Joel Nyman

Operational Data Framework for Safety Instrumented Systems

A Case Study in Functional Safety and Reliability

School of Technology and Innovations
Master's thesis
Master´s Programme in Smart Energy

Vaasa 2024

UNIVERSITY OF VAASA
School of Technology and Innovations
Author: Joel Nyman
Title of the thesis: Operational Data Framework for Safety Instrumented Systems: A Case Study in Functional Safety and Reliability
Degree: Master of Science in Technology
Discipline: Smart Energy
Supervisor: Timo Mantere
Year: 2024 **Pages:** 100

ABSTRACT:

In various industries, companies are adopting functional safety measures to address safety concerns, adhere to standards, and manage complex systems. This research is focused on ensuring the reliable operation of Safety Instrumented Systems (SISs) by emphasizing the reliability data. The study examines methodologies for collecting data, classifying failures, mitigating risks, and complying with international safety standards. Through a case study in the energy and marine power industry, a theoretical framework is developed to utilize operational data for assessing SIS performance in the form of a new Engine Safety System (ESS). By complying with IEC standards 61508 and 61511 and incorporating the framework into the ESS's Functional Safety Management Plan, the research addresses key challenges such as data collection, failure analysis, and performance verification. The primary research questions involve determining the type of data to be collected and establishing guidelines for analysing and evaluating that data. A mixed method approach is chosen, with a greater emphasis on qualitative aspects due to the nature of interpreting standards and establishing procedures.

The developed framework is presented using tables that outline the required data inputs for reporting actual demands, spurious trips, failures of other barriers, and SIS element failures. Failure report templates are provided, emphasizing the importance of identifying root causes and categorizing failures into Safe or Dangerous failures, as well as Undetected or Detected. The reliability assessment involves comparing actual performance data against the criteria defined in the Safety Integrity Requirements that have been established for the SIS, based on the outcome of the risk assessment. Different risk assessment techniques, such as Layer of Protection Analysis, Fault tree analysis, and risk matrices, are presented in this context, while key performance indicators like demand rates and failure rates are explored to highlight their role in verifying SIS performance.

The established framework, designed for the ESS to execute safety functions at Safety Integrity Level 2, is versatile and can serve as a robust foundation for the development of future Functional Safety projects within the organisation and can be applied to other SISs with different Safety Integrity level targets. The study concludes by addressing challenges associated with reliability and various data sources, such as human error and lack of functional safety training, emphasizing the significance of comprehending functional safety when operating with data of SISs.

KEYWORDS: Functional Safety, Safety Instrumented Systems, IEC Standards, Operational data, Reliability Analysis, Reliability data, Risk assessment.

VASA UNIVERSITET
Skolan för Teknologi och Innovation
Skribent: Joel Nyman
Avhandlingens titel: Operativ Datastruktur för Säkerhetskritiska System: En fallstudie inom funktionssäkerhet och tillförlitlighet
Examen: Diplomingenjör
Program: Smart Energy
Handledare: Timo Mantere
År: 2024 **Sidtal:** 100

ABSTRAKT:

Inom flera branscher implementerar företag funktionella säkerhetsåtgärder för att förbättra säkerheten, uppfylla standarder och hantera komplexa system. Denna avhandling fokuserar på att säkerställa tillförlitlig drift av säkerhetskritiska system (SIS:s), med särskild uppmärksamhet på tillförlitligheten av operativa data. Studien undersöker metoder för att samla in data, klassificera fel, minska risker och följa internationella säkerhetsstandarder. Ett teoretiskt ramverk utvecklas för insamling och användning av operativa data för att bedöma prestandan hos det säkerhetskritiska systemet. Forskningen genomförs som en fallstudie vid ett företag som specialiserar sig på energi- och marina kraftlösningar, med syftet att följa IEC standarder 61508 och 61511 och upprätthålla korrekt information om faror, fel, och relevanta händelser. Ramverket används för att utveckla en process som inkorporeras i funktionshanteringsplanen för ett nytt säkerhetssystem för motorer. Detta innebär tydlig definiering av data som behöver samlas in och upprättande av riktlinjer för analys och utvärdering av insamlade data, vilket båda utgör de primära forskningsfrågorna. En blandad forskningsmetod valdes eftersom standarderna innefattar både kvantitativa och kvalitativa krav. Dock, på grund av naturen av tolkning av krav från standarder och upprättande av procedurer, är den kvalitativa aspekten mer dominerande.

Det utvecklade ramverket presenteras med hjälp av tabeller som beskriver de nödvändiga datainmatningarna för att rapportera faktiska fel, oavsiktliga avbrott, fel i andra säkerhetsbarriärer och fel på SIS-element. Felrapporteringsmallar tillhandahålls, där betydelsen av att identifiera rotorsakerna och kategorisera fel som säkra eller farliga, liksom upptäckta eller oidentifierad. Tillförlitlighetsbedömningen innebär att jämföra faktiska prestandadata mot de kriterier som har fastställts för säkerhetsintegriteten baserat på resultatet av riskbedömningen. Olika riskbedömningstekniker, såsom lager av skyddsanalys (LOPA), felträdsanalys (FTA) och riskmatriser, presenteras i detta sammanhang, medan nyckelindikatorer som frekvensen av säkra eller farliga fel utforskas för att belysa deras roll i att verifiera SIS-prestanda. Det etablerade ramverket, som är utformat för att ESS ska kunna utföra säkerhetsfunktioner på säkerhetsintegritetsnivå 2, är mångsidigt och kan fungera som en robust grund för utveckling av framtida projekt inom funktionell säkerhet inom organisationen och kan appliceras på andra SIS med andra säkerhetsintegritetsmål. Studien avslutas med att ta upp utmaningar relaterade till tillförlitlighet och olika datakällor, såsom mänskliga fel och bristande utbildning i funktionell säkerhet, vilket understryker vikten av att förstå funktionell säkerhet när man arbetar med data relaterat till säkerhetskritiska system.

Nyckelord: Functional Safety, Safety Instrumented Systems, IEC Standards, Operational data, Reliability Analysis, Reliability data, Risk assessment.

Contents

Figures

Tables

Abbreviations

ALARP	As Low as Reasonably Practicable
CM	Conditional Modifiers
DC	Diagnostic Cover
DD	Dangerous Detected
DU	Dangerous Undetected
E/E/PE	Electrical/Electronic/Programmable Electronic
ESM	Engine Safety Module
ESS	Engine Safety System
EUC	Equipment Under Control
FMEDA	Failure Modes, Effects, and Diagnostic Analysis
FSMP	Functional Safety Management Procedure
FTA	Fault Tree Analysis
HAZOP	Hazard and Operability Analysis
HFT	Hardware Fault Tolerance
IEC	International Electrotechnical Commission
IPL	Independent Protection Layer
LOPA	Layer of Protection Analysis
KPI	Key Performance Indicator
PFD	Probability of dangerous failure on demand
PFH	Frequency of a dangerous failure per hour
PHA	Process Hazard Analysis
SD	Safe Detected
SFF	Safe Failure Fraction

SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SRS	Safety Requirements Specification
SU	Safe Undetected
TMEF	Total Mitigated Event Frequency
λ	Failure rate

1 Introduction

In an era where technological advancements drive industrial progress, the focus on safety has intensified across industries. This Master´s Thesis is a study in ensuring the reliable operation of Safety Instrumented Systems (SISs) with particular emphasis on the dependability of operational data. It examines methodologies for collecting and utilizing this data to classify failures, implement risk mitigations, and verify compliance with safety requirements outlined in international safety standards IEC 61508 and IEC 61511. The study establishes a theoretical framework for the collection of operational data, including its application in evaluating SIS performance while ensuring compliance with standards in a reliable way.

1.1 Research Purpose

This research has been written for a technology company (herein referred to as case company), that provides innovative solutions within the energy and marine markets. Technological advancements in industries have introduced many new risks and hazards that led to the development of improved safety measures (Sklet, 2006). Among these safety measures is functional safety, which in the context of product safety, refers to when the safety of a machine depends on the correct function of the control system and other risk reduction measures (IEC 61508-4, 2010, [3.1.12]).

The customers of the case company have started to demand safety according to functional safety standards, such as IEC 61508 and IEC 61511 published by the International Electrotechnical Commission (IEC). Simultaneously, the company expects this to only increase in the future. Therefore, the company has a new Engine Safety Module (ESM) under development as part of the Engine Safety System (ESS). However, the application of the IEC standards requires the implementation of peculiar ways of working and organizational aspects that are not yet fully in place. Therefore, a formal structured functional safety development project was created.

IEC 61508 requires that procedures are developed for analysing operations and maintenance performance, and for maintaining accurate information on hazardous events, safety functions, and safety-related systems (IEC 61508-1, 2010 [6.2.9]). SISs play a critical role in ensuring the safety of industrial processes and have been designed to detect and respond to hazardous conditions, preventing accidents, and protecting human life. However, SISs are complex systems and consist of several reliability parameters which shall be assessed based on the operational data of the SIS. These reliability parameters also derive from the IEC standards as risk reduction criteria. Therefore, a procedure with a framework for the collection and evaluation of operational data of the new Engine Safety System (ESS) must be established. The ESS consists of the ESM that is under development which, in combination with its associated sensors and final elements, forms a SIS.

The primary focus of this study revolves around the following two key research questions:

Question 1: What data is to be collected?
Data collection is essential for understanding the behaviour of SISs and identifying potential problems. By collecting data on SIS events, such as alarm activations and trips, operators can identify trends and patterns that may indicate impending failures. This data helps address corrective actions and find root causes and serves as the main data input for reliability assessment.

Question 2: How can the data be used for the reliability assessment of the SIS?
Performance evaluation is the process of assessing the effectiveness of SISs in meeting their safety requirements. This involves evaluating the SIS's ability to detect and respond to hazardous conditions within the criteria of the safety requirements.

1.2 Research Objectives

The objective of this study is to establish a procedure with a framework for the collection of operational data and evaluation of the overall performance of the new ESM and the whole SIS. The data that needs to be collected for the reliability assessment of the SIS is identified and motivated along with the methodology for using the collected data to assess the reliability parameters. The framework is designed for this specific functional safety development project. However, the purpose is that it also may be of use in other functional safety projects within the case company.

Throughout the whole study, an overarching objective is to ensure compliance with the IEC standards 61508 and 61511. Besides meeting the criteria defined in the requirements of these standards, they provide guidelines and recommendations about data collection and the evaluation process.

The goal of the procedure is to ensure compliance with IEC standards, aiming to fulfil the requirements of maintaining accurate information on hazards and hazardous events. By defining the necessary data to be collected and providing guidelines on reviewing gathered data, the procedure becomes an integral part of the Functional Safety Management Plan (FSMP) for this development project. In the FSMP, it will be included under "Procedures for analysing electrical, electronic, and programmable electronic (E/E/PE) safety-related system operations and maintenance performance." The established procedure is primarily intended for technical services, field services, or operating personnel engaged in the collecting of operational data of installations provided with the new ESS.

1.3 Delimitations

This thesis focuses on identifying what data to collect and establishing a framework for assessing the reliability of the new ESS. At an early stage of this study, a decision was made to

concentrate on defining the specific data input without specifying the exact software to be used due to uncertainties in the software selection process. This is further elaborated on in Chapter 4.1.2 where the data flow of the ESS is explained. Another factor that also delimits this research is that while the thesis will offer guidelines about the different risk assessment methods that serve as the foundation for reliability evaluation, no practical examples of their execution or recommendation of specific programs for analysis are considered. This makes it easier to serve as a foundation and to be adapted into other projects FSMP, as software tools are subject to updates and changes. The downside is that practical examples would have been a good way to demonstrate how this framework can be utilized, thereby enhancing reader comprehension.

The framework developed within this thesis is primarily designed for a specific ESS aiming for a certain Safety Integrity Level (SIL) as defined by the IEC standards. Hence, specific risk assessment methods have been used to establish the safety requirements. The applicability of the framework to other SISs could be considered, including those involving additional Safety Instrumented Functions (SIFs), even with other SIL targets. However, it's essential to highlight that the direct transferability of the established framework to other SISs may be subject to varying operational procedures and requirements. While the SIL itself may not necessarily impact the operational procedures, the integration of the framework with different SIS configurations should be approached with careful consideration of specific system characteristics and associated safety requirements.

2 Safety Systems and Standards

This chapter explores the origins and fundamental concepts of functional safety and the key standards that govern its implementation. The analysis includes a range of academic sources, books, reports, and the IEC standards 61508 and 61511. Functional safety is a methodical approach to ensuring that safety systems reliably perform their intended safety functions. Guidelines and requirements from the standards are presented along with techniques and measures of reliability. The theoretical framework presented in Chapter 4 is motivated through this literature study.

2.1 Functional Safety

Functional safety is a critical aspect of industrial processes, encompassing measures, and systems designed to prevent or mitigate failures in equipment and processes. The purpose of functional safety is to ensure their reliable and safe operation, particularly in scenarios where a failure could lead to serious harm, damage, or environmental impact.

Functional safety:

> Systems that lead to the freedom from unacceptable risk of injury or damage to the health of people by the proper implementation of one or more automatic protection functions (often called safety functions). A safety system consists of one or more safety functions. (TÜV SÜD, n.d.)

According to Smith and Simpson (2004, p. 5), functional safety is about identifying failures that will or may lead to serious consequences and then establishing a maximum tolerable frequency for each mode of failure. Any component or equipment that can contribute to dangerous hazards is identified and referred to as “safety-related”. Further on, the authors mention examples where functional safety has been implemented including industrial process control systems, process shutdown systems, rail signalling equipment, automotive controls, medical treatment equipment, etc.

An essential aspect of Functional Safety is to consider the Safety Integrity Levels (SILs) which are a quantifiable measure of the reliability of safety instrumented systems (SIS) in achieving functional safety objectives. The SIL levels range from SIL 1 (lowest) to SIL 4 (highest). Each level corresponds to a different level of risk reduction, with higher SIL levels indicating a greater degree of risk mitigation. (Smith & Simpson, 2004, p. 7).

To establish and maintain SIL levels effectively, the International Electrotechnical Commission (IEC) has published international standards that address functional safety. Two of these standards, such as IEC 61508 (Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems) and IEC 61511 (Functional Safety – Safety Instrumented Systems for the Process Industry Sector) play key roles in defining the principles, requirements, and guidelines for achieving functional safety. They are the two standards on which this research is based. The following key aspects are outlined in the two standards and are of relevance to this research:

- **Risk Assessment:** The initial step involves assessing the risks associated with a process or system, considering potential hazards, their severity, and their likelihood.
- **SIL Determination:** Based on the risk assessment, the appropriate SIL level is determined to achieve the desired level of risk reduction.
- **SIS Design**: Safety instrumented systems are designed, taking into consideration factors like hardware reliability, software integrity, and systematic capability.
- **Verification and Validation:** Rigorous testing and validation processes are employed to ensure that the SIS meets the specified SIL requirements.
- **Maintenance and Management:** Proper maintenance and management practices are essential to sustain the SIL level throughout the operational life of the system.

2.1.1 IEC 61508

IEC 61508 consists of seven parts and provides a standardized approach for all activities related to the safety lifecycle of systems that include electrical, electronic, and programmable electronic (E/E/PE) components used to execute safety functions (IEC, 2010a, p. 7). According to Bell (2011), the standard was developed by the IEC and goes back to 1985 when a task group was formed to create a universal standard for programmable electronic systems intended for safety applications. This ultimately led to the release of all the seven parts of IEC 61508 in multiple parts between 1998-2000. Additionally, a broader range of applications were included, such as electrical systems and electronic systems. In 2002, a review of the standard family was initiated. This comprehensive review culminated in the release of IEC 61508 Edition 2 in 2010. As of November 2023, this is still the latest version. The IEC 61508 family consists of the seven following parts:

1. **IEC 61508-1: General Requirements,** (IEC, 2010a)**:** This part provides the foundational principles and general requirements for achieving functional safety across various industries. It establishes the overall framework, defines key terms, and outlines the systematic approach to functional safety.

2. **IEC 61508-2: Requirements for E/E/PE Safety-Related Systems,** (IEC, 2010b)**:** Part two focuses on E/E/PE safety-related systems. It defines specific requirements and guidelines for designing, implementing, and maintaining these systems to meet safety integrity levels (SILs).

3. **IEC 61508-3: Software Requirements**, (IEC, 2010c): Part three delves into software aspects of safety-related systems. It outlines requirements and recommendations for the development, testing, and management of software components within safety systems.

4. **IEC 61508-4: Definitions and Abbreviations**, (IEC, 2010d): This part references definitions and abbreviations used throughout the entire IEC 61508 standard. It ensures consistent terminology and understanding across different sections of the standard.

5. **IEC 61508-5: Examples of Methods for Determination of Safety Integrity Levels,** (IEC, 2010e): Part 5 provides practical examples and methodologies for determining safety integrity levels (SILs) for safety functions. It assists organisations in assessing the required level of safety for their systems.

6. **IEC 61508-6: Guidelines on the Application of IEC 61508-2 and IEC 61508-3,** (IEC, 2010f): Part 6 offers guidance on how to apply the requirements specified in Parts 2 and 3 of the standards. It provides additional insights and recommendations for compliance.

7. **IEC 61508-7: Overview of Techniques and Measures,** (IEC, 2010g): This part provides an overview of various techniques and measures used in achieving functional safety. It helps users understand the different methods and tools available for safety-related tasks.

According to Bell (2011), parts one, two, and three are considered normative requirements. They establish the principles and specific requirements that organizations must follow to ensure functional safety. Part four is only for definitions and abbreviations while parts five, six, and seven are more informative oriented and consist mainly of guidelines and examples for development. IEC 61508 is the backbone of all the Functional Safety standards, and applicable to all industries. Due to its wide application area, it can be difficult to interpret and apply directly to each sector. Therefore, there are many sector-specific standards with IEC 61508 as a basis that have been developed for achieving functional safety (see Figure 1). Each sector or industry has its specific terminology and language which need to be captured.

By having sector-specific standards, practises and constraints of sectors are considered, and functional safety becomes more accessible and applicable to system designers, system integrators, and end users. This allows for better clarity and understanding of how to achieve functional safety without having to dive deep into IEC 61508. Additionally, it opens the possibility of having fewer complex requirements (see Bell, 2011; Charnock, 2001).

Figure 1. IEC 61508 and its adaptions as defined by TUV (SÜD, n.d.)

2.1.2 IEC 61511

One of the sector-specific standards that implements the framework of IEC 61508 is IEC 61511. According to Smith and Simpson (2016), the standard addresses functional safety within the process industry sector and guides utilizing standard products into SISs in the form of requirements for the design, implementation, operation, and performance evaluation of the SIS. The standard mentions the importance of risk assessment to identify and assess potential hazards, as well as the need for effectively managing functional safety throughout the entire lifecycle of a SIS. The first edition of IEC 61511 was published in 2003 and the second and latest edition in 2016. The standard consists of the following three parts:

1. **IEC 61511-1: Framework, definitions, system, hardware, and application programming requirements**, (IEC, 2016a): This part serves as the sole normative requirement within the 61511 family. It outlines the specifications, design, installation, operation, and maintenance guidelines for a SIS.

2. **IEC 61511-2: Guidelines for the application of IEC 61511-1:2016,** (IEC, 2016b)**:** The second part is mainly informative and works as a supplement to part 1 by guiding the specification, design, installation, operation, and maintenance of the SIS and related SIFs.

3. **IEC 61511-3: Guidance for the determination of the required safety integrity levels,** (IEC, 2016c)**:** The final is also an informative standard and gives guidance on hazard and risk analysis. This section of the standard offers detailed insights and methodologies for systematically assessing and mitigating risks associated with safety instrumented systems (SIS) and their interactions with industrial processes.

2.1.3 Relationship between IEC 61508 and 61511

Since IEC 61511 is a sector standard that uses the framework of IEC 61508, they are strongly related and often used together in the context of ensuring functional safety. However, while IEC 61508 sets the more general terms, IEC 61511 refines the principles and guidelines of IEC 61508 specifically for the process industry, where the consequences of failures can be severe (IEC, 2016a, p. 7). Unlike IEC 61508, which focuses on individual elements, IEC 61511 places more emphasis on the integration level of the SIS. This results in simplified requirements and more straightforward guidelines. IEC 61508 established requirements for new devices, embedded software, and SIL 4 applications, making it mandatory for manufacturers and suppliers to adhere to specific parts of the SIS (logical solver, final elements, sensors, valves, etc…). Meanwhile, IEC 61511 is more targeted for the designers, integrators, and end-users of the SIS. Both standards are more performance-based than prescriptive with a focus on risk analysis and the required risk reduction (see Figure 2).

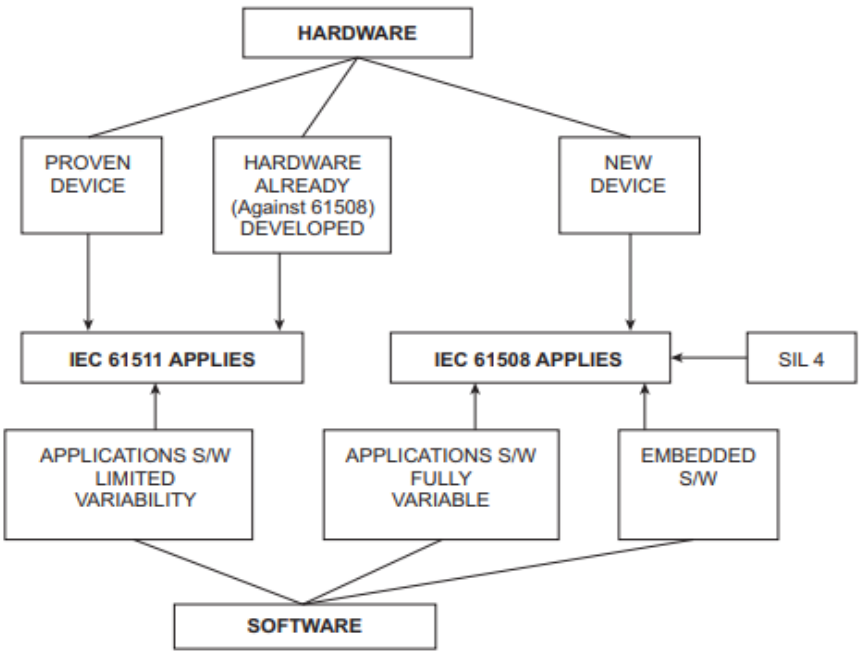

Figure 2. IEC 61508 and IEC 61511 relationship (Smith & Simpson, 2016, p. 147)

2.2 Safety Instrumented Systems

Throughout human history, people have relied on various safety barriers to protect themselves and their belongings from natural hazards and dangers. However, the Industrial Revolution introduced numerous human-induced hazards and risks that required further safety measures. This led to the development of more advanced safety barriers to prevent or mitigate the consequences resulting from these new hazards (Sklet, 2006, pp. 1-2). In the 21st century, safety measures have evolved from traditional physical barriers to encompass a range of protective systems. These systems can now include various types of barriers, such as those designed to prevent the release of radioactive materials. Additionally, they may incorporate event reporting and safety policies for comprehensive safeguards. (Hollnagel, 2004). Common safety barriers found in process plants include fire and gas detection systems, emergency shutdown systems, fire and explosion walls, passive fire protection, fire evacuation training, pressure relief systems, and more (Rausand, 2014, pp. 4-6). One of these modern safety barriers is Safety Instrumented Systems (SISs), which this thesis is focused on.

Sklet (2006) conducted a literature study to explore the definition of safety barriers. While these definitions share similarities, there is no universally agreed-upon definition for this term. Within the context of industrial safety, the author regards safety barriers as any “physical and/or non-physical means planned to prevent, control, or mitigate undesired events or accidents” (Sklet, 2006, p. 3). This is also supported by other studies (see Hollnagel, 2004; Rausand, 2014, pp. 4-5; Liu, 2020). Therefore, a safety barrier may be a technical system, operational system, or some dedicated human and organizational effort. In Figure 3, there is a demonstration of how multiple safety barriers of different types have been implemented to minimize the likelihood of potential dangers.

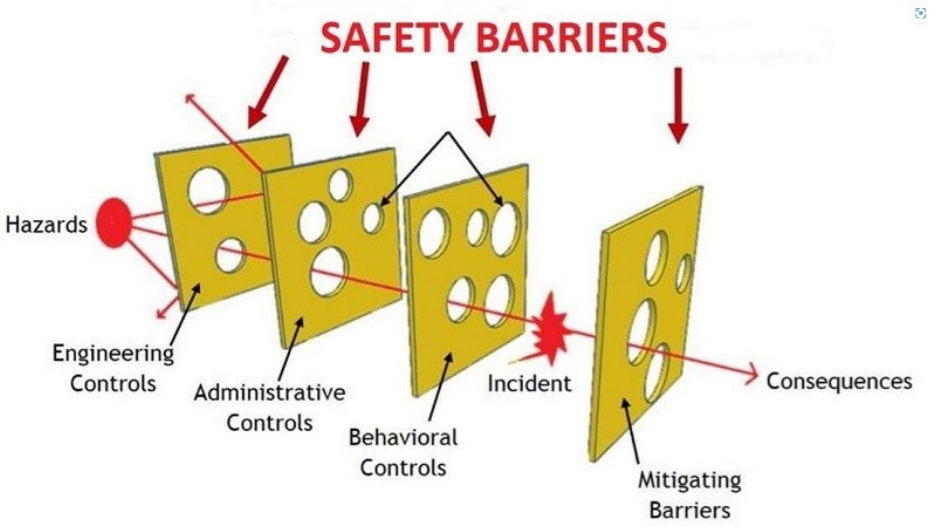

Figure 3. Example of multiple safety barriers (UIC, 2021)

Over the years, the need for comprehensive protection against various risks has increased and led to the development of different types of barriers and classification systems. According to Rausand (2014, p. 5), safety barriers may be classed as proactive: where the focus lies on preventing the undesired event from happening, with the aim to eliminate or reduce the likelihood of the event happening, and reactive: where the focus lies on mitigating the consequences of an undesired event in case they occur.

Another classification system proposed by Rausand (2014) is *active* and *passive* safety barriers, where SISs fall under the category of active barriers (p.5), a classification also supported by Sklet (2006, p.15). Sklet further distinguishes the barriers as either technical or human/operational barriers (see Figure 4). A passive barrier operates continuously and requires no action to provide protection. On the contrary, an active barrier requires a change from one state to another to achieve the same thing, often triggered by a signal or via sensors that read a measurable process such as temperature, speed, pressure, etc. According to this classification, SISs fall under the category of technical and active barriers (Sklet, 2006, p.15).

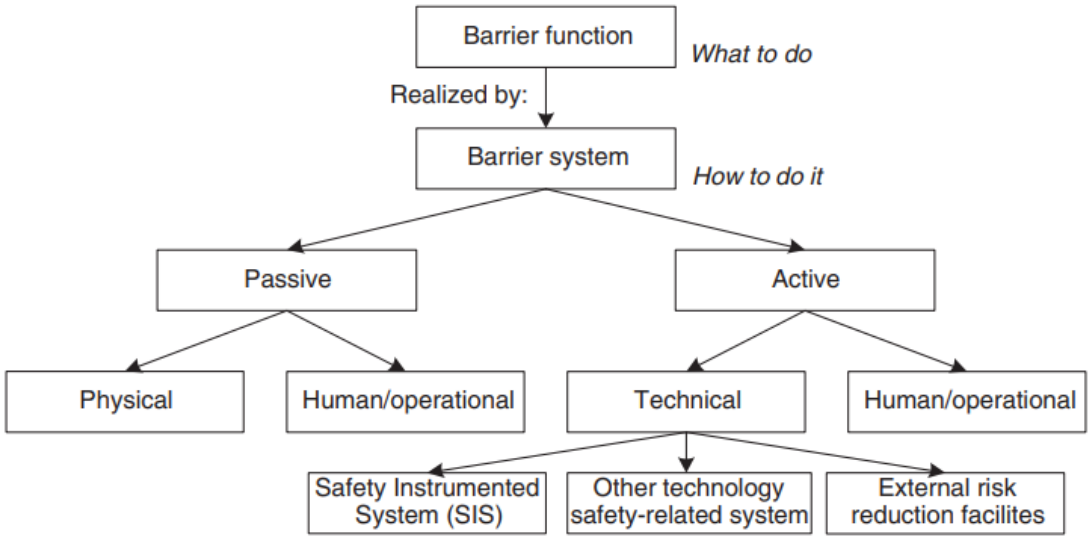

Figure 4. Classification of safety barriers (Sklet, 2006, p. 15)

Both IEC 61508 and IEC 61511 address the importance of implementing safety measures to ensure functional safety. These measures include safety barriers, such as SISs. Although the definition of a safety barrier is similar to that of a SIS, it's important to note that they are not identical. A SIS is a particular category of safety barrier, as seen in Figure 4, but not all safety barriers can meet the criteria to be considered a SIS.

2.2.1 Risk and Safety

Before further delving into SISs, it is necessary to understand the definitions of safety and risk, as they are two recurring terms in this study. Risk is defined as the combination of both the likelihood and the magnitude of harm caused by an event (IEC 61508-4 (2010, [3.1.6]) In simpler terms, risk assesses the chance of an event happening and the level of impact it could have. Safety, on the other hand, is defined as the absence of risk that is considered unacceptable (IEC 61508-4, 2010 [3.1.11]) and is achieved by including preventive or mitigating measures.

SISs are a type of mitigating measure that is used to detect and respond to hazardous events, designed to achieve a specific level of risk reduction, measured in terms of Safety Integrity Level (SIL). While risk is a measure of potential harm, safety is the state of being free from unacceptable risk. Rausand (2014, p.3) defines risk as an answer to three fundamental questions: What scenarios may lead to an undesirable outcome? What is the probability of such scenarios occurring? And lastly, what are the consequences of such occurrences in case they occur?

When engineering or designing a system, evaluating its safety is crucial. Initial to the design process, a risk acceptance criterion, or tolerable risk criteria as referred to in IEC 61508 needs to be established. These criteria define the maximum acceptable level of risk and the necessary level of risk reduction required to achieve a specific SIL. For example, if the target is to achieve SIL 2, and the preliminary system design only fulfils the criteria of SIL 1, additional safety barriers need to be installed or existing ones modified so that the risk reduction factor of SIL 2 is met. In simpler terms, the process involves setting a safety target (SIL 2, in this example) and then assessing whether the preliminary design of the SIS adequately reduces the associated risks to meet this target.

The tolerable risk refers to the level of risk that is deemed acceptable within a specific situation, considering the prevailing societal values. (IEC 61508-4, 2010 [3.1.7]). Interpreting societal values is a complex undertaking and requires thorough investigation. According to Rausand (2014), the process of defining the tolerable risk criteria includes several aspects, with risk acceptance criteria considered on the system module and Equipment under control (EUC) levels. A condition for accepting this level of risk is that risk-reducing measures have been implemented to a level so that additional measures are disproportionate compared to the benefits gained. (p.45). There are several methods available for determining the required SIL for the SIS and its Safety Instrumented Functions (SIFs). These methods are further explained in Chapter 2.5.

2.2.2 Functionality of SISs

SISs can be described as the practical implementation that plays a critical role in achieving functional safety by detecting, responding to, and mitigating hazardous events. A SIS is a type of Safety Barrier and responds to hazardous events by performing required safety functions to maintain or bring the process to a safe state. In IEC terminology, a safe state refers to when the EUC has achieved safety (IEC 61508-4, 2010, [3.1.13]). When a SIS executes these safety functions, they are commonly referred to as safety instrumented functions (SIFs). These SIFs are intended to ensure and guarantee a predetermined SIL target that the EUC must meet (Catelani et al., 2017).

As defined by the IEC 61508 family (IEC, 2010a, 2010b, 2010c): key elements of a SIS consist of three main blocks or elements: Sensors, logical solvers, and final elements (see Figure 5).

Sensor(s) is the input element of a SIS in E/E/PE Safety-related systems and serve as the eyes and ears of the system. The sensors continuously monitor and measure process parameters such as temperature, speed, pressure, flow, etc… The sensor detects deviations from safe operating conditions and transmits the signal to the logical solver.

The logic solver(s) can be considered the brains of the SIS and is responsible for determining when to initiate safety actions. The solver can be both hardware-based and/or software-based. It is usually a controller (eg. PLC) that receives and process input data from the sensors and takes actions according to the defined logic to prevent or mitigate hazardous events.

The Final Element(s) is the control element and as seen in Figure 5, the last in line of the loop. The final elements, or final control elements, can be considered as the physical implementation of the outcome of the logic solver. Typical final elements include relays, actuators, valves, etc… These devices may in turn, isolate other processes, close off pipelines, cut off power supplies, or perform other actions to prevent or mitigate accidents/failures.

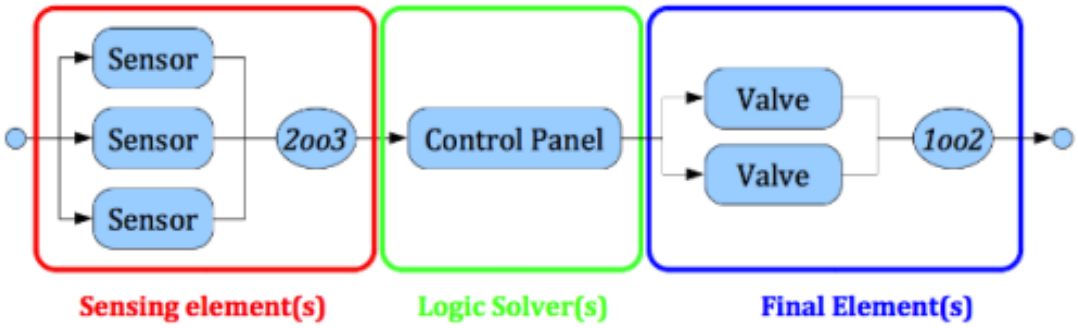

Figure 5. Functional block diagram of the SIS elements (Catelani et al., 2017)

2.2.3 Redundancy

According to the IEC 61508 standard, redundancy is the presence of multiple methods for carrying out a required function or for representing information (IEC 61508-4, 2010, [3.4.6]). This ensures that if one part fails, the system can remain operational by utilizing other items. Redundancy is mainly used to improve reliability and availability and to reduce the risk of spurious actions through different architectural configurations.

Voting arrangement is one aspect of the architecture that specifies how the redundant elements are configured. A voted group consists of a minimum of two channels performing an identical task. The voting arrangement is also referred to as a k-out-of-n system (Jahanian, 2015; Rausand, 2014, p. 101) or an M-out-of-N system (Smith & Simpson, 2016, p. 114; IEC 61508-6, 2010, Annex B). In simpler terms, this indicates that the system will only work if a minimum of k out of the n components are operational. For example, in Figure 5, three sensors measure a process independently with a voting of 2oo3 (2-out-of-3), this implies redundancy with three sensors, and the system responds if at least two of them agree. The final elements have a voting of 1oo2, requiring only one to function properly to execute the safety action.

Figure 6 illustrates an architectural block diagram of a SIS with two voting groups. The first voting group consists of three pressure transmitters. Each pressure transmitter measures the pressure of a process variable. The logic solver compares the readings from the three pressure transmitters and determines whether there is a hazardous condition. If there is a hazardous condition, the logical solver ensures the EUC is in a safe state and activates the final elements, which in this example are the shutdown valves and the circuit breaker. The exact voting arrangement is not addressed in this scenario. However, the pressure transmitters and shutdown valves are more than one unit and thereby redundant, while the logical solver and circuit breaker operate as 'stand-alone' units.

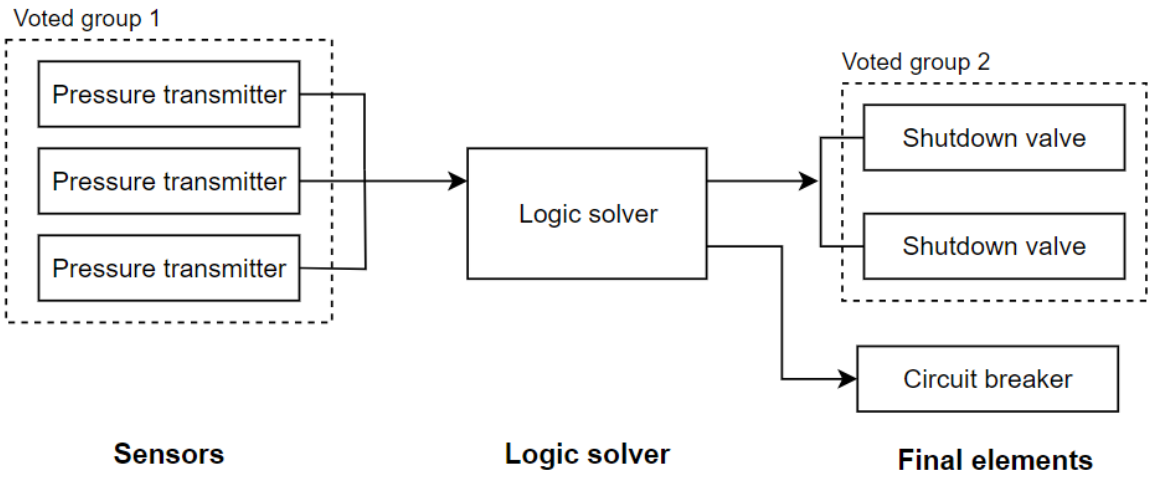

Figure 6. Voted group architecture of a SIS (Recreated from Rausand, 2014, p.26)

2.3 Failure and Failure Modes in Safety Systems

A failure is defined as "the termination of the ability to perform its required function" (IEV-191-04-01, 2005a). In SIS terminology, failure and failure modes are key concepts related to the performance and reliability of the system, especially when assessing performance. Whenever a failure occurs, it means that a component or element within the SIS was unable to fulfil its intended purpose. This can be due to multiple reasons such as hardware defects,

software errors, environmental factors, or human errors. Rausand (2014) states that a system can be classified as safety-critical when its malfunctions can cause harm to individuals, financial losses, or environmental harm (p.1). Since IEC 61508 is a standard based on evaluating risks, it implies that the requirements for the SIS have been established and defined through risk analysis findings. Safety functions are implemented to mitigate these events effectively. The author also mentions that a failure is always related to a required function, which in the context of SISs, refers to the safety functions.

A fault on the other hand, is defined as the "state of an item characterized by inability to perform a required function, excluding the inability during preventive maintenance or other planned actions, or due to lack of external resources" (IEV 191-05-01, 2005b). A fault refers to a condition that can persist for a brief or extended duration, whereas a failure is an incident that happens at a particular moment, and following a failure, the item or system is often in a state of malfunction. A relationship between these two terms is described in Figure 7. The error is the discrepancy between the actual performance and the theoretically correct value. The actual performance is allowed to deviate within a certain range but when the error gets too high, it will trigger a failure reaction and lead to a fault state of the system. A fault state occurs, as defined in IEC 61508, either by a random failure event (random hardware failures) or in a deficiency related to the item (systematic failures). These two categories are further elaborated on in chapter 2.3.1.

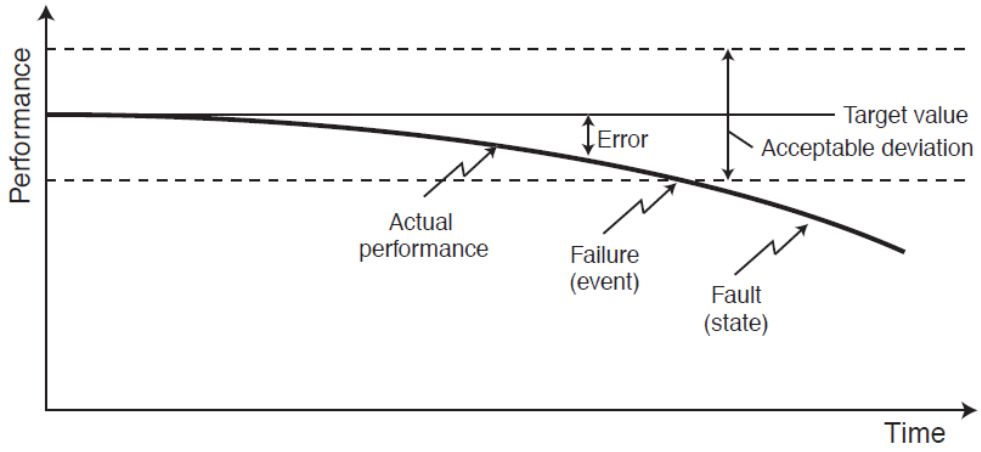

Figure 7. Relationship between failure and faults (Rausand, 2014, p. 55)

According to Smith and Simpson (2016), a failure mode is a specific way in which a component, subsystem, or system can fail due to the presence or activation of a fault. It describes the way a failure occurs and the effects it has on the system or item performance. Identifying failure modes is critical for risk assessment and reliability analysis, as it helps engineers understand the potential consequences of faults.

For example, if the situation in Figure 7 was a water pump, with the requirement that the pump must provide an output between 100 and 110 litres per minute, possible failure modes when a fault state is reached can be due to no output of the pump, too low output, too high output, or too many fluctuations that go outside the allowable range. Another example can be illustrated by considering failure modes with a water tap: If the tap is not working properly, it may be due to any of the following failure modes:

1. Failure to Open (on demand): The tap cannot be turned on when you try to open it., failure to Close (on demand): The tap remains open even when you attempt to close it.
2. Inability to Fully Open: The tap can be opened, but it doesn't reach its maximum flow capacity.

3. Failure to Regulate Flow: The tap cannot adjust the water flow as intended, causing irregular or unpredictable flow rates.
4. Leakage Through (Dripping): Water drips from the tap, even when it's supposed to be fully closed, leading to water wastage.
5. Leakage Out (From Tap Seals): Seals within the tap may fail, resulting in water leaking out from the tap's body or handles.
6. Failure to Regulate Temperature: In taps with mixing valves for hot and cold water, a failure can occur in maintaining the desired water temperature.

These are examples that demonstrate possible ways in which a water tap may malfunction. By understanding and considering possible failures, and failure modes while in the design phase of the water tap, it can help to improve the reliability of the water tap and make it more user-friendly. The same applies to SISs as well.

2.3.1 Failure Classification in IEC 61508

Failures play a vital role in the concept of reliability assurance and performance evaluation. It is necessary to assess the impact of failures on safety and design the SIS accordingly to comply with IEC 61508 (and IEC 61511). Based on the risk analysis, an SIL has been set for each safety function where possible failures have been taken into consideration. In the IEC 61508 standard, failures are categorised into two primary groups: systematic failures (including software faults) and random hardware failures (see Rausand, 2014, pp. 54-55; Smith & Simpson, 2016, p.6). The first mentioned failure pertains to a specific reason that can only be resolved by making changes to the design, manufacturing process, operational procedures, documentation, or other related elements (IEC 61508-4, 2010, [3.6.6]). A systematic failure often results from human error, design flaws, or incorrect specification during the development and design phase.

Random hardware failure can happen unexpectedly, without any predetermined timing as a result of one or more possible degradation mechanisms in the hardware (IEC 61508-4, 2010, [3.6.5]). This type of failure is further categorized as safe failure or dangerous failure with a detectability of either detected or undetected (see; IEC, 2010d; Rausand, 2014, p.60-61).

Dangerous failure: A failure of an element or system that prevents the safety function from operating. In case an actual demand should occur, the EUC will not go into the defined safe state and will remain in a hazardous state.

Safe failure: a safe failure occurs when an element or system experiences a failure, the safety function can still perform its intended role. In case an actual demand should occur, the EUC will go or remain in the defined safe state. A safe failure is often a spurious operation of the safety function, meaning that the safety function is triggered even when no real demand exists.

In case the safe or dangerous failure is detected by diagnostic tests, proof tests, operator intervention, or normal operation, it can be referred to as a detected failure. If it is not detected by the same measurements, it is an undetected failure (IEC 61508-4, 2010, [3.8.8], [3.8.9]). Rausand (2014) mentions two examples: one of a detected failure, reported as a diagnostic fault or alarm, and the other of an undetected example where the failure remains hidden until the component is asked to carry out its function (p.60). Combining the failure categories gives the following failure classes:

- **Dangerous detected failure (DD):** A failure that prevents the safety function from operating, but the condition is detected by the safety systems diagnostics.

- **Dangerous undetected failure (DU):** A failure that prevents the safety function from operating, and the condition goes undetected by the safety systems diagnostics. The failure remains hidden until the next demand activation of the safety function.
- **Safe detected failure (SD)**: A failure that triggers the safety systems diagnostics without a demand from the process (spurious operation of the safety function).
- **Undetected safe failure (SU):** Failure of a component that is part of the safety function but that does not affect the safety function. This type of failure goes undetected by the safety systems diagnostics and may increase the probability of a spurious trip occurring.

2.3.2 Failure Rates

Failure rates, according to IEC 61508-4 (2010, [3.6.16]) are expressed by the Greek letter λ (lambda) and represent the frequency or likelihood of failures occurring over time. All the failure categories mentioned in the previous chapter are represented by the lambda symbol when considered in failure rate calculations (λDD, λDU, λSD, and λSU).

Systematic failures are not random failures and are related to design flaws, specification errors, or human mistakes. These failures are not easily quantifiable and therefore, typically not considered in failure rate calculations for safety-related systems. Addressing systematic failures requires a qualitative approach where the focus lies on eliminating or mitigating the failures through processes, testing, reviewing, and following best practices rather than quantifying their occurrence in terms of failure rates (see Charnock, 2001; Rausand 2014, p.35; Smith & Simpson, 2016, p.79). Random hardware failures, on the other hand, are quantifiable and attributed to specific component failures to which failure rates are assigned. The failure rate is predicted and then compared to an accepted safe risk level. This comparison helps estimate the performance of future designs and ensures that the failure rates

meet the acceptable risk threshold. If the predictions do not meet the target risk level, the design can be adjusted accordingly until the target is met (Smith & Simpson, 2016, pp. 6-7).

2.3.3 FMEDA

According to Healy (2023), failure modes, effects, and diagnostic analysis (FMEDA) is a systematic analysis technique mainly developed by engineers from Exida to ensure that safety-critical systems, such as SISs operate reliably and safely. The technique is used to analyse the failure modes of a system, their effects, and the impact of these failures on the overall system. Each failure mode is examined in terms of its severity, probability of occurrence, and detectability. The information provided is then utilized to estimate the PFDavg for each component within the system (Rausand, 2014, p. 75). The outputs of an FMEDA typically include:

1. A list of potential failures and their associated failure modes, causes, and rates
2. A list of potential safety effects and their severity
3. A criticality matrix that ranks the potential safety effects
4. Recommendations for corrective actions

A variety of FMEDA tools are available, with spreadsheets or worksheets being commonly employed, where data is typically organized in tabular formats. Exida's report, authored by Sauk (2020), emphasizes that the precision of an FMEDA analysis relies on the component reliability data utilized in the process. The report highlights that relying on data from consumer, transportation, or telephone applications may not be appropriate for the process industries due to the differences in operating conditions and environments. For example, consumer electronics are typically used in indoor environments with controlled temperatures and humidity, while process equipment is often used in harsh environments with extreme temperatures, chemicals, and vibrations. As a result of this, the failure rates in different applications can vary heavily.

According to Catelani et al. (2010), FMEDA is an essential process for fulfilling the specifications outlined in IEC 61508. It includes the identification of potential scenarios where a safety system may fail to execute its intended functions, along with the consequences of such failures. Each component is specified with a failure rate, failure mode, and probability of occurrence, and further classified as either safe or dangerous, and undetected or detected. Besides the estimation of PFDavg, two key calculations that are part of FMEDA and essential in terms of safety assessment are safe failure fraction and Diagnostic coverage (Catelani et al., 2010). These are reliability parameters for verifying that the hardware designs meet the requirements of the functional safety standards. Chapter 2.4.3, 'Architectural constraints' provides a detailed explanation of these calculations.

2.4 Design Framework of a SIS

While the basic definition of a SIS and its functionality was described in Chapter 2.2, This chapter explains the design framework of a SIS and what the different SIL targets mean, covering key aspects essential for its functioning and reliability. Understanding how the SIL targets can be verified is essential, highlighting the importance of reliability parameters and their relationship to the target SIL.

2.4.1 Safety Lifecycle

The Safety Lifecycle outlined in IEC 61508 serves as a technical framework for organizing the requirements. The lifecycle in the standard is a 16-step closed-loop process and represents a systematic and structured approach to achieving and managing safety through the entire life of a SIS (IEC, 2010a). Rausand (2014) mentions that the life cycle of a SIS can in many cases exceed 20 years, highlighting its importance in identifying, estimating, and assessing system performance (p.40). The standard also states that an alternative lifecycle may be utilized if it adheres to the objectives and requirements of IEC 61508. In the book “The Safety Critical Systems Handbook” by Smith and Simpson (2016), a simplified version of the

lifecycle is presented which also conforms to IEC 61508 (see figure 8). This version covers all the relevant aspects but is easier to read and was therefore chosen instead of the lifecycle model presented in IEC 61508.

The lifecycle of Smith and Simpson (2016) can be divided into three phases, system analysis, system implementation, and system usage: The first part of the lifecycle represents the system analysis and involves identifying the EUC, assessing the system hazards, conducting risk analyses, and determining the allocation of SIFs along with their corresponding SILs. These requirements are then formalized into a safety requirement specification (SRS) document where all the safety-related requirements for a SIS and its associated SIFs are stated.

According to Lundteigen (2008) and Rausand (2011), There are two main categories of requirements in the SRS. Firstly, safety functional requirements, describe what the SIS is required to do and the safety functions that are needed to prevent or act upon when an undesired event occurs, such as demands. Additionally, performance criteria for each safety function are specified. The second category comprises safety integrity requirements, which define the level of performance needed from the SIS to effectively minimize identified risks. This reflects the risk-based approach to the safety lifecycle. Lundteigen (2008) states that the SRS serves as a vital document of the safety lifecycle, especially in the latter phases (p. 224). It includes the maximum tolerable risk targets and allocation of failure rate targets to the various failure modes. All the requirements, as well as the underlying assumptions, can be included in the SRS.

The middle phase of the life cycle is the system implementation phase (planning, design, verification, and installation and commission) which is the realization part where the SIS is designed according to the established requirements based on the outcome from the first part of the life cycle. Verification tests are performed and reviewed to ensure that the EUC will meet the safety requirements target and to establish if risk reduction is required.

Simultaneously, or in parallel, plans are developed for the EUC regarding operation and maintenance (testing described in chapter 2.6), validation, and commission. Lastly, the EUC is installed and commissioned and a final safety validation of the EUC is done according to the validation plan. This process entails verifying that all the allocation targets have been fulfilled. The validation process for the EUC combines predictions, reviews, and test outcomes, which shall be thoroughly documented so that there is concrete evidence that the system fulfils the safety requirements.

The last phase, system usage is the operational phase and concerns using and maintaining the EUC throughout its lifetime. As a way of verifying the system's maintainability, the EUC shall be tested and maintained according to the approved plans that have been made at earlier stages. Documentation of the results from these activities is essential, particularly of failures (Smith & Simpson, 2016).

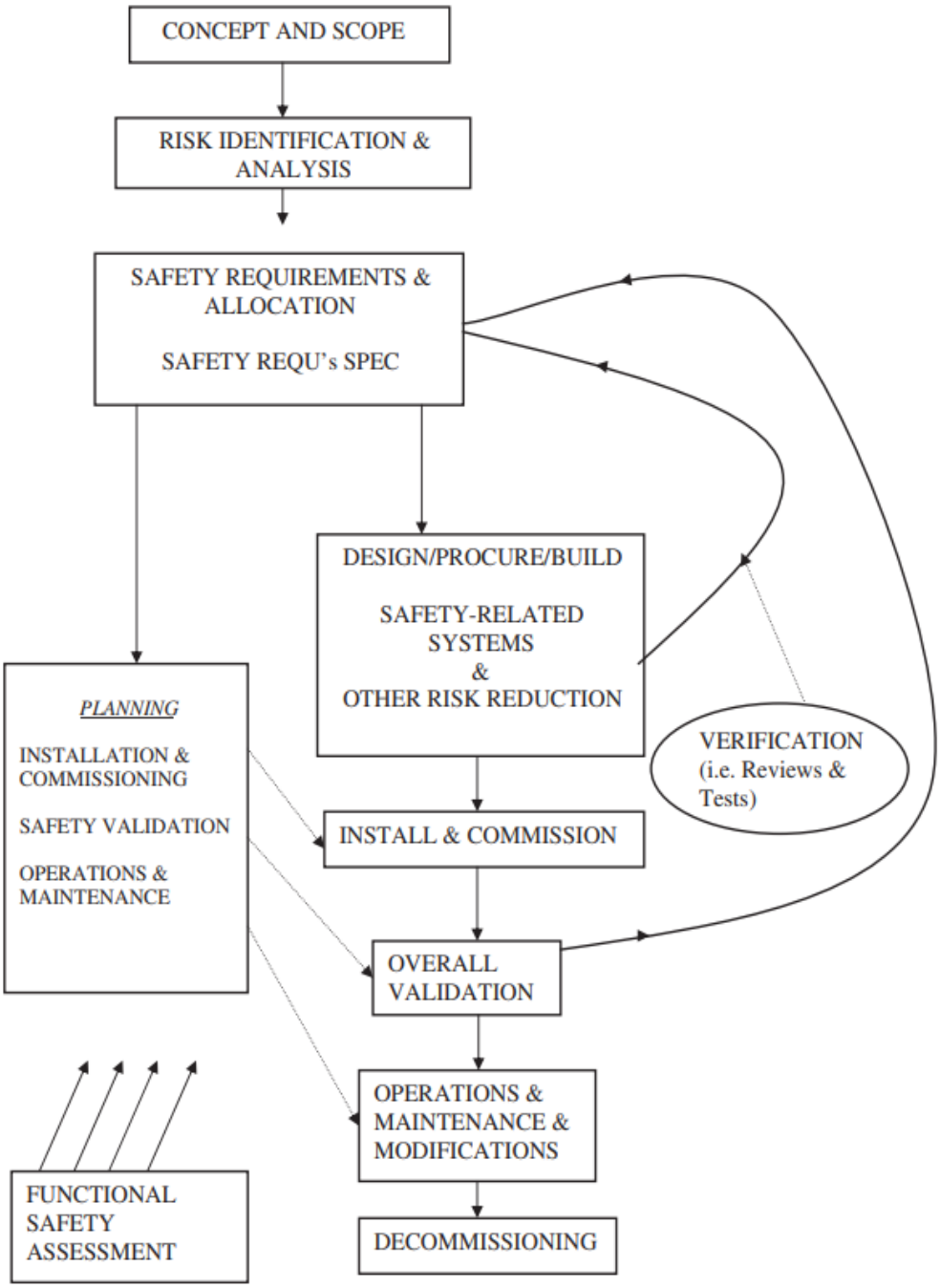

Figure 8. Overall Safety Lifecycle (Smith & Simpson, 2016, p. 10)

2.4.2 Safety Integrity Requirements

There are four SIL targets from 1 to 4 where the highest level means a higher risk reduction (as discussed in Chapter 2.1). Lundteigen (2008) categorises safety integrity into three main aspects:

1. Hardware safety integrity
2. Software safety integrity,
3. Systematic integrity and capability.

If a SIF achieves a certain SIL, it is important to ensure that all three components also fulfil the required SIL. For example, if the hardware component fulfils SIL 2 criteria for safety integrity, then both the software component and the systematic integrity and capability should also meet SIL 2 standards to fully comply with SIL 2 regulations.

Hardware safety integrity is related to two processes: calculating the reliability of the SIFs and determining architectural constraints. The first mentioned is defined by quantitative requirements. It includes the calculation of the average probability of dangerous failure on demand on the SIF (PFDavg), or the average frequency of a dangerous failure per hour of the SIF (PFH) (see Table 1).

Table 1. Safety integrity requirements for safety functions (IEC 61508-1, 2010 [7.6.2.9])

SIL	Continuous/high demand rate, PFH (average frequency of dangerous failures per hour)	Low demand rate, PFDavg (average probability of failure on demand)
4	$\geq 10^{-9}$ to $<10^{-8}$	$\geq 10^{-5}$ to $<10^{-4}$
3	$\geq 10^{-8}$ to $<10^{-7}$	$\geq 10^{-4}$ to $<10^{-3}$
2	$>10^{-7}$ to $<10^{-6}$	$\geq 10^{-3}$ to $<10^{-2}$
1	$\geq 10^{-6}$ to $<10^{-5}$	$\geq 10^{-2}$ to $<10^{-1}$

The choice between these calculations depends on the specific demand mode of operation for which the SIS is designed. As specified in IEC 61508, there are three modes of operation for safety functions:

Low demand mode: Refers to when the safety function is only activated when needed, with the aim of transitioning the EUC to a designated safe state. A vital requirement for a low demand mode system is that the number of demands does not exceed once per year. (IEC 61508-4, 2010, [3.5.16]). If the frequency is greater than that, the SIS is operating in a high or continuous mode. According to Rausand (2014), the airbag system found in cars and the fire and gas detection system used in process plants are both examples of safety barriers that operate in a mode of low demand (p. 6).

High demand mode: The high demand mode is similar to the low demand mode, but the frequency of demands is higher than one per year (IEC 61508-4, 2010, [3.5.16]). Typically, a presence-detecting safety device used on a movable robot can be classified as a safety barrier that operates in a high-demand mode (Rausand, 2014, p.5).

Continuous mode: Continuous mode refers to when the safety function is continuously active and retains the EUC in a safe state as part of normal operation (IEC 61508-4, 2010, [3.5.16]). In this mode, an undesired event occurs when the safety barrier fails. These barriers are commonly utilized in dynamic positioning systems for ships and offshore platforms. (Rausand, 2014, p.5).

The PFD range for a SIS operating in low demand mode and a SIF required to achieve SIL 2 shows that the chance of a dangerous failure upon request should not be more than 0.01 (1%). This means it needs to successfully perform its job at least 99 times out of 100 requests. If the same SIL target is needed in high demand or continuous mode, the SIF must fulfil its purpose at least 999,999 times out of 1,000,000 requests.

Table 1 from IEC 61508 specifies the PFDavg for low demand mode and PFH for high or continuous mode for all safety functions related to EUC. A safety function refers to the actions taken by the safety system to maintain or achieve a safe state of the process in case of a hazardous situation (Sklet, 2006). However, there is a distinction between safety function and Safety Instrumented Function (SIF), with the latter referring to a safety function specifically implemented by a SIS (IEC 61511-1, 2016 [3.2.65], [3.2.66]). Moreover, a SIS can carry out multiple SIFs, and each SIF has been given a specific SIL target to meet. It should be noted that not all safety functions associated with an EUC are necessarily classified as SIFs. (Rausand, 2014, p. 29).

Therefore, IEC IEC 61511-1 introduces a similar table only for SIFs (see Table 2). The main primary distinction lies in categorizing only between continuous mode and demand mode, the latter including both high demand and low demand mode. It is also mentioned that a SIF operating in low or high demand mode is allowed to use either PFH or PFDavg parameters as a specification for the required SIL. It is only a SIF operating in continuous mode that is necessary to use the PFH calculation. (IEC 61511-1, 2016 [9.2.4]). Additionally, Table 2 provides information on the required risk reduction, which is derived by dividing 1 by PFDavg.

Table 2. Safety integrity requirements for SIFs (IEC 61511-1, 2016 [9.2.4]).

DEMAND MODE OF OPERATION		
SIL	PFDavg	Required risk reduction
4	$\geq 10^{-5}$ to $<10^{-4}$	> 10 000 to ≤ 100 000
3	$\geq 10^{-4}$ to $<10^{-3}$	> 1 000 to ≤ 10 000
2	$\geq 10^{-3}$ to $<10^{-2}$	> 100 to ≤ 1000
1	$\geq 10^{-2}$ to $<10^{-1}$	> 10 to ≤ 100

2.4.3 Architectural Constraints

Architecture in functional safety terminology refers to the specific configuration of hardware and software elements in a system, such as the arrangement of SIS subsystems (IEC 61511-1, 2016 [3.2.1]). Lundteigen (2008) states that the estimated PFD fails do not cover all the factors that could lead to the malfunction of a SIS element. Moreover, the calculated PFD might suggest greater effectiveness than what is observed in real-life operations. Therefore, both IEC 61508 and IEC 61511 standards include requirements to have one or more channels to activate the SIF in the event of a malfunction in the SIS (Lundteigen, 2008, p. 10). The system's robustness is enhanced by these requirements, which serve to account for the uncertainty surrounding failure rates. Additionally, the requirements ensure that SIS designers and system integrators can not select the architecture based on PFD calculations alone. Architectural constraints can be met by choosing between two routes: Route 1H and Route 2H. The first one is explained below and is based on the SFF concept.

Route 1H:

According to Lundteigen (2008), the architectural limitations of a SIS rely on the hardware fault tolerance (HFT), which is influenced by the component type (either A or B), the Safe Failure Fraction (SFF), and the specified SIL (p.7). Generowiczs explains HFT by the following:

> HFT is the ability of a component or subsystem to continue to be able to undertake the required SIF in the presence of one or more dangerous faults in hardware. A HFT of 1 means that there are, for example, two devices and the architecture is such that the dangerous failure of one of the two components or subsystems does not prevent the safety action from occurring. (Generowicz, 2016, p. 2)

Safe Failure Fraction (SFF) is defined by the IEC 61508 standard as the ratio of the average failure rate of safe plus dangerous detected failures and safe plus dangerous failures (IEC 61508-4, 2010, [3.6.15]). Once the failure rates of all subsystems have been considered, it is possible to calculate the SFF ratio (1).

$$SFF = \frac{\lambda SD + \lambda SU + \lambda DD}{\lambda SD + \lambda SU + \lambda DD + \lambda DU} \quad (1)$$

The SFF ratio is expressed in percentages. 100 % is the best achievable, ensuring that no dangerous failures go undetected by automatic diagnostics. Once the SFF is known, it is possible to see the HFT for the specific SIF based on the required SIL (see Table 3). However, depending on how well the component's failure mode and behaviour are defined, they are sorted as either type A or B. Table 3 shows the relationship of both component types and their corresponding HFT for the required SIL. If a B component with the same SFF is used, the required SIL may not be fulfilled since the component is not reliable enough and may require a higher HFT or SFF for the same SIL. See IEC 61508 for more details on type classification (IEC 61508-2, 2010 [7.4.4.1]).

Table 3. SFF and HFT for type A and B components (IEC 61508-2, 2010 [7.4.4.2.2]).

SFF	Hardware Fault tolerance		
	0	1	2
HFT Type A components			
< 60 %	SIL 1	SIL 2	SIL 3
60 % - < 90 %	SIL 2	SIL 3	SIL 4
90 % - < 99 %	SIL 3	SIL 4	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4
HFT Type B components			
< 60 %	Not allowed	SIL 1	SIL 2
60 % - < 90 %	SIL 1	SIL 2	SIL 3
90 % - < 99 %	SIL 2	SIL 3	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4

The SFF ratio is a direct input into the HFT level, which in turn, determines if redundancy is required. If the calculated SFF is less than 60%, and the necessary risk reduction is SIL 2, then the HFT is set to 1 for type A components and HFT set to 2 for type B components. This means that one, respectively two additional components must perform the same task to meet SIL 2. Thus, implementing the voting system as elaborated on in Chapter 2.2.3. SFF calculations strive to minimize the potential for DU failures by incorporating redundancy, effective diagnostic testing, and design principles.

Diagnostic coverage: Another reliability parameter that is also represented in the calculation step of SFF is the Diagnostic Coverage (DC), which is related to dangerous failures. DC is a measure of the effectiveness of system diagnostics, expressed as a percentage of a safety function. A high DC means that a large proportion of potential failures are detected. Sensor elements and logical solver usually have a high DC in the range of 50-99 % due to their embedded software, while the final element is often lower than 30 % (Rausand, 2014, pp. 83-84). The DC is calculated by dividing the dangerous detected failure rate for each component by the total failure rate of dangerous failures (2).

$$DC = \lambda DD / (\lambda DD + \lambda DU) \quad (2)$$

Route 2H:

Route 2H is a newer approach that was first introduced in the 2nd edition of the IEC 61508 family back in 2010. It is an alternative approach for determining appropriate HFT based on field feedback for elements and historical records to confirm likely future failure rates.

According to the IEC 61508-2 (2010, [7.4.4.3.3]), if Route 2H is selected, the reliability information utilized for quantifying the impact of random hardware failures must be derived from practical experience, such as field feedback, with equipment employed in a comparable application and environment. This information should be collected in accordance with

published standards. Evaluation of the reliability data considers the quantity of field feedback, expert judgment, and specific tests. Hence, to utilize 2H effectively, the equipment must be designed and manufactured according to the requirements set by IEC 61508. (Norwegian Oil and Gas Association, 2020, pp. 39-40).

IEC 61511 introduces a distinct table outlining the minimum HFT requirements for a Safety SIS) or its subsystem implementing a SIS based on the SIL (refer to Table 4). For more details regarding Route 2H, refer to IEC 61511-1 (2016, [11.4]).

Table 4. Minimum HFT requirements according to SIL (IEC 61511-1, 2016 [11.4.6])

SIL	Minimum required HFT
1 (any mode)	0
2 (low demand mode)	0
2 (continuous mode)	1
3 (high demand mode or continuous mode)	1
4 (any mode)	2

2.4.4 Systematic Capability

Like the Route 2H of architectural constraints, Systematic Capability was first introduced in the 2nd edition of IEC 61508 in 2010 and included in the 2nd edition of IEC 61511-1 in 2016. Systematic Capability is a measurement of confidence, ranging from SC 1 to SC 4 that determines the level of confidence in the systematic safety integrity of a device. This measurement determines whether the device meets the specified SIL requirements when used in accordance with the instructions provided in the device's safety manual (61511-1, 2016 [3.2.80]).

Systematic Capability refers to the ability of a system or its component to be designed, implemented, and maintained in a manner that reduces the likelihood of these failures,

thereby increasing systematic integrity. As established in Chapter 2.3, systematic failures and errors are not easily quantified, and not covered by the PFD/PFH calculations. Therefore, IEC 61508 introduces various strategies and measures to effectively control systematic failures caused by hardware design, environmental stress, and systematic operational failures (refer to Table A.15-18 in IEC 61508-2, 2010). These techniques are categorized as no recommendation given (-), not recommended (NR), recommended (R), highly recommended (HR), or mandatory (M). Table 5 provides a selection of techniques listed in Table A.15 in IEC 61508-2 for controlling systematic failures in hardware design. The mention of low, medium, or high signifies the level of effectiveness needed when employing these techniques. In general, the higher the SIL target, the more necessary it is to have additional documents or consider certain measures highly recommended. The same principle applies to the level of effectiveness required.

Table 5. Techniques for controlling systematic failures (IEC 61508-2, 2010, [A.15])

Technique/measure	SIL 1	SIL 2	SIL 3	SIL 4
Program sequence monitoring	HR low	HR low	HR medium	HR high
Failure detection by on-line monitoring	R low	R low	R medium	R high
Test by redundant hardware	R low	R low	R Medium	R high
Diverse hardware	-	-	R medium	R high

The table above focuses only on systematic failures related to hardware design that manufacturers can implement and adhere to, as per IEC 61508 standards. Other similar tables exist for different design purposes, giving manufacturers the means to make sure their components are appropriate for the specific SIL target. As specified in IEC 61511-1 (2016, [11.5.3.1]), there must be sufficient evidence illustrating that the device is suitable for utilization in SISs.

Moreover, IEC 61511 tackles the issue of human errors in the safety life cycle by introducing measures that can be applied to every phase. These guidelines assist users in meeting the minimum requirements to maintain the desired integrity of their SIS. They offer procedures, methods, and tools to minimize potential human errors during the requirement specification and design phases. It is recommended to include these measures from the IEC standards when implementing the SIS. The Systematic Capability rating (SC1 to SC4) grades the degree of adherence to these procedures, methods, and tools. An SC1 rating equals a Systematic Capability corresponding to SIL 1 (IEC 61511-1, 2016 [11.5.3]). Devices certified under IEC 61508 may also undergo a comprehensive third-party audit, accredited to verify compliance with all the requirements. In that case, the SIL certificate should display the corresponding SC level to demonstrate compliance.

2.5 Reliability Allocation

Establishing integrity targets is an essential part of the safety life cycle (see Figure 8). It is the process of assigning a specific SIL level to a SIF in a system which is done based on the level of risk reduction required to achieve functional safety. As specified in IEC 61511-1 (2016, [8.1]), the main goals of the hazard and risk analysis are to determine the following:

- The hazards and hazardous events of the process and associated control equipment
- The event sequence leading to the hazardous event and associated process risks.
- The requirements for risk reduction.
- The safety functions required to achieve the necessary risk reduction and which of these safety functions are SIFs.

To understand and ensure a successful allocation it is necessary to identify the risk reduction required. Further on, to understand the risks related it is necessary to identify possible hazards. There are various possible methods for doing a hazard and risk analysis that consist of

both quantitative and qualitative approaches and techniques that can be utilized in the process to evaluate the associated risks, as well as hybrid measures (Smith & Simpson, 2016, p. 170). According to Smith and Simpson (2016, p.6), quantitative safety targets are set by predicting the frequency of hardware failures and comparing them to some tolerable risk target. On the other hand, to meet qualitative safety goals, the focus is on reducing the occurrence of systematic failures by implementing various defences and design practices based on the severity of the acceptable risk level.

Only the most essential methods relevant to this thesis are presented, even if it is not directly related to the process of data collection, they are part of the performance evaluation of a SIS since that includes revisiting risk assessment calculations. It is important to understand the various risk analysis methods to define and understand the purpose and need of operational data.

2.5.1 Process Hazard Analysis

To establish the risks to be addressed in the risk analysis, a process hazard analysis (PHA) shall be conducted to identify possible hazardous events related to the EUC and associated systems, excluding safety-related functions. The PHA should provide enough information to uncover possible deviations from the minimum SIL requirements. The study should address various aspects of the process, including start-up, shut-down, maintenance, and other operational modes. It should also consider hazards caused by human error, operational mistakes, the uniqueness and complexity of the installation and interfaces, as well as operating and maintenance procedures among other factors. (Norwegian Oil and Gas Association, 2020, p. 25).

PHA can be conducted through various techniques, and the choice depends on many factors such as type of installation, complexity of the EUC, and the stage of the lifecycle (see Figure 8) in which the hazard study is conducted (Norwegian Oil and Gas Association, 2020, p. 25).

Common techniques include Hazard and operability study (HAZOP), Hazard identification (HAZID), Structured what-if-technique (SWIFT), and FMEDA. According to the European Commercial Aviation Safety Team (2009), HAZOP is a widely used technique that systematically examines each component of a system to identify deviations from design, while the SWIFT technique involves comprehensive and structured team discussion that explores hypothetical scenarios, hazards, and their consequences. FMEDA is also widely used in various industries to assess the reliability of the SISs by systematically analyzing each component, failure modes, their effects, and criticality. For more information on these methods, refer to the work by ECAST (2009), Rausand (2014), and Smith and Simpson (2016).

The most important outcome of a PHA is to have all undesired or hazardous events listed. These events shall not occur in the normal operation of a system and a PHA study helps address conditions that could result in such hazardous events, including demands, upsets, and deviations in such processes. Once these events are identified, risk analysis methods shall be implemented to assess the likelihood and consequences of these events. A common approach for this purpose is the Fault Tree Analysis (FTA) (Rausand, 2014, p. 44).

The results of the risk analysis are a quantification of risk, presented via one or more risk metrics, for example, accident rate and individual risk per annum (IRPA). The risk metrics help establish the risk acceptance criteria or tolerable risk as defined in IEC 61508 (IEC, 2010d) and work as the basis for the allocation process.

In order to establish an acceptable level of risk for a particular hazardous event, it must be taken into account the event's frequency and its consequences, and then offer a judgement on what is deemed rational. The acceptable level of risk is dependent on various factors, including the severity of the event, the number of people exposed to danger, the frequency, and the duration of exposure, among others. A common approach is the ALARP principle, which stands for “As Low As Reasonably Practicable”, where the focus is to find a balance

between the cost, effort, and time required to reduce a risk and the benefits gained from that reduction (Rausand, 2014, pp. 45-48).

Figure 9 is a generalized model from the IEC 61508 standard which shows the general principles for the risk reduction concept of a low demand system. For this type of system, it is the Probability of dangerous failure on demand (PFD) that is the critical factor, in a high demand system, it is the dangerous failure rate (PFH). EUC risk refers to the risk that arises from the EUC or its interaction with its control system (IEC 61508-4, 2010d, [3.1.9]). The tolerable risk, on the other hand, signifies the level of risk that is deemed acceptable in a particular context, based on the current values of society (IEC 61508-4, 2010, [3.1.7]). The tolerable risk is commonly known as the risk acceptance criteria.

Additionally, the residual risk refers to the risk that persists after precautions have been taken (IEC 61508-4, 2010, [3.1.8]). Once the EUC risk and tolerable risk have been determined, the necessary risk reduction can be computed by subtracting the tolerable risk from the EUC risk.

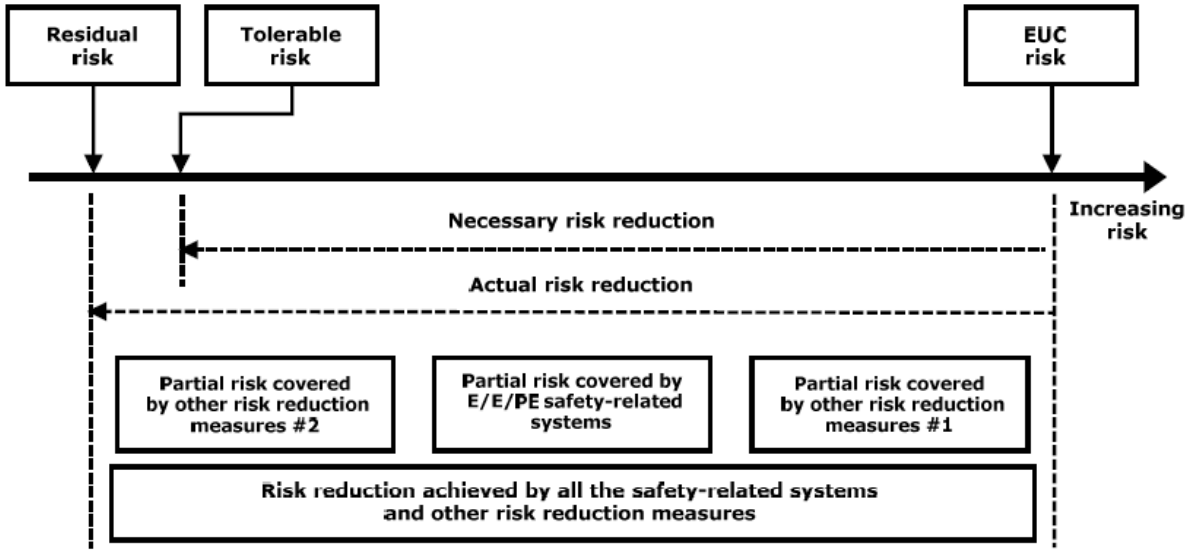

Figure 9. Risk reduction concept for low demand systems (IEC 61508-5, 2010, [A.1])

2.5.2 Fault Tree Analysis Model

Fault tree analysis (FTA) is a commonly used method for assessing the reliability of a system and SIL allocation. It assists in investigating various potential events or combinations of events that may result in hazardous situations or major consequences. FTA also involves determining the probability of occurrence for the top event. (IEC 61508-7, 2010, [B.6.6.5]). FTA is a graphical method where the analysis starts at the top event (a system failure) and branches or paths of the tree represent possible events that may cause the top event. These possible events are in turn referred to as input events and represented by logical operators (and, or, etc), called logical gates. See Figure 10 for an example of how FTA has been used when analysing a failure of a fire protection system. Rausand (2014) mentions that FTA is also used to identify aspects such as components, safety barriers, structure, etc. that may need improvement to reduce the probability of the top events (p. 105). Further on, the author mentions that typical top events for a SIS are failure of the SIF to perform on demand and spurious activation of the SIF (failure where no real demand existed).

The process starts with identifying hazardous scenarios, often conducted through HAZOP studies. The fault tree diagram is qualitatively designed to visually show the relationship between the different events and/or conditions that could lead to the top event (see Figure 10). After the qualitative analysis is completed, FTA can be further used to perform quantitatively probabilistic calculations of the top event.

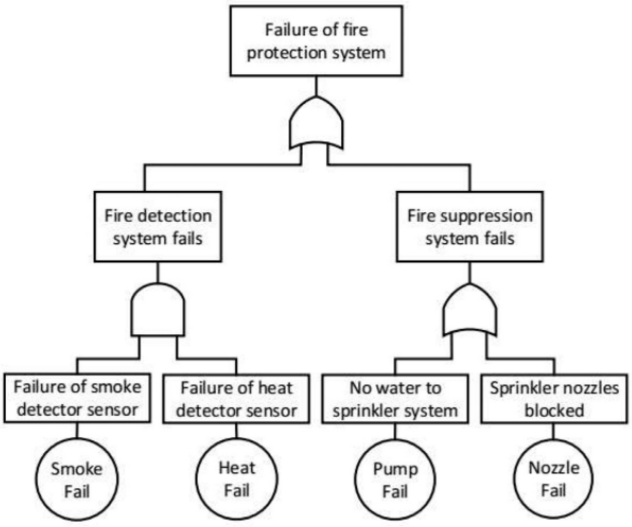

Figure 10. Example of FTA (Kabir, 2017)

2.5.3 Layer of Protection Analysis

Lopa is a simplified semi-quantitative risk analysis methodology referred to in both IEC 61508-5 Annex F (IEC, 2010e) and IEC 61511-3 Annex F (IEC, 2016c). LOPA examines each hazard identified in HAZOP separately, taking into account the potential causes and risks, as well as the protective measures in place to prevent or reduce the impact of these hazards. LOPA evaluates the protection layers (including safety functions) and is a method for determining if the existing risk reduction is sufficient enough and what their SIL should be. The results from LOPA may also indicate that additional safety functions are necessary, including what their SIL should be. LOPA includes quantitative aspects such as PFD calculations and the frequency of initiating events with qualitative assessments to evaluate risk levels associated with these protection layers. Therefore, making it a semi-quantitative method (Willey, 2014). Torres-Echeverria (2016) mentions that LOPA, along with Risk Graphs are two widely used methods for SIL-determination processes in the Oil and Gas industry.

In Figure 11, a flowchart of the LOPA process is presented, while Figure 12 provides a sample of a LOPA worksheet. Whether LOPA serves as a means of validating an upgraded protection layer or for SIL determination, the required input data is quite similar. The key considerations related to data input, as outlined by IEC 61508 and 61511 and according to multiple authors (Angelito et al., 2018; Willey, 2014; Torres-Echeverria, 2016; Rojas, 2023), are presented below:

1. **Select a hazardous scenario and initiating events:** The HAZOP study is complete, and the hazardous scenarios have been analysed along with their consequences (without considering any layers of protection). Based on this data, a tolerable risk can be selected. Following is to estimate the frequency of each initiating event, that may lead to the specific hazardous scenario and to estimate the frequency and severity of the event.
2. **Establish Independent Protection Layers (IPLs):** IPLs function as safeguards that can prevent an unfavourable outcome in a specific situation, regardless of the cause or any other protective measures. They come in the form of devices, systems, or actions. Each event must have identified IPLs, along with their Probability of Failure on Demand (PFD) and meet three criteria: 1) effectively preventing the undesired consequence, 2) being independent of the initiating event and other protection layers, and 3) being auditable, so their effectiveness can be validated.
3. **Identify Conditional Modifiers (CMs):** These are factors that may impact the risks related to a hazardous event and/or frequency of the event having consequences.
4. **Calculate the Total Mitigated Event Frequency (TMEF):** To calculate TMEF, the frequency of the initiating event shall be multiplied by the PFD for each IPL, and then consider the probability of each CM. Afterwards, the outcomes obtained from all the initiating events are summed up.
5. **Evaluate Risk Acceptability:** Check if the TMEF calculation is within the acceptable limit of the target risk. This can for example be done using risk matrices (see Chapter

2.5.4) as the severity levels of the consequences have already been categorized. If the calculation exceeds the limits, supplementary measures must be implemented to mitigate the risk. Simultaneously, this assessment determines the required level of risk reduction.

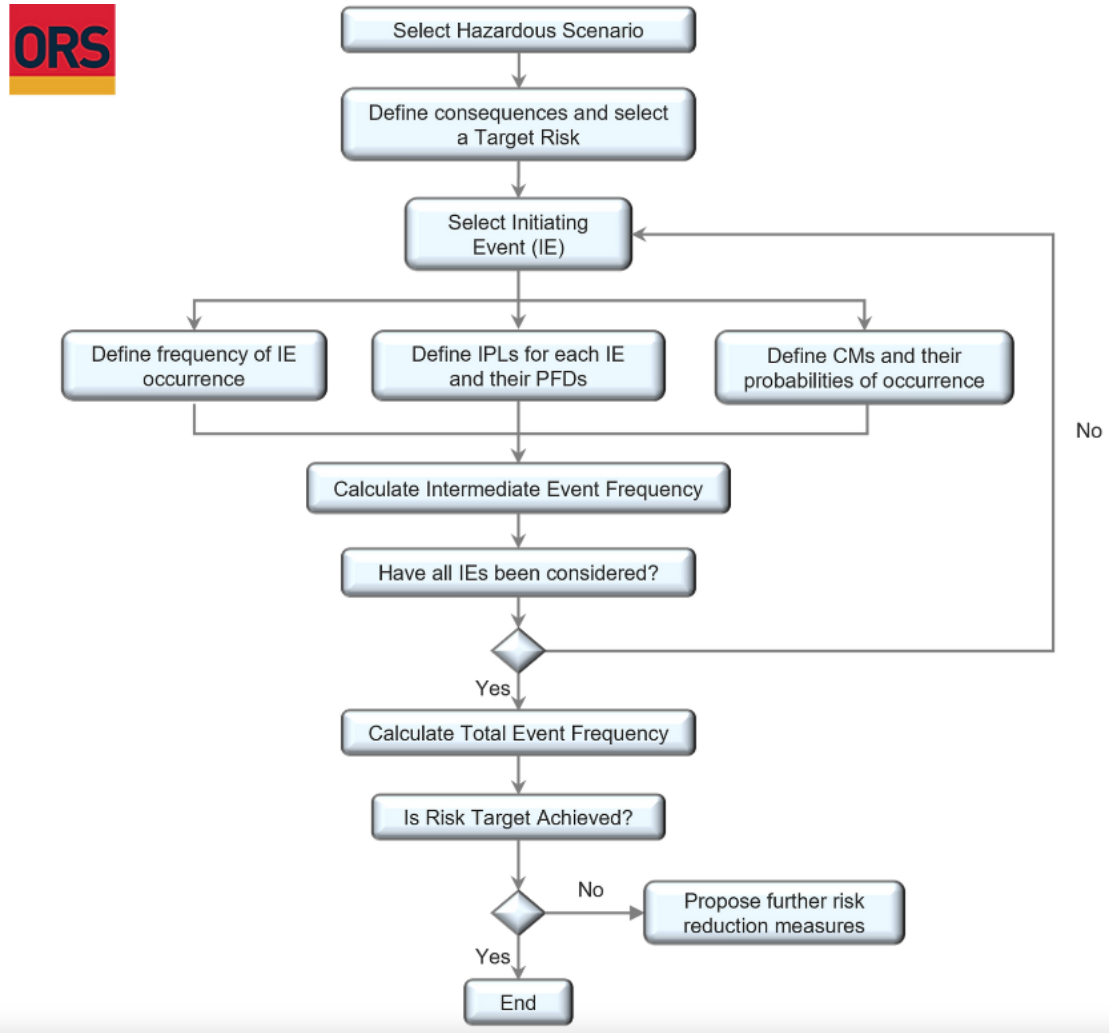

Figure 11. Flowchart of the LOPA process (Rojas, 2023)

1	2	3	4	5	6	7	8	9	10	11	12	13
Impact event description	Severity level	Initiating cause description	Initiation likelihood (freq per year)	Protection Layers (probability of failure)				Conditional Modifiers		Intermediate event likelihood	Tolerable risk likelihood	Risk reduction factor
				Basic control system	Alarms & operator action	Other protection devices	Other mitigation measures	Occupancy factor	Probability of ignition			

Figure 12. Example of a LOPA worksheet (Torres-Echeverria, 2016)

2.5.4 Risk Matrices and Allocation

While the preceding sections delve into quantitative and qualitative methods for hazard and risk analysis, it is worth mentioning the role of risk matrices in the broader safety assessment process. Risk matrices provide a visual representation of risks based on their likelihood and consequences, aiding in the prioritization of potential hazards. In the IEC 61508 standard, they are referred to as Hazardous Event Severity Matrices (IE 61508-5, 2010, [G.2]).

Risk matrices are particularly valuable in the early stages of risk identification and assessment, helping to categorize risks into different levels. These categorizations are important for further analysis, including the determination of Safety Integrity Levels. In conjunction with methods such as LOPA and FTA, risk matrices enhance the overall comprehension of risks associated with situations where quantification of the risk is challenging or not possible. (IEC, 2010e, p. 44). According to Torres-Echeverria (2016), this approach depends on a qualitative comprehension of the likelihood and consequences of hazardous events, as well as the extent of protective measures in place. When an additional IPL is implemented, one order of magnitude is provided in risk reduction. Figure 13 illustrates this concept, based on the matrix found in IEC 61508-5 (2010, [G.1])

The matrix takes various factors into account, such as the severity rating, the likelihood of the hazardous event, and the number of independent protection layers (IPLs) associated with the specific hazard. For instance, in Figure 13, after identifying a potential hazard

through the Process Hazard Analysis (PHA), the severity and likelihood of the event are evaluated, and the matrix assists in determining the SIL target necessary for mitigating that specific event. For example, if a hazardous event has a high probability and severe consequences, according to Figure 13, the required SIL for the SIF would be SIL 3, assuming that only one IPL exists to reduce the risk of the event. However, if there are two IPLs in place, the target SIL would be SIL 2 instead. Furthermore, the letters A, B, and C serve to indicate whether supplementary measures for risk reduction are necessary (letter A), if further analysis is needed to determine the necessity of additional risk reduction measures (letter B), or if the risk is sufficiently low that a separate SIF is not required (letter C).

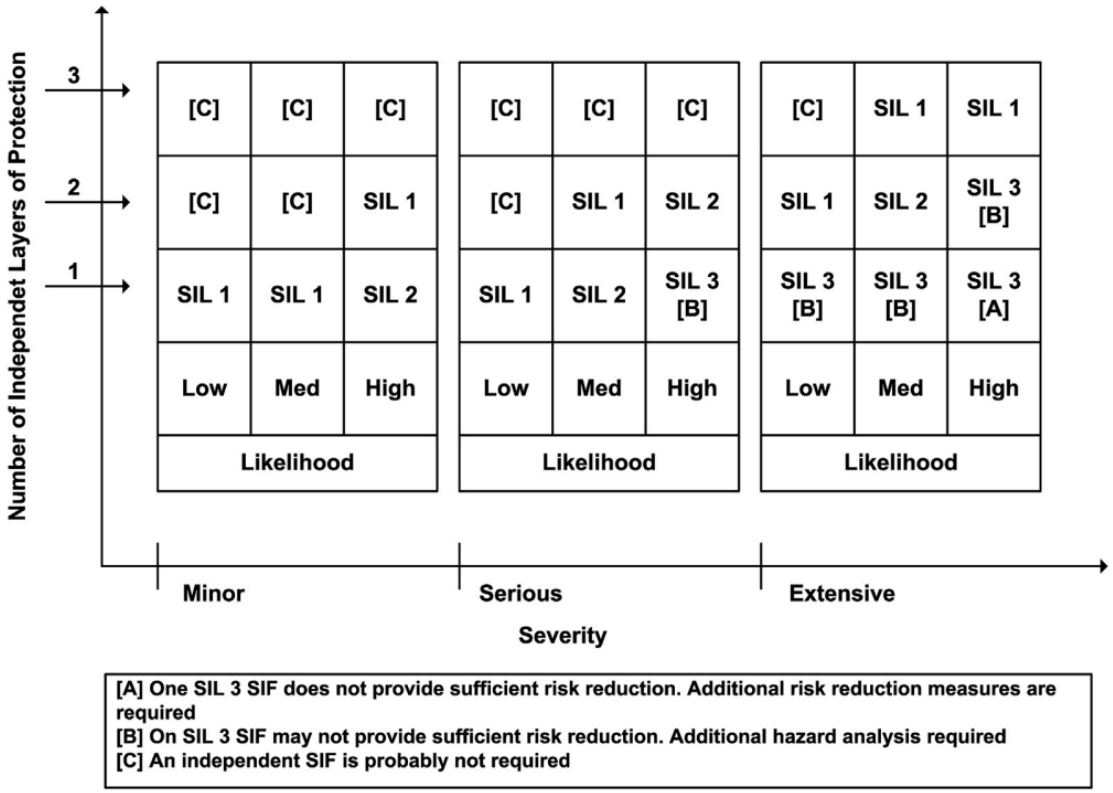

Figure 13. Hazardous event severity matrix (Torres-Echeverria, 2016)

2.6 Testing

SISs shall be regularly tested to verify that the SIFs are fully functional and to verify their correct behaviour under specific fault conditions, thereby revealing potential faults. SIFs that are designed for low demand mode, where the failures are expected to be max once per year indicate that it is highly unlikely, they will occur and therefore the functionality must be ensured. As for the operational phase of the SIS, Rausand (2014) has split the tests into three groups: Proof tests, Partial tests, and Diagnostic tests. These tests are necessary for maintaining the effectiveness and reliability of the SIS throughout its operational lifecycle (pp.78-84).

Proof test: Also referred to as "periodical test" is a planned periodic test with the main purpose of detecting DU faults so that they can be fixed. This kind of test involves applying a simulated demand on the SIF and verifying that correct behaviour is ensured. The entire SIS shall be tested, including sensors, logic solver, and final elements. The execution of a proof test shall follow a written procedure that has been developed and defined in the SRS. (IEC 61511, 2016a). Additionally, in Section 16.3.1.3 of IEC 61511-1, it is stated that the frequency of proof tests for a SIF depends on its target PFDavg or PFH calculation. This aligns with the assumption of the Norwegian Oil and Gas Association (2021, p. 227) that when annual targets are used for DU failures, the equipment shall be tested at least once a year. There are no restrictions on the number of tests conducted for a specific target value. Nevertheless, if the equipment is tested for example once every two years, the allowed number of failures will be twice as much.

Partial test: Similar to proof tests, partial tests are planned tests designed to detect DU faults. This type of test is more targeted, focusing on specific components to ensure that individual elements or functions within a SIS are functioning correctly. Typically conducted during the operational phase between the proof tests, and with as little interference with the SIS as

possible (Rausand, 2014). An example of this is partial stroke testing, where a valve is only partially closed, impacting the process flow enough so that DU failures may be detected without interfering with the operational functionality of the SIS.

Diagnostic test: Modern SISs often include diagnostic features that continuously monitor the health of the system by executing self-tests. Failures detected by diagnostic tests are detected failures and classified as either DD or SD (IEC, 2010d). According to Rausand (2014), common faults detected by diagnostic tests include sensor signals out of an acceptable range, the final element in incorrect positions or states, signal losses, etc (pp. 82-83). The term “diagnostic coverage” quantifies the probability of identifying dangerous failures within a SIS by the diagnostic test.

2.7 Reliability data sources

According to Rausand and Lundteigen (2014), there are four categories of data when performing reliability analysis: technical data, operational data, reliability data, and test and maintenance data (see Figure 14). Technical data is required mainly to understand all the functionalities of the SIS, while operational data is necessary for understanding the functioning of elements, channels, and subsystems.

The focus of this chapter is on reliability data, which is related to failure rates or data that support these estimations. Additionally, test and maintenance data are also necessary inputs to the quantitative SIL analysis and include parameters such as proof test interval, Diagnostic Coverage, Mean Time to Restore, duration of a test, and more. Both operational data and test and maintenance data can be inputs into reliability data.

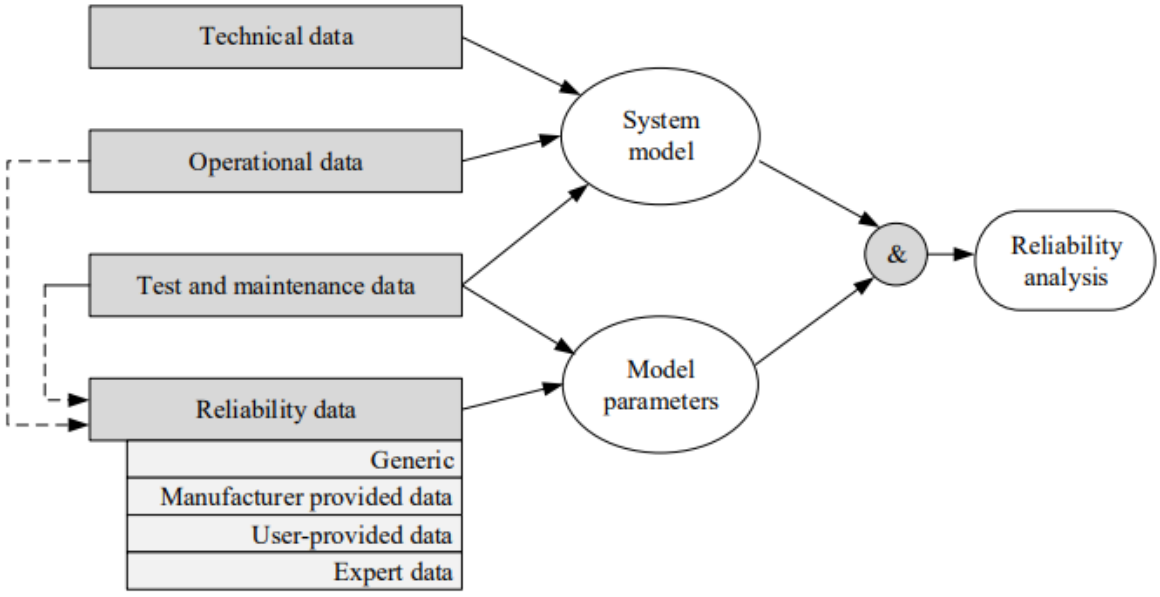

Figure 14. Data types and their applications (Lundteigen & Rausand, 2014, p. 6)

The importance of reliability and the necessity of distinguishing correct failure modes for risk assessments have been mentioned. In simpler terms, the more reliable the data is, the more trustworthy the estimations are since it affects the PFDavg estimations and other reliability parameters. As defined in IEC 61511-1:

> The reliability data used when quantifying the effect of random failures shall be credible, traceable, documented, justified, and shall be based on field feedback from similar devices used in a similar operating environment (IEC 61511-1, 2016, [11.9.3]).

Additionally, the same section also states that this could encompass various types of data such as historical data gathered by the operator, manufacturer or vendor data derived from device-collected data, and information obtained from general field feedback reliability databases. Rausand (2014, pp. 165-158) and The Norwegian Oil and Gas Association (2023, pp. 42-45) categorize reliability data into four distinct groups:

Generic data: Derived from operational experiences in similar applications covering multiple installations and comparable equipment types. Organizations often gather and publish this kind of data in handbooks, which typically include a mixture of practical know-how and information provided by manufacturers, tailored to a particular industry sector like the offshore oil and gas industry (Lundteigen & Rausand, 2014, p. 5). Examples of such data sources are the Offshore and Onshore Reliability Data (OREDA) handbooks and the PDS data handbook, which specifically targets reliability analysis for SIL analyses according to IEC 61508 and IEC 61511 standards. Rausand (2014) mentions that when considering generic data, one should be careful since the data is often a mixture of field and test data, and not always easy to distinguish the actual source. along with considering that the handbooks or databases have been issued by neutral and trustworthy organizations (p. 166). However, the use of generic data can be very useful, especially in the early phases of a project. As the project advances and more details about the specific equipment and its operating conditions become available, efforts should be made to switch from generic data to reliability data that more precisely matches the project's unique requirements (Norwegian Oil and Gas Association, 2020, p. 43).

Manufacturer-provided data: Data from manufacturers regarding specific components, often based on the manufacturer's internal statistics, in-house testing, or failure rate estimation techniques. A common problem with this is that manufacturers usually do not get failure reports back from end users. Therefore, the failure data provided by manufacturers should be carefully documented concerning how the results have been obtained, and in the worst case, the failure data might be underestimated. Manufacturers may also have used a third party to assess the data, based on testing, comparison with similar products, and field experience, often based on an FMEDA analysis. (Norwegian Oil and Gas Association, 2020, p. 43 & Rausand, 2014, p. 166).

User-provided data: This data, also referred to as operator data, is necessary for end-users of SISs to collect during the operational phase. This information is used to update the initial estimates of the PFDavg and/or other SIL targets. This type of data is also used to ensure that the performance of SIFs and barrier elements is following their requirements (e.g. as defined in the SRS). The Norwegian Oil and Gas Association (2023) highlights that many companies maintain their own "preferred" dataset for this type of data, usually derived from gathering reliable information from their own operated installations (p.43).

Expert Judgement: In situations where there is a lack of experience data, such as with new technology, Rausand (2014) suggests that Expert Judgment can be used as a data source. This can also be helpful in cases where reliability information is not available or when assessing the impact of reliability data from a different operational setting (IEC 61511-1, 2016, [11.9.3]).

3 Methodology

In this chapter, the methodology applied to this research is explained, motivated, and justified. The research strategy, approach, and implementation are discussed, clarifying the development of the procedural framework presented in Chapter 4 (results). This chapter also outlines the evaluation of the procedure, literature review, and internal documents of the company. The purpose of this chapter is to give the reader an understanding of how this study has been conducted.

3.1 Research Strategy

3.1.1 Case Study

Simons (2009) mentions that Case studies are a common research strategy that gained recognition in the late 1960s in the UK and the USA. Traditional models like the objectives model and system analysis could not effectively explain the success or failure of curriculum innovation. There was a need for alternative methods that captured the participant's perspective, responded to audience needs, and understood the socio-political context. Case studies became one of the approaches that embrace these features and are now a widely accepted research strategy, and may be related to a specific company, project, or system (Simons, 2009). The author mentions that the exact definition of a case study varies depending on circumstances and discipline area. Yin (2009) defines a case study as “an empirical inquiry which investigates a phenomenon in its real-life context. In a case study research, multiple methods of data collection are used, as it involves an in-depth study of a phenomenon”. Simons (2009), in his study, examined multiple reports on case studies and concluded that the definition aligns with Yin´s definition. Both Yin and Simons highlight that a case study is more of a research strategy or design to study a social unit and mention that it is not the specific methodology (such as qualitative or quantitative) that defines a case study, even if it shapes the form of the study.

Application of IEC 61508 and IEC 61511 requires the implementation of peculiar ways of working and organizational aspects. This requires the establishment of a procedure with a framework for the collection and evaluation of reliable data specific to SIL-compliant systems. The procedure is a documented process within the case company and is mainly based on requirements deriving from IEC 61508 and the specific process industry-specific standard, IEC 61511. However, it also considers internal documentation, company guidelines, and organizational aspects. Therefore, a case study approach was chosen as a method to know which risk assessment methods have been implemented, the type of data to focus on, and more specifically, which IEC requirements to address given the extensive coverage of the standards.

3.1.2 Quantitative and Qualitative

Throughout this study, the focus has been to understand the processes and practices related to reliability data and performance evaluation for a SIL 2-compliant safety system. This thesis includes qualitative aspects in terms of understanding organizational processes and document analysis and therefore, more qualitative oriented (Fischler, Mixed Methods, 2015). However, as mentioned in Chapter 2, the reliability allocation of SISs includes both quantitative and qualitative methods. In the evaluation of system performance, numerical data related to failures are considered (such as PFD). The use of numerical data and specific calculations are characteristics of quantitative research (Fischler, Mixed Methods, 2015). Even if the actual calculations are not considered for this case study, there is a focus on collecting numerical data and specific calculations for assessing system performance.

Qualitative research:

> A type of educational research in which the researcher relies on the views of participants; asks broad, general questions; collects data consisting largely of words (or text) from participants; describes and analyses these words for themes; and conducts the inquiry in a subjective, biased manner. (Fischler, 2015, p. 7)

Quantitative research:

> A type of educational research in which the researcher decides what to study; asks specific, narrow questions, collects quantifiable data from participants (many participants); analyses these numbers using statistics; and conducts the inquiry in an unbiased, objective manner. (Fischler, 2015, p. 4)

3.1.3 Mixed Methods Research

By utilizing both quantitative and qualitative data collection methodologies in a single study to understand a research problem, the research methodology can be considered mixed methods research (Fischler, 2015). According to Cameron (2009), this has proven to be an appropriate solution when the research questions or parts of it cannot be fully answered by quantitative or qualitative studies alone. Additionally, it allows the researchers to simultaneously consider both confirmatory and exploratory questions. For example, a confirmatory question for this thesis is to what extent the implemented procedure aligns with the quantitative requirements specified in IEC 61508 and IEC 61511. Simultaneously, exploratory questions are beneficial in terms of gaining a better understanding of specific causes. Examples include investigating factors contributing to failures and demands, as reported in the failure reports, and answering the amount of information required about the failures to identify root causes and potential patterns.

The Exploratory Sequential Design is a type of mixed methods research design, where qualitative data is used as a foundation for gathering quantitative data. In the explanatory sequential design, the process is reversed (Cameron, 2009). While it is not easy to address a specific research methodology for this case study, the establishment of the procedure itself is related to the Exploratory Sequential design. The failure reports include many fields where the user needs to manually type in the description of the failure, root cause, impact on safety, etc… In practice, this process may include open-ended interviews with key personnel, thereby reflecting a qualitative approach. Afterwards, the data may be assessed and in

performance evaluation (analysis), be compared to the quantitative requirements regarding demand, failures, and failure classification (DD, DU, SD, SU). However, Throughout the whole study, there has been a larger focus on understanding, interpreting, and synthesizing information, instead of considering how to use the collected data in practice. Therefore, the qualitative approach has been more dominant.

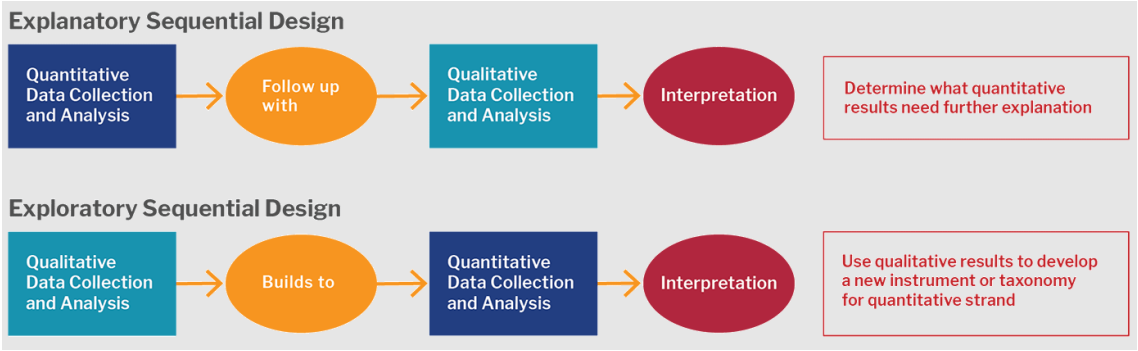

Figure 15. Exploratory and Explanatory Sequential design. (Harvard Catalyst, n.d.)

3.1.4 Document Analysis

Document analysis serves as a systematic procedure for reviewing or evaluating various documentation, from organizational and institutional documents to diaries, newspapers, and articles. The objective of document analysis, as described by Corbin and Strauss (2008), is to gain comprehension, reveal patterns, and generate empirical knowledge within the principles of qualitative research. Bowen (2009) states that document analysis is an appropriate approach in qualitative case studies and is occasionally utilized as an additional method in mixed-methods studies.

The systematic approach that is implemented involves carefully reading, categorizing, and interpreting content. Bowen (2009) mentions that it is an efficient and cost-effective method that is more targeted towards data selection instead of data collection. Since many

documents are in the public domain, the availability and exactness are high due to identifiable names and references. The author also mentions challenges with document analysis such as insufficient details, meaning that the documents may be produced for other tasks than research. Another challenge is biased selectivity, which means that the selected documents may be aligned with organizational policies and procedures where the agenda might be something different.

For this study, compliance with IEC standards IEC 61508 and IEC 61511 is of most importance. Document analysis is implemented to extract specific requirements and guidelines from these standards regarding reliability data and performance evaluation. The focus of data selection instead of data collection aligns well with this study as well since one of the purposes is to identify the data to be collected. Furthermore, in terms of organization, the case company's internal documents, like the Functional Safety Management Plan (FSMP), are also subject to document analysis.

3.1.5 Semi-structured interviews

Semi-structured interviews refer to the combination of two architectures: Structured interviews, where questions are predetermined in both topic and order and unstructured interviews, where no questions are predetermined (George, 2023). Semi-structured implements a thematic framework where the analysis is conducted to identify, analyse, and find patterns in the data. According to Adeyoe-Olatunde and Olenik (2021), the primary benefit of semi-structured interviews is that while maintaining a focused approach on the subject, it allows for exploratory questions that may arise during the interview. This aligns well with the idea of utilizing exploratory questions in mixed methods research as Jameson (2009) stated. The flexibility and open-ended nature of semi-structured interviews are beneficial when it comes to understanding and interpreting the IEC requirements, and for discussing exploratory questions. Therefore, a semi-structured approach was chosen for conducting interviews with key members of the project team. These interviews were incorporated into

regular status update meetings and feedback sessions in a more informal way. This approach allowed for a dynamic exchange of information, addressing both specific questions and spontaneous exploratory questions, close to the definition of semi-structured interviews.

3.2 Data collection and analysis

Regarding data collection and analysis, the data types have been categorized into five distinct groups. The literature review serves as a comprehensive compilation of critical theories related to SISs, failures, SIL-compliant systems, and their relation to reliability data. Three key sources for this research are:

- Smith and Simpson (2016): The Safety Critical Systems Handbook: A straightforward Guide to Functional Safety: IEC6108 (2010 Edition), IEC 61511 (2016 Edition) & Related Guidance.
- Rausand (2014): Reliability of Safety-Critical Systems: Theory and Application
- Norwegian Oil and Gas Association (2020): Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry (Recommended SIL requirements).

Besides the literature review, there are the IEC standards 61508 and 61511, which are pivotal documents for functional safety compliance. The third category is the FSMP of the case company. The FSMP includes the way of working, responsibilities in applicable functional safety lifecycle phases, and how functional safety is implemented to design and on which basis. It describes how the functional safety objectives are achieved and maintained on a required level to meet the defined SIL. Given that the procedure will be part of the FSMP, careful consideration was given to the overall structure of the document.

The fourth group is other internal documents, including the SRS of the new ESS within the company, implemented risk identification methods, and various quality documents. These

documents play a key role in enhancing understanding and clarity. Lastly, the fifth group is semi-structured interviews that contribute open-ended insights into the progress of the established procedure. For a complete list of sources for this study, see Table 6.

Table 6. Overview of data/document sources.

Method/ document	Type	Analysis	Notes
Literature review	Qualitative	Document analysis	Critical theories related to SISs, failures, SIL-compliant systems, and their relation to reliability data.
IEC standards: 61508 and 61511	Qualitative/ Quantitative	Document analysis	The two main IEC standards for functional safety compliance.
Functional Safety Management Plan	Qualitative	Document analysis	The internal procedure of the case company represents way-of-working, and responsibilities in the safety lifecycle phases and implementation.
Other internal documents	Qualitative/ Quantitative	Document analysis	Other documents that have contributed to this research in terms of understanding and clarity.
Interviews	Qualitative	Thematic analysis	Open-ended interviews in the form of status-update meetings and feedback sessions within the project team.

4 Case Study - Results

This chapter is divided into two main parts: operational data collection and performance evaluation. An introduction to the case study is also given. Based on the presented theory, a procedure with a framework for handling operational data and evaluating SIS performance has been developed in accordance with IEC 61508 and IEC 61511 standards. The procedure has been tailored to the specific case company's own needs and structure, ensuring a practical and effective approach to functional safety.

4.1 Case Description

One of the core competencies of the case company is the development of marine and energy power solutions. In recent years, customers have started to demand safety according to functional safety standards. This is something that is expected to only increase in the future. Therefore, a new Engine Safety Module (ESM) with SIL 2 level safety functions has been developed. However, in addition to hardware-related requirements, procedures and organizational aspects need to be in place as well. One of these procedures is for analysing operations and maintenance performance and to maintain accurate information on hazards and hazardous events, safety functions, and E/E/PE safety-related systems, as defined in IEC 61508 (IEC 61508-1, 2010 [6.2.9]). During the operation and maintenance phases, data must be collected on failures and failure rates, test outcomes, demands, accidents, etc. Afterwards, the data shall be analysed and compared with the assumptions made during risk assessment. If mismatches are discovered, relevant parts of the risk assessment calculations must be re-evaluated, which might lead to modifications of the process design.

The deliverables of this specific procedure are to define what kind of data to be collected, and how the data can be used for performance evaluation of the SIS and/or reliability assessments. The purpose of the procedure is to write it in a way that may be of relevance to other Engine Safety System (ESS) projects where SIL compliance is required.

4.1.1 Engine Safety Module

The ESM will be responsible for performing SIL 2-compliant safety functionalities as part of the Engine Safety System (ESS). All the safety functions of the ESS are designed to operate in low-demand mode, with an anticipated maximum of one demand per year (refer to Chapter 2.4.2). Additionally, the engines are controlled by other modules, which are non-safety automation control systems. The safety system is to maintain safety by initiating a safe state when required. The system will be an improvement to the current non-SIL-compliant systems. For the risk assessment, HAZOP studies and FTA have been used to identify potential hazards. A Risk matrix has been used as a basis for risk analysis, describing the different risk categories, consequence levels with likelihood levels, and overall tolerable risk acceptance criteria, shaping the basis for safety functional requirements (see Chapter 2.4.1 for more information about the requirements). The Safety integrity requirements have been identified through the LOPA, FTA, and SIL classification Excel sheet, where the safety integrity level is defined based on the risk reduction needed to reach an acceptable tolerable risk level as defined in the risk matrix. The key feature of the new ESS is to execute safety functions that protect the engine from the following:

- From overspeed
- From using an engine with excessive torsional vibrations, indicating cylinder overpressure, piston seizure, or piston top detachment.
- From using the engine with low lubricant pressure
- From using the engine, with too high lubricant temperature, or too high jacket outlet cooling water temperature
- From using the engine with emergency stop activated.

All the above-listed events are scenarios when a safe state shall be initiated and represent the SIFs of the new ESS. They are all listed in a Safety Requirement Specification (SRS) and a summary of the SIFs can be seen in the architectural block diagram (see Figure 16). In case any of the SIFs are activated, the ESM cuts off the power supply of the electrical injection system and prevents fuel injection. In addition, the ESM trips the generator circuit breaker.

The figure shows all the sensors, the ESM module (logical solver), and the final elements along with the voting configuration of each SIF as well. The voting configuration where multiple sensors are used is 1oo2 (1-out-of-2). Of the final elements, the generator circuit breaker uses the same 1oo2 while the power supplies for the systems fuel injection (PSD cut-off relays) have a voting of 2oo2.

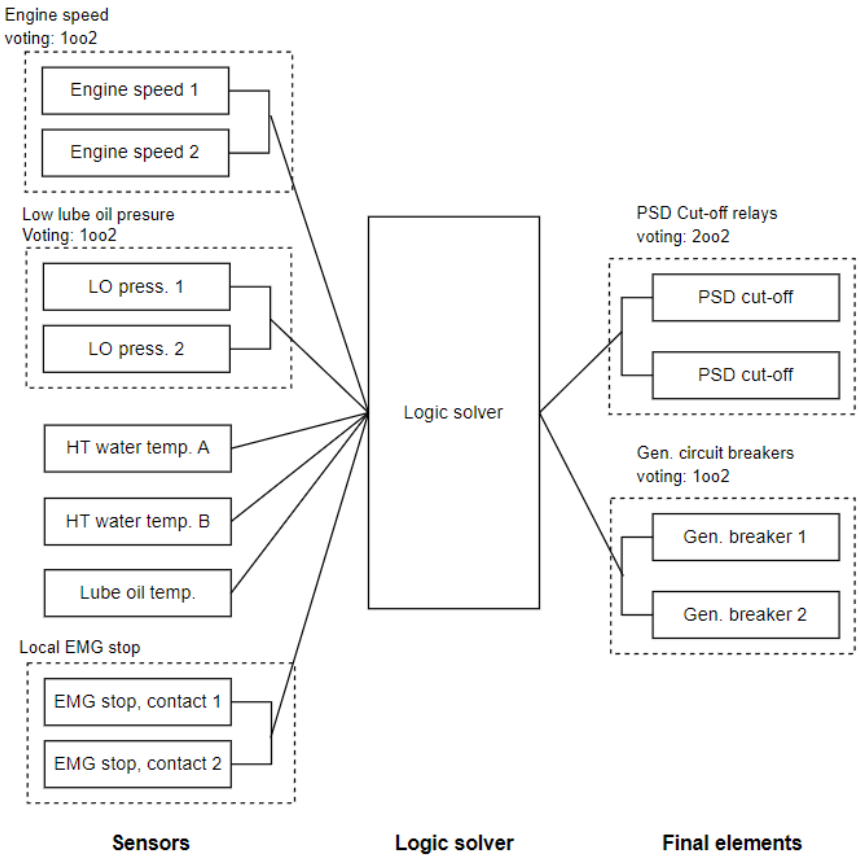

Figure 16. Architectural block diagram of the ESS

4.1.2 Data flow

The new ESM represents the logical solver that is to be installed as an independent on-engine safety system. The case company has its own embedded control system for control and monitoring of its engines that each installation is integrated with. All the data from ESM

shall be accessed through the embedded control system. There is also an operator interface system, where it is possible to view data, and store and gather process data to create analyses such as trends or reports. From this system, the data shall be stored in the cloud for up to 18 months. The cloud-based system is scalable and accessible, making it a good system to store and analyse SIS failure data from any location. However, this concerns the process data itself and does not consider the qualitative aspects of the investigation required to identify the root cause and categorization of failures. During the time of this study, the exact program to be used for reporting demands and failures was not clear. Therefore, it was early on agreed on to focus on the necessary data to be collected and how to evaluate it, instead of considering any specific program or software. This led to the creation of two failure report templates where everything is manually reported. In the future, some of the data inputs of the report templates may be possible to be automatically filled in or selected from a list of options. Both are included as appendixes and will be referred to and motivated in this chapter.

4.2 Operational Data Collection

In accordance with the IEC 61508 standard (IEC, 2010a), section 6.2.9, which states that 'Procedures shall be developed for maintaining accurate information on hazards and hazardous events, safety functions and E/E/PE safety-related systems,' The purpose of this chapter is to examine the operational data that needs to be collected to evaluate functional safety performance. In the IEC 61511-1 (2016) standard, section 16.2.9, It is stated the necessity of comparing the expected behaviour and actual behaviour of the SIS.

The following things are mentioned to be monitored:

1. The demand rate on each SIF
2. The actions taken following a demand on the system.
3. The failures and failure modes of equipment forming part of the SIS, including those identified during normal operation, inspection, testing, or demand on a SIF.
4. The cause of the demands.

5. The cause and frequency of spurious trips.
6. The failure of equipment forming part of any compensating measures.

At the beginning of the project, it was stated that of the listed requirements above, the demand rate on each SIF would be provided back to check if the demand rate is as per design more automatically, along with actions taken. However, the failure, failure modes, failure of equipment, and the cause of demands or spurious trips require investigation to fully understand the situation. Correct specification of failure cause and detection method is essential to sort the failures into DU, DD, SD, or SU, which further on, is necessary for reliability and performance evaluation (Norwegian Oil and Gas Association, 2020, p. 212). For better clarity, this chapter is divided into three subchapters, each with a framework for collecting data when there is an actual demand or spurious trips (4.2.1), failure of other barriers (4.2.2), or failure of SIS elements (4.2.3). Each subchapter offers insights into necessary data inputs, reporting templates, and methodologies for systematic evaluation. The choice of sorting this procedure into these three groups came from discussions within the project team.

4.2.1 Actual demand or Spurious trip

Whenever an actual demand or spurious operation of the SIF occurs, and there is no failure of any of the SIS elements, the ESM shall initiate a transition to a safe state. This may happen if any of the sensors detect an incorrect measurement, or in case any limit is exceeded. If that occurs, the ESM shall read this and move the final elements (GCB relays and PSD cut-off relays) to their safe state. If a trip occurs due to demand, meaning that the SIS has been activated in response to a real event (such as engine overspeed, low lube oil pressure, etc…), or a spurious trip has occurred (instrument malfunction, software error, etc…), the data must be sufficient to verify that the SIF behaved as expected. Table 7 provides the necessary data input in the event of an actual trip due to demand or a spurious trip. The product number, name of the installation, and engine type are fields that may come from a list of options, where the user selects the correct installation that the new ESM has been installed on.

These fields serve as metadata about the event and aid in tracking and analysis. The SIF (sensor tag) is necessary for defining which SIF was triggered and caused the system to go into a safe state. Simultaneously, it is vital to always consider the status of the final elements, were they activated or not? because if the SIF was triggered, no matter the type of event, and one of the final elements was not activated, the event can be classified as a dangerous failure (IEC 61508-4, 2010, [3.6.7]). The status of the event field also helps in tracking the resolution process by specifying whether the investigation is ongoing, open, closed, or fixed. Other data input fields need to be manually entered to investigate the event further. More details about these fields are provided after Table 7.

Table 7. Data input for actual demands and spurious trips.

Demand (activations) & Spurious trips of SIF	
Type of event:	Demand / Spurious trip:
Date:	DD-MM-YYYY
Time:	hh:mm:ss
Product number:	-
Name of installation:	-
Engine type:	-
SIF (sensor TAG):	**Select** the sensor tags of the SIF that was activated (engine speed sensors, lube oil pressure sensors etc…)
Status of the final elements:	**Activated:** The FE were in the correct mode: (Gen. Breaker open & driver cut-off open (non-conducting state)) **Failed**: one of the elements was not activated.
Status of the event:	Under investigation / Open / Closed / fixed
Description of the failure:	*Description of what has happened*
Location:	*the physical or functional location of the failed component or subsystem within the system*
The root cause of the demand/spurious trip:	*What triggered the cause? Hazardous conditions? Process malfunction?*
Actions:	*Were any actions taken to address the cause of the demands/spurious trips, improve SIF performance or prevent future demands/spurious trips?*
Additional info/comment	*Any relevant information about the demands/spurious trips or performance of the SIF that may help address the matter*

Description of the failure: This field shall provide detailed information about the circumstances that led to the event. This includes any specific conditions or actions that occurred that may have been a relevant factor leading up to the event. An explanation of the behaviour of the system during the event. The responses of the sensors, logic solver, and final elements may also be addressed if any deviations from a normal operation occur.

Location: After selecting a specific SIF (sensor tag), The location can already be considered as known, at least from a functional perspective. However, if the specific sensor is located near any other components or system, it can help in terms of understanding relationships between different components. Simultaneously, knowing the exact location and accessibility may help with future maintenance and corrective actions. It may also help when considering historical context if there have been issues with the specific installation earlier.

Cause of the demand/spurious trip: Accurately identifying and understanding the root cause of an actual demand or spurious trip of a Safety Instrumented System (SIS) is crucial for ensuring the overall reliability and effectiveness of the system. This data input is also required by the IEC standards as elaborated on in Chapter 2.3.1. It is necessary to investigate the cause to establish if it is a random hardware failure or systematic failure and define the correct failure mode, as it directly impacts reliability parameters such as the Safe Failure Fraction (SFF), Diagnostic cover (DC), and PFD calculations. All spurious activations are defined as a safe failure in IEC 61508 Terminology, further classified as safe detected (SU) or safe undetected (SU) (IEC 61508-4, 2010, [3.6.8]). The diagnostic tests that the ESM performs may cause increased spurious activations of the ESM and cause a transition to a safe state. However, the estimated SFF is so high that this is also required since the SFF ratio considers all failure modes (DD, DU, SD, SU). Refer to Chapter 2.4.3 for more comprehensive information on SFF. Basically, the impact of a DU failure on the SFF ratio diminishes with an increase in the detection of other failure types. The overarching goal is to minimize DU failures, given their critical role in ensuring reliability.

If the event occurred due to a hazardous condition, meaning that an actual demand existed, the nature of the hazard shall be described and how it contributed to the activation of the safety function. However, if it is due to a spurious trip operation, it may be due to various reasons such as human errors, installation errors, supporting equipment, sensor drifts, the voting architecture of sensors, etc. Rausand (2014, p. 365). Therefore, a thorough description of the exact cause is crucially needed.

Actions: If any were actions taken to address the cause of the demands/spurious trips, improve SIF performance, or prevent future events from occurring, it is to be documented in this field. In case faulty components were replaced immediately it can be documented in this field, or in case the event occurred due to human errors, and preventive measures were taken to avoid this from happening again. Documentation of actions taken can also be beneficial in understanding if the status of the event is set to any of the mentioned options.

Additional info/comments: Any information that may provide additional insights into the root cause of the event or that may be helpful. Examples include contributing factors, operator observations, or any patterns in trends of the data that can be found.

For a template of a failure report regarding a single failure due to actual demand or spurious trip, see Appendix 1. The template also includes some other data inputs specific to the case company, such as reporting personnel involved, signatures of involved personnel, department, etc. However, the central data inputs remain the same as mentioned in Table 7. A thorough investigation may be required to identify the root cause. Therefore, the process has been identified in its own section of the failure report, as part B of Appendix 1.

4.2.2 Failure of other barriers

Process plants often include many different safety barriers. While SISs are categorized as active technical safety barriers (Sklet, 2006), other barriers might fail which can decrease

the effectiveness of the SIF and/or increase the likelihood of hazardous events, leading to a demand on the system. Examples of such barriers include different mechanical barriers, alarms, and interlocks and their causes may be human error, environmental factors, equipment failures, etc… (Rausand, 2014, p. 4) For a detailed relationship between safety barriers and SISs, see Chapter 2.2.

As discussed in chapter 2.5.3, 'layer of protection analysis', LOPA is a risk assessment technique to determine if the risk reduction is sufficient for meeting the specific SIL and considers possible causes and risks associated with hazards that have been identified during the HAZOP study. During the LOPA process, all mitigation and prevention measures have been included, providing a clear picture of existing safeguards in place. Such safeguards include various safety barriers that have been identified as protection layers to prevent or mitigate process hazards. Therefore, it is necessary to gather data about the reliability of these barriers as they are part of LOPA, and their effectiveness has an impact on the overall risk reduction required.

To distinguish failure of other barriers from other types of failures it is necessary to investigate the cause of the activation and to consider the context in which it occurs. In the absence of a control system, there will be a high demand for the safety system, which can potentially lead to unsafe conditions. Table 8 shows the required data input for reporting barrier failure. While the data input is similar to that outlined in Table 7, there are some differences. Instead of selecting a tag for the specific sensor of the SIF, a tag for the barrier can be chosen (if it exists). This field content may vary by installation, which is why it has been marked with TBD (to be determined). The status of Final Elements could also be left out since it is not a report of an actual demand, spurious trip, or any element of the SIS.

The information needed for reporting the failure of other barriers is also partly inputted manually and includes fields like status, description, location, root cause, actions, and

additional information. These fields are the same as those found in Table 7 for reporting actual demands or spurious trips. Therefore, the description provided in the table is enough and there is no need to provide further details. A template for failure reports of other barriers is available in Appendix 2.

Table 8. Data input for the failure of other barriers

Failure of other barriers:	
Date:	DD-MM-YYYY
Time:	hh:mm:ss
Name of installation:	-
Product number:	-
Engine type:	-
Barrier: (equipment tag, software tag etc..)	TBD
Status of the event:	Under investigation / Open / Closed / fixed
Description of the failure:	*Description of what has happened, what barrier failed and specific mode of failure (e.g., failed sensor, malfunction of the control system).*
Location:	*The physical or functional location of the failed component or subsystem within the system.*
Root cause:	*What exactly caused the failure, including any contributing factors or underlying issues that may have led to the failure?*
Actions:	*Describe the corrective actions that have been taken or will be taken to prevent similar failures from occurring in the future, including any changes to the design of the barrier.*
Additional info/comment:	*Any relevant information about the failure that may help address the matter.*

4.2.3 Failure of a SIS element

Failure of a SIS element refers to when a component or subsystem of the SIS, such as a sensor, logic solver, or final control element fails to perform its intended function. A failure of a SIS element can occur at any time, regardless of the presence of a hazardous condition, and like a failure of other barriers, it can affect the effectiveness of the safety system and increase the risk of a hazardous event. Effectively dealing with SIS element failures requires the

classification of these failures. It is important to gather adequate data so that the failure can be categorized into one of the following failure modes:

- **Dangerous detected failure (λDD):** A failure that prevents the safety function from operating, but the condition is detected by the safety systems diagnostics.
- **Dangerous undetected failure (λDU):** A failure that prevents the safety function from operating, and the condition goes undetected by the safety systems diagnostics.
- **Safe detected failure (λSD)**: A failure that triggers the safety systems diagnostics without a demand from the process (spurious operation of the safety function).
- **Undetected safe failure (λSU):** Failure of a component that is part of the safety function but has no effect on the safety function. This type of failure goes undetected by the safety systems diagnostics and may increase the probability of a spurious trip occurring. Such a failure can be a sensor that provides slightly incorrect readings within an acceptable range but does not trigger the safety systems diagnostics. This type of failure may be noticed during proof tests or other functionality checks.

Depending on the failure, the SIS may not respond appropriately to a demand or hazardous event. A failure of a SIS might also reduce the ability of the safety system to accurately detect and respond to real threats, thereby reducing the reliability of the SIS. A failure of a SIS may also result in spurious activation of the SIS (Lundteigen & Rausand, 2008, p. 1). This also highlights the importance of investigating the root cause of a spurious trip occurrence. For this case study, where the voting configuration of all sensors, and the GCB relay (final element) is either 1oo1 or 1oo2, it means that a failure of one sensor may be enough to cause a spurious activation of the SIS. A SIS failure can also be revealed incidentally during normal operation. An example of that is a shutdown valve which for some reason needs to be closed during operation but is noticed to be stuck (Norwegian Oil and Gas Association, 2020, p. 229). In that case, the failure shall be investigated and reported. The same applies in case a

SIS element fails during proof tests or any other test. Table 9 displays the required input data for reporting a failure of a SIS element. Although it shares similarities with Tables 7 and 8, there are some differences. It is important to select the specific SIS element, which could be an equipment tag for any of the sensors, logical solvers, or final elements. As this report focuses on failures, the potential impact on the safety of associated processes or systems, including safety or operational consequences, must also be considered. To minimize the number of failure templates, it was decided that the failure report for failure of other barriers (Appendix 2) will also be used to report a failure of a SIS element, as the only additional aspect is the "impact on safety".

Table 9. Data input for failure of a SIS element

Failure of SIS element	
Date:	DD-MM-YYYY
Time:	hh:mm:ss
Name of installation:	-
Product number:	-
Engine type:	-
Status of the event:	Under investigation / Open / Closed / fixed
SIS element:	Sensor tag / Logical solver / Final Element
Description of the failure: (SIS element type and failure mode)	*Description of what has happened, which SIS element failed and the specific mode of the failure*
Location	*The physical or functional location of the failed component or subsystem within the system*
Root cause:	*What exactly caused the failure, including any contributing factors or underlying issues that may have led to the failure*
Impact on safety	*Describe the impact of the failure on the safety of the associated process or system, including any safety or operational consequences that resulted.*
Actions:	*Describe the corrective actions that have been taken or will be taken to prevent similar failures from occurring in the future, including any changes to the design, maintenance, or operation of the SIS and its associated elements*
Additional info/comment	*Any relevant information about the failure that may help address the matter*

4.3 Evaluation of SIS Performance

Based on the presented theory and this case study, ensuring the performance of SIS is of paramount importance. The guidelines and requirements presented in IEC 61508 establish the foundational principles for achieving functional safety in various industries. The standard provides a framework for designing, implementing, and operating safety-related systems to mitigate potential hazards and risks. Furthermore, the subsequent standard, IEC 61511-1, focuses on process industries, specifically addressing the functional safety requirements for SIS in the process sector. The following requirements stated in section 5.2.5.3 in IEC 61511-1 (IEC, 2016a) provide guidance on evaluating the performance of the SIS against its safety requirements. Each requirement is listed below along with a short explanation of how the requirement has been interpreted.

- *"Identify and prevent systematic failures which could jeopardize safety":*
    - This step involves conducting periodic assessments of the SIS design, installation, and maintenance practices to ensure that they meet the specific safety requirements.
- *"Monitor and assess whether the reliability parameters of the SIS are in accordance with those assumed during the design":*
    - Involves tracking and analysing Key Performance indicators (KPIs) including, failure rates, failure causes, failure modes, diagnostic coverage, proof test intervals, and other reliability parameters that are specific to each SIF.
- *"Define the necessary corrective action to be taken if the failure rates are greater than what was assumed during the design".*
    - Updating maintenance strategies, optimizing testing procedures, improving component reliability, or revising the system configuration to ensure it meets the required SIL.

- *"Compare the demand rate on the SIF during actual operation with the assumptions made during risk assessment when the SIL requirements were determined".*
    - This evaluation helps validate whether the SIF is being subjected to demands within the expected range and whether the risk reduction measures implemented are effective in mitigating the identified hazards.

4.3.1 SIS performance during operation

The performance of the SIS shall be evaluated by comparing the actual performance data with the performance criteria defined in the Safety Requirement Specification (SRS). The SRS includes information on demand rates, failure rates, SIL requirements, and any other performance criteria that have been derived from the risk assessment. Particularly demand rates and failure rates are essential to be considered when analysing operational performance, as highlighted in IEC 61508-1, section 6.2.12 (IEC, 2010a). If the SIS is not performing as expected, corrective action must be taken, this means revisiting key calculations, such as LOPA, FTA, and SIL classification Excel, as defined in the SRS of the ESS and may include modifications or enhancements to the EUC control system or other safety-related system.

To assess SIS performance, the main intention is to verify that the experienced safety integrity of the SIS during operation is acceptable. The criteria are defined through SIL requirements which are given on a function (SIF) level. Therefore, the first thing to do is to check the safety systems design documentation, the SRS, or the project specific FSMP to identify all SIFs to be evaluated. As a low demand system, each SIF's expected demand is no more than once per year. This requires clear documentation of each occurring event and the root causes. As highlighted by the Norwegian Oil and Gas Association (2021), it is the number of DU failures that are safety critical (p. 227). Based on the data input from the manual failure reports, it shall be possible to categorize the failures as either DD, DU, SD, or SU based as it is essential for the quantitative SIL requirements verification.

The evaluation process and results shall be documented in a report, including the SIFs evaluated, the performance criteria used, the data collected, the evaluation results, and any corrective actions taken. The evaluation process shall also be reviewed and updated periodically to ensure that it remains effective. This includes revising performance criteria, updating data collection methods, or modifying procedures. The results of the analysis, including identified improvements and any adjustments made to the overall safety and integrity requirements, and system interfaces, shall be reported to relevant stakeholders and management.

An annual performance review of the SIS performance shall be conducted. The frequency of SIS testing depends on several factors such as the SIS category, process character, failure modes, and testing methods. All tests, including proof tests, partial tests, and diagnostic tests, should be considered. Since all the SIFs of the ESS operate in low demand mode, and the target PFDavg of each SIF is based on annual target value, it has been agreed that a review of the performance shall take place once per year. This aligns with the assumption of the Norwegian Oil and Gas Association (2021, p. 227), which states that when annual targets are used, the equipment shall be tested at least once a year. The exact review frequency can be defined in the organization's safety management system or as part of the project´s specific FSMP. The flowchart (see Figure 17) outlines the process of evaluating SIS performance based on the principles of IEC 61508 and IEC 61511. It includes steps such as identifying safety functions, gathering performance data, assessing operational performance, comparing with requirements, determining corrective actions, implementing those actions, and documenting the evaluation process.

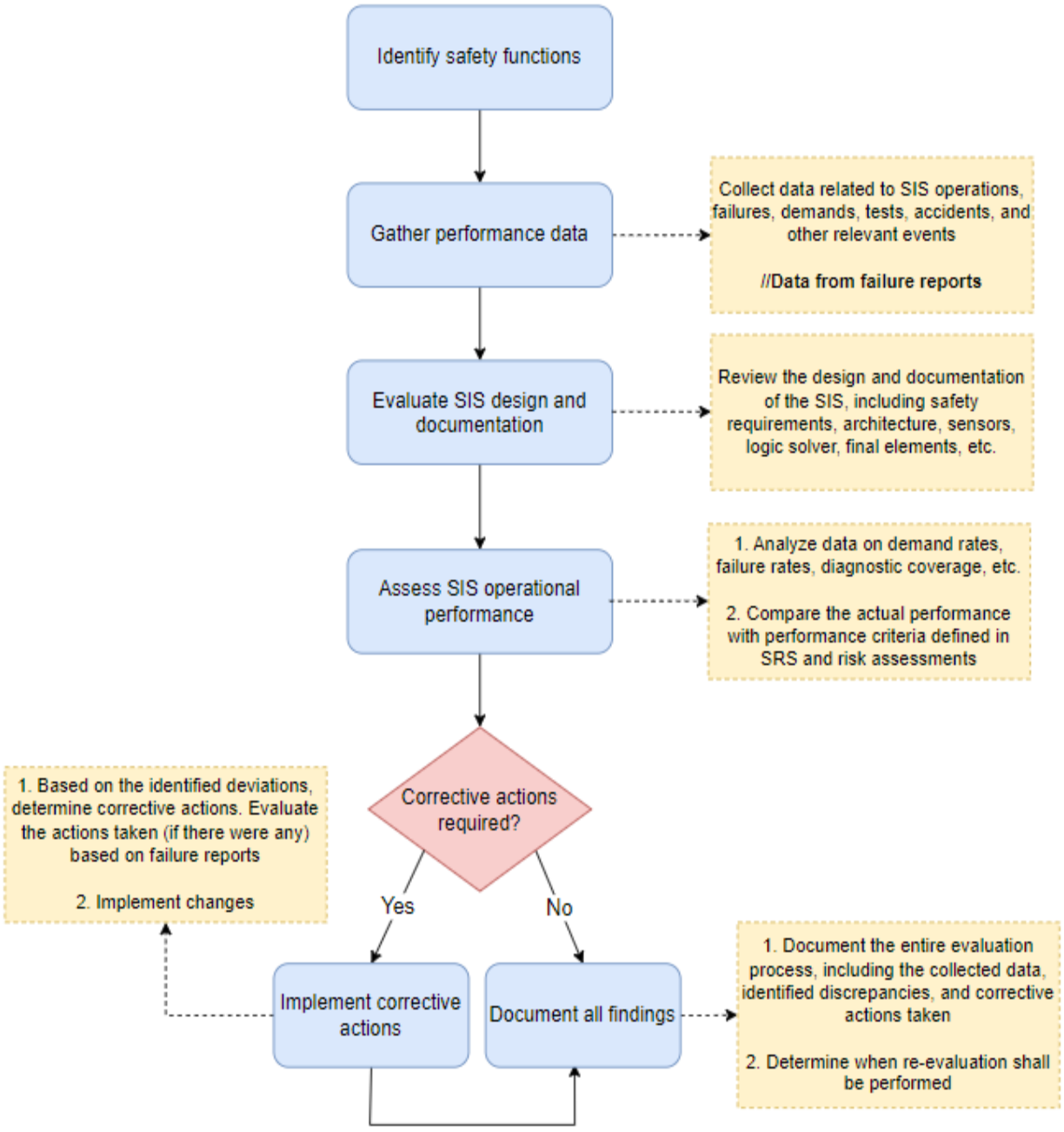

Figure 17. SIS performance evaluation process.

4.4 Reliability verification

Ensuring the reliability of a SIS requires the combination of both qualitative and quantitative assessments. Qualitative procedures are necessary for addressing systematic failures, and quantitative assessments mean comparing demand rates with risk assessment estimations. The classification of failures into DD, DU, SD, and SU is necessary for several calculations that play a part in the verification of assessing the reliability. For example, Through the LOPA process, a required demand rate and target PFD have been established which serves as the main performance indicator. However, the need for categorizing failures also affects other reliability measures. For example, a Failure Mode and Effect Analysis (FMEDA) has been conducted for all subsystems of the SIS and provides details about the failure rates, failure modes, and PFD of the components within the SIS (sensors, ESM, and Final elements).

Safe Failure fraction (SFF) and Diagnostic Cover (DC) which are explained in Chapter 2.4.3, both have their own estimations and contribute to the overall reliability of the safety system and in mitigating potentially hazardous conditions. If a failure of a component has occurred, the operational data is essential in terms of evaluating if the calculated SFF and DC estimations of the component are in line with the estimations. The DC contributes to risk reduction by ensuring that a high percentage of potential failures are identified before they lead to a hazardous scenario, and the SFF represents the fraction of the total failures of a component that is considered safe. Both are parameters of reliability measurement and address failure modes, their effects, and the diagnostic capabilities of the safety system.

4.4.1 Main information sources

One significant challenge in overseeing SISs lies in the variety of sources from which the relevant parameters shall be collected. Information about failures of the SIS, demands, and spurious trips come from various operation and maintenance activities. Different systems may also be utilized. The SIS failure reporting and maintenance system is shown in Figure 18

in a high-level diagram, showing the main information sources. The diagram is similar to the one presented by the Norwegian Oil and Gas Association (2020, p. 238). However, the diagram has been slightly modified to address the requirements of this case study.

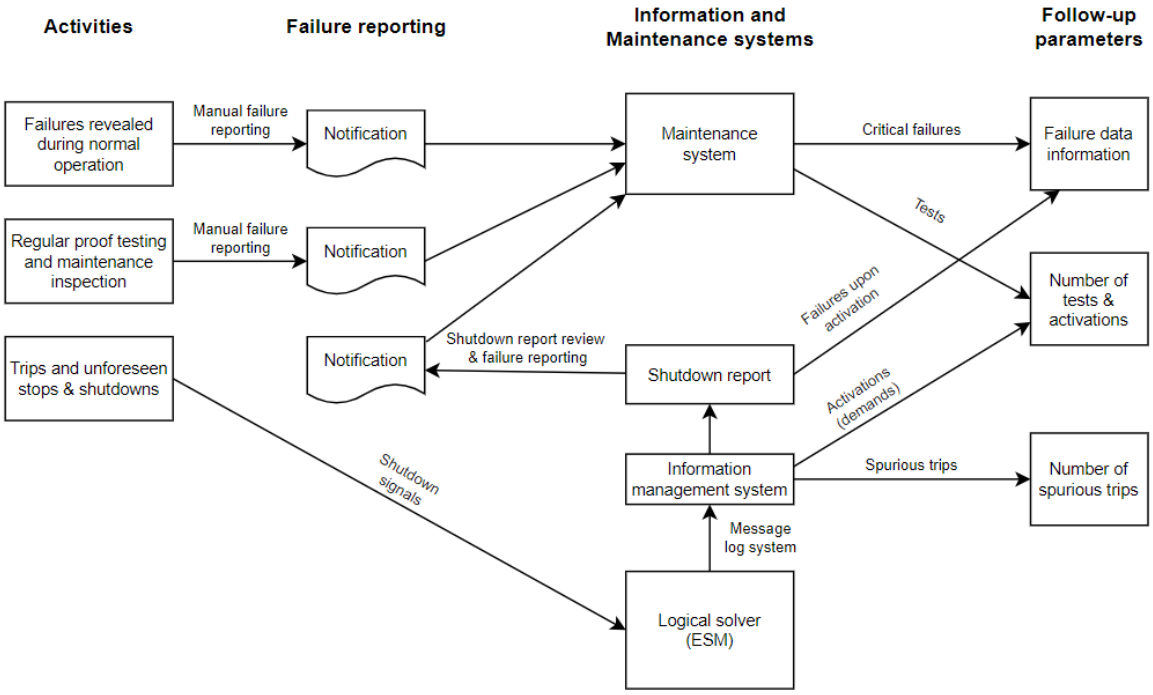

Figure 18. Overview of the main information sources

The diagram shows how SIS failures, demands, and spurious trips are collected from a variety of sources, by utilizing the manual failure reports and data input presented in Chapter 4.2. The SIS itself provides data on activations, tests, and spurious trips. The message log system records all events that occur on the ESM. The shutdown report shall be reviewed manually and compared to the manual failure reports to understand in which scenario the event has occurred. The maintenance system provides data on maintenance inspections and repairs and is notified by the activities shown in the diagram. The shutdown report provides data on trips, and unforeseen stops and shutdowns.

This data is then stored in the information management system. Since all the events are stored as a logbook entry of the ESM, the information management system can be used to keep track of spurious trips as well as the number of activations. The shutdown report is reviewed manually to understand in which scenario the event has occurred. This information is then used to follow up on the failure data and identify potential problems. The follow-up parameters use information both from the information management system and the maintenance system where the failure reports have been stored.

While the diagram shows the main information sources, the specific implementation may vary depending on factors such as project size, complexity, specific customer requirements, and integration with other systems. For example, incorporating process control systems or enterprise resource planning systems may require additional components or modifications. Additionally, contracts with customers may impose access restrictions, affecting the diagram's components and accessibility. As emphasized by the Norwegian Oil and Gas Association (2020), the detailed system implementation ultimately depends on the specific plant installation. It is highlighted in the FSMP of all safety-related systems equipped with ESM-30S that the accessibility of operational data is dependent on the Operation and Maintenance agreement with the customer. If no such agreement is made, the product owner or functional safety experts cannot receive such information.

4.4.2 Other challenges

Along with the difficulties of dealing with various sources of information, there are a few more challenges that are worth mentioning when it comes to SIS and reliability. These challenges are based on the analysis of the findings from this thesis, as well as discussions within the project team.

Human error: The reliance on manual input for operational data collection introduces a critical factor of human error. Ensuring the accuracy and completeness of information becomes

challenging, potentially leading to misclassification of failures and compromising data quality. For example, what if the operators cause an error and try to blame it on someone else? Therefore, the data must be thoroughly evaluated. Another human error challenge is that it may be difficult to capture all relevant information. These are contributing reasons why the failure reports must be signed and approved by both the operator and supervisor. By doing so, it provides accountability during performance reviews and makes it easier to know the personnel involved.

Lack of functional safety training: Accurately recording and categorizing failure events can be challenging, especially for low demand systems where demand rates are low. It can also be difficult to determine the root cause of some failures, especially if they are not accompanied by any observable symptoms or system malfunctions. By understanding functional safety, and the importance of defining failure modes, it is easier to know what to focus on. A lack of awareness or understanding might lead to inconsistent reporting practices.

Data accessibility: Integrating the ESM into the existing control system and ensuring seamless data flow might encounter technical challenges. Accessibility of data, especially when stored in the cloud, needs to be carefully managed to prevent data loss or unauthorized access.

Other associated challenges include the aspect of balancing automation and manual reporting. Striking a balance between these two can be challenging. For example, if the process is fully automatized, it must be guaranteed that the situational awareness of the system is reliable. Simultaneously, manual reporting is time-consuming and, the aspect of lack of functional safety training can impact the outcome. Additionally, since the required SIL is based on LOPA analysis with multiple layers of protection. These are protections that are not proof tested, how can it be verified that these exist and operate as expected throughout the entire lifecycle of the SIS? By having thorough documentation of the specifications of

each protective layer, it is possible to conduct design reviews and analyse their strengths and weaknesses.

Finally, there is also a need to consider traceability. If a sensor is found to be responsible for multiple false trips and is replaced, it must be properly recorded. This ensures that when evaluating the system's performance, it is evident whether the replaced sensor or the original one is being used. Similarly, if several sensors or other elements of the SIS have been replaced, it is crucial to document all these changes. This documentation serves as a means to gain an understanding of the system's history.

5 Discussion

While the challenges associated with data collection and performance evaluation of SISs were mentioned in Chapter 4.4, this chapter discusses the whole research and associated limitations. Furthermore, recommendations for future work are presented.

5.1 Discussion and Conclusion

This thesis aimed to establish a procedure with a theoretical framework for the collection of operational data and evaluation of SIS performance, with a specific focus on the operational data of a new Engine Safety System (ESS). This study is part of a development project and is written in a descriptive and informative way for potential use in other projects where SIL compliance is required within the case company. It aims to help involved personnel understand the relationship between operational data, risk assessments, and performance evaluation. SISs play a crucial role in ensuring the safety of industrial processes, and compliance with standards is integral to ensuring their effectiveness. IEC 61508 is the backbone standard and sets the main requirements of achieving functional safety while IEC 61511 is the process-sector standard. Ensuring compliance with these standards has been a central focus throughout the whole research.

The IEC standards IEC 61508 and IEC 61511 comprise several requirements, and during the research, it was noticed that understanding how to enact these requirements requires a closer examination of risk assessment methods and the overall design of the SIS. For example, the standard states that “procedures shall be developed for maintaining accurate information on hazards and hazardous events” (IEC 61508-1, 2010, [6.2.9]). While this requirement specifies what shall be done, it does not answer how to establish a procedure. Therefore, the risk assessment methods that have been used to determine the safety integrity requirements were necessary to consider as well as the whole design of the SIS. Chapter 2.4 delves into the safety integrity requirements and Chapter 2.5 into the methods that have

been used in this Case Study to fulfil the safety requirements. In chapter 4, the necessary data input was presented, highlighting the importance of data collection, and categorization of failures. In the same chapter, a flowchart of the process for performance evaluation is presented (see Figure 17). All the reliability parameters, necessary for assessing performance have been established from the risk assessment techniques detailed earlier.

One limitation of this research is that it deals with the first SIL-compliant ESS, making it impossible to follow any prior operational data procedures at this level. Therefore, it was not possible to use any other functional safety project as a reference and review how operational data is handled. As highlighted by the Norwegian Oil and Gas Association (2020), the detailed system implementation depends on the specific plant installation. The same principle goes for this Case Study. The new ESS will be installed on several installations and the exact information flow may vary from project to project. Therefore, this thesis is descriptive in nature and highlights the importance of risk assessment techniques, the operational data, the categorization of failures, and how failures of the SIS, or other existing barriers affect the safety and reliability assessment. The established procedure has been saved as a separate document within the database of the Case Company. This thesis excludes the document since it contains internal information. However, the result is the same as presented in Chapter 4 (same data input table and flow chart of performance evaluation). The procedure is primarily intended for technical services, field services, or operating personnel engaged in the collecting of operational data for SISs. To fully understand the procedure, requires that the personnel understand ESM working principles, including SIL-related safety devices like sensors and actuators, as well as an understanding of functional safety management. All of these are areas which this thesis helps address, in line with the goal of this thesis to assist the company in maintaining accurate information on hazards and hazardous events by defining the necessary data to be collected and by providing guidelines on how to review the gathered data.

Another factor that limits this research is that while The Safety-Critical Systems Handbook by Smith and Simpson (2016), and Reliability of Safety-Critical Systems: Theory and Application by Rausand (2014) have been two important books of this research, there are no straight-forward approaches for interpreting the requirements of the IEC standards. Each company has its own dataset and requirements to follow and the way a specific company has met compliance with the standards varies.

5.2 Future work

Building on the discussion, this study has identified a couple of areas for future research. Thorough investigations into each risk assessment technique and their suitability for the case project could provide valuable insights. Additionally, focusing on the validation and improvement of these methods could be a possible future work. A study that delves into the human factor, how it influences SIS performance, addressing potential errors or misinterpretations, and studying the broader safety culture within the organizations is also a potential area for future research.

Another study could be to develop or improve tools for automating the collection and analysis of operational data, implementing automated systems for reporting demands, spurious trips, and failures could streamline the process, reduce manual efforts, and further strengthen the accuracy of the data collection. This builds up to another study of standardized reporting software. For example, ExSILentia is a system that streamlines the Process Safety Management work process and the SIS safety lifecycle (Exida, n.d.). The specific software has its own embedded failure rate database helps streamline communication across organizations and between different apartments and provides a standardized approach. How to use this software in practice, in combination with the way-of-working aspect of the case company can be a good place to start for future studies. The study could also include other software and compare their advantages and disadvantages.

References

Adeyoe-Olatunde, O., & Olenik, N. (2021). Research and scholarly methods: Semi-structured interviews. *Journal of the American College of Clinical Pharmacy*. doi:10.1002/jac5.1441

Angelito, G., Ozansoy, C., & Shi, J. (2018). Developments in SIL determination and calculation. *Reliability Engineering and System Safety*, 148-161. doi:https://doi.org/10.1016/j.ress.2018.04.028

Bell, R. (2011). Introduction and Revision of IEC 61508. In C. Dale, & T. Anderson (Ed.), *Advances in Systems Safety* (pp. 273-291). London: Springer London Ltd. Retrieved from https://doi.org/10.1007/978-0-85729-133-2_16

Bowen, G. (2009, August). Document Analysis as a Qualitative Research Method. *Qualitative Research Journal*. doi:10.3316/QRJ0902027

Cameron, R. (2009). A sequential mixed model research design: Design, analytical and display issues. *International Journal of Multiple Research Approaches*. doi:10.5172/mra.3.2.140

Catelani, M., Ciani, L., & Luongo, V. (2010). The FMEDA approach to improve the safety assessment according to the IEC61508. *Microelectronics Reliability*, 1230-1235.

Catelani, M., Ciani, L., & Luongo, V. (2013). Safety Analysis in Oil &Gas Industry in compliance with Standards IEC61508 and IEC61511: Methods and Applications. *2013 IEEE International Instrumentation and Measurement Technology Conference (I2MTC).* IEEE. Retrieved from https://ieeexplore.ieee.org/document/6555503

Catelani, M., Ciani, L., & Venzi, M. (2017, June 6). Logic Solver Diagnostics in Safety Applications. *15th IMEKO TC10 Workshop on Technical Diagnostics.* Budapest: https://www.imeko.org/publications/tc10-2017/IMEKO-TC10-2017-021.pdf.

Charnock, C. (2001). IEC 61508 – A Practical Approach to its Application in the Process Industry. *SYMPOSIUM SERIES No. 148*(148). Retrieved from https://www.icheme.org/media/10197/xvi-paper-52.pdf

Corbin, J., & Strauss, A. (2008). *Basics of qualitative research: Techniques and procedures for developing grounded theory.* SAGE Publications. Retrieved from https://us.sagepub.com/en-us/nam/basics-of-qualitative-research/book235578#features

ECAST. (2009, March 1). *Guidance on Hazards Identification.* Retrieved from EASA PRO: https://www.easa.europa.eu/en/document-library/general-publications/ecast-guidance-hazards-identification

Exida. (n.d.). *System Engineering Tools - Overview*. Retrieved 12 28, 2023, from Exida: https://www.exida.com/software

Fischler, A. S. (2015). *Mixed Methods.* Retrieved from https://education.nova.edu/Resources/uploads/app/35/files/arc_doc/mixed_methods.pdf

Fischler, A. S. (2015). *Mixed Methods.* Retrieved from https://education.nova.edu/Resources/uploads/app/35/files/arc_doc/mixed_methods.pdf

Generowicz, M. (2016). *Achieving Compliance in Hardware Fault Tolerance.* Retrieved from I&E Systems: https://www.iesystems.com.au/wp-content/uploads/2018/06/Achieving-Hardware-Fault-Tolerance-Updated-Nov-2016.pdf

George, T. (2023, June 22). *Semi-Structured Interview*. Retrieved December 1, 2023, from Scribbr: https://www.scribbr.com/methodology/semi-structured-interview/

Harvard Catalyst. (n.d.). *BASIC MIXED METHODS RESEARCH DESIGNS*. Retrieved November 12, 2023, from Harvard Catalyst: https://catalyst.harvard.edu/community-engagement/mmr/hcat_mmr_sm-6090567e0f943-60905896c80af-60e5fdbc2399e-60e5fdd8057fc-610bf777da6a0-610bf7808de24-610bf792228a4-610bf8685d8f5-610bf871cbea9/

Healy, P. (2023, April 18). *What is a FMEDA?* Retrieved 10 10, 2023, from Exida: https://www.exida.com/Blog/what-is-a-fmeda

Hollnagel, E. (2004). *Barrier and accident prevention.* Hampshire, UK.

IEC. (2010a, May). IEC 61508-1. *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 1: General Requirements, 2*. Geneva, Switzerland: International Electrotechnical Commission.

IEC. (2010b, May). IEC 61508-2. *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems, 2*. International Electrotechnical Commission.

IEC. (2010c, May). IEC 61508-3. *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 3: Software requirements, 2*. Geneva, Switzerland: International Electrotechnical Commission.

IEC. (2010d, May). IEC 61508-4. *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 4: Definitions and abbreviations, 2*. Geneva, Switzerland: International Electrotechnical Commission.

IEC. (2010e, May). IEC 61508-5. *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 5: Examples of methods for the determination of safety integrity levels, 2*. Geneva, Switzerland: International Electrotechnical Commission.

IEC. (2010f, May). IEC 61508-6. *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3, 2*. Geneva, Switzerland: International Electrotechnical Commission.

IEC. (2010g, May). IEC 61508-7. *Functional safety of electrical/electronic/programmable electronic safety-related systems - Part 7: Overview of techniques and measures, 2*. Geneva, Switzerland: International Electrotechnical Commission.

IEC. (2016a). IEC 61511-1. *Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and application*

programming requirements, 2. Geneva, Switzerland: International Electrotechnical Commission.

IEC. (2016b). 61511-2. *Functional safety - Safety instrumented systems for the process industry sector - Part 2: Guidelines for the application of IEC 61511-1:2016, 2*. Geneva, Switzerland: International Electrotechnical Commission.

IEC. (2016c). IEC 61511-3. *Functional safety - Safety instrumented systems for the process industry sector - Part 3: Guidance for the determination of the required safety integrity levels, 2*. Geneva, Switzerland: International Electrotechnical Commission.

IEC. (n.d.). *International Electrotechnical Commission*. Retrieved October 2, 2023, from Safety and functional safety: https://www.iec.ch/functional-safety/faq

IEV 191-05-01. (2005b). *International Electrotechnical Commission*. Retrieved from https://std.iec.ch/terms/terms.nsf/9bc7f244dab1a789c12570590045fac8/dd5e125c408ba3acc12570ab002e9bb3?OpenDocument

IEV-191-04-01. (2005a). *International Electrotechnical Commission Glossary*. Retrieved October 9, 2023, from https://std.iec.ch/terms/terms.nsf/9bc7f244dab1a789c12570590045fac8/dd5e125c408ba3acc12570ab002e9bb3?OpenDocument

Jahanian, H. (2015). Generalizing PFD formulas of IEC 61508 for KooN configurations. *ISA transactions*(55), 168-174. Retrieved from https://doi-org/10.1016/j.isatra.2014.07.011

Kabir, S. (2017). An overview of fault tree analysis and its application in model based dependability analysis. *Expert Systems With Applications*, 114-135. Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S0957417417300714

Liu, Y. (2020). Safety barriers: Research advances and new thoughts on theory, engineering and management. *Journal of Loss Prevention in the Process Industries, 67*. Retrieved from https://doi.org/10.1016/j.jlp.2020.104260

Lundteigen, M. A. (2008, January). Safety instrumented systems in the oil and gas industry: Concepts and methods for safety and reliability assessments in design and operation.

Trondheim, Norway: Norwegian University of Science and Technology. Retrieved from https://www.osti.gov/etdeweb/servlets/purl/952060

Lundteigen, M. A., & Rausand, M. (2008). Spurious activation of safety instrumented systems in the oil and gas industry: Basic concepts and formulas. *Reliability Engineering & System Safety, 93*(8), 1208-1217. doi:https://doi-org.proxy.uwasa.fi/10.1016/j.ress.2007.07.004

Lundteigen, M. A., & Rausand, M. (2014). *Reliability Data Sources.* Retrieved from Norwegian University of Science and Technology: https://www.ntnu.edu/documents/624876/1277046207/SIS+book+-+chapter+06+-+Reliability+data+sources/9800ec63-3c6c-4472-8cd2-018157145068

Norwegian Oil and Gas Association. (2020). *APPLICATION OF IEC 61508 and IEC 61511 IN THE NORWEGIAN PETROLEUM INDUSTRY.* Retrieved from Offshore Norge: https://offshorenorge.no/contentassets/adc7e1512f90400cb7fe9f314600bed6/070---recommended-guidelines-for-the-application-of-iec-61508-and-iec-61511-rev.-06.pdf

Rausand, M. (2014). *Reliability of Safety-Critical Systems: Theory and application.* Trondheim, Norway: Wiley. doi:10.1002/9781118776353

Rojas, E. B. (2023, July 14). *Layers of Protection Analysis (LOPA): Importance, Methodology, and Application in Hazardous Scenario*. Retrieved October 15, 2023, from ORS: https://www.ors-consulting.com/lopa-importance-methodology-application

Sauk, G. (2020, October 19). *Failure Modes, Effects and Diagnostic Analysis.* Retrieved from https://www.emerson.com/documents/automation/functional-safety-certificate-fmeda-report-rosemount-remote-seals-en-77230.pdf

Simons, H. (2009). *Case Study Research in Practice.* SAGE publications. Retrieved from https://ebookcentral-proquest-com.proxy.uwasa.fi/lib/tritonia-ebooks/detail.action?docID=743724.

Sklet, S. (2006). Safety barriers: Definition, classification, and performance. *Journal of Loss Prevention in the Process Industries*(19), 494-506. Retrieved from https://doi-org/10.1016/j.jlp.2005.12.004

Smith, D. J., & Simpson, K. G. (2004). *Functional Safety A straightforward guide to applying IEC 61508 and related standards* (2nd ed.). Elsevier. Retrieved from https://books.google.fi/books?id=J4L2L-fXO14C&printsec=frontcover&hl=sv&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

Smith, D. J., & Simpson, K. G. (2016). The Safety Critical Systems Handbook A Straightforward Guide to Functional Safety: IEC 61508 (2010 Edition), IEC 61511 (2016 Edition) & Related Guidance.

SÜD, T. (n.d.). *Functional Safety Overview*. Retrieved October 2, 2023, from TÜV SÜD: https://www.tuvsud.com/en-us/services/functional-safety/about

Torres-Echeverria, A. C. (2016). On the use of LOPA and risk graphs for SIL determination. *Journal of Loss Prevention in the Process Industries*(41), 333-343. Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S0950423015300863

UIC. (2021, August 31). *The first meeting of the "Safety barrier"*. Retrieved October 15, 2023, from eNews: https://uic.org/com/enews/article/the-first-meeting-of-the-safety-barrier-task-force-held-on-24-august-confirmed

Willey, R. J. (2014). Layer of Protection Analysis. *Procedia Engineering*(84), 12-22. Retrieved from https://www.sciencedirect.com/science/article/pii/S1877705814017263

Yin, R. K. (2017). *Case Study Research and Applications.* COSMOS Corporation. Retrieved from https://us.sagepub.com/en-us/nam/case-study-research-and-applications/book250150#description

Appendices

Appendix 1. Failure report template for actual demand / spurious trip

This form is to be used for reporting any failure due to actual demand or spurious trip. It consists of two parts. Part A is intended for primary reporting and part B, is for investigation and related procedures to complete it.

Part A:

<table>
<tr><td colspan="3">Type of Incident: Demand / spurious trip</td></tr>
<tr><td colspan="2">Reported By: (Name)</td><td>Date: xx.xx.xxxx</td></tr>
<tr><td colspan="3">Personnel involved: (name(s))</td></tr>
<tr><td>Department:</td><td>Shift:</td><td>Time: xx:xx</td></tr>
<tr><td colspan="2">Product number:</td><td>Location:</td></tr>
<tr><td colspan="2">Name of installation:</td><td>Engine type:</td></tr>
<tr><td colspan="2">SIF sensor tag:</td><td>Status of the event: Open / closed / under investigation / fixed</td></tr>
<tr><td colspan="3">Status of the four final elements:</td></tr>
<tr><td colspan="3">Description of failure (what happened?):

Demand:
Description of the safety function and the hazardous event that triggered the trip on demand:

Spurious trip:
Description of the safety function and the circumstances leading to a spurious trip.</td></tr>
<tr><td colspan="3">Immediate action taken: Were any actions taken to address the cause of the demands/spurious trips, improve SIF performance or prevent future demands/spurious trips?</td></tr>
</table>

Consequences / Extent of damage observed: *Did the failure cause any damage and/or were there any safety or environmental risks that were mitigated by the SIF?*
Further investigation required by the Technical Service department:

Part B:

Supervisor name: *Name*	**Date & Time:** xx.xx.xxxx
Personnel involved: *Name(s)*	
The root cause of the demand/spurious trip: *What triggered the cause? Hazardous conditions? Process malfunction?*	
Proposed corrective action: *Besides the actions taken, should something be done differently after analysing the failure?*	
Additional info: *Any relevant information about the demands/spurious trips or performance of the SIF that may help address the matter*	
Supervisor's signature:	Date: xx.xx.xxxx
Departmental head's signature:	Date: xx.xx.xxxx
Approval signature of the Plant Manager:	Date: xx.xx.xxxx
The author:	

Appendix 2. Failure report template for failure of SIS element / other barrier

<table>
<tr><td colspan="3">Type of Incident: failure of other barrier/ failure of SIS element</td></tr>
<tr><td colspan="2">Reported By: (Name)</td><td>Date: xx.xx.xxxx</td></tr>
<tr><td colspan="3">Personnel involved: (name(s))</td></tr>
<tr><td>Department:</td><td>Shift:</td><td>Time: xx:xx</td></tr>
<tr><td colspan="2">Product number:</td><td>Location:</td></tr>
<tr><td colspan="2">Name of installation:</td><td>Engine type:</td></tr>
<tr><td colspan="2">SIS Element/barrier:</td><td>Status of the event:</td></tr>
<tr><td colspan="3">Description of failure (what happened?):

Description of what has happened, which barrier or SIS element failed and specific mode of failure (failed sensor, malfunction of the control system etc…)</td></tr>
<tr><td colspan="3">Root cause:

What exactly caused the failure, including any contributing factors or underlying issues that may have led to the failure</td></tr>
<tr><td colspan="3">Impact on safety/consequences: Describe if the failure had any impact on the safety of the associated process or system, including any safety or operational consequences that resulted.</td></tr>
<tr><td colspan="3">Actions taken: Describe the corrective actions that have been taken or will be taken to prevent similar failures from occurring in the future, including any changes to the design of the barrier or the design, maintenance, or operation of the SIS and its associated elements</td></tr>
<tr><td colspan="3">Further investigation required by the Technical Service department: YES</td></tr>
<tr><td colspan="3">Additional info: Any relevant information about the demands/spurious trips or performance of the SIF that may help address the matter</td></tr>
<tr><td>Signatures:
The author:</td><td>Supervisor:</td><td>Dept /Plant Head:</td></tr>
</table>