward guide to applying IEC 61508 and related standards*. Elsevier: Butterworth Heinemann, Oxford, UK, 2nd edition.

[117] Summers, A. (2003a). Differences between IEC 61511 and ISA 84. In *Safety Instrumented Systems for the Process Industry*, pages 45–54. Instrumentation, Systems, and Automation Society, Research Triangle Park, NC.

[118] Summers, A. (2004). Update on ANSI/ISA 84.00.01-2003. In *Proceedings of the Annual Symposium on Instrumentation for the Process Industries*, pages 73–79. Instrumentation, Systems, and Automation Society, Research Triangle Park, NC.

[119] Summers, A. (2007). Status of SIS good engineering practices. In *Proceedings of the Annual Symposium on Instrumentation for the Process Industries*, pages 39–. Instrumentation, Systems, and Automation Society, Research Triangle Park, NC.

[120] Summers, A. and Zachary, B. (2000). Partial-stroke testing of safety block valves. *Control Engineering*, 47(12):87–89.

[121] Summers, A. E. (1998). Techniques for assigning a target safety integrity level. *ISA Transactions*, 37(2):95–104.

[122] Summers, A. E. (2000). Viewpoint on ISA TR84.0.02 – Simplified methods and fault tree analysis. *ISA Transactions*, 39(2):125–131.

[123] Summers, A. E. (2003b). Introduction to layers of protection analysis. *Journal of Hazardous Materials*, 104(1-3):163–168.

[124] Summers, A. E. (2005). Can you safely “grandfather” your SIS? *Chemical Processing*, 68(8):42 – 44.

[125] Summers, A. E. (2006). IEC 61511 and the capital project process – A protective management system approach. *Journal of Hazardous Materials*, 130(1-2):28–32.

[126] 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.

[127] UKOOA (1995). *Guidelines for instrument-based protecive systems*. United Kingdom Offshore Operators Association, London, UK.

[128] Van Heel, K., Knegtering, B., and Brombacher, A. (1999). Safety lifecycle management, a flowchart presentation of the IEC 61508 overall safety lifecycle model. *Quality and Reliability Engineering International*, 15(6):493 – 500.

[129] Ward, D. (1996). Guidelines for the development of automotive software. *Software Engineering Journal*, 11(2):76–81.