Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Engineering
Department of Mechanical and Industrial Engineering

Romeo Jr Gianan Avila

Functional Safety Analysis of a Subsea Compressor Protection System

Master's thesis in Reliability, Availability, Maintainability and Safety (RAMS)
Supervisor: Yiliu Liu
Co-supervisor: Fubin Qian
July 2021

NTNU
Norwegian University of
Science and Technology

Romeo Jr Gianan Avila

Functional Safety Analysis of a Subsea Compressor Protection System

Master’s thesis in Reliability, Availability, Maintainability and Safety (RAMS)
Supervisor: Yiliu Liu
Co-supervisor: Fubin Qian
July 2021

Norwegian University of Science and Technology
Faculty of Engineering
Department of Mechanical and Industrial Engineering

NTNU
Norwegian University of
Science and Technology

Preface

This master's thesis is the requirement for the subject TPK4950, spring semester of 2021. This work is conducted in collaboration with DNV. The topic *'Functional Safety Analysis of a Subsea Compressor Protection System'* is the working title of this paper. It is conceptualized by the author and his supervisor with the help of the partner company by providing a case study and its related data. The thesis is conducted to develop a knowledge in functional safety, introduce new concepts and utilization and to prepare the author for an actual application of Reliability, Availability, Maintainability and Safety (RAMS) in the industry.

The master's thesis demonstrates a general overview of functional safety, a literature review and a functional safety analysis based on the case study and within the frames of IEC 61508, IEC 61511 and other related standards.

The report is written for readers that are interested in functional safety, its methods and applications in the industry, specifically in the process industry. The reader of this report is assumed to have a background in RAMS and functional safety standards and references. The target group is also assumed to be familiar with the terminologies used in the report.

Trondheim, 2021-07-10

Romeo Jr Gianan Avila

Acknowledgment

I would like to express my deepest gratitude to all the people who helped, supported and inspired me to accomplish this master's thesis.

First, I would like to thank Associate Professor Yiliu Liu, for his valuable contribution and constructive advises during the writing of the report. His feedback and comments helped me shape this master's thesis into its complete form. I would also like to thank Mr. Fubin Qian from DNV, for providing the case study and data resources for the thesis. His timely responses and willingness to help every time I ask questions is really appreciated. It was a pleasure working with you both. I would also like to thank all the professors who have imparted their knowledge with us, special mention to Mr. Jørn Vatn, Mr. Per Schjølberg and Mr. Antoine Rauzy. Despite the circumstances, you still managed to share your expertise.

Secondly, to my friends and classmates who supported and cheered me from the beginning of my master's journey all the way up to the completion of this master's thesis. You guys made it all seemed bearable. Special mention to Ja, Pat, Eunice, Marvz, Kevs, Jorge, Lyn, Arve, Priye, Christian and Clarissa. Also to my RAMS classmates Olav, Prassana, Tima, Eivind, Tord, Dan and Kris. And of course to my Valgrinda table tennis playmates, Andreas and Simen. Also to my tennis friends Sigbjørn, Peter and Ragnild. I would also like to thank Pascale, who is supporting me all the way from Lucerne, and to Daniel, all the way from Stuttgart. You all made my time at NTNU and Trondheim, an enjoyable and unforgettable experience. Thank you so much!

Lastly, to my ever supportive family who never lost their faith in me. To Mama Lydia, Papa Romy, Ate Cherrie and Kuya Paolo, thank you for being there for me every time I need you, and for the belief that I will be able to accomplish this thesis despite the odds.

Romeo Jr. Avila

Executive Summary

With the fast growing demand of resources from the society, comes a much greater need for a more reliable and safer industries. Accidents in the past which caused loss of lives, damage to properties and destruction to the environment have impacted us more than we can imagine. Because of this, safety standards and recommended practices have been developed by different technical organizations to guide the industry practitioners to design, validate, operate and maintain the systems in a more reliable and safer way.

Risk analysis has always been practiced in the process industry and has proven to help identify, assess, quantify and mitigate the hazards that are brought by these systems. In order to mitigate these hazards, different protection layers are utilized, such as safety instrumented system, which is conceptualized through its safety instrumented function. To design, maintain and assess these functions, functional safety analysis is being carried out.

This master's thesis conducts an in-depth functional safety analysis of a subsea compressor anti-surge protection system presented in a case study. First, an introduction to the topic is discussed, followed by presenting the main objective which is *'to conduct a functional safety analysis using the procedure in the standard in a subsea application'*, then followed by elaborating how the study is approached, and finally, discussing the limitations of the paper.

After the preliminary introduction, the paper enumerates the different industry standards related to functional safety, such as IEC 61508 and IEC 61511. Important risk and reliability theories used all throughout the study, such as SIF (safety instrumented function) and SIS (safety instrumented system), are also introduced. It is the followed by a thorough literature review of the two main topics which are functional safety and anti-surge system. Lastly, different mathematical and risk analysis methods that is vital in achieving a successful functional safety analysis are elaborated.

The introduction and presentation of all the important concepts is then followed by an in-depth functional analysis. The analysis begins by introducing the case study, the conditions and the main problem to be solved. It is then followed by the steps reflected in IEC 61508 and IEC 61511 until SRS (safety requirements specifications) is produced. The results from the analysis show that the safety functions in the case study are reliable. It also suggests strategies in order to achieve the desired safety functions, solutions to the problem and ways improve the reliability of the system in the study.

After results and discussion, the paper then concludes that the functional safety analysis procedures presented in the standard is applicable for subsea safety functions. The paper recommends that more studies should be conducted to formulate a specific functional safety analysis for subsea SIFs and that subsea specifications should be more established in the future.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Background

With the fast growing demand of resources from the society, comes a much greater need for a more reliable and safer industries. Accidents in the past which caused loss of lives, damage to properties and destruction to the environment have impacted us more than we can imagine. Because of this, safety standards and recommended practices have been developed by different technical organizations to guide the industry practitioners to design, validate, operate and maintain the systems in a more reliable and safer way.

Process industry has always been a leader in promoting safety practices and procedures. The risks associated to the possible hazards present in the industry is substantial that any establishment would not dare to take. While it is best to achieve safety of the systems through inherently safe processes and design, this alone is not enough to overcome the possible hazards that the system possess. Additional protective systems are therefore required and recommended to mitigate the risks in acceptable level. Protective systems are implemented in different technologies such as mechanical,chemical, pneumatic, hydraulic, electric, electronic or programmable electronic IEC 61511 :2016. It is either one or a combination of these technologies helps the system to achieve tolerable risks.

Functional safety as defined by IEC 61508 :2010 is a part of the overall safety that depends on a system or equipment operating correctly in response to its inputs. It can be determined by considering the systems as a whole and the environment with which they interact. One of the methods to achieve and implement functional safety of a system is through the use of electrical, electronic and programmable electronic (E/E/PE). Safety functions related to E/E/PE are called safety instrumented function (SIF) which is implemented through the use of safety instrumented systems (SIS).

1.2 Objectives

The main objective of this master thesis is to conduct a functional safety analysis using procedure in the standards and utilize it with a subsea component thorough a case study to confirm its effectiveness on subsea field. To be able to achieve the main objective, sub-objectives are formulated and are reflected below:

1. Present general information regarding functional safety.

2. Perform a literature review about functional safety and anti-surge systems.

3. Present and compare main frameworks of risk, reliability concepts and procedures that are vital in achieving functional safety.

4. Demonstrate functional safety analysis of subsea compressor protection system using cognitive analysis with the aid of reliability measures such as mathematical methods and risk analysis methods.

5. Implement new solutions and approach that is suitable in achieving functional safety of a subsea safety component.

6. Conclude and recommend applicable design and strategies for the safety functions based on the achieved results from the functional safety analysis and through in-depth study of the topic.

1.3 Approach

Theoretical background and literature review are presented in order to provide a knowledge based framework for the thesis. Concepts, formulas and terminologies used in Chapter four are all presented in detail on Chapters two and three. The functional safety analysis presented is based on the case study regarding a subsea compressor protection system. Standards such as IEC 61508 and IEC 61511 are the general source of information and concept in conducting the analysis. Due to the unavailability of data for subsea compressors, topside equipment data is used. Sources such as exida certificates and ORE [2009] are utilized for the equipment information. Some assumptions are also made by the author due to data scarcity. After results are summarized an analyzed, discussions are given. Other suggestions in the discussion are based from research and literature reviews of the author. At the end of the thesis, conclusions are stated and recommendations are enumerated.

1.4 Literature survey

This master thesis would have not been completed without the availability of data and information. These sources are one of the keys in accomplishing the objectives of the project. A thorough literature study is conducted with sources from scientific databases such as; Science Direct, Google Schoolar, Web of Science, Compendex and Oria. Conference papers and international standards are the major sources. Books on reliability theories and functional safety engineering are also utilized.

Relevant articles are sorted and selected among vast amount of literature. The focus of literature review are on the following areas:

1. Existing studies and research works on functional safety in the process industry.
2. Existing risk and safety assessments of different systems.
3. Existing standards, specifications and requirements relating to reliability, safety integrity and functional safety.

1.5 Limitations

Certain boundaries are set on the master thesis which delimits the scope and its coverage. The limitations are the following:

1. The result of the thesis is based on the limited data and information accessed by the author and provided to him by the partner company during the whole duration of the study.
2. The focus of the master thesis is limited only to the case study provided by the company and to the acquired literature information from the literature reviews conducted.
3. The scope of the master thesis is limited to perform a functional safety analysis of a subsea compressor protection system from the case study provided by the company.
4. The terms, descriptions and explanations of methods and concepts are limited only to the standards and references used in the thesis.
5. The limited availability of data regarding subsea compressor limits the result of the computation only to the study. Assumptions are made on certain information which based on the author's research.
6. The master thesis is time bound with a limited duration within the Spring 2021 semester.
7. Only research papers and books from year 1995 onward are considered and the standards used are all latest versions.

1.6 Outline

The master thesis is organized with the following structure:

- Chapter one - states a brief introduction of functional safety, its importance and impact to the society. It also presents objectives of the thesis, its approach, limitations and structure;
- Chapter two - this chapter presents vital information and theories relating to the the topic of the master thesis. It involves concepts, definitions, methods, regulations and key standards that is essential to support the paper and supplement the reader. It also presents literature review acquired from scientific papers, articles and research works related to the topic;
- Chapter three - this chapter presents the mathematical models and risk analysis methods that are essential in conducting a functional safety analysis;
- Chapter four - presents the case study in detail and conducts thorough functional safety analysis. The analysis is presented in systematic way. Cognitive analysis is used with the help of mathematical model and risk analysis method introduced in chapter three in order to achieve results;
- Chapter five - presents the results of functional safety analysis conducted and discussed it in detail;
- Chapter six - presents the general conclusions of the master thesis and enumerate recommendations from the results and conclusions.

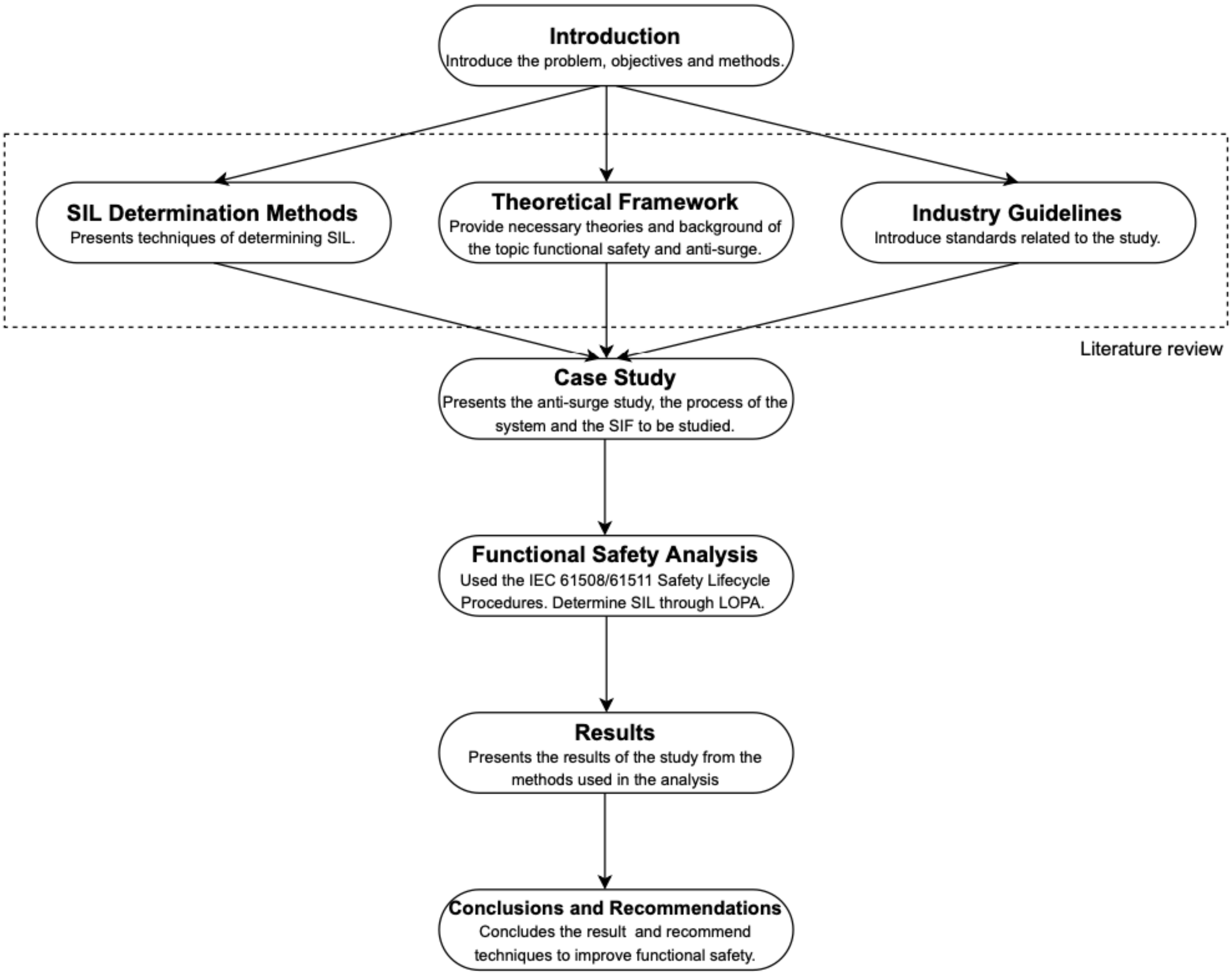

Introduction
Introduce the problem, objectives and methods.
SIL Determination Methods
Presents techniques of determining SIL.
Theoretical Framework
Provide necessary theories and background of the topic functional safety and anti-surge.
Industry Guidelines
Introduce standards related to the study.
Literature review
Case Study
Presents the anti-surge study, the process of the system and the SIF to be studied.
Functional Safety Analysis
Used the IEC 61508/61511 Safety Lifecycle Procedures. Determine SIL through LOPA.
Results
Presents the results of the study from the methods used in the analysis
Conclusions and Recommendations
Concludes the result and recommend techniques to improve functional safety.

Figure 1.1: **Structure of the Master Thesis**

Chapter 2

Theoretical background

2.1 Industry standards, specifications and database

In order to organize and create a unified system globally, standards are developed. International organizations of different fields produce technically acceptable concepts and solutions that serve as their bible. The standards presented on this section are essential to support the topic of the master thesis.

2.1.1 IEC 31010

This standard with a general title of *Risk Management - Risk assessment techniques* has been published by International Electrotechnical Commission (IEC) in coordination with ISO. It presents information regarding the ideal selection and implementation of risk assessment strategies applicable to different circumstances. Risk assessment is part of the requirements in conducting a functional safety analysis.

2.1.2 IEC 61508

The standard IEC 61508 under the general title *Functional safety of electrical/electronic/programmable electronic safety related system* is drafted by the IEC which is a worldwide organization for standardization compromising all national electrotechnical committees. The standard's objective is to present the theory of functional safety within the areas of electrical, electronic or programmable electronic (E/E/PE) systems that are subjected to safety implications.

The standard is widely used in different industries such as process, manufacturing, railway, automotive and nuclear. The standard comprises seven parts which are described below:

- IEC 61508-1: General requirements;

- IEC 61508-2: Requirements for electrical/electronic/programmable electronic safety related systems;
- IEC 61508-3: Software requirements;
- IEC 61508-4: Definition and abbreviation;
- IEC 61508-5: Examples of methods for the determination of safety integrity levels;
- IEC 61508-6: Guidelines on the application of IEC 61508-2 and IEC 61508-3;
- IEC 61508-7: Overview of techniques and measures.

The approach used on this standard is general and is recommended to guide different industries that is using E/E/PE systems as part of their functional safety.

2.1.3 IEC 61511

The general title of this standard is *Functional safety - Safety instrumented systems for the process industry sector* which is developed by the IEC. The standard is specifically developed for the process industry sector and is based on the generic standard IEC 61508. It includes terminology and requirements for specification, hardware design and application programming, commissioning, validation, operation, maintenance and testing of SIS components. The standard comprises three parts which are described below:

- IEC 61511-1: Framework, definitions, system, hardware and application programming requirements;
- IEC 61511-2: Guidelines for the application of IEC 61511-1;
- IEC 61511-3: Guidelines for the determination of the required safety integrity levels.

2.1.4 API RP 17V

The standard API RP 17V stands for American Petroleum Institute Recommended Practice 17V. API is an American organization that produces standards and recommended practices for oil and gas industry. API RP 17V under the general title *Recommended practices for analysis, design, installation, and testing of safety systems for subsea applications* presents recommendations for designing, installing, and testing a process safety system for subsea applications. The basic concepts of subsea safety systems are discussed and protection methods and requirements of the system are outlined.

2.1.5 GL 070

The standard GL 070 under the general title *Application of IEC 61508 and IEC 61511 in the Norwegian petroleum industry (Recommended SIL Requirements)* is published by the Norwegian Oil and Gas Association. The standard serves as a guideline which standardize and simplify the application of IEC 61508 and IEC 61511 for the use in the Norwegian petroleum industry. This guideline proposes a predefined performance requirements for functions that are already identified as required in international and national standards adopted by the Norwegian Petroleum sector.

2.1.6 OREDA

OREDA which stands for *Offshore Reliability Data* provides reliability data for topside, subsea and some onshore exploration and production (EP) equipment. The purpose of the OREDA project is to contribute to an improved safety, cost-effectiveness in design and operation of oil and gas EP facilities, through collection and analysis of maintenance and operational data, establishment of high quality data base, and exchange of reliability, availability, maintenance and safety (RAMS) technology among participating companies.

2.1.7 PDS method handbook

PDS method handbook under the general title *Reliability Prediction Method for Safety Instrumented System* is published by SINTEF in coordination with multiple companies. The handbook provides PDS method which is used to quantify the safety unavailability and loss of production for safety instrumented systems (SISs).

2.2 Risk and reliability theories

This section introduce basic concepts and vital theories relating to risk management and functional safety. These topics are essential to the paper and are the key concepts in the literature review.

2.2.1 Risk theories

Risk management

As defined by ISO 31000 :2018 is a coordinated activity that direct and control an organization with regard to risk. It deals with identifying, planning, preventing or mitigating the risk. Risk is inevitable and exist in all industries so managing it properly would save money, protect property, environment and human life.

Risk assessment

Risk assessment is the general method of risk identification, risk analysis and risk evaluation. IEC 31010 :2019 introduced techniques for assessing risks and one of its classification is by analysing controls. One of the techniques for analysing controls that introduced in the standard is layer of protection analysis (LOPA).

HAZOP study

Hazard and Operability (HAZOP study) according to IEC 61511 :2016 is a structure and systemaic analysis that identifies and evaluates hazards in a process plant, and non-hazardous operability problems that compromise its ability to achieve design productivity. HAZOP results are the basis of impact events used in LOPA and other methods to identify safety functions of a specific system.

2.2.2 Reliability theories

Safety Instrumented Function (SIF)

SIF as defined by IEC 61511 :2016 is a safety function to be implemented by a safety instrumented system (SIS). It is a specific function that aims to protect the process and maintain its safe state. Safety instrumented function handles a specific hazardous event and is aimed to mitigate its impact event, with all other layers of protection. SIF which is achieved through SIS is one of the most reliable risk management technique by implementing an advanced and reliable technology which is also considered as the most effective among layers of protection in mitigating risks.

Safety Instrumented System (SIS)

SIS is an instrumented system used to implement one or more SIFs according to IEC 61511 :2016. SIS typically comprises a sensor, logic solver and final element. Its architecture depends on the the SIL requirement it should achieve. Figure 2.1 shows a sample safety instrumented system for a safety function of high pressure incident in a subsea gas compression system.

Safety instrumented system is an important part of functional safety analysis because it helps to achieve the required functional safety of a certain hazardous event. It has usually the largest risk reduction factor among the other layers of protection.

A SIS can be utilized as either a proactive or a reactive barrier. Proactive barriers are control barriers that are put in place in order to stop hazardous event from occurring while reactive barriers are activated after the hazardous event occurred and are used to prevent one or more event sequences that may occur after the hazardous event Rausand [2011]. Proactive barriers are usually high demand systems that are functioning continuously or frequently or low demand system that respond to certain infrequent process deviations, though low demands systems are mostly reactive Liu and Rausand [2011].

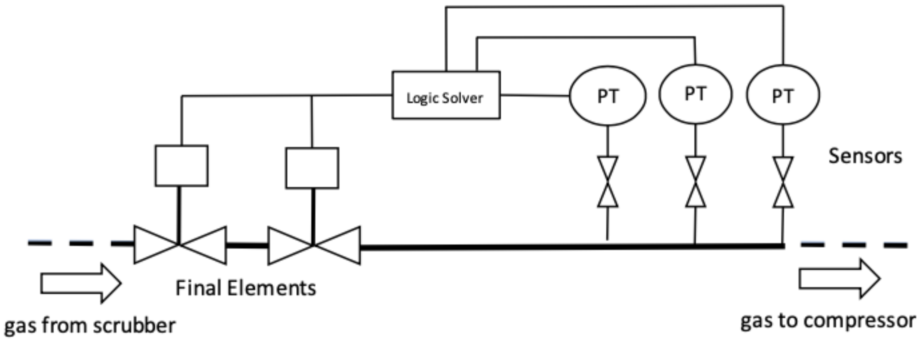


Figure 2.1: **Safety Instrumented System Architecture**

Safety Integrity Level (SIL)

SIL as defined by IEC 61508 :2010 is a discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level four has the highest level of safety integrity and safety integrity level of one has the lowest. It is used as a basis of quantifying the safety integrity requirements of safety function of an E/E/PE safety related systems. SIL determination is an important part of functional safety analysis as it decides the level of protection that a certain system requires. Allocating wrong level can be detrimental to the system and may cause under designed safety instrumented systems.

SIL is determined by three target measures which are the target probability of dangerous mode failures to be achieved, they are;

- low demand mode of operation - the average probability of dangerous failure on demand of safety function (PFD_{avg});
- high demand mode of operation- the average frequency of a dangerous failure on the safety function [h^{-1}], (PFH);
- continuous demand mode of operation- the average frequency of a dangerous failure on the safety function [h^{-1}], (PFH).

These modes of operations are assigned a value based on their safety integrity level classification.

Reliability measures

In order to determine the SIL classification of a SIF, it is vital to know the operation mode of the system. Operation mode is based on how the safety function is being demanded to function.

Table 2.1 and Table 2.2 below show the target failure measures of a safety function for both low and high/continuous demand modes of operation.

Table 2.1: **Safety Integrity Level - Target failure measures for a safety function operating in low demand mode of operation** (IEC 61508 :2010)

Safety Integrity Level (SIL)	Average probability of dangerous failure on demand (PFD_{avg})
4	$10^{-5} to \leq 10^{-4}$
3	$10^{-4} to \leq 10^{-3}$
2	$10^{-3} to \leq 10^{-2}$
1	$10^{-2} to \leq 10^{-1}$

Table 2.2: **Safety Integrity Level - Target failure measures for a safety function operating in high demand mode or continuous demand mode of operation** (IEC 61508 :2010)

Safety Integrity Level (SIL)	Average frequency of a dangerous failure of the safety function (h^{-1}) (PFH)
4	$10^{-9} to \leq 10^{-8}$
3	$10^{-8} to \leq 10^{-7}$
2	$10^{-7} to \leq 10^{-6}$
1	$10^{-6} to \leq 10^{-5}$

According to IEC 61508 :2010, high demand mode is where the safety function in only performed on demand, in order to transfer the equipment under control (EUC) to a specified state, and where the frequency of demand is greater than once per year. Same definition goes to low demand mode except for the frequency of demands which is no greater than once per year.

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

$$PFD_{avg} = 1 - \frac{1}{\tau}\int_0^{\tau} R(t)dt \tag{2.1}$$

High demand mode computation includes failure intensity which is $\omega(t)$. T is the time duration. Average frequency of dangerous failure of safety function is calculated with the formula:

$$PFH(T) = \frac{1}{T}\int_0^{T} \omega(t)dt \tag{2.2}$$

Failure classification

One of the purpose of functional safety analysis is to eliminate systematic failures and reduce the occurrence of random failures. It is therefore vital to introduce these types of failure. Probability of failure of components are also important in completing the safety requirement specifications (SRS) which needs to be accomplished in functional safety analysis. Figure 2.2 shows failure classification and categories as presented in IEC 61508 :2010

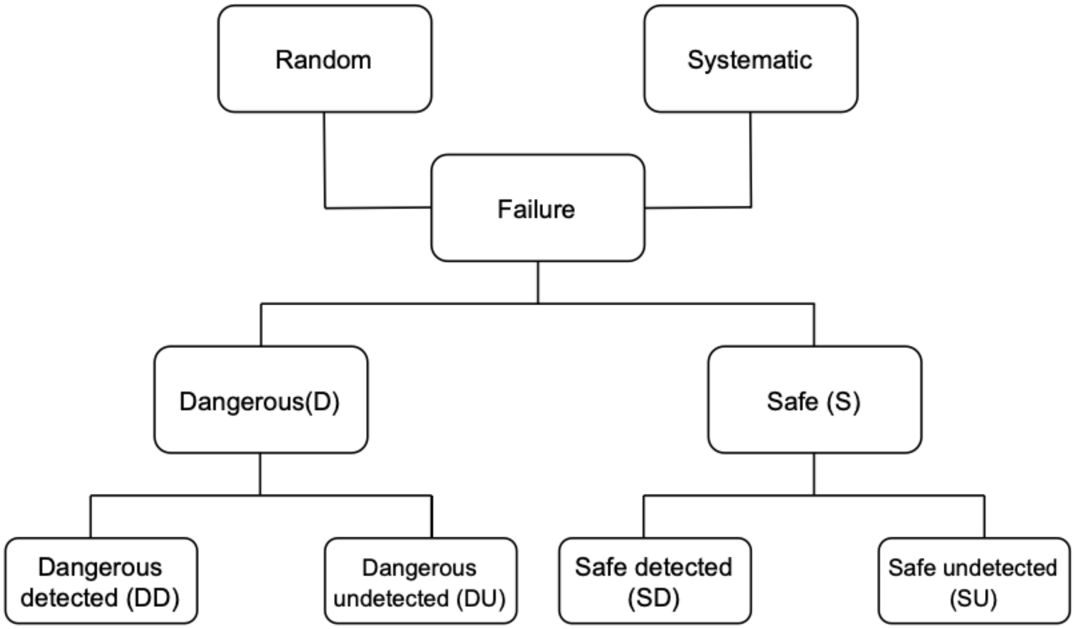


Figure 2.2: **Failure Classification Diagram**

EIV [192-03-01] defines failure as the loss of ability to perform. A failure of an item is an event that results to fault. IEC 61508 :2010 classifies failure as either random failure or systematic failure.

- Random failure - a type of failure occurring at a random time which results from one of more possible degradation mechanisms in the hardware. Example of random failures are aging and stress failures;

- Systematic failure - a type of failure related in a deterministic way to a certain cause, which can only be eliminated by a modification of the design or the manufacturing process, operational procedures, documentation or other relevant factors. Example of systematic failure are design failure and interaction failure.

IEC 61508 :2010 further distinguish failure as detected and undetected. ISO/TR 12489 :2013 defines these terms more precisely. Here are the definition:

- Detected failure - a type of failure which is immediately evident to operation and maintenance personnel as soon as it occurs. A typical example are failures reported as diagnostic faults or alarms;
- Undetected failure - a type of failure which is not immediately evident to operations and maintenance personnel. A typical example is a failure that is hidden until the component is asked to carry out its function.

Finally, these failures are further broken down into their smallest classification which are enumerated below:

- Dangerous detected(DD) - a critical diagnostic alarm reported by the component, which will, as long as it is not corrected, prevent the safety function from being executed;
- Dangerous undetected (DU) - a critical dangerous failure which is not reported and remains hidden until the next test or demanded activation of the safety function;
- Safe detected (SD) - a non-critical alarm raised by the component;
- Safe undetected (SU) - a spurious (untimely) activation of a component when not demanded.

2.3 Functional safety

Safety according to IEC 61508 :2010 is defined as an absence of unacceptable risk causing injury or of damage to the health of the people, either directly, or indirectly as a result of damage to property or to the environment. Functional safety comes to play when a system or equipment is involved. It as a part of the overall safety that depends on the correct response of a system or an equipment to its inputs according IEC 61508 :2010. Functional safety plays a major role in different industries in order to maintain the safety operation of their systems. This enables them to confidently provide the services they offer without hassle and achieve their business targets.

Functional safety is concerned with the safety achieved by safety-related systems that are primarily implemented by electrical/electronic/programmable electronic (E/E/PE) technologies. The umbrella standard IEC 61508 helps different industries achieve functional safety.

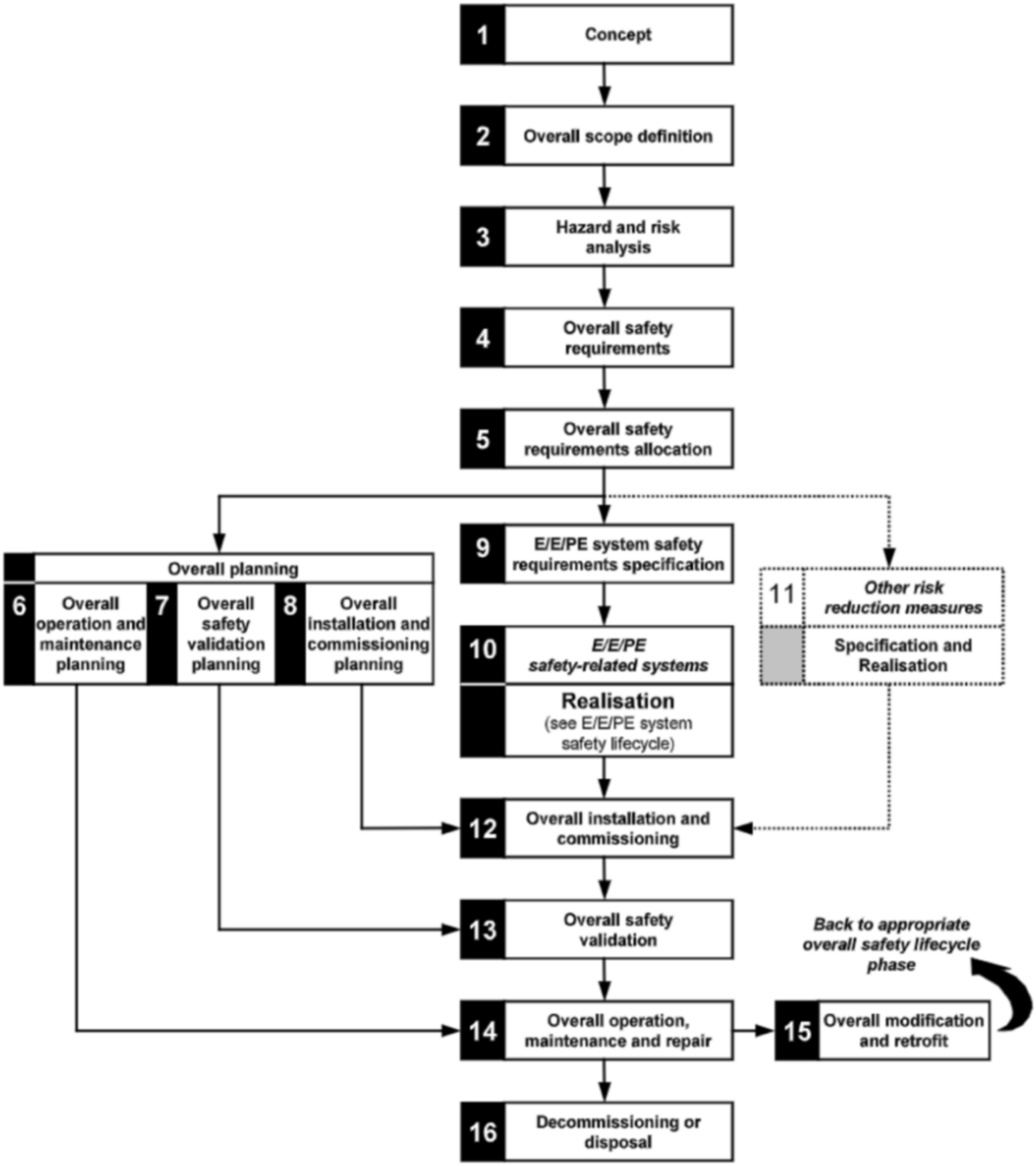

1
Concept
2
Overall scope definition
3
Hazard and risk analysis
4
Overall safety requirements
5
Overall safety requirements allocation
Overall planning
6
Overall operation and maintenance planning
7
Overall safety validation planning
8
Overall installation and commissioning planning
9
E/E/PE system safety requirements specification
10
E/E/PE safety-related systems
Realisation (see E/E/PE system safety lifecycle)
11
Other risk reduction measures
Specification and Realisation
12
Overall installation and commissioning
13
Overall safety validation
Back to appropriate overall safety lifecycle phase
14
Overall operation, maintenance and repair
15
Overall modification and retrofit
16
Decommissioning or disposal

Figure 2.3: **Overall Safety Life-Cycle System Block Diagram** (IEC 61508 :2010)

2.3.1 Safety life-cycle system

Functional safety is achieved through safety life-cycle system. From conceptualization up to decommissioning, functional safety plays an important part. Reflected in Figure 2.3 is the step-by-step practice in achieving functional safety. Smith [2011] on his book, divided and grouped the safety life-cycle procedure and explained the steps in a simpler manner.

Concept and scope

It defines exactly what is the equipment under control (EUC) and the parts being controlled. Understands the EUC boundary and its safety requirements. The scope recognizes the extent of the hazard and identification techniques (e.g. HAZOP). Requires a safety plan for all the life-cycle activities.

Hazard and risk analysis

This involves the quantified risk assessment by considering the consequences of failure (often referred to as HAZAN (Hazard Analysis).

Safety requirements and allocation

This step addresses the whole system and set maximum tolerable risk targets and allocated failure targets to the various failure modes across the system. Defines what the safety function is by establishing the failures that are protected and how it is protected. This step also assigns SIL for each safety function.

Plant operation and maintenance

Safety operation and maintenance procedures are planned on this step. The effect of human error is important here. This also involves recording actual safety-related demands on systems as well as failures.

Plan the validation

Planning for the overall validation of all the functions is done on this step. It involves pulling together the evidence from all the verification activities into a coherent demonstration of conformance to the safety related requirements.

Plan installation and commissioning

Planning the safety procedures of installation and commissioning is done on this step. Effect of human error is major factor on this step.

Safety requirements specification

Describes all the safety functions in detail.

Design and build the system

It means creating the actual safety systems electrical,electronic,pneumatic, and/or other protection levels.

Install and commission

Implement the installation and create records of events during installation and commissioning, especially failures.

Validate that the safety systems meet the requirements

This involves checking that all the allocated targets (above)have been met. It involves mixture of predictions, reviews and test results. There is validation plan and records that all the tests have been carried out and recorded for both hardware and software to see that they meet the requirements of the target SIL. It is important that the system is re-validated from time to time during its life, based on record data.

Operate, maintain and repair

Documentation of incidents in operation and mechanical failures are important part of functional safety.

Control modifications

It is also important not to forget that modifications are, in effect, re-designed and that the life-cycle activities should be activated as appropriate when changes are made.

Disposal

Decommissioning carries its own safety hazards which should be taken into account.

Verification

Demonstrating that all life-cycle stage deliverable were met in use.

Functional safety assessment

Carry out assessments to demonstrate compliance with the target SILs.

2.3.2 Functional safety in the process industry

Functional safety in the process industry is focused on the safety life-cycle of safety instrumented system (SIS) and uses IEC 61511 as the standard. It starts from hazard and risk assessment (HRA), disregarding the concept and scope step. It is already assumed that this step is done and HRA will produce an impact event that will require safety instrumented function to be accomplished by SIS. After safety function allocation, safety requirements specification (SRS) for the SIS is done. Followed by design and engineering of SIS, installation, commissioning and validation, operation and maintenance, modification and finally decommissioning.

Functional safety of SIS is achieved through compliance of safety standards for all the steps mentioned. Process industry possessed one of the most established and reliable SIS life-cycle. This is due the vastness of the field and the amount of recorded data which is being used as a basis to improve reliability and maintainability of its systems.The complete SIS life-cycle overview is found on Appendix B.

2.3.3 Functional safety on different industries

With IEC 61508 serving as the umbrella standard for functional safety, all other industries has produce their own standard. Functional safety on other industries are as vital as the process industry functional safety. Reflected in Figure 2.4 is the different industry standards relate to IEC 61508. The safety life-cycle for other industries are almost identical, so the focus of this section is to present the difference on their SIL allocation.

- Railway industry - according to EN 50126 :2017, besides the quantitative aspect, safety integrity also addresses factors such as quality management, safety management and technical management. SIL is fixed on high demand mode of operation;

- Manufacturing industry - guided by the standard IEC 62061 :2015, the industry have a specific SIL estimation during design of machine and a qualitative approach for SIL assignment for a specific machine hazard. IT has only three levels of SIL, which is on high demand mode;

- Automotive industry - guiding the industry's functional safety is ISO 26262 :2018. The industry is using the term ASIL, which stands for automotive safety integrity level and has levels from A to D and on high demand mode. Both hardware and software is carefully analyzed with consideration of random and systematic faults;

- Nuclear industry - IEC 61513 :2011 is the main reference for functional safety for this industry. Safety functions of postulated initiating events (PIE) are identified on early stages of the plant design and are given initial function category. There are three categories of safety function identified for this industry.

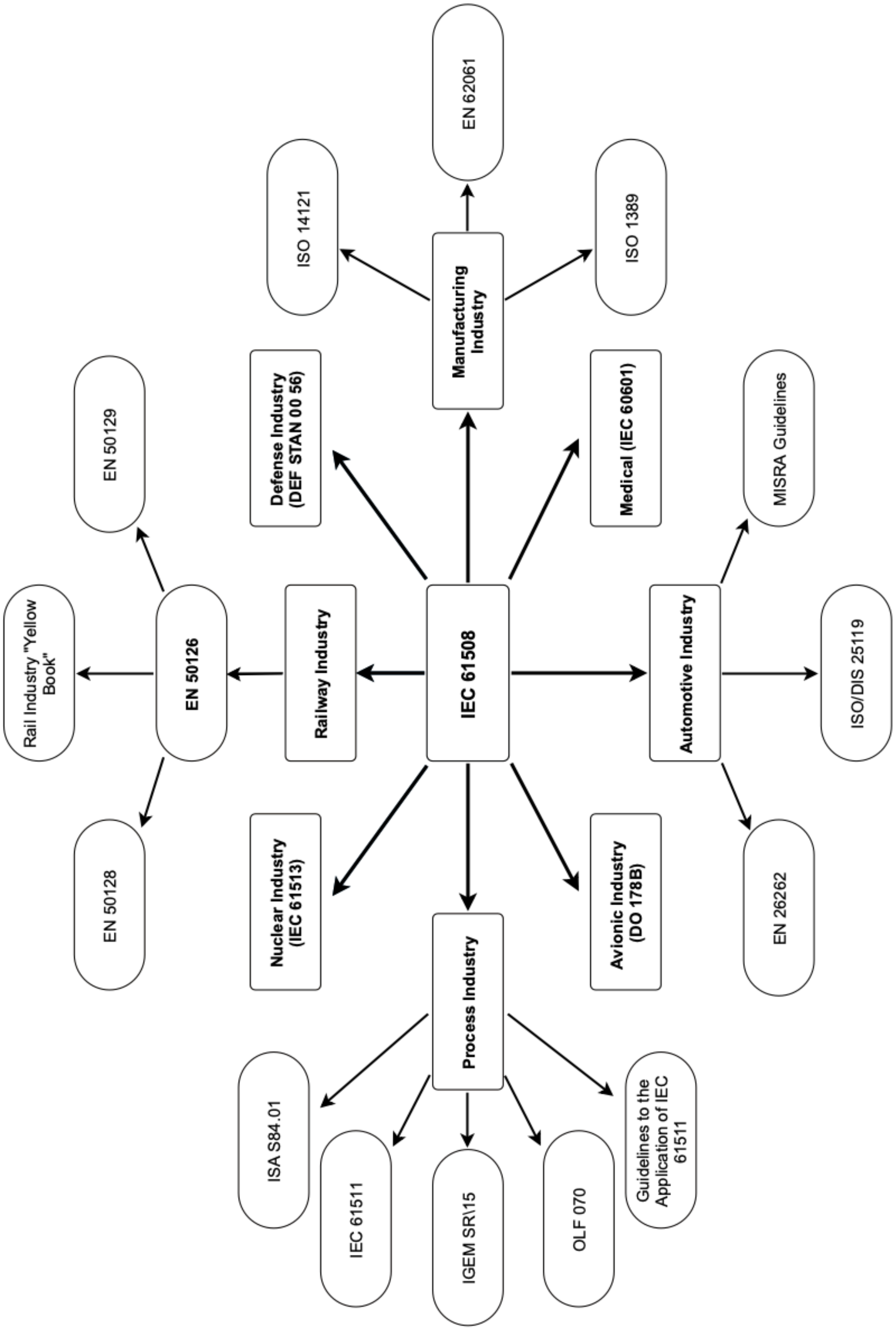


Figure 2.4: **IEC 61508 Relative Industry Standards** (Smith [2011])

2.4 Anti-surge system

Anti-surge system is a part of a compressor system that protects the compressor from surging which further leads to mechanical damage. Compressor system is a highly complex mechanical equipment that involves not only the compressor itself but also numerous pipes, valves, sensors, a liquid removal facility and a liquid pump according to Kim et al. [2018]. Compressor is used in oil and gas to boost pressure from the upstream hydrocarbon facilities where it is extracted up to the downstream facilities where it is further processed.

2.4.1 Compressor surge

Singleton explains that under normal operating conditions, compressors run at constant speed and has a specific relationship between the pressure head across the compressor and the flow through it. But the steady relationship is distracted by unexpected changes in flow, pressure and density, usually caused by sudden variations in demand downstream of the compressor. All these can give rise to formidable pulsations of pressure and flow known as surge. Compressor pressure and flow characteristic is reflected in Figure 2.5.

Surge features has been summarized by Ren et al. [2012] and are enumerated below:

- When close to surge or surge occurs, the outlet pressure and inlet flow may appear severe volatility, pressure and flow meters will swing back and forth strongly;
- When close to surge condition, periodically vibratory airflow may result in periodically changed noise, and the noise will be louder under surge condition, engine know may happen at times, too;
- The compressor's cylinder and bearing will vibrate severely when surge occurs, the amplitude of vibration will be much larger than normal condition. It may also result in the vibration of the whole machine;
- Axial displacement will increase and sometimes it may even be larger than the design value. The change process can be observed through axis displacement table and axis vibration table.

Singleton emphasized that during surge conditions, compressor finds the flow too low for conversion to the discharge pressure, which makes the pressure in the discharge pipe exceeds the impeller outlet pressure. This creates back flow. In order to avoid this condition, a discharge line with a control valve and its required instrumentation is added in order to recycle the fluid to the compressor suction. This discharge line which recycles the fluid back to the suction line in order to maintain a normal flow condition in the compressor is called anti-surge system.

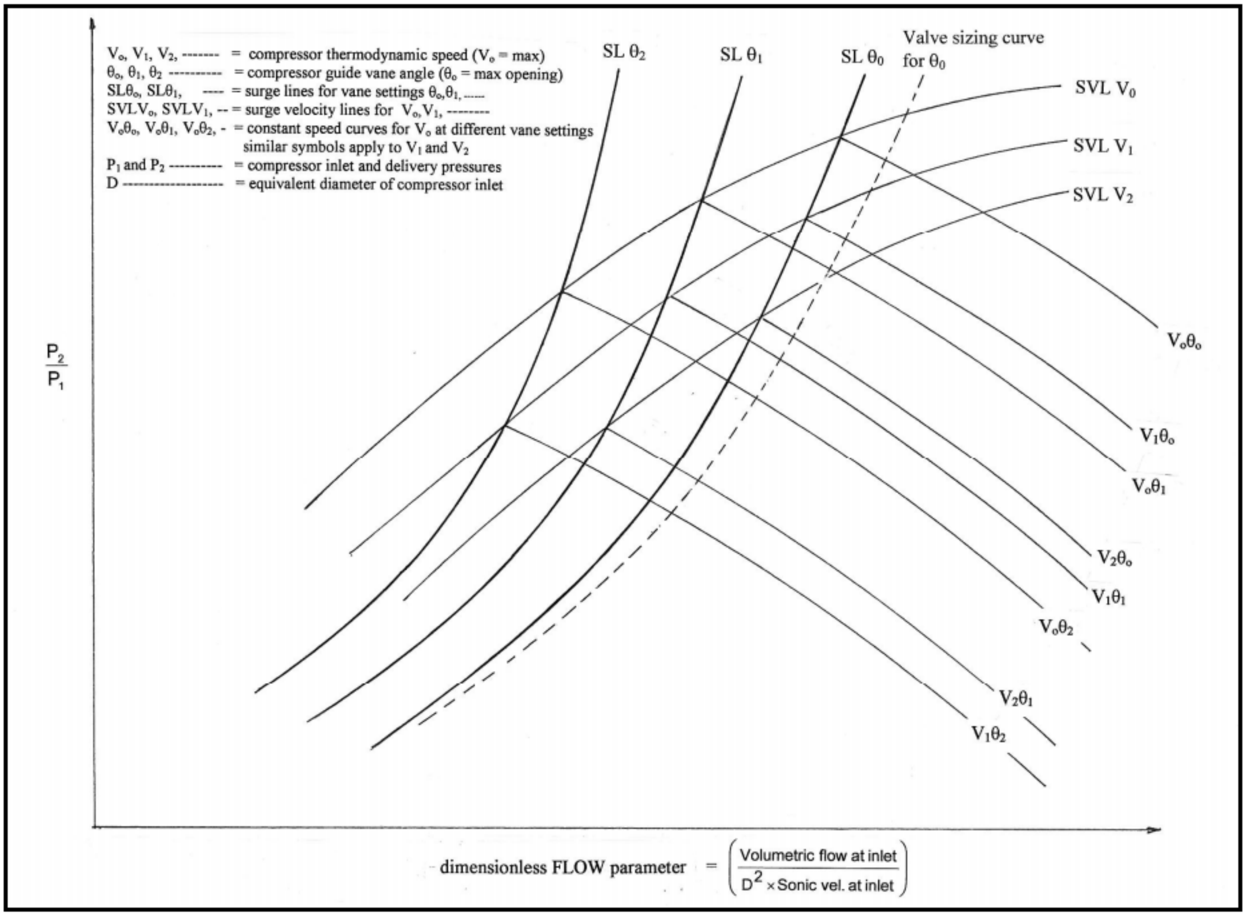


Figure 2.5: **Compressor Map** (Singleton)

2.4.2 Compressor anti-surge system

Anti-surge system in the compressor is designed in order to protect the compressor from surging. Once the surge limit is reached, the anti-surge valve opens and reverts the flow back to the suction line through the anti-surge discharge line. Anti-surge control system usually depends on multiple inputs such as differential pressure, inlet and outlet pressure, inlet and outlet temperature and flow conditions. These inputs are fed by the instruments located at the suction and discharge of the compressor. These instruments are used to measure and control parameters.

According to Almasi [2012], compressor and process applications vary so much that it could be difficult, if not impossible, to device a surge control scheme that is universal and standard. He is also added that each application must be evaluated in order to determine the required control functions and anti-surge system design requires in-depth knowledge of instrumentation and control as well as good understanding of the compressor and machine load characteristics.

2.4.3 Subsea gas compression system

A new technology has emerged with the installation of the first subsea gas compressor in Åsgard facilities on the Norwegian Continental Shelf last September 2015 and immediately followed by Gullfaks subsea gas compression project. These technologies are the first of its kind. Subsea gas compression are proven to be cost efficient, higher gas recovery and safer to the environment.

According to Bai and Bai [2010], compared to topside processing, the advantage of subsea processing are: accelerated and increased production and recovery, enabling marginal field developments, especially fields at deep-water/ultra deep-water depths with long tie-backs, extended production from existing fields, enabling tie-in of satellite developments into existing infrastructure by removing fluid, handling constraints, improved flow management and reduced impact on the environment.

With the installation and commissioning of subsea gas compression system includes the anti-surge system that protects it from surging. Kim et al. [2018] affirms that subsea gas compressor unit is composed of the following; subsea gas compressor, anti-surge valve, liquid discharge valve, and sensors. As shown in Figure 2.6, anti-surge valve in subsea compressor includes instruments such as pressure, temperature and flow. There is still a luck of study and recorded data with regards to subsea anti-surge systems due to its short span of usage.

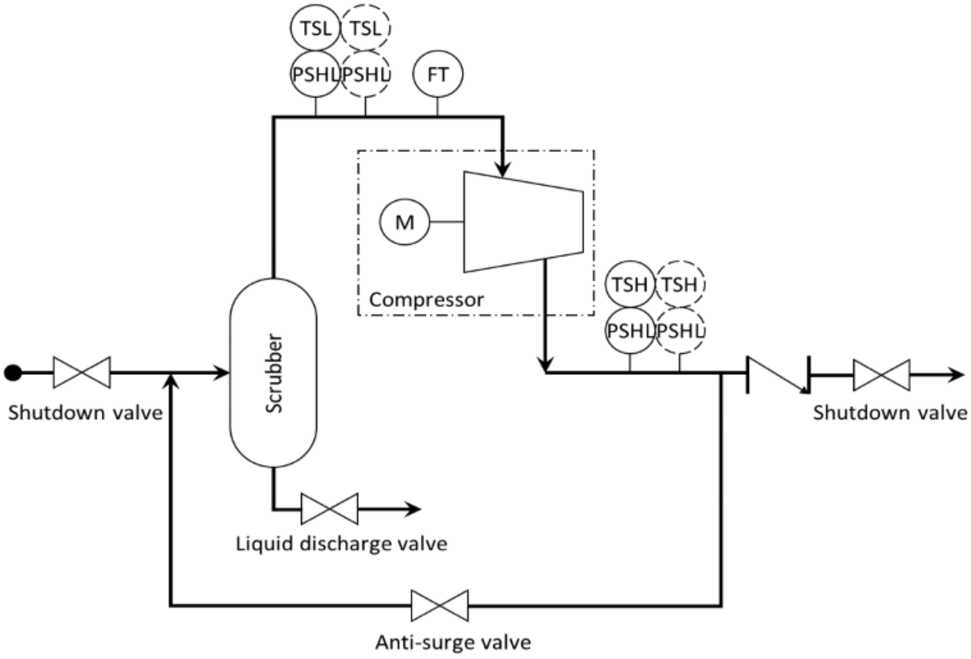


Figure 2.6: **Typical Subsea Dry Gas Compression System** (API RP 17V :2015)

Chapter 3

SIL Determination Approach

SIL determination is vital part of safety life-cycle covered in functional safety assessment. Either to check the integrity of the existing SIS or designing a new one, SIL determination helps either to improve the system or achieve safety targets. The safety integrity level to be assigned to a specific SIF can be determined by using qualitative and quantitative approach. Depending on the requirements and data availability, it can be a simple approach or a complex mathematical model. This chapter presents SIL level determination using combined qualitative and quantitative risk assessment approach and probability of failure determination based on mathematical models.

3.1 Methods for determination of required SIL

Based on IEC 61511, there are six recommended methods for determining SIL of a given safety instrumented function. Each method is presented in general, except for LOPA. This method is used in Chapter 4, so its detailed information is presented.

3.1.1 Layer of Protection Analysis (LOPA)

There are a number of known applications of LOPA being used today, and determining the SIL is one of them. LOPA is used as method for determining SIL if the system in focus is already in operation. On this stage, it analyzes possible hazards and determine whether additional safety function is required and if so, SIL is determined for each of them. LOPA is a simplified form of assessment that typically uses order of magnitude categories for initiating event frequency, consequence severity, and the likelihood of failure of independent protection layer (IPL) to approximate the risk scenario CCP [2001]

LOPA is identified on this paper as a risk assessment technique to measure the effectiveness of the layers of protection of an existing system and determine the SIL requirement by assessing the initial layers.

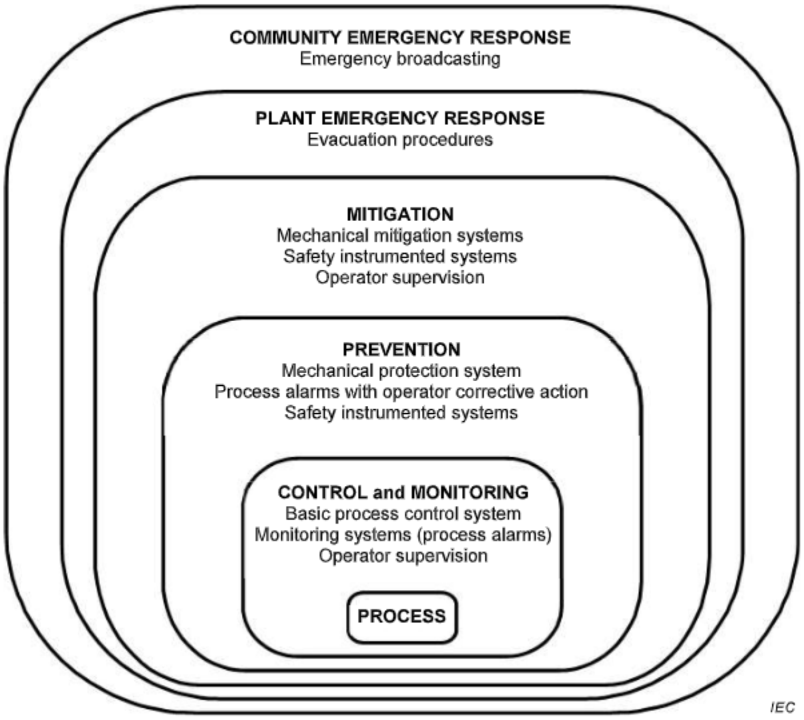

COMMUNITY EMERGENCY RESPONSE
Emergency broadcasting
PLANT EMERGENCY RESPONSE
Evacuation procedures
MITIGATION
Mechanical mitigation systems
Safety instrumented systems
Operator supervision
PREVENTION
Mechanical protection system
Process alarms with operator corrective action
Safety instrumented systems
CONTROL and MONITORING
Basic process control system
Monitoring systems (process alarms)
Operator supervision
PROCESS
IEC

Figure 3.1: **Typical Protection Layers** (IEC 61511 :2016)

Layers of protection

As shown in Figure 3.1, layers of protection consists of different levels. These levels are the most important input in performing a LOPA. A protection layer consists of a group of equipment and/or administrative controls that function in concert with other protection layers to control or mitigate risk according to IEC 61511 :2016 Each layer must be independent to each other to be considered in the analysis. Here are the basic layers of protection considered in the analysis:

- Design - it is the preliminary line of defense to hazard and is important to be reliable. This layer is usually determined by the engineers involved in the initial design stage. Adapting safer design concepts mitigate probable ramification of an occurrence Willey [2014];

- Basic process control system (BPCS), alarms and operator supervision - this protection layer involves basic process designs which involves instruments to monitor the process and alarms to notify if abnormal events happen. It also involves operator's actions to alarms;

- Critical alarm with operator corrective action and mechanical protection system - a protection layer that requires more serious action from the operator and is dependent on operator's skill for it to be successful. It is also important that mechanical protection such as manual shut-off valves or circuit breakers are working for this layer to be effective;

- Safety instrumented system (SIS) and mechanical mitigation system - considered as the last layer of defense after basic protection layers have failed, SIS is designed to detect a specific hazard condition and act to bring the process to a safe state according to Chastain-Knight [2019]. Mechanical mitigation protection such as relief devices comes after SIS failure and acts and the ultimate line of defense before evacuation procedures are required. High reliability is suggested on these devices;

- Physical protection, plant emergency response and community response - these layers of protection are considered as post-hazardous event layer. It means that all layers that comes before them have failed to control or mitigate the hazardous event. It is usually not included in performing a LOPA but still being considered as part of the overall layer of protection.

Independent protection layer (IPL)

It is a type of safety defense that impedes a hazardous event from happening without being affected by the actual initiating event of by any other safety protection in the same scenario Willey [2014].

LOPA requirements

Regardless of the purpose of LOPA, whether for verification of an upgrade of protection layer or for SIL determination, it requires almost identical data input. Enumerated below are the required information for a LOPA report adapted from IEC 61508 :2010 and Willey [2014]:

- Impact event description - usually identified in hazard operability (HAZOP) study, the event description will be the basis of the analysis;

- Severity level - in order to measure the risk tolerance of the event, severity level is required. It is usually identified in risk matrix;

- Initiating cause -the reason why the impact event may occur. All initiating cause should be enumerated;

- Initiation likelihood - the probability that initiating cause may occur. It is usually in events per year and data can be based on generic sources or proof test intervals;

- Design - usually not given credit in LOPA because it is assumed that the initiating cause is within the system design. Its important criteria are; specificity, effectiveness, independence, dependability and auditability;
- Control system -given credit on the report if the control function mitigates the consequences of the initiating event;
- Alarms - given credit on the report if hardware and software used are separate and independent to the control system and located on a permanently manned location. Operator training and skills are also considered;
- Additional mitigation - these layers are usually mechanical, structure or procedural. It is measured on how reliable the operator mitigates the alarm or how they react to incidents in case of fire. Restrictions on access to certain areas are also considered. Gas alarm, deluge systems and dikes are also part of this layer;
- Intermediate event likelihood - this is required to be computed if you want to know whether additional safety function is required. It is acquired by multiplying initiation likelihood, design, control system, alarms and additional mitigation inputs. The answer will be then compared to the tolerable risk frequency of the associated risk level and an additional safety function is required if it's lower;
- Safety instrumented system - an independent layer that is automatic and usually obtains a good credit for risk reduction depending on its design. It is designed for a specific safety function but may cover multiple functions as well;
- Plant emergency and community response - not part of the LOPA but still considered as vital because of its impact to the community and environment. It is usually dependent on the training and skills of the personnel and their equipment to be used in case they are demanded.

3.1.2 Event tree analysis

Rausand [2004] defines event tree analysis (ETA) as an inductive procedure that shows all the possible outcomes resulting from an accidental (initiating) event, taking into account whether installed safety barriers are functioning or not, and additional events and factors. It can be used to identify all potential accidents scenarios and consequences in a complex system.

ETA is used for existing plants that has existing active protection barriers. It is used used in order to know if the the barriers are enough to mitigate the initiating event or what SIL is need for it to be mitigated. ETA does not usually consider common cause failures and the holistic dependencies between the safety function and BPCS.

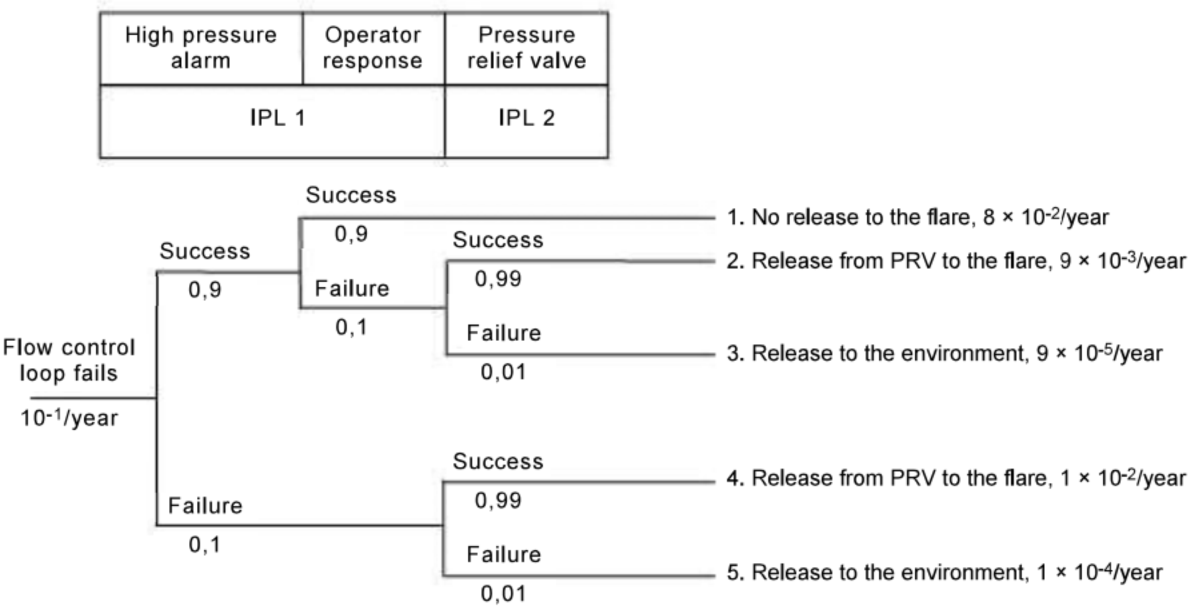

High pressure alarm
Operator response
Pressure relief valve
IPL 1
IPL 2
Flow control loop fails
10-1/year
Success
0,9
Failure
0,1
Success
0,9
Failure
0,1
Success
0,99
Failure
0,01
Success
0,99
Failure
0,01
1. No release to the flare, 8 × 10-2/year
2. Release from PRV to the flare, 9 × 10-3/year
3. Release to the environment, 9 × 10-5/year
4. Release from PRV to the flare, 1 × 10-2/year
5. Release to the environment, 1 × 10-4/year

Figure 3.2: **Event Tree Analysis Sample** (IEC 61511 :2016)

Figure 3.2 shows an event tree analysis for a ’flow control loop failure’ scenario. The event is divided by the failure and success of each protection layer. The final frequency of each similar outcome is added together to get the final frequency. If the result is higher than the process safety target, then a protection layer is required to be added. Taking in mind that SIF is the last option to use when all other types of protection layers is not possible.

3.1.3 Safety layer matrix

IEC 61511 :2016 classifies safety layer matrix as a qualitative method that develops a matrix which identifies the potential risk reduction that can be associated with the use of protection layers. The matrix is based on the operating experience and risk criteria of the specific company, the design, operating and protection philosophy of the company, and the level of safety that the company has established as its safety process target.

The safety layer matrix has inputs of hazardous event likelihood and hazardous severity rating. Hazardous event is classified as either low, medium or high.

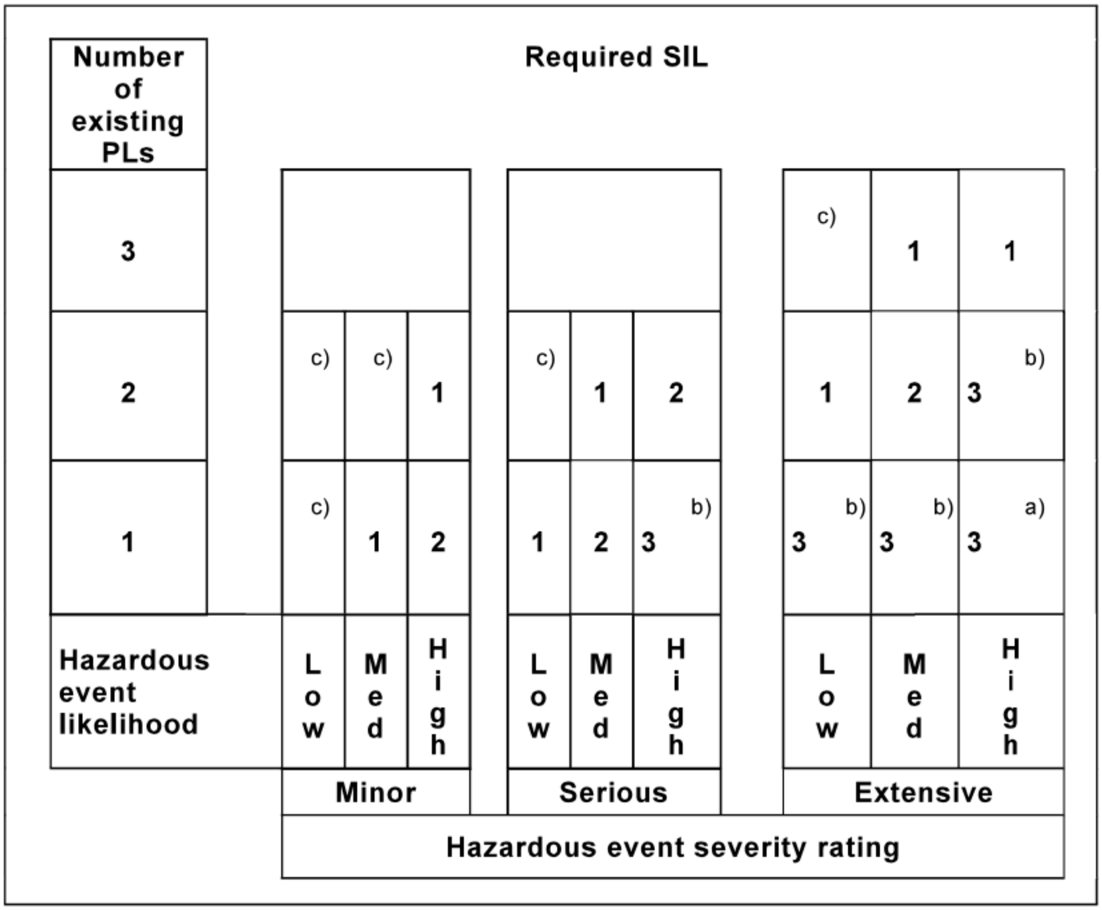
- Low - events such as multiple failures of diverse instruments or valves, multiple human errors in a stress free environment, or spontaneous failures of process vessels;

- Medium - events such as dual instrument, valve failures, or major releases in loading/unloading areas;

- High - events such as process leaks, single instrument, valve failures, or human errors that result in small releases or hazardous materials.

Hazardous severity rating is also classified in three categories such as; minor, serious and extensive.

- Minor - minor damage to equipment. No shutdown of the process. Temporary injury to personnel and damage to the environment;
- Serious - damage to equipment. Short shutdown of the process. Serious injury to the personnel and the environment;
- Extensive - large scale damage of equipment. Shutdown of a process for a long time. Catastrophic consequence to personnel and the environment.



Required SIL

Number of existing PLs	Minor			Serious			Extensive		
Hazardous event likelihood	Low	Med	High	Low	Med	High	Low	Med	High
3							c)	1	1
2	c)	c)	1	c)	1	2	1	2	3 b)
1	c)	1	2	1	2	3 b)	3 b)	3 b)	3 a)

Hazardous event severity rating

Figure 3.3: **Safety Layer Matrix Sample** (IEC 61511 :2016)

Both hazardous event likelihood and hazardous severity rating are considered in the safety layer matrix as reflected in Figure 3.3. These categories are intersecting with the number of protection layers present for the said hazardous event, considering SIF. The number on the columns represents the SIL required and the letters represent whether SIF is sufficient or not. Safety layer matrix method is limited to company provided data from their own experience and consideration. It makes the method less effective. It also assumes as stress free environment which is impossible. It also does not cover SIL 4 categories which maybe required to some safety instrumented function.

3.1.4 Calibrated risk graph

As define by IEC 61511 :2016, calibrated risk graph is a semi-qualitative method that enables the SIL of a SIF to be determined from knowledge of the risk factors associated with the process and the BPCS. The approach used a number of parameters, which together describe the nature of the hazardous situation when a SIS fails or is not available. Calibrated risk graph is also used to determine the need of risk reduction where the consequences include acute environmental damage or asset loss.

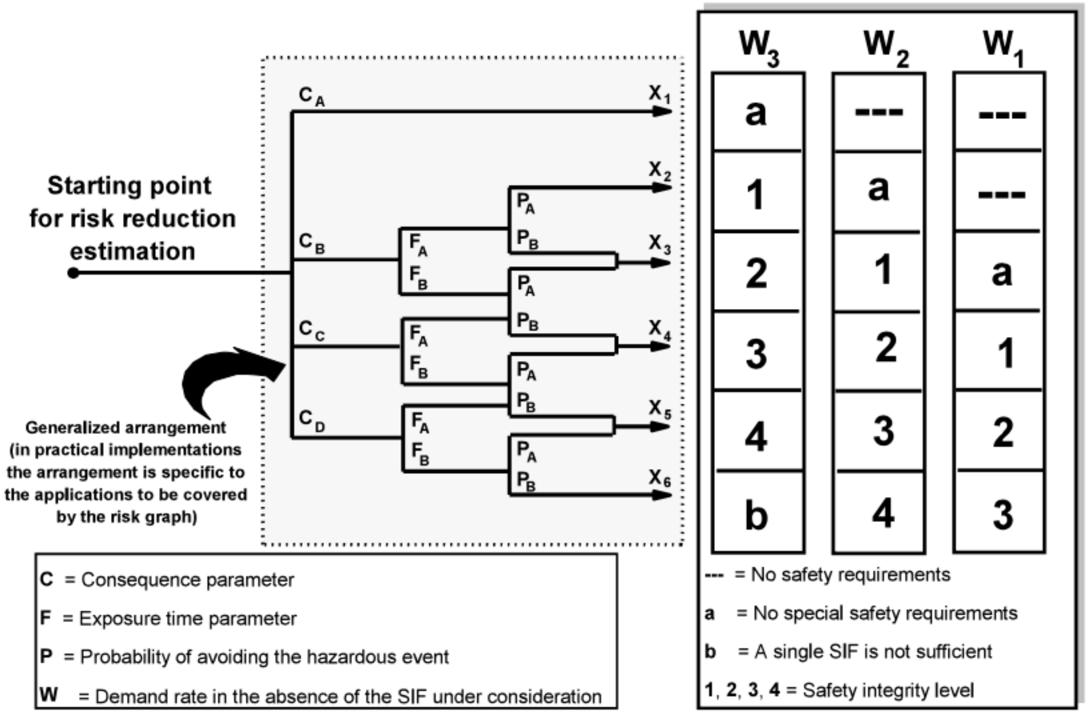
The SIL determination of calibrated risk graph is based on the combination of the numerical values of different parameters. The four parameters used in the calibrated risk graph in the process industry as described in IEC 61511 :2016 are the following:

- Consequence (C) - number of fatalities and/or serious injuries likely to result from the occurrence of the hazardous event. Determined by calculating the numbers in the exposed area when the area is occupied taking into account the vulnerability to the hazardous event;

- Occupancy (F) - probability that the exposed area is occupied at the time of hazardous event. Determined by calculating the fraction of time the area is occupied at the time of the hazardous event;

- Probability of avoiding the hazard (P) - probability that exposed persons are able to avoid the hazardous situation which exists if the SIF fails on demand. This depends on their being independent methods of alerting the exposed person to the hazard prior to the hazard occurring and there being method of escape.

- Demand rate (W) - the number of times per year that the hazardous event would occur in the absence of the SIF under consideration. This can be determined by considering all failures which can lead to the hazardous event and estimating the overall rate of occurrence.


Starting point for risk reduction estimation
Generalized arrangement (in practical implementations the arrangement is specific to the applications to be covered by the risk graph)
C_A
C_B
C_C
C_D
F_A
F_B
P_A
P_B
X_1
X_2
X_3
X_4
X_5
X_6
C = Consequence parameter
F = Exposure time parameter
P = Probability of avoiding the hazardous event
W = Demand rate in the absence of the SIF under consideration
--- = No safety requirements
a = No special safety requirements
b = A single SIF is not sufficient
1, 2, 3, 4 = Safety integrity level

W_3	W_2	W_1
a	---	---
1	a	---
2	1	a
3	2	1
4	3	2
b	4	3

Figure 3.4: **Calibrated Risk Graph Sample** (IEC 61511 :2016)

Figure 3.4 shows a sample calibrated risk graph based on a specified criteria for a chemical process. The description of categories should be adjusted based on the project requirement and company specifications. Parameters are adjusted so that it fits the range of intended applications and risk tolerability. Higher SILs are observed to be given to the categories with the maximum values and with higher demand rate per year. Complete detail of the category is reflected in Appendix C.

3.1.5 Risk graph

Risk graph method is almost similar to calibrated risk graph which is introduced in the prior subsection. IEC 61511 :2016 defines it as a qualitative method that enables the SIL of a SIF to be determined from knowledge of risk factors associated with the process and BPCS. The approach uses a number of parameters which together describe the nature of hazardous situation when SIS fails or are not available. Risk graph's purpose is more on personnel protection but can also be used to determine the need for risk reduction where the consequences include acute environmental damage or asset loss.

The SIL determination of risk graph is based on the combination of the numerical values of different parameters. The four parameters used in the risk graph in the process industry as described in IEC 61511 :2016 are the following:

- Severity (S) - consequence of the hazardous event. Classification has been developed to deal with injury and death of people;
- Exposure time (A) - frequency of presence in the hazardous zone multiplied with the exposure time. It is also developed to deal with injury and death of people;
- Possibility of avoidance of consequences (G) - takes into account supervision of process, supervised or unsupervised, rate and development of hazardous event, etc;
- Probability of unwanted occurrence (W) - estimates the frequency of the unwanted occurrence taking place without the addition of any SIS (E/E/PE or other technology) but including any external risk reduction facilities.

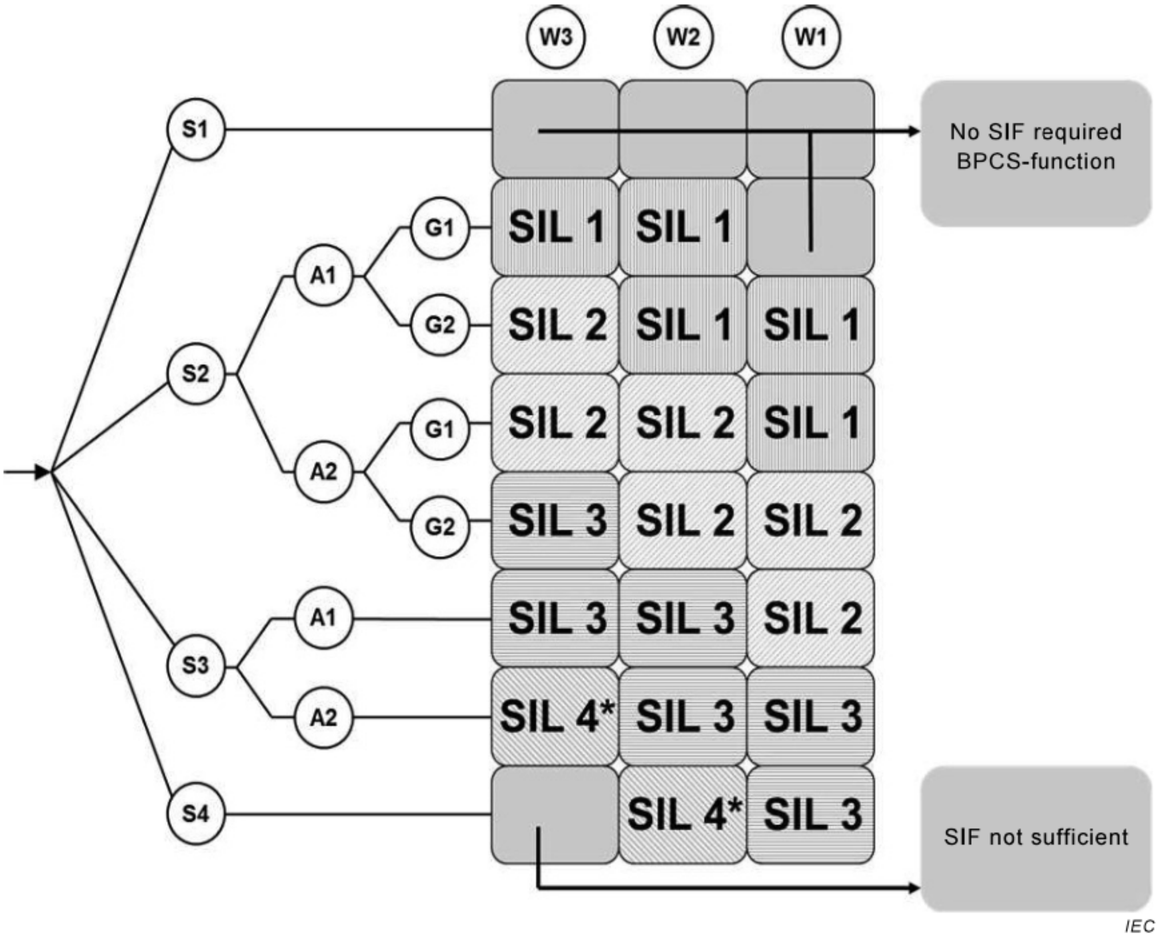


Figure 3.5: **Risk Graph Sample** (IEC 61511 :2016)

Figure 3.5 shows a sample risk graph for personal protection and relationship to SIL's. The description of categories should be adjusted based on the project requirement and company specifications. It is important to consider risk requirements from the owner and any applicable regulatory authority. Interpretation and evaluation of each risk graph should also be described and documented in clear and understandable terms. Higher SIL levels are observed to be given to the categories with the higher exposure to the hazards and with higher demand rate per year. Complete detail of the category is reflected in Appendix D.

3.1.6 Minimum SIL requirements from GL 070

Minimum SIL requirement is a SIL requirement calculated for standard safety functions, using applicable data. GL 070:2018 defines minimum SIL requirements for commonly used SIFs in the Norwegian offshore oil and gas industry.

The minimum SIL requirements in the guideline only applies to the underlying assumptions mentioned in the standard. It identifies SIL requirements for SIFs (PSD functions), global SIFs (ESD, FGDS etc), subsea SIFs, some blowout preventer (BOP) functions and workover related SIFs. The purpose of introducing the minimum SIL requirements are:

- Simplify and standardized the process to set performance standard for barriers;
- Ensure consistency in the approach to determine performance standards;
- Ensure that the performance of new or modified SIFs are benchmarked against similar functions that through operation and historical records have demonstrated satisfactory reliability.

The guideline also involves management of functional safety, detailing of safety lifecycle activities, recommended content of key SIS documentation, requirements to personnel competence, follow-up of SIS in the operational phase, and what to regard as a sufficient level of independence. The complete minimum SIL requirement from NOG 070 is in Appendix E.

3.2 Mathematical models for determining SIL

Mathematical models are used for a more precise approach using the data coming from multiple sources and with different considerations. These are used to determine the PFD and PFH calculations when systems are more complicated and requires state transitions. These models are either categorized by:

- Formula approximation : IEC standard formula, fault tree model and PDS method;
- State transition model : Markov model and Petri net

3.2.1 IEC formula

The standard IEC 61508 :2010 introduced formulas for acquiring the probability of failure on demand (PFD) and average frequency of dangerous failure (PHF) in order to be applied for SIS subsystems up to three elements. The required data in order to use this method are:

- λ_{DU} - dangerous undetected failure
- λ_{DD} - dangerous detected failure
- λ_{D} - total dangerous failure
- τ - proof test interval
- MTR - mean repair time
- MTTR - mean time to restore

In order to compute the PFD, total dangerous failure λ_D, channel equivalent mean down time (t_{CE}) and system equivalent mean down time (t_{GE}) is computed. They are expressed in the following equations:

$$\lambda_D = \lambda_{DU} + \lambda_{DD} \tag{3.1}$$

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{\tau}{2} + MTR\right) + \frac{\lambda_{DD}}{\lambda_D}(MTTR) \tag{3.2}$$

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{\tau}{3} + MTR\right) + \frac{\lambda_{DD}}{\lambda_D}(MTTR) \tag{3.3}$$

The PDF formula for single system (PFD_{1oo1}) presented in IEC 61508 IS:

$$\boldsymbol{PFD_{1oo1} = \lambda_D t_{CE}} \tag{3.4}$$

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

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

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

$$\boldsymbol{PFH_{1oo1} = \lambda_{DU}} \tag{3.6}$$

The formula presented on this report is only for single element systems and without the consideration of common cause factors. Complete formula of PFD and PFH up to three element systems is reflected in IEC 61508.

3.2.2 Fault tree analysis model

Fault tree analysis (FTA) is a commonly used method for reliability analysis and is suggested in IEC 61508 as a one of approach for SIS reliability analysis. Main elements of fault tree which includes TOP event, gates (and/or/koon), basic events and transfer symbols (triangles). According to Rausand [2014], typical TOP events for a SIS are; the SIF cannot be performed (fail to stop/flow upon demand) and the SIF is activated spuriously (stops the flow when not demanded).

Using the FTA, we may calculate the average PFD by first finding the failure function $Q_O(t)$ for the top event and then calculate the PFD average by the formula:

$$\boldsymbol{PFD_{avg} = \frac{1}{\tau}\int_0^{\tau} Q_0(t)dt} \tag{3.7}$$

Or by the upper bound approximation using the minimal cut sets $(MCSs)^2$ with the formula:

$$\boldsymbol{PFD_{avg} \leq 1 - \prod_{j=0}^{K}(1 - Q_{j,avg})} \tag{3.8}$$

The latter approach is often preferred. The average frequency of dangerous failure PFH is computed using fault tree by considering the elements in the working state. The PFH is calculated using the formula:

$$\boldsymbol{PFH(T) = \frac{1}{T}\int_0^{T} \omega_S(t)dt} \tag{3.9}$$

3.2.3 PDS method

The PDS method is used to quantify the safety unavailability and loss of production for safety instrumented systems (SISs). It implements analytical formula and offers an effective and practical approach towards implementing the quantitative aspects of IEC standards. PDS method is considered to be realistic as it accounts for all major factors affecting reliability during system operation, such as:

- All major failure categories/causes;
- Common cause failures;
- Automatic self-tests;
- Functional (manual) testing;
- Systematic failures;
- Complete safety function;

- Redundancies and voting logic

For a single component, PFD is calculated with the formula:

$$\boldsymbol{PFD_{1oo1} = \lambda_{DU}(\frac{\tau}{2})} \tag{3.10}$$

where:

- τ - period between functional testing, including the unavailability due to undetected failures only;
- λ_{DU} - constant failure rate;
- $\frac{\tau}{2}$ - average period of time that the component is unavailable given that the failure may occur at a random point in time within the test interval τ.

Further, a duplicated module voted 1oo2, considering both common cause failure (CCF) and independent failures, the formula of PDF for both are:

$$PFD_{1oo2}^{(CCF)} = \beta(\lambda_{DU}\frac{\tau}{2}) \tag{3.11}$$

$$PFD_{1oo2}^{(ind.)} = \frac{(\lambda_2\tau)^2}{3} \tag{3.12}$$

Hence, including both the common cause and the contribution from independent failures, the formula for a 1oo2 voted system is:

$$\boldsymbol{PFD_{1oo2} = \beta(\lambda_{DU}\frac{\tau}{2}) + \frac{(\lambda_2\tau)^2}{3}} \tag{3.13}$$

So the formula for any voting logic in the PDS method considering the MooN and ignoring independent failures is:

$$\boldsymbol{PFD_{MooN}^{CCF} = C_{MooN}\beta(\lambda_{DU}\frac{\tau}{2}); (M < N)} \tag{3.14}$$

When getting the PFH for single component system, PDS method uses the same formula as IEC 61508 which is:

$$\boldsymbol{PFH_{1oo1} = \lambda_{DU}} \tag{3.15}$$

Finally, the formula for PFH considering other voting logic and for 1ooN is:

$$\boldsymbol{PFH_{1ooN} = \frac{(\lambda_{DU}\tau)^N}{\tau}} \tag{3.16}$$

3.2.4 Markov model

Markov model is an alternative method for solving PFD and PFH as recommended in IEC 61508. IEC 61508 :2010 says that the method is analytic and straight forward. It is also suitable for multistate and dynamic systems and able to model system sates beyond its failure rates. Markov method can be used to find analytical formulas, calculate steady state and time-dependent probabilities and able to determine MTTFs.
In order to solve PFD and PFH using Markov approach, the following steps are followed:

1. Define the system states.

2. Set up the state transition diagram.

3. Calculate the steady state or time dependent probabilities.

4. Determine PFD or PFH by considering all "jumps" into the dangerous states.

To calculate PFD using Markov method based on time dependent probabilities, we use the formula:

$$\boldsymbol{PFD_{avg} = \frac{1}{\tau}\int_0^{\tau} PFD(t)dt} \tag{3.17}$$

Calculating the PFD for steady state probabilities, we use the formula:

$$\boldsymbol{PFD_{avg} = \sum_{i \epsilon D} P_i} \tag{3.18}$$

To calculate PFH we use the formula:

$$\boldsymbol{PFH(t) = \omega_s(t) = \sum_{i \epsilon M_c} \Lambda_i p_i(t)} \tag{3.19}$$

3.2.5 Petri net

Petri net is another method which PFD and PFH can be calculated. This method can be used for systems with complex behaviours. It is an efficient way of modelling dynamic systems by building a finite sate automaton behaving as close as possible as E/E/PE safety-related systems under study according to IEC 61508 :2010. Petri nets have been proven to be very efficient for this purpose for the following reasons:

- They are easy to handle graphically;

- The size of the models increases linearly according to the number of components to be modelled;

- They are very flexible and allow modelling all types of constraints;

- They are perfect support for Monte Carlo simulation.

It can be used for components which jumps across the states of working, dangerous failed undetected, under testing, dangerously failed detected, ready for repair and under repair. Reflected in Figure 3.6 is a sample Petri net modelling.

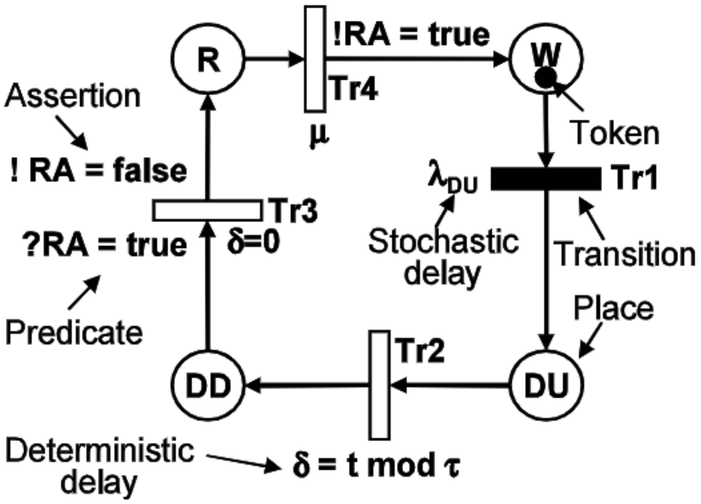


Figure 3.6: **Petri net for Modelling a Single Periodically Tested Component** (IEC 61508 :2010)

Petri nets maybe used directly to evaluate PFDavg of the component because the mean marking of place W (working) which is equal to the ratio of time spent in W (example with W marked token in the figure) to the duration T, is in fact the average availability A of the component. The formulas for getting PFD and PFH as shown in IEC 61508 :2010 are the following:

$$\boldsymbol{PFD_{avg} = 1 - A} \tag{3.20}$$

$$\boldsymbol{PFH(T) = N_{bf}/T} \tag{3.21}$$

where A is the availability, T is the transition duration, and N_{bf} as frequency of the transition failure.

Chapter 4

Functional Safety Analysis of Anti-surge Protection System

The case study is provided by DNV which includes a system description and SIF that needs to be addressed.

4.1 Case study description

The test facility in the K project includes the following major components: a subsea compressor, two parallel air coolers, a de-liquidiser and a liquid separator. The anti-surge and pressure control valve (PV-0014) lies between the air coolers and de-liquidiser, and a liquid separator. Figure 4.1 depicts these components of concern in a simplified diagram.

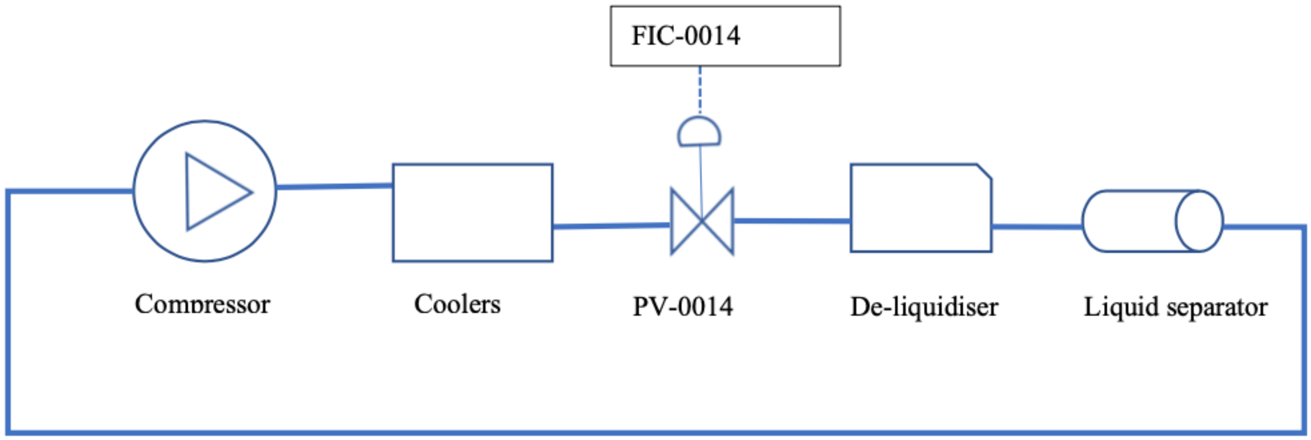


Figure 4.1: **Illustrative Diagram of the Components** (DNV)

Controller FIC-0014 controls the anti-surge valve (PV-0014) based on the following inputs:

- PDT-0007A - pressure difference over multi-phase meter, indicative of flow through compressor.
- PT-0008A - pressure at compressor inlet.
- PT-0009A - temperature at compressor inlet.
- PT-0010A - pressure at compressor outlet.
- PT-0011A - temperature at compressor outlet.
- ZT-0014 - position of anti-surge 334-PV-0014.

Note that PV-0031 needs to be opened simultaneously with the anti-surge valve (PV-0014), and is therefore one of the final elements of the safety instrumented function.

The anti-surge functionality is implemented and it measures the inlet flow, inlet pressure and outlet pressure to compare the operation point with the compressor map. If surge is detected, then 1 is added to surge counter and the anti-surge controller will open the anti-surge valve. If the compressor is staying in surge then the surge counter is increased with 1 for every 5 seconds (default). When the surge counter reaches 3 (default) then the compressor trips. This functionality is always verified (tuned) before the compressor can be released for unsupervised operation.

The purpose of the integrated anti-surge control system in the test loop is to prevent flow reversal that occurs in the compressor when operating below a certain flow rate and above a certain compression level. The reverse flow through the compressor may cause damage to the compressor.

Apart from the anti-surge protection, other functionalities protecting the compressor are identified, including:

- A PSD function is actuated when flow below LL is measured by flow indicator FI-0007.
- The HazOp report considers a deviation ’Higher pressure than 90 barg’. The relevant protection functions are PSD actuated at downstream PI-0043 HH, and PSV-0013.

4.1.1 System process

The closed test loop consists of a compressor, a gas cooler, a de-liquidiser, a liquid separator and a static mixer. The gas will be compressed by the compressor and will enter into the gas cooler installed downstream of the compressor discharge. After the gas is cooled, the stream pressure is reduced by pressure reduction valve installed downstream of the cooler. The 2-phase fluid then enters into a de-liquidiser where gas and liquid are separated. The separated liquid then enters into liquid-liquid separator where 2-liquid phases are separated out. The flow of two liquid phases will be measured and controlled by the flow meter and control valves installed downstream of the liquid-liquid separator. The gas from de-liquidiser and liquid stream from liquid-liquid separator will be mixed in a static mixer before entering the compressor suction again. A multi-phase flow meter is installed in the suction line of the compressor to measure the flow rates of the suction stream. The pressure in the loop will be controlled by the combined anti-surge/pressure reduction valve installed downstream of the cooler.

4.1.2 Case study SIF

It is known that the mentioned compression system with existing SIS have the disadvantage of being slow and do not prevent immediate damage to the compressor. These functions however help in reducing the probability of the damage to the compressor which is just not enough. In order to improve the condition, safety instrumented function is created for the specific purpose. The safety instrumented function is:

"The anti-surge functionality does not react quickly enough to prevent the compressor from surging and from subsequent damage."

The anti-surge functionality includes the internal functionality in the compressor package and the external functionality controlling the anti-surge valve as described above. How the internal and external functionality together realize the required AIL (asset integrity level) is not part of this report.

4.1.3 Case study conditions, limitations and assumptions

In order to conduct a more realistic functional safety analysis, assumptions are made. There are also limitations on the study due to lack of information and some certain conditions to be met. These are the following:

- The case study, though performed in a test facility, is assumed to be commissioned in an actual subsea environment;

- It is assumed in the analysis that the compressor system in which the anti-surge is used, have an upstream and downstream facilities connected, though not reflected on the diagrams;

- The test loop as mentioned in the case study is assumed as the environment of the compressor system which includes anti-surge system;

- The existing SIF of the given anti-surge system is assumed to be 'pressure recovery function from compressor discharge line to compressor suction line'.
- No instrument name is given to the pressure transmitter controlling PV-0031, it is named PT-0013A on this case study;
- No HRA reports are provided, so hazards are identified through certain standards and articles related to the case study;
- No parameters are given to the author, unless otherwise stated, they are only assumptions. Component data are based on the author's research and study;
- The functional safety analysis is based on the steps from safety life-cycle reflected in Figure 2.3 and is only until safety requirement specification (SRS) stage.

4.2 Concept and overall scope definition

Though the SIF is already given on the case study, the functional safety analysis on this paper still starts with a clear understanding of the compressor system. It is of great importance to understand the concept and overall scope definition of the system. Figure 2.3 shows that it is the first step in a safety life-cycle of a system.

4.2.1 Concept

This section presents a thorough familiarity of the equipment under control (EUC), which is the subsea compressor, its required control functions and physical environment. Undesirable events and its causes are presented to give the general idea of the system conditions.

The subsea compressor in the case study is assumed to be a dry gas sealed compressor which is generally non-contacting, dry running face seals, mainly used in high speed applications. Applicable standards for this specific type of compressor is API 617 and NS-EN ISO 10439-1:2015. Requirements for designing and manufacturing a compressor is not discussed on this paper but rather the required control functions of the compressor on the system.

Control function

Based on the given inputs from the system description, these are the control functions applicable to the EUC:

- It should be able to handle hydrocarbons, mainly gases from the upstream;
- It cannot tolerate too low gas flow;

- It should not allow flow reversal;
- It cannot tolerate low/high temperature;
- It cannot be operated if the pressure downstream is too high;
- It is assumed to withstand maximum pressure but should not feed downstream with the same pressure in case of blockage;
- It cannot be operated when discharge pressure is lower than suction pressure;
- A shutdown system is required to protect downstream equipment;
- It should not operate during abnormal conditions.

The control function requirements enumerated above are the EUC's functions that should be maintained in order to have a normal operation. Based on the SIF of the case study, the existing SIS architecture does not react quickly enough to prevent the compressor from surging and from subsequent damage, which means that an improvement is necessary to the system. Surging relates to the multiple control functions mentioned. It is the main focus of this functional safety analysis.

Physical environment

The compressor is not a stand alone equipment and cannot function on its own. It is mainly composed of a compressor unit, control system and driver which is the motor. It requires support from other equipment and instruments for it to be able to fulfill its duty.

Figure 4.2 shows the inclusion of the existing SIS architecture based on the given illustrative diagram of the system in the case study. The diagram shows the overall physical environment of the compression system including coolers, de-liquidiser, liquid separator and the EUC which is the compressor with its safety devices. Based on the diagram reflected in Figure 4.2, flow indicator controller (FIC-0014) receives all the signals coming from the instruments and automatically send signal to PV-0014 (anti-surge valve) to control the flow in the loop. Components are flow indicator, pressure transmitters, temperature transmitters, logic solver, anti-surge valve and pressure control valve. It is not reflected on the diagram, but PT-0012A is the one controlling PV-0031. The diagram also shows that two SISs are present.

The next section discusses the equipment and instruments which is part of the physical environment of the compressor. How it affects the overall performance of the compression system is explained in detail. A more detailed introduction to the EUC and the compression system is presented first.

The compressor

Compressors in oil and gas are mechanical devices which reduce the volume of a gas in a bid to increase its pressure. These equipment are used during the initial treatment of crude oil before the gas is transported through pipelines, supply chain and to the final consumers. Subsea compressors are remotely operated, much safer and produces low carbon footprint.

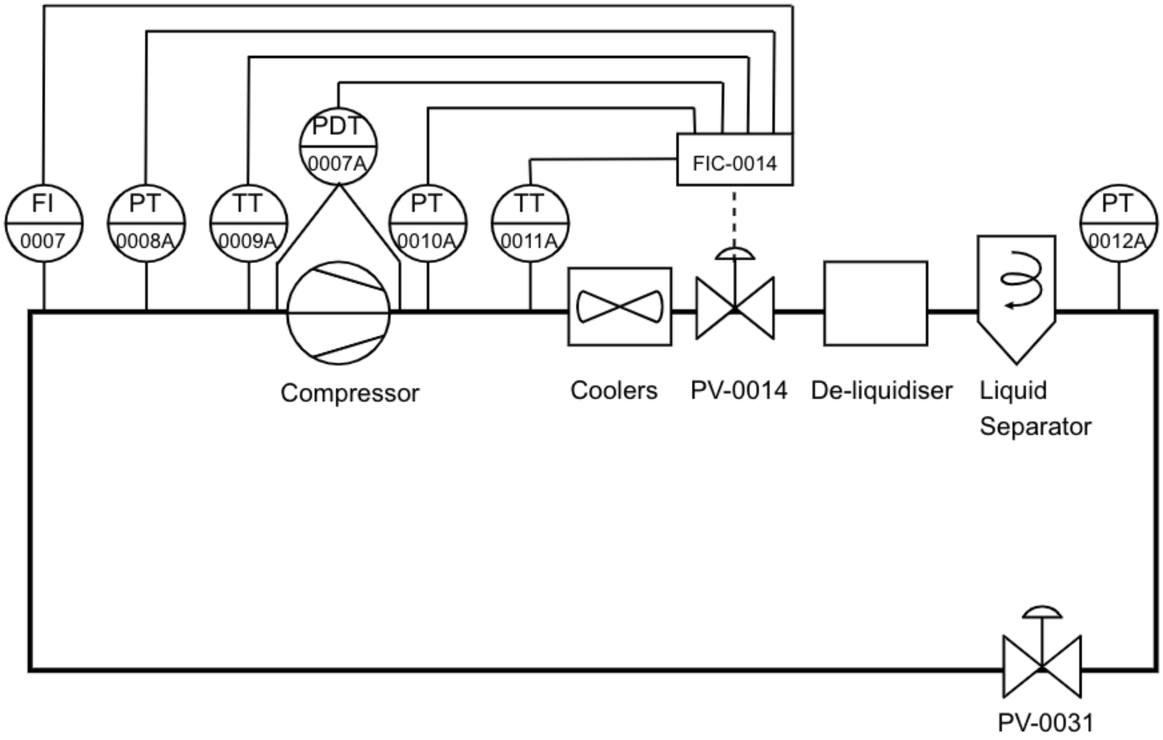


Figure 4.2: **Illustrative Diagram of the Components with SIS Architecture**

The compressor used in the case study is HOFIM or High-Speed Oil-Free Integrated Motor which features high-speed induction motor coupled with the barrel type compressor and active magnetic bearings. The unit is hermetically sealed and fully encapsulated, providing the highest possible level of safety. The magnetically-levitated system ensures highest reliability and availability. The motor has a compression power of 11.5MW and discharge pressure up to 3,190 psi [MAN] . The compressor itself has a system with high reliability based on the tests conducted by the manufacturer. Due to data unavailability, internal safety system of the compressor is not discussed on this paper. Internal functions that are discussed on this paper are assumptions based on existing compressor knowledge.

Safety-related instruments and equipment

- Flow Instruments - instruments which helps to control and regulate the flow of gas in the compressor. It includes transmitters and logic controllers. The flow transmitters monitors the flow of gas entering the compressor and sends signal to the associated controller if the flow rate exceeds certain set limits. These signals are usually referred to as alarms. The controllers then send signal to the associated valve and the valve actuates if the set limits (high or low alarms) are reached. On this case study, a PSD (Process Shutdown) valve is actuated when flow below LL is measured by the flow indicator FI-0007. FI-0007 is also assumed to be used as one of the inputs for the anti-surge valve to monitor surging. It is an important input because flow change is one of the indicator of a surge;

- Temperature Instruments - instruments which help to control and regulate the temperature of the gas flowing through the compressor. It includes temperature transmitter and logic controllers. The temperature transmitters monitor the temperature of the gas entering and leaving the compressor and sends signal to associated controller if the temperature is not within the certain limits. These signals are usually referred to as alarms. The controller will then send signal to the associated valve and the valve actuates if the set limits (high or low alarms) are reached. On this case study, there are two temperature transmitters; TT-0009A and TT-0011, located on the compressor inlet and outlet. These are connected to FIC-0014 which controls the anti-surge valve (PV-0014). Temperatures arise rapidly during surge so temperature inputs are of great importance;

- Pressure Instruments - instruments which help control and regulate the pressure of gas in the compressor. It includes pressure transmitters and logic controllers. The pressure transmitter monitors the pressure of the gas entering and leaving the compressor and will send a signal to the associated controller if the pressure is not within the certain set limits. The controller will then send signal to the associated valve and the valve actuates if the set limits (high or low alarms) are reached. On this case study, there are three pressure transmitters; PT-0008A, PT-0010 and PT-0012A. Two are located on the compressor inlet and outlet and the other one is after liquid separator. PT-0008A and PT-0010 are connected to FIC-0014 which controls the anti-surge valve (PV-0014) and PT-0012A is connected to a logic control and control PV-0031. A differential pressure transmitter PDT-0007A, is also included and indicates pressure difference over multi-phase meter, indicative of flow through compressor;

- Valves - Comes in the variants of control valves, pressure valves, flow and temperature. The controller receives the pressure signals from the sensor, compares them with pressure drop or rise for the desired flow and if the actual flow is different, adjusts the control valve to increase or decrease the flow. It can also be temperature and flow signal that is sent to the logic controller and actuates the valve. On this case study, anti-surge and pressure control valve is used and will be the main focus. PV-0014 lies between the coolers and de-liquidiser. The anti-surge valve is being controlled FIC-0014 controller. Based on the conditions given on the case study description, both valves opens simultaneously when it is required.

Non safety-related instruments and equipment

- Coolers - it increases the compressor efficiency by reducing the inlet temperature and gas volume rate to the compressor. It also increases the overall compression station efficiency by promoting gas condensation whereby a larger fraction of the flow can be pumped instead of compressed. It also prevents hydrate by reducing water content in the gas by reducing the temperature;

- De-liquidiser - it is an inline, cyclonic separator with the purpose of extracting liquid droplets from a gas dominated stream to produce a single-phase gas flow. The liquid reject is degassed by gravity separation in a degassing boot. Due to its compactness, the de-liquidiser is a very effective solution for applications where a limited space is available or where space and weight reductions are key parameters;

- Liquid separator - it separates gas and liquid so that the fluids can be treated separately. This is done in cyclones at the inlet of gravity separators or vertical gravity separator. A scrubber is a type of separator which main function is to prepare the gas for compression. It is used when there are small amounts of liquid;

- Static mixer - it plays an important in process such as stream blending, additive mixing, liquid dispersion, emulsion formation, chemical reactors, laminar-flow heat transfer and mass transfer. It provides highly efficient mixing with no moving parts and are therefore maintenance free.

4.2.2 Overall scope definition

The EUC is bounded within the compressor itself, its motor, its own control system and the safety system protecting it. Due to data unavailability, the compressor's own control system is disregarded and focus of the analysis is on the safety control system within its environment, which is specifically the anti-surge protection.

Anti-surge system involves both internal and external functionality of the compressor but the analysis is only within the external functionality. Internal functionality such as vibration monitoring or flow control inside the compressor are not discussed. Equipment such as coolers, de-liquidiser and liquid separator are all considered outside the boundary, though they also create and impact on the overall system operation. As presented in the case study, anti-surge safety system includes flow, pressure, temperature, controller and valve with an additional component such as pressure transmitter and pressure control valve after liquid separator. These components are all located externally from the compressor.

4.3 Hazard and risk assessment

After discussing the concept, identifying the required control functions, physical environment of the EUC and finally elaborating the overall scope definition, hazard and risk assessment is presented. Hazard and risk analysis is the third step based on the overall safety life-cycle reflected in Figure 2.3 from IEC 61508 standard but it's the first step of a SIS safety life-cycle according to IEC 61511.

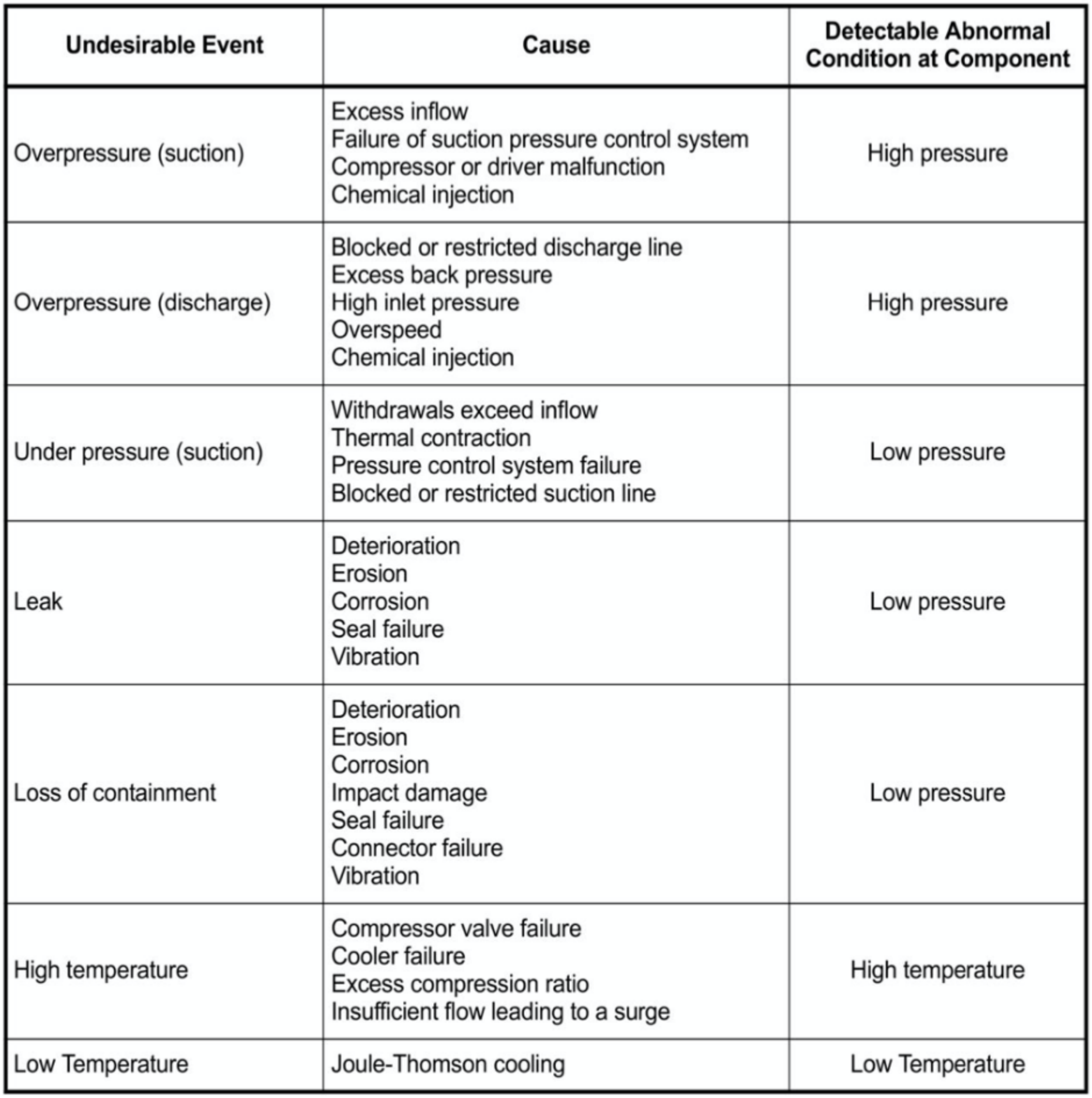
Even though the SIF are already given on the case study, it is still important to do the HRA to conduct a thorough functional safety analysis. The purpose of HRA on this report is to present the overall view of the hazard and hazardous events of the process and associated equipment. It also presents the risks associated to the hazardous event, the requirements for risk reduction and the safety functions required to achieve the risk reduction. At the end of the HRA, the hazard and hazardous event related to the given SIF is presented.

The compressor system is assumed to be commissioned in a subsea environment, therefore all the risks from hazards identified on the EUC is related to this environment. As mentioned in subsection 4.1.3, there are no HRA reports provided along with the case study, therefore, HRA from relevant standards are utilized. Figure 4.3 reflects the typical subsea compressor undesirable events, its causes and the abnormal condition detectable at the component. The safety analysis table is from recommended practice (RP) released by the American Petroleum Institute (API), which based the entries from their long experience on this field. The RP has also released the safety functions required in order to achieve reduction of the risks associated to undesirable events mentioned in the safety analysis table. Safety functions are reflected in Figure 4.4.

The safety analysis table and checklist presented in the RP reference have a process-level approach which is the usual HRA approach. Kim et al. [2018] on their article presented a system level approach for accidents, hazards and safety constraints related to subsea gas compression. The inputs shown in Table 4.1 has a different strategy but can be useful when impact events are identified, like the one used in LOPA.

Based on the safety analysis table reflected in Figure 4.3, under pressure (suction) is identified as the undesirable event that would require the SIF *'the anti-surge functionality does not react quickly enough to prevent compressor from surging and subsequent damage'* . The given

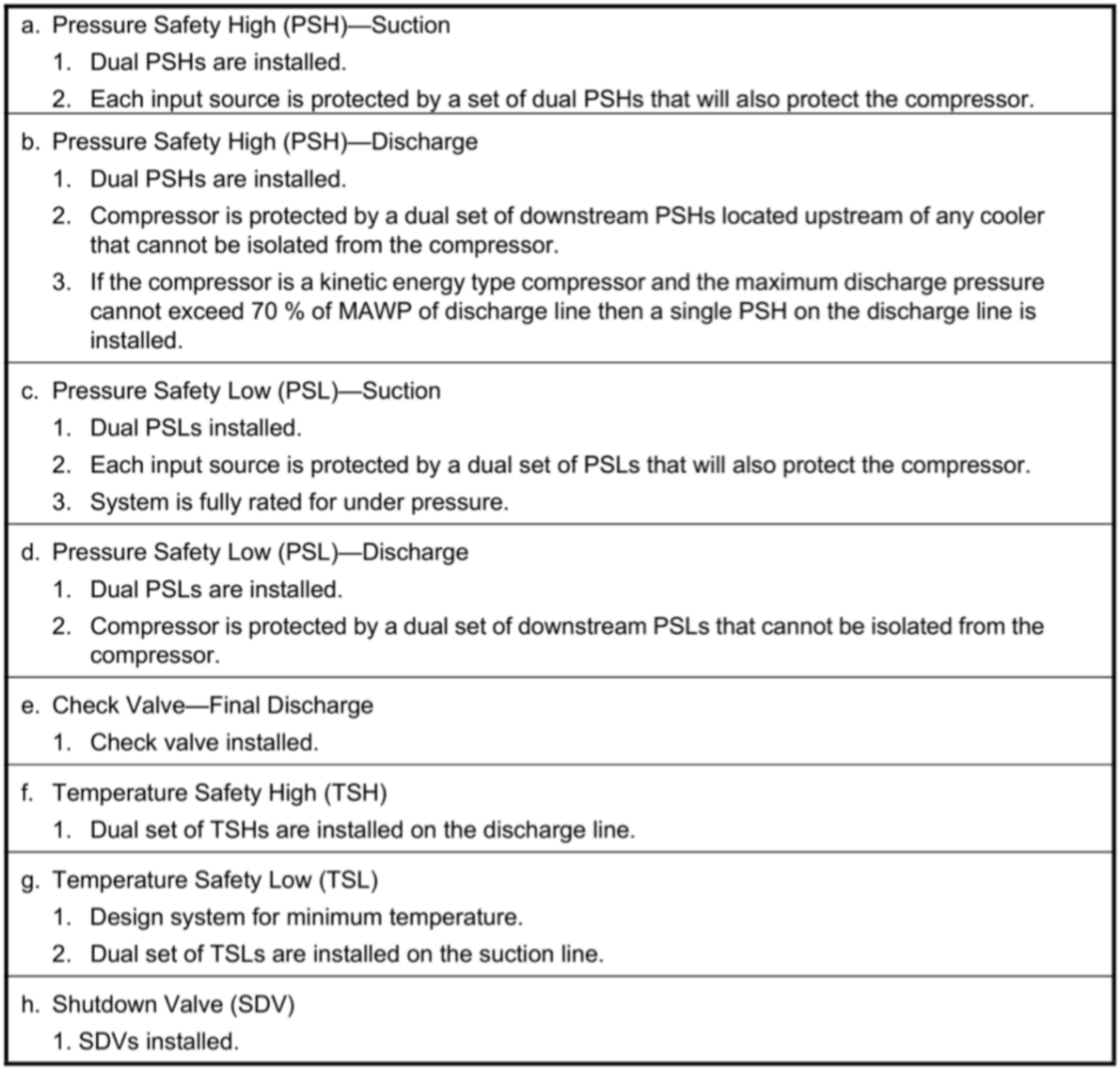
SIF on the case study which is mentioned on the previous statement is related to existing SIF stated in subsection 4.1.3. Both of them aims to maintain the normal flow of the compressor by supplying pressure from the discharge line to suction during the undesirable event 'suction under pressure'. Under pressure is caused by thermal contraction, pressure control system failure, blocked or restricted suction line and the withdrawals exceed inflow. The hazardous event is surging which can cause mechanical damage to the compressor, rise in temperature, loud noise due to vibration and others.



Undesirable Event	Cause	Detectable Abnormal Condition at Component
Overpressure (suction)	Excess inflow Failure of suction pressure control system Compressor or driver malfunction Chemical injection	High pressure
Overpressure (discharge)	Blocked or restricted discharge line Excess back pressure High inlet pressure Overspeed Chemical injection	High pressure
Under pressure (suction)	Withdrawals exceed inflow Thermal contraction Pressure control system failure Blocked or restricted suction line	Low pressure
Leak	Deterioration Erosion Corrosion Seal failure Vibration	Low pressure
Loss of containment	Deterioration Erosion Corrosion Impact damage Seal failure Connector failure Vibration	Low pressure
High temperature	Compressor valve failure Cooler failure Excess compression ratio Insufficient flow leading to a surge	High temperature
Low Temperature	Joule-Thomson cooling	Low Temperature

Figure 4.3: **Safety Analysis Table** (API RP 17V:2015)

This will further lead to impact events such as release of gas to the environment, sea pollution, damage of valuable components and reduced productivity. Safety functions specific to hazardous event such surging are complied by the existing SISs in the case study given and are almost identical to overall recommended safety devices that should be included in designing a subsea compression system that is reflected in Figure 4.4.



a. Pressure Safety High (PSH)—Suction
   1. Dual PSHs are installed.
   2. Each input source is protected by a set of dual PSHs that will also protect the compressor.

b. Pressure Safety High (PSH)—Discharge
   1. Dual PSHs are installed.
   2. Compressor is protected by a dual set of downstream PSHs located upstream of any cooler that cannot be isolated from the compressor.
   3. If the compressor is a kinetic energy type compressor and the maximum discharge pressure cannot exceed 70 % of MAWP of discharge line then a single PSH on the discharge line is installed.

c. Pressure Safety Low (PSL)—Suction
   1. Dual PSLs installed.
   2. Each input source is protected by a dual set of PSLs that will also protect the compressor.
   3. System is fully rated for under pressure.

d. Pressure Safety Low (PSL)—Discharge
   1. Dual PSLs are installed.
   2. Compressor is protected by a dual set of downstream PSLs that cannot be isolated from the compressor.

e. Check Valve—Final Discharge
   1. Check valve installed.

f. Temperature Safety High (TSH)
   1. Dual set of TSHs are installed on the discharge line.

g. Temperature Safety Low (TSL)
   1. Design system for minimum temperature.
   2. Dual set of TSLs are installed on the suction line.

h. Shutdown Valve (SDV)
   1. SDVs installed.

Figure 4.4: **Safety Analysis Checklist** (API RP 17V:2015)

Based on the safety analysis table reflected above, the system in the case study have all the required instruments for a subsea compression system. The current SIS architecture fell short to comply with the desired operating results as mentioned on the SIF which means additional SIS is assumed to be required to satisfy the safety function.

Table 4.1: **System level accidents, hazards and safety constraints** (Kim et al. [2018])

System-level accident	System-level hazard	System-level safety constraints
People die or are injured due to large amount of gas release	Subsea gas compressor continues to supply gas when gas leaks to the environment	Subsea gas compressor must stop compressing gas when gas leaks to the environment
The sea is polluted due to large amount of gas release		
Valuable subsea components are damaged	Compressor operates outside normal operations conditions	Compressor must be protected from extreme operating conditions that can damage the compressor
Production is reduced or interrupted unnecessarily	Compressor unit stops compressing gas when not necessary	Compressor unit must never stop compressing gas when not necessary
	Compressor operates outside optimal conditions	Compressor must be operated within optimal conditions.

4.4 Allocation of safety functions to protection layers

After identifying the specific hazard and the risks associated to the EUC, safety function is then developed. This is an important stage of functional safety analysis as it identifies whether a SIF is required to comply with the safety function of a specific hazardous event. SIF should be the last option when all other non-instrumented safety functions cannot satisfy the safety requirement.

Due to the availability of the SIF in the case study, it can be assumed that a SIS is required. Though this might be true, it also possible that a SIS handles two or more SIF. Thorough analysis is conducted on this section using standard concepts.

In order to find out whether additional SIS is required from the given SIF, two steps are conducted on the analysis. First, safety integrity levels of the existing SIS is identified using the IEC 61508 and PDS method formulas. After identifying the SILs, LOPA is performed in order to verify whether the protection layers specific for intermediate event likelihood related to surging, is lower compared to its tolerable mitigated event likelihood. If in case it is higher, then an additional SIS is recommended.

4.4.1 SIL identification using IEC 61508

Before conducting the SIL identification, SIF is introduced. It is mentioned on the case description that the existing anti-surge control system is integrated. It means that both of the SIS are considered in the computation. The SISs has a common SIF. Because it is not given, the assumed SIF for the existing anti-surge system is *'pressure recovery function from compressor discharge line to compressor suction line'*.

In order to proceed with SIL identification using IEC 61508 formulas, equipment data is required. Due to the unavailability of data for subsea equipment, topside equipment data are used in the study. Exida certificates are used because it provides detailed information that is needed in order to compute the PFD. The data for the sensor is reflected in Figure 4.5, logic solver in Figure 4.6 and the final element in Figure 4.7. The complete SIL certificates for the equipment is found in Appendix F.

To start the SIL identification, it should be noted that two SISs are computed. One with the anti-surge system (SIS-1), and the other as pressure control system (SIS-2). After identifying SILs of the SISs, it will be combined using the PDS method for multiple SISs.

Both low demand and high demand mode is considered for the computation of the existing SISs. Anti-surge system demand is not known, at least based on research by the author, because subsea compression system does not have much data to base on. The first subsea compression system was commissioned in 2015 with anti-surge system similar to the given case study. The author has no access to the data so considering both demands is the best option.

SIS-1 computation - anti-surge control

SIS-1 is composed of components such as: sensors (two pressure transmitters, one flow indicator and one differential pressure transmitter (2oo4)), one logic controller (1oo1) and anti-surge control valve (1oo1). 2oo4 voting logic is used for the sensor which means that two sensors are required to send alarm signals in order for the anti-surge valve to take action. Sensor parameters for anti-surge valve such as flow rate, differential pressure and linear pressures are very sensitive to surge. It is also assumed that the sensors have identical features so data are similar. The chosen sensor can be used as flow, differential pressure and linear pressure. IEC 61508 method is used for PFD and PDS method is used for calculating PFH. Temperature sensor is neglected due to its difference in specifications.

PFDavg computation

In order to compute the PFDavg of anti-surge control system, individual PFDavg of the components are required to be computed and totalled. The working formula for the PFDAvg is:

$$\boldsymbol{PFD_{avg} = PFD_{avg,sensor} + PFD_{avg,logic} + PFD_{avg,valve}} \tag{4.1}$$

PFD_{avg} for the sensor:
Getting the $PFD_{avg,sensor}$ with 2oo4 voting logic and CCF consideration, we use the formula:

$$\boldsymbol{PFD_{avg,s} = PFD_{avg}^{ind} + PFD_{avg}^{CCF}} \tag{4.2}$$

$$\boldsymbol{PFD_{avg,s} = \left[24\lambda_D{}^3 t_{CE} t_{G2E} t_{GE}\right] + \left[\beta\lambda_{DU}(\frac{\tau}{2} + MTR) + \beta_D\lambda_{DD}MTTR\right]} \tag{4.3}$$

where:

$$\lambda_D = (1-\beta)\lambda_{DU} + (1-\beta_D)\lambda_{DD} \tag{4.4}$$

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{\tau}{2} + MTR\right) + \frac{\lambda_{DD}}{\lambda_D}(MTTR) \tag{4.5}$$

$$t_{G2E} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{\tau}{3} + MTR\right) + \frac{\lambda_{DD}}{\lambda_D}(MTTR) \tag{4.6}$$

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{\tau}{4} + MTR\right) + \frac{\lambda_{DD}}{\lambda_D}(MTTR) \tag{4.7}$$

Getting the values from the sensor data and beta factor from PDS method handbook, we have:
Given:

$$\lambda_{DU} = 34 \times 10^{-9} \qquad \tau = 12 months \qquad \beta = 7\%$$
$$\lambda_{DD} = 685 \times 10^{-9} \qquad MTR = 10 days \qquad \beta_D = 5\%$$
$$\lambda_{SU} = 6 \times 10^{-9} \qquad MTTR = 40 days$$

Solution: To get λ_D:

$$\lambda_D = (1-\beta)\lambda_{DU} + (1-\beta_D)\lambda_{DD}$$
$$\lambda_D = \left(1-0.07)(34 \times 10^{-9}\right) + \left(1-0.05)(685 \times 10^{-9}\right)$$
$$\lambda_D = 6.82 \times 10^{-7}$$

For t_{CE}:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{\tau}{2} + MTR\right) + \frac{\lambda_{DD}}{\lambda_D}(MTTR)$$
$$t_{CE} = \frac{34 \times 10^{-9}}{6.82 \times 10^{-7}}\left(\frac{8640}{2} + 240\right) + \frac{685 \times 10^{-9}}{6.82 \times 10^{-7}}(960)$$
$$t_{CE} = 1192 hours$$

For t_{G2E}:

$$t_{G2E} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{\tau}{3} + MTR\right) + \frac{\lambda_{DD}}{\lambda_D}(MTTR)$$
$$t_{G2E} = \frac{34 \times 10^{-9}}{6.82 \times 10^{-7}}\left(\frac{8640}{3} + 240\right) + \frac{685 \times 10^{-9}}{6.82 \times 10^{-7}}(960)$$
$$t_{G2E} = 1118 hours$$

For t_{GE}:

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{\tau}{4} + MTR\right) + \frac{\lambda_{DD}}{\lambda_D}(MTTR)$$
$$t_{GE} = \frac{34 \times 10^{-9}}{6.82 \times 10^{-7}}\left(\frac{8640}{3} + 240\right) + \frac{685 \times 10^{-9}}{6.82 \times 10^{-7}}(960)$$
$$t_{GE} = 1084 hours$$

For PFD_{avg}^{CCF}:

$$PFD_{avg}^{CCF} = \beta\lambda_{DU}(\frac{\tau}{2} + MTR) + \beta_D\lambda_{DD}MTTR$$
$$PFD_{avg}^{CCF} = \left(0.07\right)(34 \times 10^{-9}\right)\left(\frac{8640}{2} + 240\right) + \left(0.05\right)(685 \times 10^{-9}\right)(960)$$
$$PFD_{avg}^{CCF} = 4.373 \times 10^{-5}$$

Therefore:

$$PFD_{avg,s} = PFD_{avg}^{ind} + PFD_{avg}^{CCF}$$
$$PFD_{avg,s} = \left[24{\lambda_D}^3 t_{CE} t_{G2E} t_{GE}\right] + \left[\beta\lambda_{DU}(\frac{\tau}{2} + MTR) + \beta_D\lambda_{DD}MTTR\right]$$
$$PFD_{avg,s} = \left[24(6.82 \times 10^{-7})^3 \times 1192 \times 1118 \times 1084\right] + (4.373 \times 10^{-5})$$
$$\boldsymbol{PFD_{avg,s} = 1.11 \times 10^{-8}}$$

PFD_{avg} for the logic solver:
Getting the $PFD_{avg,logic}$ in Equation 4.1 with 1oo1 voting logic, we use the formula:

$$\boldsymbol{PFD_{avg,l} = \lambda_D t_{CE}}$$

Getting the values from logic solver, we have:
Given:

$$\lambda_{DU} = 3 \times 10^{-9} \qquad \tau = 5years$$
$$\lambda_{DD} = 932 \times 10^{-9} \qquad MTR = 10days$$
$$\lambda_{SU} = 11 \times 10^{-9} \qquad MTTR = 40days$$

Solution: To get λ_D:

$$\lambda_D = (\lambda_{DU}) + (\lambda_{DD})$$
$$\lambda_D = \left(3.9 \times 10^{-9}\right) + \left(932 \times 10^{-9}\right)$$
$$\lambda_D = 9.35 \times 10^{-7}$$

For t_{CE}:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{\tau}{2} + MTR\right) + \frac{\lambda_{DD}}{\lambda_D}(MTTR)$$
$$t_{CE} = \frac{3.9 \times 10^{-9}}{9.35 \times 10^{-7}}\left(\frac{43200}{2} + 240\right) + \frac{932 \times 10^{-9}}{9.35 \times 10^{-7}}(960)$$
$$t_{CE} = 1048hours$$

Therefore:

$$PFD_{avg,l} = \lambda_D t_{CE}$$
$$PFD_{avg,l} = (79.35 \times 10^{-7}) \times 1048$$
$$\boldsymbol{PFD_{avg,l} = 9.8 \times 10^{-4}}$$

PFD_{avg} for the valve:
Getting the $PFD_{avg,valve}$ in Equation 4.1 with 1oo1 voting logic, we use the formula:

$$\boldsymbol{PFD_{avg,v} = \lambda_D t_{CE}}$$

Getting the values from valve data, we have:

Given:

$$\begin{aligned} \lambda_{DU} &= 622 \times 10^{-9} & \tau &= 12 months \\ \lambda_{DD} &= 447 \times 10^{-9} & MTR &= 10 days \\ \lambda_{SU} &= 0 & MTTR &= 40 days \end{aligned}$$

Solution: To get λ_D:

$$\lambda_D = (\lambda_{DU}) + (\lambda_{DD})$$
$$\lambda_D = \left(622 \times 10^{-9}\right) + \left(447 \times 10^{-9}\right)$$
$$\lambda_D = 1.07 \times 10^{-6}$$

For t_{CE}:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{\tau}{2} + MTR\right) + \frac{\lambda_{DD}}{\lambda_D}(MTTR)$$
$$t_{CE} = \frac{622 \times 10^{-9}}{1.07 \times 10^{-6}}\left(\frac{8640}{2} + 240\right) + \frac{447 \times 10^{-9}}{1.07 \times 10^{-6}}(960)$$
$$t_{CE} = 3087 hours$$

Therefore:

$$PFD_{avg,v} = \lambda_D t_{CE}$$
$$PFD_{avg,v} = (1.07 \times 10^{-6}) \times 3087$$
$$\boldsymbol{PFD_{avg,v} = 3.3 \times 10^{-3}}$$

Results:

After getting the individual PFD_{avg} of the components, we use Equation 4.1 to get the total PFD_{avg} of SIS-1 for anti-surge control.

$$\boldsymbol{PFD_{avg} = PFD_{avg,sensor} + PFD_{avg,logic} + PFD_{avg,valve}}$$

Where:

$$PFD_{avg,sensor} = 1.11 \times 10^{-8}$$
$$PFD_{avg,logic} = 9.8 \times 10^{-4}$$
$$PFD_{avg,valve} = 3.3 \times 10^{-3}$$

So:

$$PFD_{avg} = (1.11 \times 10^{-8}) + (9.8 \times 10^{-4}) + (3.3 \times 10^{-3})$$
$$\boldsymbol{PFD_{avg,system} = 4.28 \times 10^{-3}}$$

Results:

Based on the acquired result of $PFD_{avg,system} = 4.28 \times 10^{-3}$, the existing anti-surge control SIS has an integrity value within the quantitative range of SIL 2 with reference to the low demand mode classification from Table 2.1.

PFH computation

In order to compute the PFH of the SIS-1 or anti-surge control, individual PFH of the components are required to be computed and totalled. It is assumed in high demand mode that the safety system puts the EUC into a safe state on detection of any failure. The working formula for the total PFH of the system using PDS method:

$$\boldsymbol{PFH_{sys} = PFH_{sensor} + PFH_{logic} + PFH_{valve}} \tag{4.8}$$

For individual components:

$$\boldsymbol{PFH_{comp} = \lambda_{DU}} \tag{4.9}$$

For components with voting logic of MooN:

$$\boldsymbol{PFH_{MooN} = C_{MooN}\beta\lambda_{DU} + \frac{N!}{(N-M+1)!}(\lambda_{DU}\tau)^{N-M+1}/\tau} \tag{4.10}$$

where λ_{DU} is only considered because it is assumed that there is only one failure that will occur during the magnitude of proof test.

Solution:

PFH_{comp} for the sensor:

Getting the PFH_{MooN} in Equation 4.10 with 2oo4 voting logic, we use the formula:

$$\boldsymbol{PFH_{MooN} = C_{MooN}\beta\lambda_{DU} + \frac{N!}{(N-M+1)!}(\lambda_{DU}\tau)^{N-M+1}/\tau}$$

Getting the values from the pressure transmitter data, we have:
Given:

$$\lambda_{DU} = 34 \times 10^{-9} \qquad \tau = 12 months$$
$$\lambda_{DD} = 685 \times 10^{-9} \qquad MTR = 10 days$$
$$\lambda_{SU} = 6 \times 10^{-9} \qquad MTTR = 40 days$$
$$C_{MooN}\beta = 1.1$$

Solution:
Using direct substitution of the values to the Equation 4.10, we get:

$$PFH_{2oo4} = 1.1(3.4 \times 10^{-9}) + 4\frac{(3.4 \times 10^{-9}.8640)^3}{8640}$$

$$\boldsymbol{PFH_{2oo4} = 3.74 \times 10^{-9}}$$

Gathering the data of sensor with 2oo4 logic and logic solver and valve with individual components, we get the following values:

$$PFH_{sensor} = 3.74 \times 10^{-9}$$
$$PFH_{logic} = 3 \times 10^{-9}$$
$$PFH_{valve} = 622 \times 10^{-9}$$

So:

$$PFH_{sys} = (3.74 \times 10^{-9}) + (3 \times 10^{-9}) + (622 \times 10^{-9})$$
$$\boldsymbol{PFH_{sys} = 6.28 \times 10^{-7}}$$

Results:
Based on the acquired result of $PFH_{sys} = 6.28 \times 10^{-7}$, SIS-1 integrity value is within the quantitative range of SIL 2, with reference to the high demand mode classification from Table 2.2.

SIS-2 computation - Pressure control

SIS-2 is composed of components such as: one pressure transmitter (1oo1), one logic solver (1oo1) and one pressure control valve (1oo1). IEC 61508 method is used.

PFDavg computation

In order to compute the PFDavg of the pressure control system, individual PFDavg of the components are required to be computed and totalled. The working formula for the PFDAvg is:

$$\boldsymbol{PFD_{avg} = PFD_{avg,sensor} + PFD_{avg,logic} + PFD_{avg,valve}} \tag{4.11}$$

PFD_{avg} for the sensor:
Getting the $PFD_{avg,sensor}$ in Equation 4.11 with 1oo1 voting logic, we use the formula:

$$\boldsymbol{PFD_{avg,s} = \lambda_D t_{CE}}$$

where:

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

Getting the values from the pressure transmitter data, we have:

Given:

$$\lambda_{DU} = 34 \times 10^{-9} \qquad \tau = 12 months$$
$$\lambda_{DD} = 685 \times 10^{-9} \qquad MTR = 10 days$$
$$\lambda_{SU} = 6 \times 10^{-9} \qquad MTTR = 40 days$$

Solution: To get λ_D:

$$\lambda_D = (\lambda_{DU}) + (\lambda_{DD})$$
$$\lambda_D = \left(34 \times 10^{-9}\right) + \left(685 \times 10^{-9}\right)$$
$$\lambda_D = 7.19 \times 10^{-7}$$

For t_{CE}:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{\tau}{2} + MTR\right) + \frac{\lambda_{DD}}{\lambda_D}(MTTR)$$
$$t_{CE} = \frac{34 \times 10^{-9}}{7.19 \times 10^{-7}}\left(\frac{8640}{2} + 240\right) + \frac{685 \times 10^{-9}}{7.19 \times 10^{-7}}(960)$$
$$t_{CE} = 1132 hours$$

Therefore:

$$PFD_{avg,s} = \lambda_D t_{CE}$$
$$PFD_{avg,s} = (7.19 \times 10^{-7}) \times 1132$$
$$\boldsymbol{PFD_{avg,s} = 8.14 \times 10^{-4}}$$

PFD_{avg} for the logic solver:
Getting the $PFD_{avg,logic}$ in Equation 4.1 with 1oo1 voting logic, we use the formula:

$$\boldsymbol{PFD_{avg,l} = \lambda_D t_{CE}}$$

Getting the values from logic solver data, we have:

Given:

$$\lambda_{DU} = 3 \times 10^{-9} \qquad \tau = 5 years$$
$$\lambda_{DD} = 932 \times 10^{-9} \qquad MTR = 10 days$$
$$\lambda_{SU} = 11 \times 10^{-9} \qquad MTTR = 40 days$$

Solution: To get λ_D:

$$\lambda_D = (\lambda_{DU}) + (\lambda_{DD})$$
$$\lambda_D = \left(3.9 \times 10^{-9}\right) + \left(932 \times 10^{-9}\right)$$
$$\lambda_D = 9.35 \times 10^{-7}$$

For t_{CE}:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{\tau}{2} + MTR\right) + \frac{\lambda_{DD}}{\lambda_D}(MTTR)$$
$$t_{CE} = \frac{3.9 \times 10^{-9}}{9.35 \times 10^{-7}}\left(\frac{43200}{2} + 240\right) + \frac{932 \times 10^{-9}}{9.35 \times 10^{-7}}(960)$$
$$t_{CE} = 1048 hours$$

Therefore:

$$PFD_{avg,l} = \lambda_D t_{CE}$$
$$PFD_{avg,l} = (79.35 \times 10^{-7}) \times 1048$$
$$\boldsymbol{PFD_{avg,s} = 9.8 \times 10^{-4}}$$

PFD_{avg} for the valve:
Getting the $PFD_{avg,valve}$ in Equation 4.1 with 1oo1 voting logic, we use the formula:

$$\boldsymbol{PFD_{avg,v} = \lambda_D t_{CE}}$$

Getting the values from valve data, we have:
Given:

$$\lambda_{DU} = 622 \times 10^{-9} \qquad \tau = 12 months$$
$$\lambda_{DD} = 447 \times 10^{-9} \qquad MTR = 10 days$$
$$\lambda_{SU} = 0 \times 10^{-9} \qquad MTTR = 40 days$$

Solution: To get λ_D:

$$\lambda_D = (\lambda_{DU}) + (\lambda_{DD})$$
$$\lambda_D = \left(622 \times 10^{-9}\right) + \left(447 \times 10^{-9}\right)$$
$$\lambda_D = 1.07 \times 10^{-6}$$

For t_{CE}:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{\tau}{2} + MTR\right) + \frac{\lambda_{DD}}{\lambda_D}(MTTR)$$
$$t_{CE} = \frac{622 \times 10^{-9}}{1.07 \times 10^{-6}}\left(\frac{8640}{2} + 240\right) + \frac{447 \times 10^{-9}}{1.07 \times 10^{-6}}(960)$$
$$t_{CE} = 3087 hours$$

Therefore:

$$PFD_{avg,v} = \lambda_D t_{CE}$$
$$PFD_{avg,v} = (1.07 \times 10^{-6}) \times 3087$$
$$\boldsymbol{PFD_{avg,s} = 3.3 \times 10^{-3}}$$

Results:
After getting the individual PFD_{avg} of the components, we use Equation 4.11 to get the total PFD_{avg} of SIS-2 or the pressure control system.

$$\boldsymbol{PFD_{avg} = PFD_{avg,sensor} + PFD_{avg,logic} + PFD_{avg,valve}}$$

Where:

$$PFD_{avg,sensor} = 8.14 \times 10^{-4}$$
$$PFD_{avg,logic} = 9.8 \times 10^{-4}$$
$$PFD_{avg,valve} = 3.3 \times 10^{-3}$$

So:

$$PFD_{avg} = (8.14 \times 10^{-4}) + (9.8 \times 10^{-4}) + (3.3 \times 10^{-3})$$
$$\boldsymbol{PFD_{avg,system} = 5.032 \times 10^{-3}}$$

Results:
Based on the acquired result of $PFD_{avg,system} = 5.032 \times 10^{-3}$, the existing pressure control SIS has an integrity value that is within the quantitative range of SIL 2, with reference to the low demand mode classification from Table 2.1.

PFH computation

In order to compute the PFH of the existing pressure control system, individual PFH of the components are required to be computed and totalled. It is assumed in high demand mode that the safety system puts the EUC into a safe state on detection of any failure. The working formula for the total PFH of the system is:

$$\boldsymbol{PFH_{sys} = PFH_{sensor} + PFD_{logic} + PFD_{valve}} \tag{4.12}$$

For individual components:

$$\boldsymbol{PFH_{comp} = \lambda_{DU}} \tag{4.13}$$

Solution:
Gathering the data of individual components, we get the following values:

$$PFH_{sensor} = 34 \times 10^{-9}$$
$$PFH_{logic} = 3 \times 10^{-9}$$
$$PFH_{valve} = 622 \times 10^{-9}$$

So:

$$PFH_{sys} = (34 \times 10^{-9}) + (3 \times 10^{-9}) + (622 \times 10^{-9})$$
$$\boldsymbol{PFH_{sys} = 6.59 \times 10^{-7}}$$

Results:
Based on the acquired result of $PFH_{sys} = 6.59 \times 10^{-7}$, the pressure control system SIS integrity value is within the quantitative range of SIL 2 with reference to the high demand mode classification from Table 2.2.

Total PFDavg for the SIF

PDS Method :2013 recommended a formula for system comprising multiple SIS. It is utilized on the analysis of the integrated control system on this paper because they are identified to have similar SIF and comprising two SIS layers. The formula is only for PFD, so PFH is not computed. The formula recommended on the handbook is:

$$\boldsymbol{PFD_{avg} = CF \times PFD_{avg}(SIS-1) + PFD_{avg}(SIS-2)} \tag{4.14}$$

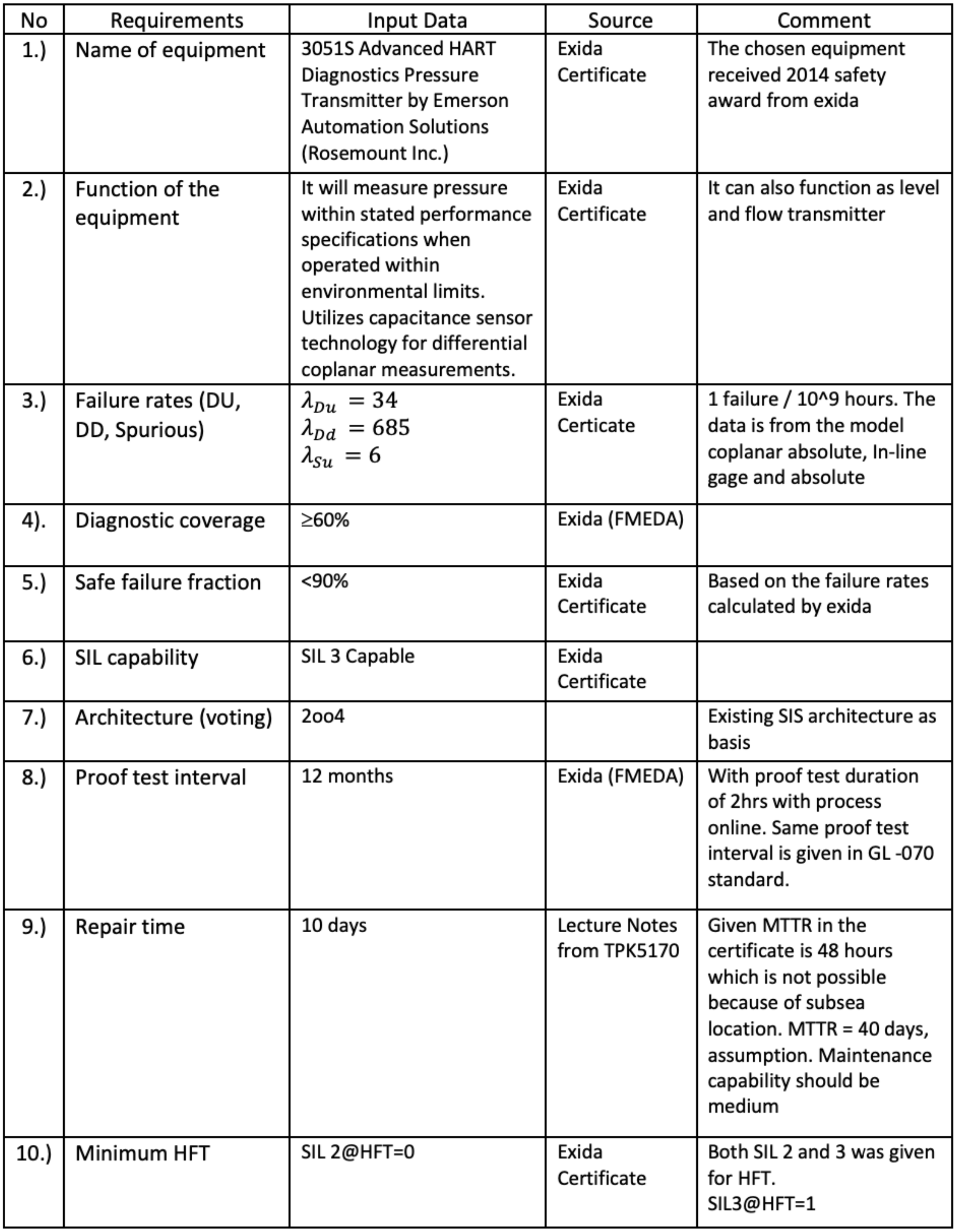
Solution:
Gathering the results for PFDavg of SIS-1 and SIS-2, we have the following values:

$$PFD_{SIS1} = 4.28 \times 10^{-3}$$
$$PFD_{SIS2} = 5.032 \times 10^{-3}$$

So:
Using 1.33 as the correction factor (CF) reflected in the book, we get:

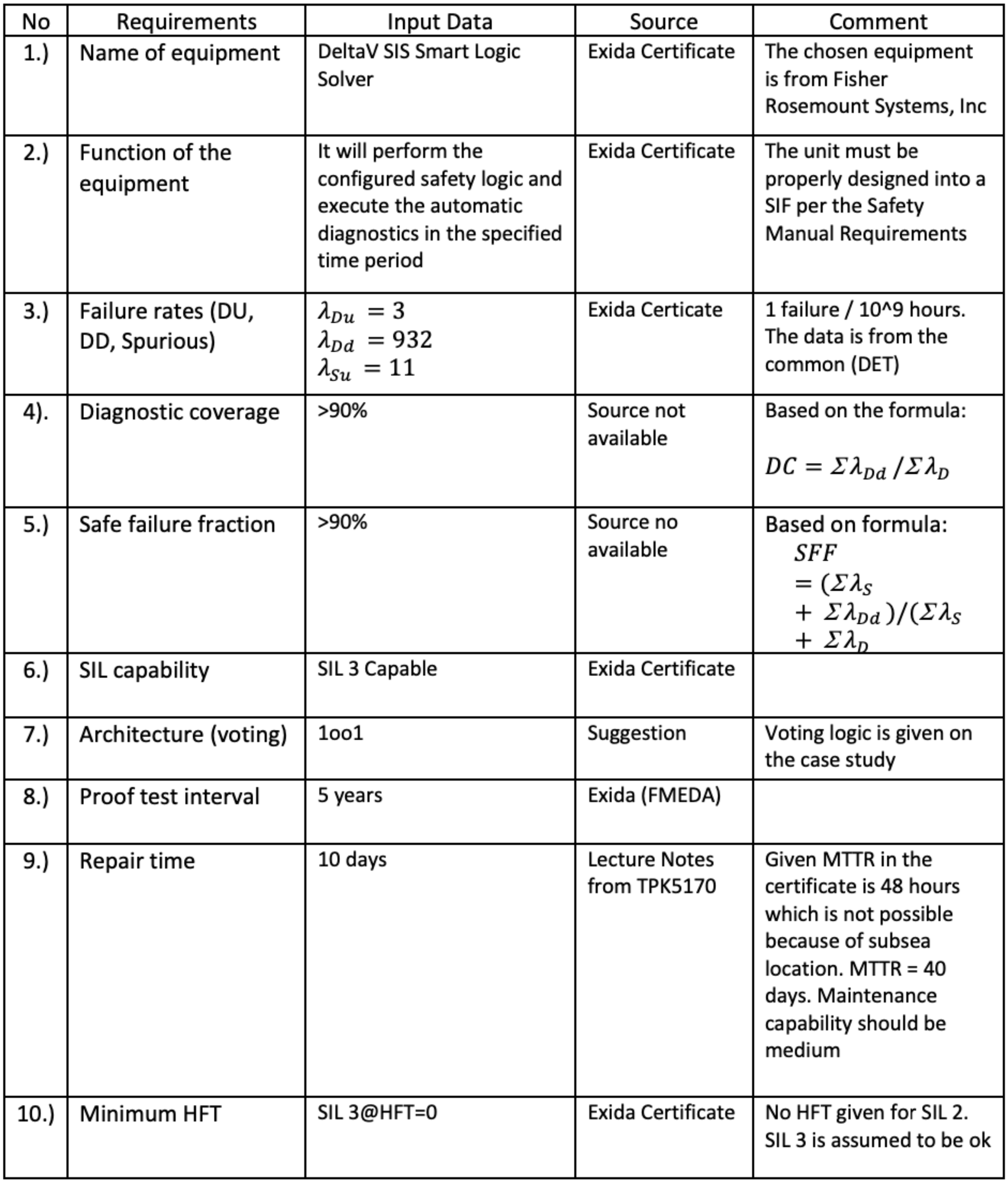
$$PFD_{avg} = 1.33 \times (4.28 \times 10^{-3}) \times (5.032 \times 10^{-3})$$
$$\boldsymbol{PFD_{avg} = 2.86 \times 10^{-5}}$$

Results:
Based on the acquired result of $PFD_{avg} = 2.86 \times 10^{-5}$, the integral anti-surge system with anti-surge control SIS and pressure control SIS for the SIF *'pressure recovery function from compressor discharge line to compressor suction line'* has an integrity value that is within the quantitative range of SIL 4, with reference to the low demand mode classification from Table 2.1.



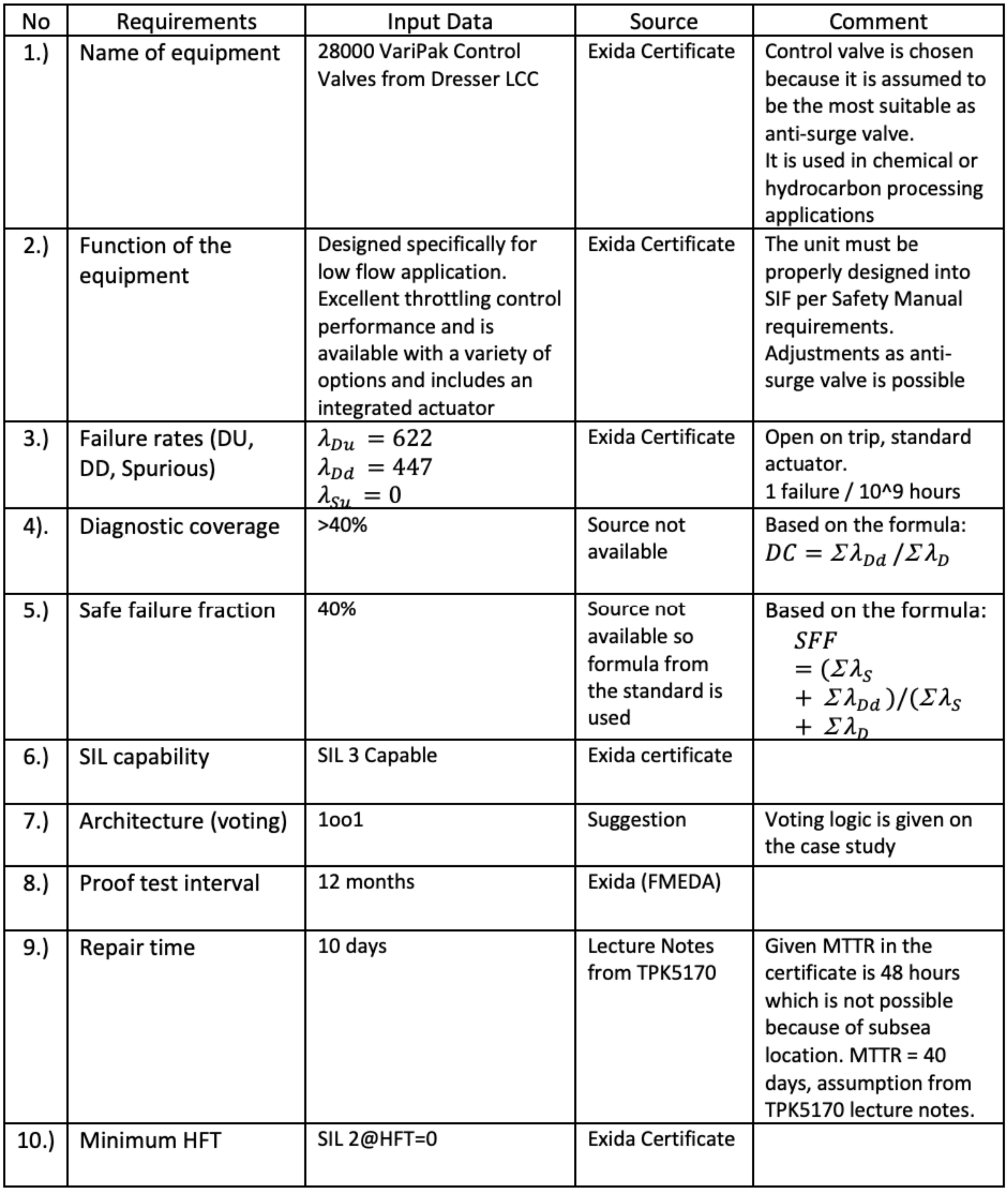
No	Requirements	Input Data	Source	Comment
1.)	Name of equipment	3051S Advanced HART Diagnostics Pressure Transmitter by Emerson Automation Solutions (Rosemount Inc.)	Exida Certificate	The chosen equipment received 2014 safety award from exida
2.)	Function of the equipment	It will measure pressure within stated performance specifications when operated within environmental limits. Utilizes capacitance sensor technology for differential coplanar measurements.	Exida Certificate	It can also function as level and flow transmitter
3.)	Failure rates (DU, DD, Spurious)	$\lambda_{Du} = 34$ $\lambda_{Dd} = 685$ $\lambda_{Su} = 6$	Exida Certicate	1 failure / 10^9 hours. The data is from the model coplanar absolute, In-line gage and absolute
4).	Diagnostic coverage	≥60%	Exida (FMEDA)	
5.)	Safe failure fraction	<90%	Exida Certificate	Based on the failure rates calculated by exida
6.)	SIL capability	SIL 3 Capable	Exida Certificate	
7.)	Architecture (voting)	2oo4		Existing SIS architecture as basis
8.)	Proof test interval	12 months	Exida (FMEDA)	With proof test duration of 2hrs with process online. Same proof test interval is given in GL -070 standard.
9.)	Repair time	10 days	Lecture Notes from TPK5170	Given MTTR in the certificate is 48 hours which is not possible because of subsea location. MTTR = 40 days, assumption. Maintenance capability should be medium
10.)	Minimum HFT	SIL 2@HFT=0	Exida Certificate	Both SIL 2 and 3 was given for HFT. SIL3@HFT=1

Figure 4.5: **Pressure Transmitter Data**



No	Requirements	Input Data	Source	Comment
1.)	Name of equipment	DeltaV SIS Smart Logic Solver	Exida Certificate	The chosen equipment is from Fisher Rosemount Systems, Inc
2.)	Function of the equipment	It will perform the configured safety logic and execute the automatic diagnostics in the specified time period	Exida Certificate	The unit must be properly designed into a SIF per the Safety Manual Requirements
3.)	Failure rates (DU, DD, Spurious)	$\lambda_{Du} = 3$ $\lambda_{Dd} = 932$ $\lambda_{Su} = 11$	Exida Certicate	1 failure / 10^9 hours. The data is from the common (DET)
4).	Diagnostic coverage	>90%	Source not available	Based on the formula: $DC = \Sigma\lambda_{Dd} / \Sigma\lambda_D$
5.)	Safe failure fraction	>90%	Source no available	Based on formula: $SFF = (\Sigma\lambda_S + \Sigma\lambda_{Dd})/(\Sigma\lambda_S + \Sigma\lambda_D$
6.)	SIL capability	SIL 3 Capable	Exida Certificate	
7.)	Architecture (voting)	1oo1	Suggestion	Voting logic is given on the case study
8.)	Proof test interval	5 years	Exida (FMEDA)	
9.)	Repair time	10 days	Lecture Notes from TPK5170	Given MTTR in the certificate is 48 hours which is not possible because of subsea location. MTTR = 40 days. Maintenance capability should be medium
10.)	Minimum HFT	SIL 3@HFT=0	Exida Certificate	No HFT given for SIL 2. SIL 3 is assumed to be ok

Figure 4.6: **Logic Solver Data**



No	Requirements	Input Data	Source	Comment
1.)	Name of equipment	28000 VariPak Control Valves from Dresser LCC	Exida Certificate	Control valve is chosen because it is assumed to be the most suitable as anti-surge valve. It is used in chemical or hydrocarbon processing applications
2.)	Function of the equipment	Designed specifically for low flow application. Excellent throttling control performance and is available with a variety of options and includes an integrated actuator	Exida Certificate	The unit must be properly designed into SIF per Safety Manual requirements. Adjustments as anti-surge valve is possible
3.)	Failure rates (DU, DD, Spurious)	$\lambda_{Du} = 622$ $\lambda_{Dd} = 447$ $\lambda_{Su} = 0$	Exida Certificate	Open on trip, standard actuator. 1 failure / 10^9 hours
4).	Diagnostic coverage	>40%	Source not available	Based on the formula: $DC = \Sigma\lambda_{Dd} / \Sigma\lambda_D$
5.)	Safe failure fraction	40%	Source not available so formula from the standard is used	Based on the formula: $SFF = (\Sigma\lambda_S + \Sigma\lambda_{Dd})/(\Sigma\lambda_S + \Sigma\lambda_D$
6.)	SIL capability	SIL 3 Capable	Exida certificate	
7.)	Architecture (voting)	1oo1	Suggestion	Voting logic is given on the case study
8.)	Proof test interval	12 months	Exida (FMEDA)	
9.)	Repair time	10 days	Lecture Notes from TPK5170	Given MTTR in the certificate is 48 hours which is not possible because of subsea location. MTTR = 40 days, assumption from TPK5170 lecture notes.
10.)	Minimum HFT	SIL 2@HFT=0	Exida Certificate	

Figure 4.7: **Valve Data**

4.4.2 LOPA for surging

The purpose of the LOPA is to analyze and identify the layers of protection of the given system in the case study. The goal of this analysis is to verify whether the integral anti-surge protection system satisfies the SIL requirement of the impact event related to it. The LOPA is therefore conducted with all other protection layers except for the anti-surge system integral SIS. The LOPA also aims to identify the total intermediate event likelihood related to surging when all the protection layers are in place.

The impact event and its severity level used in the LOPA is usually based on HAZOP study. For this specific LOPA, the initiating event is based on the formulated SIF for the existing system in the case study. From there, a step by step procedure is presented based on IEC 61511, then compiled to a LOPA report form reflected in Figure 4.8 which is based on IEC 61508 sample.

Introduction

The LOPA covers surging of compressor due to flow reversal that occurs in the compressor when operating below a certain flow rate and above certain compression level. All the assumed protection layers related to this impact event is included on this analysis. It is also worth noting that assumption of upstream hydrocarbon and downstream supply is considered in the overall picture.

Instruments such as pressure transmitter, temperature transmitter, flow indicator are in placed for monitoring and controlling purposes. A process shutdown system is assumed to be located downstream to protect both the compressor and the down stream equipment. Due to the assumption that this system is placed in subsea, manual access to equipment is not considered but alarm monitoring and shutdown remote access is assumed to be in place.

Impact event and severity level

Parameter deviation within the compressor and its environment is identified as a change in the normal compression system. The parameter deviation is usually cause by a blocked line or an abnormal equipment condition which causes surging or pulsations of pressure in the compressor and eventually causing damage to its mechanical part. Due to the remote location of compressor, the severity level of the mechanical damage is based on how it impacts the whole compression system, downstream equipment, the overall processing of the hydrocarbons and the subsea environment. Due to the impact of the possible consequences, a level of E or extensive is given. It is also considered to cause death and injury to the people on the topside if large amount of gas is released.

Initiating cause

Surging in the compressor are initially caused by high pressure from the downstream which in turn causes flow reversal on the system. The flow reversal then affects the parameters in the compressor which in turn may cause surging. One of the initiating cause identified is insufficient flow. Insufficient flow is cause by blocked lines or unstable pressure supply from upstream. Insufficient flow causes abnormal change in parameters which then causes surging. These abnormal conditions causes mechanical damage to the compressor.

Initiating likelihood

As there is not much data available yet to base the likelihood of the initiating causes because of its subsea location, a conservative estimate of 0.1 per year is given. The value is normally given to any initiating event in the LOPA.

General process design

It is assumed that the process design of the system has already contributed to the safety of the system by implementing the correct process and using the proper materials. It is therefore given 1.0 for this specific LOPA which means it does not have any mitigating effect.

Basic process control system (BPCS)

The process control system of the existing compressor system on this LOPA study is assumed not to possess any equipment or instrument to mitigate the initiating cause, so a value of 1.0 is given for the BPCS column. Compressor design might possess mitigating measure for the initiating cause but its internal functionality is not discussed on this paper.

Alarms

The compressor system is designed with multiple instruments with the purpose of monitoring the process. Any process deviation on the system will trigger an alarm to the operators on the topside. The alarm can be considered as a protection layer because operator intervention means early action to protect the system from the impact event. A value of 0.1 is given to this category.

Safety instrument system (SIS)

As mentioned in the case description, a process shutdown system with sensor, logic solver and valve is considered as part of the layer that will protect the system from high pressure and flow reversal. The shutdown valve is will automatically close the system upon detection of abnormal process conditions, therefore protecting the compressor system. A value of 0.1 is given for the reduction factor of the SIS.

Additional mitigation

Due to the possible consequence of the event on the topside, which is death or injury due to large amount of gas released, it is considered that proper training is conducted to the operators in case the event occurs. It is also assumed that physical protection for gas release is installed on the topside. A value of 0.1 is given for this category.

Intermediate event likelihood

After assigning all the values for different protection layers and initiation likelihood, from columns four to seven, they are multiplied altogether per impact description. The individual results for each impact event is then added to produce the intermediate event likelihood. The resulting value for this LOPA is (2×10^{-4}) per year.

Tolerable mitigated event likelihood

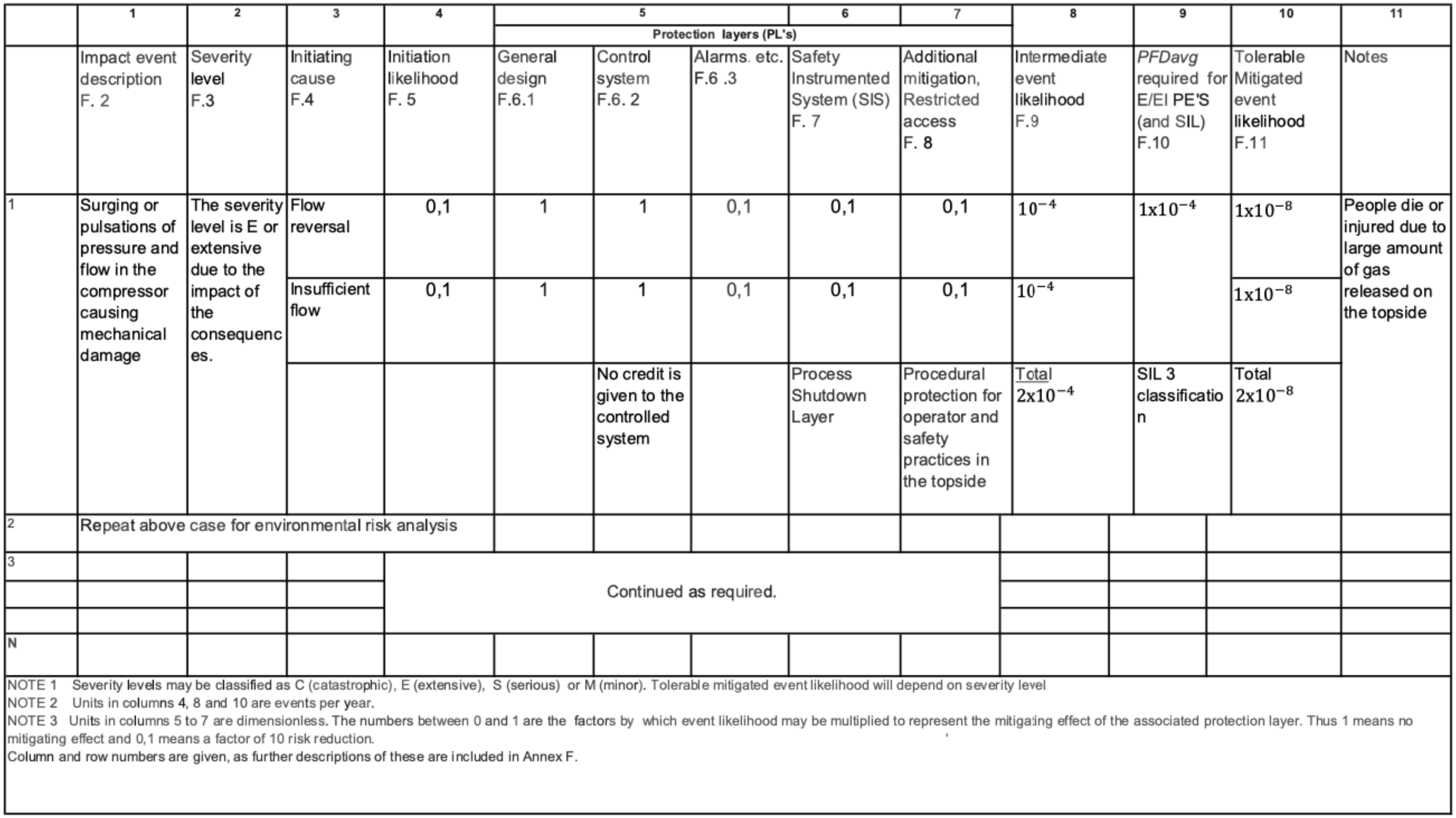
This section defines the tolerable value of the impact event that is mitigated by the existing layers of protection.The impact event will cause mechanical damage to the compressor, affect hydrocarbon processing, environmental damage and loss of human life. It is categorized as E or extensive. Based on Dowell III [1998], E category is given (1.0×10^{-8}) for target mitigated event likelihood per year.

PFDavg and SIL requirements

After obtaining the total intermediate event likelihood and the total tolerable mitigated event likelihood, the PFD requirement is acquired by diving the former to the latter. The value obtained for intermediate event likelihood is (2×10^{-4}) and the value acquired for tolerable mitigated event likelihood is (1.0×10^{-8}). The resulting value is (1.0×10^{-4}) per year which is classified as SIL 3 level. The LOPA results table is presented in Figure 4.8.

With the result from LOPA, it is confirmed by the acquired value of $PFD_{avg} = 2.86 \times 10^{-5}$ (SIL 4) for the the existing SIF, that it is suitable enough to protect the impact event from occurring. It means that no additional is required in terms of protection for surging. This is discussed in detail in the results. But to comply with the SIF in the case study, a new SIS is proposed.

The SIF *"the anti-surge functionality does not react quickly enough to prevent the compressor from surging and from subsequent damage."* means the issue within the operating condition. It is therefore proposed to have a second smaller and quicker anti-surge valve parallel to the existing.



	1	2	3	4	5			6	7	8	9	10	11
					Protection layers (PL's)								
	Impact event description F. 2	Severity level F.3	Initiating cause F.4	Initiation likelihood F. 5	General design F.6.1	Control system F.6. 2	Alarms. etc. F.6 .3	Safety Instrumented System (SIS) F. 7	Additional mitigation, Restricted access F. 8	Intermediate event likelihood F.9	*PFDavg* required for E/EI PE'S (and SIL) F.10	Tolerable Mitigated event likelihood F.11	Notes
1	Surging or pulsations of pressure and flow in the compressor causing mechanical damage	The severity level is E or extensive due to the impact of the consequences.	Flow reversal	0,1	1	1	0,1	0,1	0,1	10^{-4}	$1x10^{-4}$	$1x10^{-8}$	People die or injured due to large amount of gas released on the topside
			Insufficient flow	0,1	1	1	0,1	0,1	0,1	10^{-4}		$1x10^{-8}$	
						No credit is given to the controlled system		Process Shutdown Layer	Procedural protection for operator and safety practices in the topside	Total $2x10^{-4}$	SIL 3 classification	Total $2x10^{-8}$	
2	Repeat above case for environmental risk analysis												
3				Continued as required.									
N													

NOTE 1 Severity levels may be classified as C (catastrophic), E (extensive), S (serious) or M (minor). Tolerable mitigated event likelihood will depend on severity level

NOTE 2 Units in columns 4, 8 and 10 are events per year.

NOTE 3 Units in columns 5 to 7 are dimensionless. The numbers between 0 and 1 are the factors by which event likelihood may be multiplied to represent the mitigating effect of the associated protection layer. Thus 1 means no mitigating effect and 0,1 means a factor of 10 risk reduction.

Column and row numbers are given, as further descriptions of these are included in Annex F.

Figure 4.8: **Layer of Protection Analysis for Surging**

Fault tree analysis for surging

In order to have a clearer understanding of the impact event, the fault tree analysis for mechanical damage caused by surging in the compressor is presented. There is no available sources for failure data in a subsea compressor, so compressor topside equipment data is used. The failure probability of (1.024×10^{-6}) per year, for compressor mechanical damage cause by surging, is the result acquired through the fault tree analysis reflected in Figure 4.9. It is acquired by multiplying the two compressor failure modes. Parameter deviation (12.26×10^{-6} per hr) and erratic output (9.54×10^{-6} per hr) which yielded the result.

The values of the basic events in the fault tree is not reflected due to the unavailability of data. It is only presented in order to present the sequence of faults from basic event going to the TOP event, which is mechanical damage due to surging. The compressor failure mode data from OREDA is found on the Appendix G.

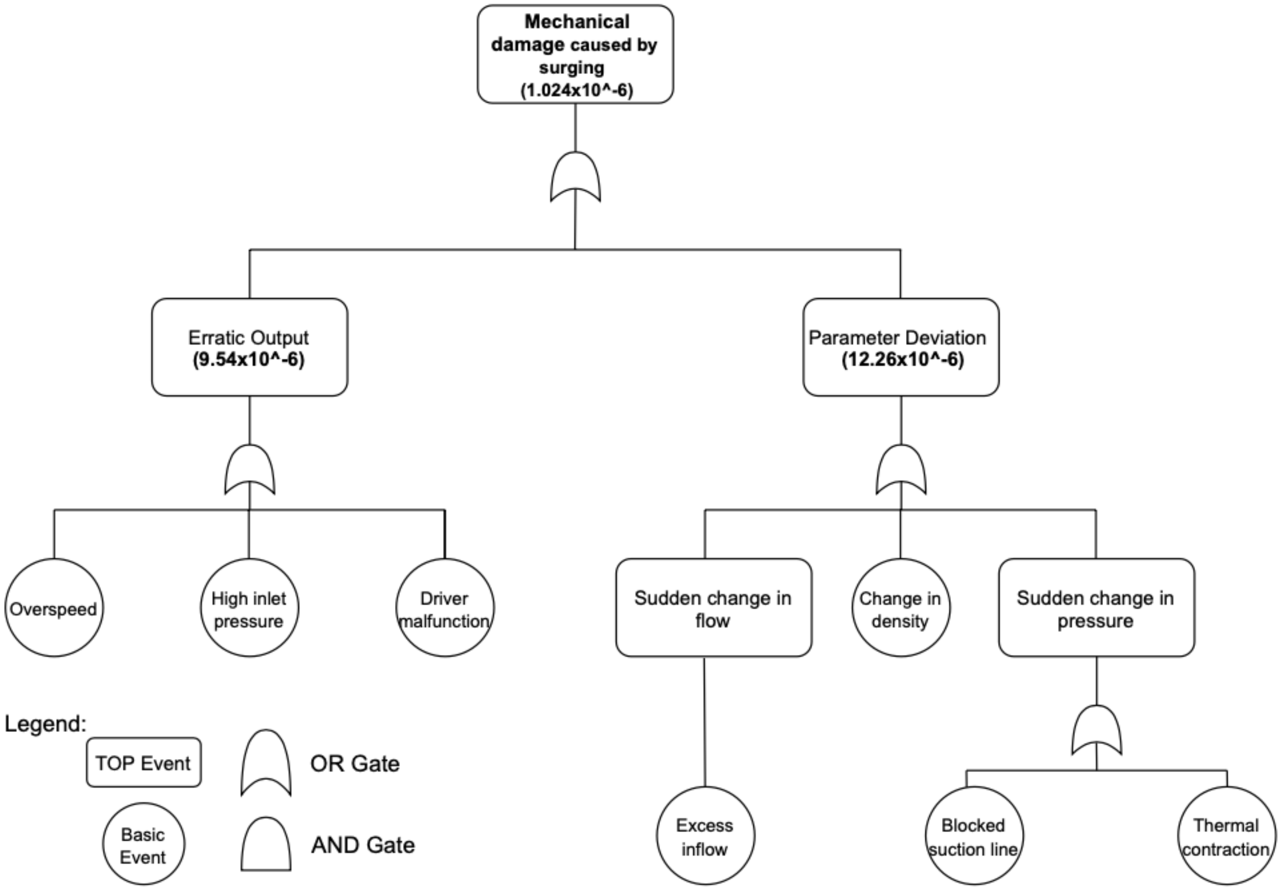


Figure 4.9: **Fault Tree Analysis for Surging**

4.5 Safety requirements specifications

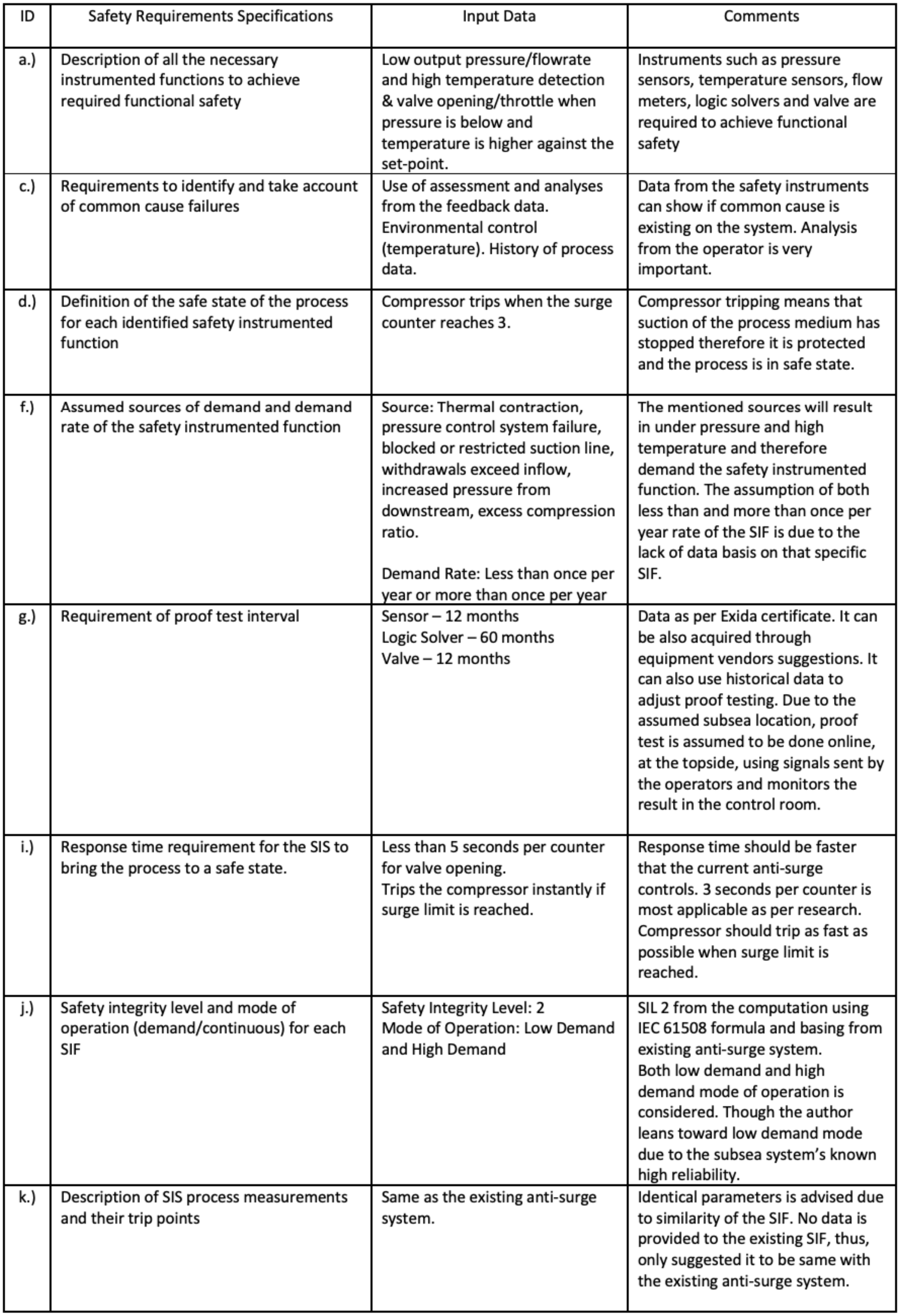
Safety requirements specification (SRS) are safety requirements that are obtained from the allocation of SIFs and from identifying the hazards and risks of the system. It is written to aid comprehension and interpretation by those who utilize the information at any phase of life-cycle so it should be clear, precise, verifiable, maintainable and feasible.

Reflected in Figure 4.10 is the SRS based on the conducted functional safety analysis which includes ID No. of the requirement from the standard GL 070:2018, Table E.2. The list of content on the SRS is for ESD system referenced from IEC 61511, cl. 10.3. Information about the requirements and explanation regarding the information and assumptions are presented. The input on the SRS table is based on the SIF: *"The anti-surge functionality does not react quickly enough to prevent the compressor from surging and from subsequent damage"*. The given SIF for the SRS is also related to the assumed SIF of the existing anti-surge system which is *'pressure recovery function from compressor discharge line to compressor suction line'*..

The SRS table below contains information that relates to the case study and is based on the assumption of a subsea location. The input data is the culmination of the preceding stages of the functional safety analysis conducted on this chapter. Comment section is added to explain the reason behind the input.

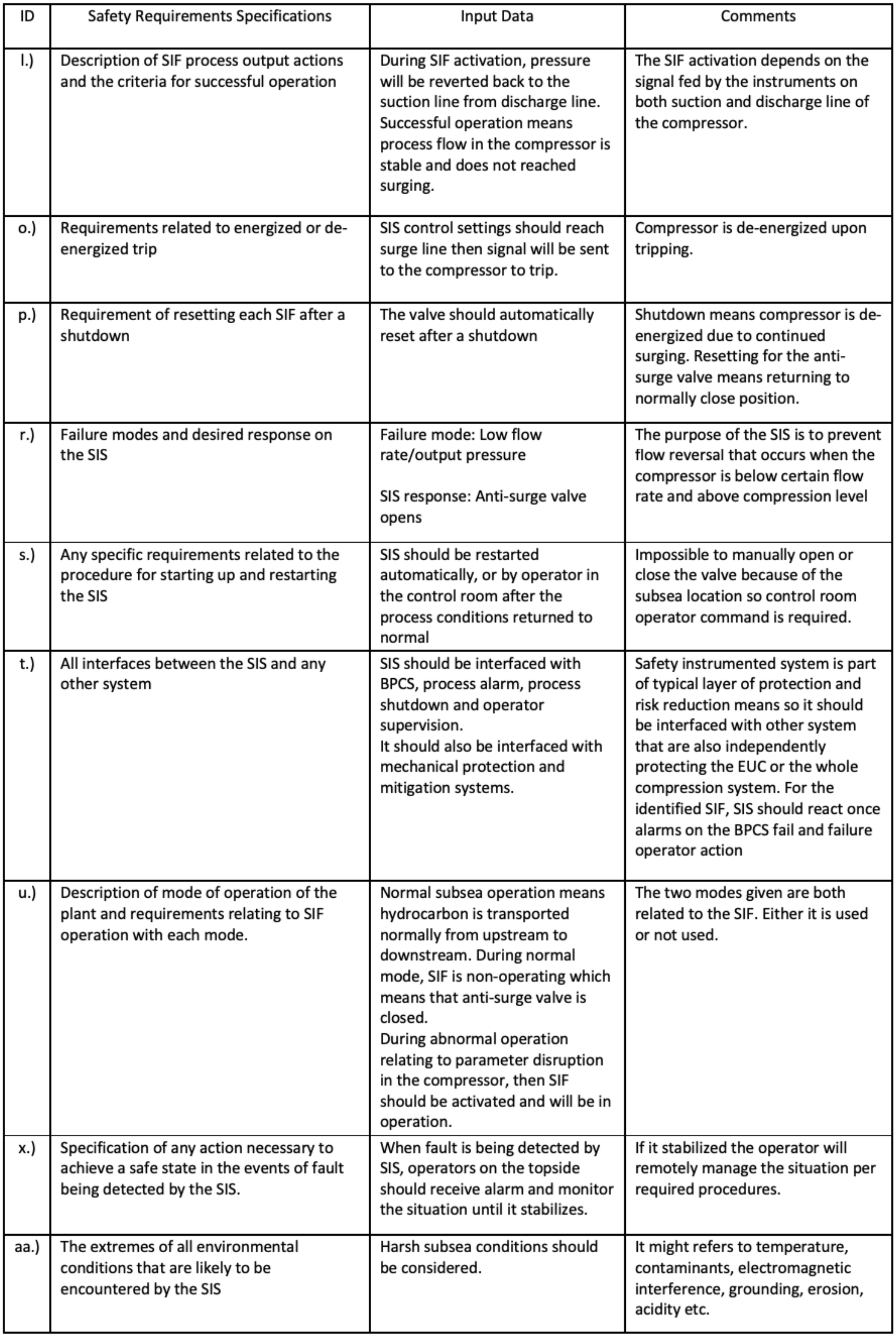
The items included are carefully selected to fit the safety requirements of the system. The chosen category is 'EDS system' which suits anti-surge protection system. Hydrocarbon is the main medium that flows through the system. The purpose in the process industry is to specify the requirements for each SIS, in terms of the required SIF and their associated safety integrity, in order to achieve the required functional safety.

The SRS in Figure 4.10 is assumed to guide the additional SIS in terms of its design and specifications. Results and discussion section elaborates all the results and output of the functional safety analysis conducted.



ID	Safety Requirements Specifications	Input Data	Comments
a.)	Description of all the necessary instrumented functions to achieve required functional safety	Low output pressure/flowrate and high temperature detection & valve opening/throttle when pressure is below and temperature is higher against the set-point.	Instruments such as pressure sensors, temperature sensors, flow meters, logic solvers and valve are required to achieve functional safety
c.)	Requirements to identify and take account of common cause failures	Use of assessment and analyses from the feedback data. Environmental control (temperature). History of process data.	Data from the safety instruments can show if common cause is existing on the system. Analysis from the operator is very important.
d.)	Definition of the safe state of the process for each identified safety instrumented function	Compressor trips when the surge counter reaches 3.	Compressor tripping means that suction of the process medium has stopped therefore it is protected and the process is in safe state.
f.)	Assumed sources of demand and demand rate of the safety instrumented function	Source: Thermal contraction, pressure control system failure, blocked or restricted suction line, withdrawals exceed inflow, increased pressure from downstream, excess compression ratio. Demand Rate: Less than once per year or more than once per year	The mentioned sources will result in under pressure and high temperature and therefore demand the safety instrumented function. The assumption of both less than and more than once per year rate of the SIF is due to the lack of data basis on that specific SIF.
g.)	Requirement of proof test interval	Sensor – 12 months Logic Solver – 60 months Valve – 12 months	Data as per Exida certificate. It can be also acquired through equipment vendors suggestions. It can also use historical data to adjust proof testing. Due to the assumed subsea location, proof test is assumed to be done online, at the topside, using signals sent by the operators and monitors the result in the control room.
i.)	Response time requirement for the SIS to bring the process to a safe state.	Less than 5 seconds per counter for valve opening. Trips the compressor instantly if surge limit is reached.	Response time should be faster that the current anti-surge controls. 3 seconds per counter is most applicable as per research. Compressor should trip as fast as possible when surge limit is reached.
j.)	Safety integrity level and mode of operation (demand/continuous) for each SIF	Safety Integrity Level: 2 Mode of Operation: Low Demand and High Demand	SIL 2 from the computation using IEC 61508 formula and basing from existing anti-surge system. Both low demand and high demand mode of operation is considered. Though the author leans toward low demand mode due to the subsea system's known high reliability.
k.)	Description of SIS process measurements and their trip points	Same as the existing anti-surge system.	Identical parameters is advised due to similarity of the SIF. No data is provided to the existing SIF, thus, only suggested it to be same with the existing anti-surge system.

Figure 4.10: **Safety Requirements Specifications** (1/2)



ID	Safety Requirements Specifications	Input Data	Comments
l.)	Description of SIF process output actions and the criteria for successful operation	During SIF activation, pressure will be reverted back to the suction line from discharge line. Successful operation means process flow in the compressor is stable and does not reached surging.	The SIF activation depends on the signal fed by the instruments on both suction and discharge line of the compressor.
o.)	Requirements related to energized or de-energized trip	SIS control settings should reach surge line then signal will be sent to the compressor to trip.	Compressor is de-energized upon tripping.
p.)	Requirement of resetting each SIF after a shutdown	The valve should automatically reset after a shutdown	Shutdown means compressor is de-energized due to continued surging. Resetting for the anti-surge valve means returning to normally close position.
r.)	Failure modes and desired response on the SIS	Failure mode: Low flow rate/output pressure SIS response: Anti-surge valve opens	The purpose of the SIS is to prevent flow reversal that occurs when the compressor is below certain flow rate and above compression level
s.)	Any specific requirements related to the procedure for starting up and restarting the SIS	SIS should be restarted automatically, or by operator in the control room after the process conditions returned to normal	Impossible to manually open or close the valve because of the subsea location so control room operator command is required.
t.)	All interfaces between the SIS and any other system	SIS should be interfaced with BPCS, process alarm, process shutdown and operator supervision. It should also be interfaced with mechanical protection and mitigation systems.	Safety instrumented system is part of typical layer of protection and risk reduction means so it should be interfaced with other system that are also independently protecting the EUC or the whole compression system. For the identified SIF, SIS should react once alarms on the BPCS fail and failure operator action
u.)	Description of mode of operation of the plant and requirements relating to SIF operation with each mode.	Normal subsea operation means hydrocarbon is transported normally from upstream to downstream. During normal mode, SIF is non-operating which means that anti-surge valve is closed. During abnormal operation relating to parameter disruption in the compressor, then SIF should be activated and will be in operation.	The two modes given are both related to the SIF. Either it is used or not used.
x.)	Specification of any action necessary to achieve a safe state in the events of fault being detected by the SIS.	When fault is being detected by SIS, operators on the topside should receive alarm and monitor the situation until it stabilizes.	If it stabilized the operator will remotely manage the situation per required procedures.
aa.)	The extremes of all environmental conditions that are likely to be encountered by the SIS	Harsh subsea conditions should be considered.	It might refers to temperature, contaminants, electromagnetic interference, grounding, erosion, acidity etc.

Figure 4.11: **Safety Requirements Specifications** (2/2)

4.6 Management of change

This section is added to support the arguments in discussion item four in section 5.2. It presents the new SIS architecture that includes the additional anti-surge valve, as recommended. Management of change (MOC) according to GL 070:2018 is aimed to ensure that modifications to any SIS are properly reviewed, approved and planned prior to making the change and to ensure that the required safety integrity of the SIS is maintained in the event of any changes made to the SIS. According to the same standard, MOC procedure may be required as a result of modifications in areas such as changed set-point due to changes in operating conditions, modified process conditions and component with different characteristics. All of these items fit the addition of anti-surge valve component with different characteristics and operating conditions. It is also applicable to discussion item no. 1 but it will not be discussed on this section.

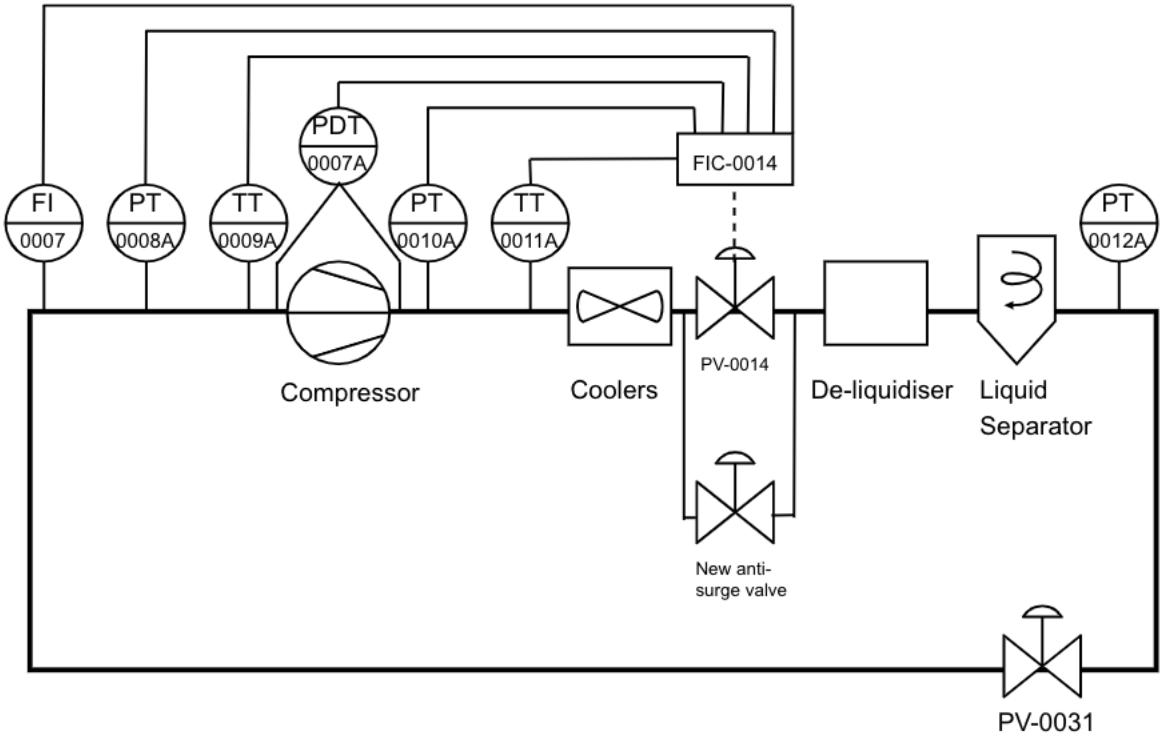


Figure 4.12: **Proposed SIS Architecture**

Figure 4.12 shows the proposed new SIS architecture. This new architecture is assumed to satisfy the SIF *"The anti-surge functionality does not react quickly enough to prevent the compressor from surging and from subsequent damage."*.The operating conditions which is valve opening is assumed to be quicker than the original valve, so it will prevent the compressor from surging and further damage. The valve size is also assumed to be smaller in order to satisfy the fast reactive condition. Specific technical details of the valve and its control system is suggested to be designed by qualified process engineers, instrument and control engineers and valve design engineers in coordination with the compressor vendor.

With the new SIS architecture comes the new voting logic for SIS-1 which is the anti-surge control. The new voting logic proposed for the new SIS architecture is now; 2oo4 for sensors, 1oo1 for logic solver and 1oo2 for the final element. 1oo2 voting logic for the final element means that it requires only one faulty signal from the valves before the compressor shutdowns due to surging. This adds reliability to the SIS.

The change on the architecture means that the PFDavg for the valve is also changed. Presented below is the computation of the new PFDavg of the valve with voting logic of 1oo2 and using IEC 61508 formula: PFD_{avg} for the valve:
Getting the $PFD_{avg,valve}$ for 1oo2 voting logic and consideration of CCF, we use the formula from Equation 4.2 and with PFD_{avg}^{ind} changed for 1oo2 logic :

$$\boldsymbol{PFD_{avg,v} = PFD_{avg}^{ind} + PFD_{avg}^{CCF}}$$

$$\boldsymbol{PFD_{avg,v} = \left[2\lambda_D^2 t_{CE} t_{GE}\right] + \left[\beta\lambda_{DU}(\frac{\tau}{2} + MTR) + \beta_D\lambda_{DD}MTTR\right]}$$

Getting the values from valve data and using the beta factor from PDS handbook, we have:

Given:

$$\lambda_{DU} = 622 \times 10^{-9} \qquad \tau = 12months \qquad \beta = 12\%$$

$$\lambda_{DD} = 447 \times 10^{-9} \qquad MTR = 10days \qquad \beta_D = 5\%$$

$$\lambda_{SU} = 0 \times 10^{-9} \qquad MTTR = 40days$$

Solution: To get λ_D:

$$\lambda_D = (1-\beta)(\lambda_{DU}) + (1-\beta_D)(\lambda_{DD})$$

$$\lambda_D = (1-0.12)(622 \times 10^{-9}) + (1-0.05)(447 \times 10^{-9})$$

$$\lambda_D = 1.00 \times 10^{-6}$$

For t_{CE}:

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

$$t_{CE} = \frac{622 \times 10^{-9}}{1.00 \times 10^{-6}}\left(\frac{8640}{2} + 240\right) + \frac{447 \times 10^{-9}}{1.00 \times 10^{-6}}(960)$$

$$t_{CE} = 3265hours$$

For t_{GE}:

$$t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{\tau}{3} + MTR\right) + \frac{\lambda_{DD}}{\lambda_D}(MTTR)$$
$$t_{GE} = \frac{34 \times 10^{-9}}{6.82 \times 10^{-7}}\left(\frac{8640}{3} + 240\right) + \frac{685 \times 10^{-9}}{6.82 \times 10^{-7}}(960)$$
$$t_{GE} = 1118 hours$$

For PFD_{avg}^{CCF}:

$$PFD_{avg}^{CCF} = \beta\lambda_{DU}(\frac{\tau}{2} + MTR) + \beta_D\lambda_{DD}MTTR$$
$$PFD_{avg}^{CCF} = \left(0.12)(622 \times 10^{-9}\right)\left(\frac{8640}{2} + 240\right) + \left(0.05)(477 \times 10^{-9}\right)(960)$$
$$PFD_{avg}^{CCF} = 3.632 \times 10^{-4}$$

Therefore:

$$PFD_{avg,v} = PFD_{avg}^{ind} + PFD_{avg}^{CCF}$$
$$PFD_{avg,v} = \left[2\lambda_D^2 t_{CE} t_{GE}\right] + \left[\beta\lambda_{DU}(\frac{\tau}{2} + MTR) + \beta_D\lambda_{DD}MTTR\right]$$
$$PFD_{avg,v} = \left[2(1.00 \times 10^{-6})^2 \times 3265 \times 1118\right] + 4.373 \times 10^{-5}$$
$$\boldsymbol{PFD_{avg,v} = 5.10 \times 10^{-5}}$$

With the result, the additional valve improves the PFDavg from (3.3×10^{-3}) to (5.10×10^{-5}). Incorporating this value to get the total PFDavg of SIS-1:

$$\boldsymbol{PFD_{avg} = PFD_{avg,sensor} + PFD_{avg,logic} + PFD_{avg,valve}}$$

Where new PFDavg value for valve is used:

$$PFD_{avg,sensor} = 1.11 \times 10^{-8}$$
$$PFD_{avg,logic} = 9.8 \times 10^{-4}$$
$$PFD_{avg,valve} = 5.10 \times 10^{-3}$$

So:

$$PFD_{avg} = (1.11 \times 10^{-8}) + (9.8 \times 10^{-4}) + (5.10 \times 10^{-3})$$
$$\boldsymbol{PFD_{avg,system} = 1.03 \times 10^{-3}}$$

This result improves the total SIS-1 PFDavg from (4.28×10^{-3}) to (1.03×10^{-3}). And finally, using the formula from PDS method handbook to get the PFDavg for the integrated anti-surge valve system incorporating the additional valve:

$$\boldsymbol{PFD_{avg} = CF \times PFD_{avg}(SIS1) + PFD_{avg}(SIS2)}$$

Gathering the new results for PFDavg of SIS1 and from SIS2, we get the following values:

$$PFD_{SIS1} = 1.031 \times 10^{-3}$$
$$PFD_{SIS2} = 5.032 \times 10^{-3}$$

So:
Using 1.33 as CF (correction factor) reflected on the book, we get:

$$PFD_{avg} = 1.33 \times (1.03 \times 10^{-3}) \times (5.032 \times 10^{-3})$$
$$\boldsymbol{PFD_{avg} = 6.90 \times 10^{-6}}$$

This result brings to a much improved PFDavg for the integrated anti-surge valve from (2.86×10^{-5}) to (6.90×10^{-6}). It means that the additional anti-surge valve which is smaller and quicker not only satisfies the SIF requirements but also improves the reliability of the system. Lower PFD means lower chances of failing while it is demanded to work. This result also improves the overall effectiveness of the protection layers for surging.

Chapter 5

Results and Discussion

5.1 Results

After the thorough functional safety analysis of the given case study, starting from concept presentation up to the safety requirements specifications and using cognitive analysis on reliability measures with the help of the given standards, the following results are stated:

1. *It is found through IEC 61508 and PDS method that the current integral anti-surge protection system has a PFDavg of (*2.86×10^{-5}*) and is within quantitative range of SIL 4 using low demand formulas.*

   The value is acquired by combining the average PFDs of SIS-1 ($PFD_{SIS1} = 4.28 \times 10^{-3}$) which is the anti-surge control categorized as SIL 2 and SIS-2 ($PFD_{SIS2} = 5.032 \times 10^{-3}$) which is the pressure control categorized as SIL 2.

2. *The result of LOPA for an impact event of surging revealed that a value of (*1.0×10^{-4}*) per year which classified as SIL 3 is required to be added to the existing protection layers.*

   LOPA considered all the protection layers except for the existing integral anti-surge protection systems. This is done in order to know the required SIS of the SIF and to know whether the existing SIS satisfies the requirement. With the result of (1.0×10^{-4}) per year, it means that the PFDavg of (2.86×10^{-5}) yielded from IEC 61508 and PDS method for the integral anti-surge control system satisfies the requirement of the LOPA. The given value is classified as SIL 4 which is above the SIL 3 requirement.

3. *Considering the integral anti-surge system SIL value of (*2.86×10^{-5}*) with other protection layers produce the total intermediate event likelihood of (*5.72×10^{-9}*).*

   This is a very good value which is well above the tolerable mitigated event likelihood of (2×10^{-8}). It means that the combination of all the protection layers, including the existing SIS, are well enough to satisfy the safety requirements

4. *Based on the reliability methods used in the analysis, the existing anti-surge SIS satisfies the SIF 'anti-surge functionality does not react quickly enough to prevent the compressor from surging and and from subsequent damage' in terms of the SIL needed to protect the system.*

   This is based on the previous statement that the SIF in the case study is related to the assumed SIF of the existing system. It means that the issue of the SIF is in the operating condition or control parameters of the anti-surge valve. Issue is discussed thoroughly in recommendation.

5. *Safety Requirements Specifications data in Figure 4.10 is based on the functional safety analysis*

   The SRS data is the final result of the functional safety analysis based on the SIF given on the case study. The data shows that the safety requirements are similar with the existing anti-surge safety systems. It was mentioned repeatedly on the preceding sections that both of them have the same purpose of preventing the surge to occur. The difference with the safety requirements specifications with the SIF in the case study are the functional details. Item 'i' states that response time should be less than 5 seconds per counter for valve opening. It means that faster execution time is given to the new SIF, which eventually complies to the issue of not reacting fast enough to prevent the compressor from surging. All other items on the SRS is assumed to be similar with the existing anti-surge protection systems.

6. *The result of PFH computation for the two SIS which are the anti-surge SIS and pressure control SIS are* (6.28×10^{-7}) *and* (6.59×10^{-7}) respectively.

   Both the results of the two SIS belongs to SIL 2 categories. It means that it has similar SIL categories for the low demand computation. High demand system computation is also conducted to present an alternate solution, if in case it turns out that the SIF has a high demand mode of operation. Confirmation should be done from the data gathered on the existing subsea compression facilities.

5.2 Discussion

Based on the results of the functional safety analysis, the following discussions are enumerated:

1. *Based on the results of the analysis, the existing SIS architecture already satisfies the SIL requirements of the safety function for surging, it is therefore not recommended to have another safety instrumented system for the purpose of protecting the system from surging.*

   Based on the functional safety analysis conducted and in-depth research on anti-surge systems , it is recommended to adjust the settings of the valve on it's control system in order to satisfy the SIF in the case study. The range of timings of 5 seconds on each counter is not quick enough to response to surging. It means that this setting should be changed, with the help of the designers, manufacturers and vendors.

2. *If it is not feasible to adjust the settings of the existing anti-surge control or not advisable as per the design engineers and vendors, it is therefore recommended to add a smaller and quicker anti-surge valve parallel to the existing.*

   This smaller and quick reactive valve is offered to rapidly open and reduce downstream pressure. The valve size can be a determining factor of slower travel to opening. The smaller the valve is, the shorter the travel time. It is also advised that associated instruments should react rapidly to small transients fluctuations in flow and pressure. The time elapse from the first indication of surge to the first major flow reversal can be less than 0.07 seconds so the instrumentation must be able to detect these fast process changes, but, equally, the control valve must be capable following these instructions [Singleton]. It is also recommended to check the effectiveness of the instruments used for detection and whether they response on the right time. Process engineers and instrument engineer with the valve designer and compressor vendor are recommended to discuss the issue and come up with parameters that will satisfy the timing needed so that the valve will react as quickly as possible.

3. *The additional smaller and quicker anti-surge valve is recommended to be included in the existing anti-surge SIS architecture.*

   It will now be then, 2oo4 for sensors, 1oo1 for logic solver and 1oo2 for the final element instead of 1oo1. This change is also expected to increase the reliability of the SIS due to the additional final element. The proposed new architecture is reflected on section 4.6 along with the new PFDavg computation for the new SIS.

4. *It is recommended to use the SRS produced on this functional safety analysis on designing the safety requirement of the new SIS for the SIF in the case study.*

   It is worth noting that the produced SRS satisfies the requirement of the SIF, which is to react quickly upon surging. The contents is assumed to be almost identical to the SRS used for the existing anti-surge system except for the response time of the valve during surging.

5. *If it is deemed feasible, process and design wise, it is recommended to have a hot-gas-bypass as another option along with the second suggestion of a quicker and smaller anti-surge valve.*

   It will take the recycle flow immediately from the compressor discharge and bypass it to suction. It reacts quickly and bypasses gas in defined time duration, up to the time that main anti-surge valve is sufficiently open and decreases stream pressure to suitable level to avoid surge. Almasi [2012].

6. *It is suggested that instruments on the suction and discharge of the compressor comply with the API RP-17V which has two pressure and temperature transmitters on both sides.*

   The additional instruments is suggested to create an alarm, should process parameters be abnormal. If the existing instruments is already used for alarms, alongside of being used for anti-surge systems, it is therefore advised to avoid this because of the common cause failures that might arise. VMS or vibration monitoring system is also suggested to be included in the compressor's internal safety protection layer. The vibration monitoring instrument should create an alarm for the operators on the topside.

7. *After the SIS is designed, installed and commissioned, it is recommended to continue the functional safety analysis by following the steps from safety life-cycle overview presented in IEC 61511.*

   Continued monitoring, verification and assessment of SIS is required in order to achieve functional safety until its decommissioning

Chapter 6

Conclusion and Recommendation

Risk analysis has always been practiced in the process and has proven to help identify, assess, quantify and mitigate the hazards that can harm human, property and the environment. In order to mitigate these hazards, different protection layers are utilized, such as safety instrumented system, which is conceptualized through its safety instrumented function. To design, maintain and assess these functions, functional safety analysis is being carried out.

A case study on a subsea compressor protection system is utilized in order to present and apply functional safety analysis of a system through this paper. By means of the problem given in the case study in the form of SIF *'anti-surge functionality does not react quickly enough to prevent the compressor from surging and and from subsequent damage'*, the paper presented a thorough functional safety analysis, from concept and scope definition up to formulating a specific safety requirements for the SIF mentioned. The paper utilized mathematical models such IEC 61508 formula and PDS method in order achieve results. After utilizing these models, a semi-quantitative risk analysis method is used to further analyzed the results provided by the mathematical models.

Based on the functional safety analysis performed using the steps elaborated in the IEC 61508 and IEC 61511, and using cognitive analysis on reliability measures, it is can be concluded that the existing SIS architecture satisfies the SIL requirements of the SIF. It has also been verified that the current protection layers are effective enough to protect the system and that it complies to the requirements of safety function.Through the analysis, it can also be concluded that the SIF can be managed in several ways. First, control functions adjustment of the existing SIS to make it quicker. Second, a smaller and quicker anti-surge valve parallel to the existing should be added, if the first solution doesn't seem feasible. Lastly, an additional hot-gas-bypass is also part of the recommended solution.

Functional safety analysis yields vital results that help in designing a safety instrumented function and maintaining or confirming that they are still safe to use. The paper verifies the effectiveness of the steps reflected in IEC 61508 and IEC 61511 and has proven that it can be used for subsea application. The methods used on this paper can be a basis for functional safety analysis of similar nature, specifically for anti-surge system or with other subsea SIFs. Finally, it is concluded that successful execution of functional safety analysis can be achieved with the help of a qualified personnel, a reliable data, a good management cooperation and a careful execution of procedures in the standards. Achieving functional safety promotes a safer and more reliable industries. An industry that is free from the risks that can harm human, property and the environment.

Based on the results, discussions and conclusions presented, the recommendations are the following:

1. *More studies and research should be conducted to formulate a specific functional safety analysis for subsea component safety functions.*

   Because of the remote location of the subsea components and its unique environment, special consideration should be applied when conducting functional safety analysis. Although some publications such as GL 070:2018 has set some minimum SIL requirements for subsea SIFS, it is still not enough and doesn't cover all the components, especially with the subsea compressor systems. Due to the expected extensive impact of a subsea accidents, it is therefore wise to invest in research and studies in order to maintain the system's safety and reliability.

2. *Demand modes for subsea safety instrumented functions should be established.*

   In order to design a proper safety instrumented system, demand mode of its SIF should be identified. There is not much data available and researches when it comes to the demands of this safety instrumented functions for subsea. Subsea compressor's data record for the past five years, for example, can be used to establish some of the demands of its safety instrumented functions. This is also applicable to all other safety functions within the subsea field.

3. *More study should be conducted to establish a designated specifications for subsea components.*

   Based on the research of this study, it has been known that most of the specifications for the subsea components are still very much relying on the topside data. Though it is reliable in general, some components do not easily adopt to subsea conditions, so an established specification is needed. A standardized specification for subsea components means a safer and more reliable subsea systems.

Appendix A

Acronyms

API American petroleum institute

ASIL Automotive safety integrity level

BPCS Basic process control system

CCF Common cause factor

CCPS Center for Chemical Process Safety

CENELEC European Committee for Electrotechnical Standardization

DNV Det Norske Veritas

DD Dangerous detected failure

DU Dangerous undetected failure

E/E/PE Electrical, electronic or programmable electronic

EP Exploration and production

EUC Equipment under control

ESD Emergency shutdown

ETA Event tree analysis

FGDS Fire and gas detection system

FTA Fault tree analysis

GL Guideline

HAZAN Hazard analysis

HAZOP Hazard operability

HEF Hazard event frequency

HRA Hazard and risk assessment

IC Instrumentation and control

IPL Independent protection layer

ISO International Organization for Standardization

IEC International Electrotechnical Commission

LOPA Layer of protection analysis

MDT Mean down time

MOC Management of change

MTR Mean repair time

MTTR Mean time to restore

NOG Norwegian oil and gas association

OREDA Offshore reliability data

PFD Average probability of dangerous failure on demand

PFH Average frequency of dangerous failure

PHA Preliminary hazard analysis

PIE Postulated initiating event

PSD Process shutdown

QM Quality management

RAMS Reliability, availability, maintainability, and safety

RP Recommended practice

RRF Risk reduction factor

SD Safe detected failure

SU Safe undetected failure

SIF Safety instrumented function

SIL Safety integrity level

SINTEF Stiftelsen for industrial og teknisk forskning

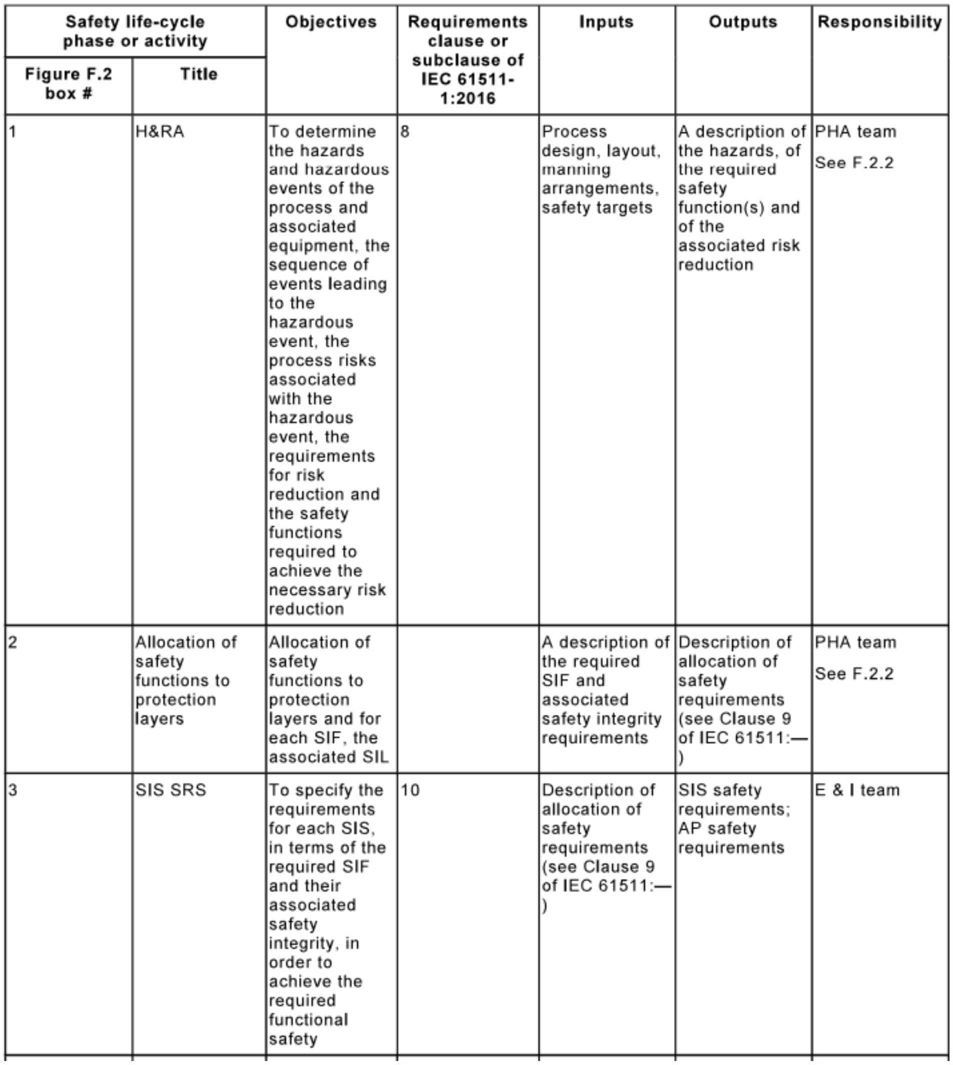
SIS Safety instrumented system

SRS Safety requirements specifications

THR Tolerable hazard rate

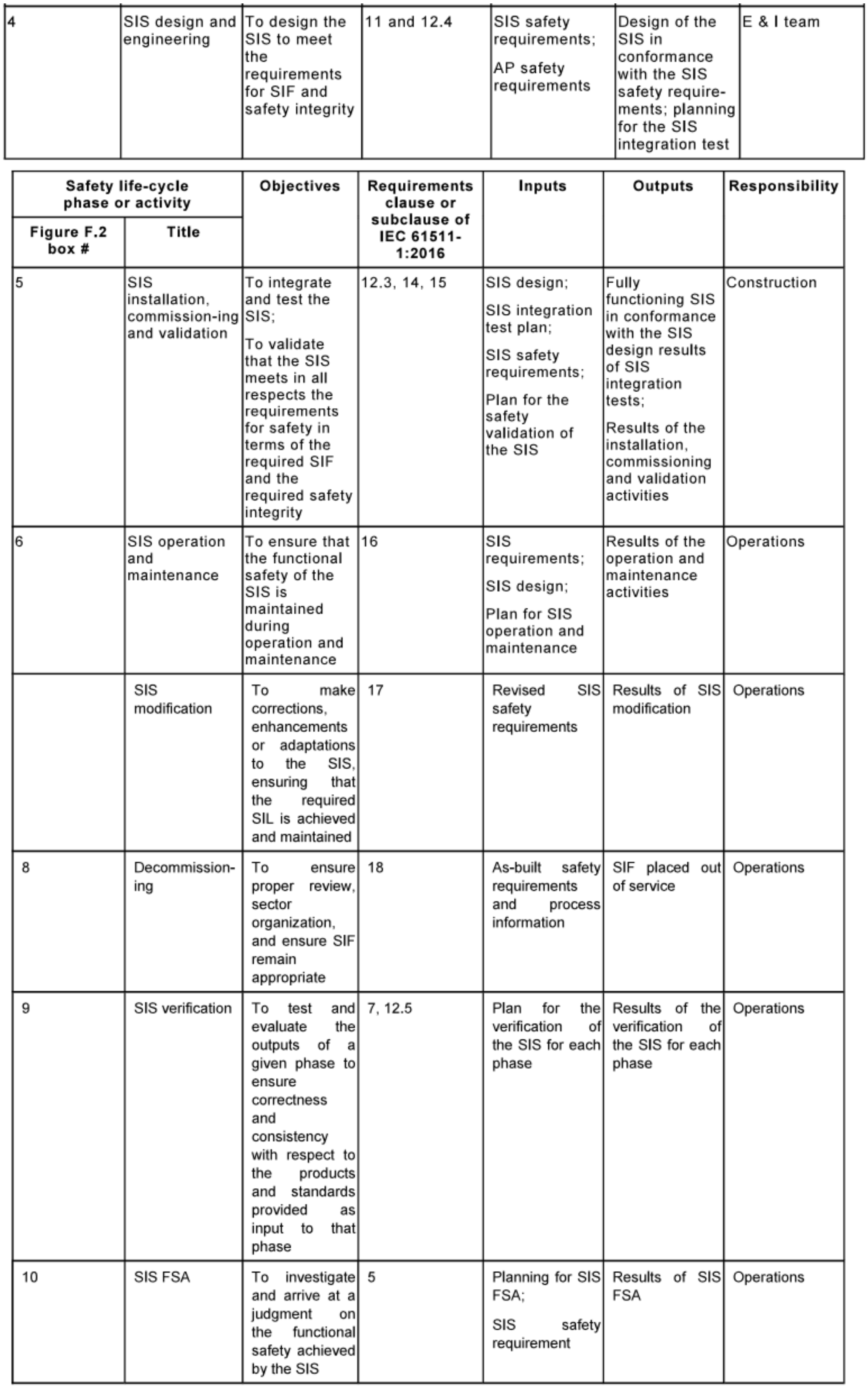
Appendix B

SIS Safety Lifecycle Overview



Safety life-cycle phase or activity		Objectives	Requirements clause or subclause of IEC 61511-1:2016	Inputs	Outputs	Responsibility
Figure F.2 box #	Title					
1	H&RA	To determine the hazards and hazardous events of the process and associated equipment, the sequence of events leading to the hazardous event, the process risks associated with the hazardous event, the requirements for risk reduction and the safety functions required to achieve the necessary risk reduction	8	Process design, layout, manning arrangements, safety targets	A description of the hazards, of the required safety function(s) and of the associated risk reduction	PHA team See F.2.2
2	Allocation of safety functions to protection layers	Allocation of safety functions to protection layers and for each SIF, the associated SIL		A description of the required SIF and associated safety integrity requirements	Description of allocation of safety requirements (see Clause 9 of IEC 61511:—)	PHA team See F.2.2
3	SIS SRS	To specify the requirements for each SIS, in terms of the required SIF and their associated safety integrity, in order to achieve the required functional safety	10	Description of allocation of safety requirements (see Clause 9 of IEC 61511:—)	SIS safety requirements; AP safety requirements	E & I team

Figure B.1: **SIS Safety Lifecycle Overview** (1/2) (IEC 61511 :2016)



Safety life-cycle phase or activity		Objectives	Requirements clause or subclause of IEC 61511-1:2016	Inputs	Outputs	Responsibility
Figure F.2 box #	Title					
4	SIS design and engineering	To design the SIS to meet the requirements for SIF and safety integrity	11 and 12.4	SIS safety requirements; AP safety requirements	Design of the SIS in conformance with the SIS safety requirements; planning for the SIS integration test	E & I team

5	SIS installation, commission-ing and validation	To integrate and test the SIS;
		To validate that the SIS meets in all respects the requirements for safety in terms of the required SIF and the required safety integrity
			12.3, 14, 15	SIS design;
				SIS integration test plan;
				SIS safety requirements;
				Plan for the safety validation of the SIS
					Fully functioning SIS in conformance with the SIS design results of SIS integration tests;
					Results of the installation, commissioning and validation activities
						Construction

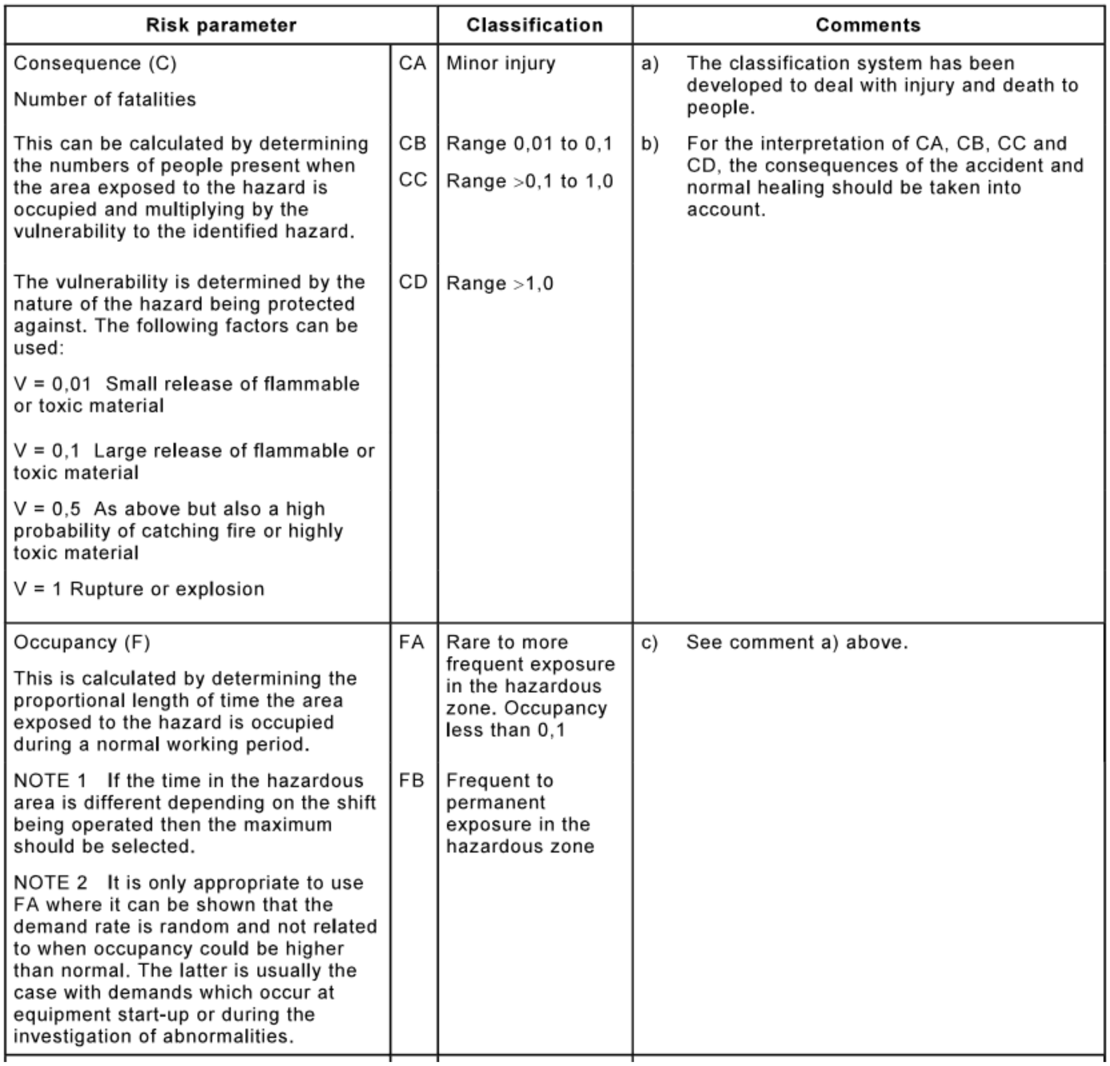
6	SIS operation and maintenance	To ensure that the functional safety of the SIS is maintained during operation and maintenance	16	SIS requirements;
				SIS design;
				Plan for SIS operation and maintenance
					Results of the operation and maintenance activities	Operations

	SIS modification	To make corrections, enhancements or adaptations to the SIS, ensuring that the required SIL is achieved and maintained	17	Revised SIS safety requirements	Results of SIS modification	Operations
8	Decommission-ing	To ensure proper review, sector organization, and ensure SIF remain appropriate	18	As-built safety requirements and process information	SIF placed out of service	Operations
9	SIS verification	To test and evaluate the outputs of a given phase to ensure correctness and consistency with respect to the products and standards provided as input to that phase	7, 12.5	Plan for the verification of the SIS for each phase	Results of the verification of the SIS for each phase	Operations
10	SIS FSA	To investigate and arrive at a judgment on the functional safety achieved by the SIS	5	Planning for SIS FSA; SIS safety requirement	Results of SIS FSA	Operations

Figure B.2: **SIS Safety Lifecycle Overview** (2/2) (IEC 61511 :2016)

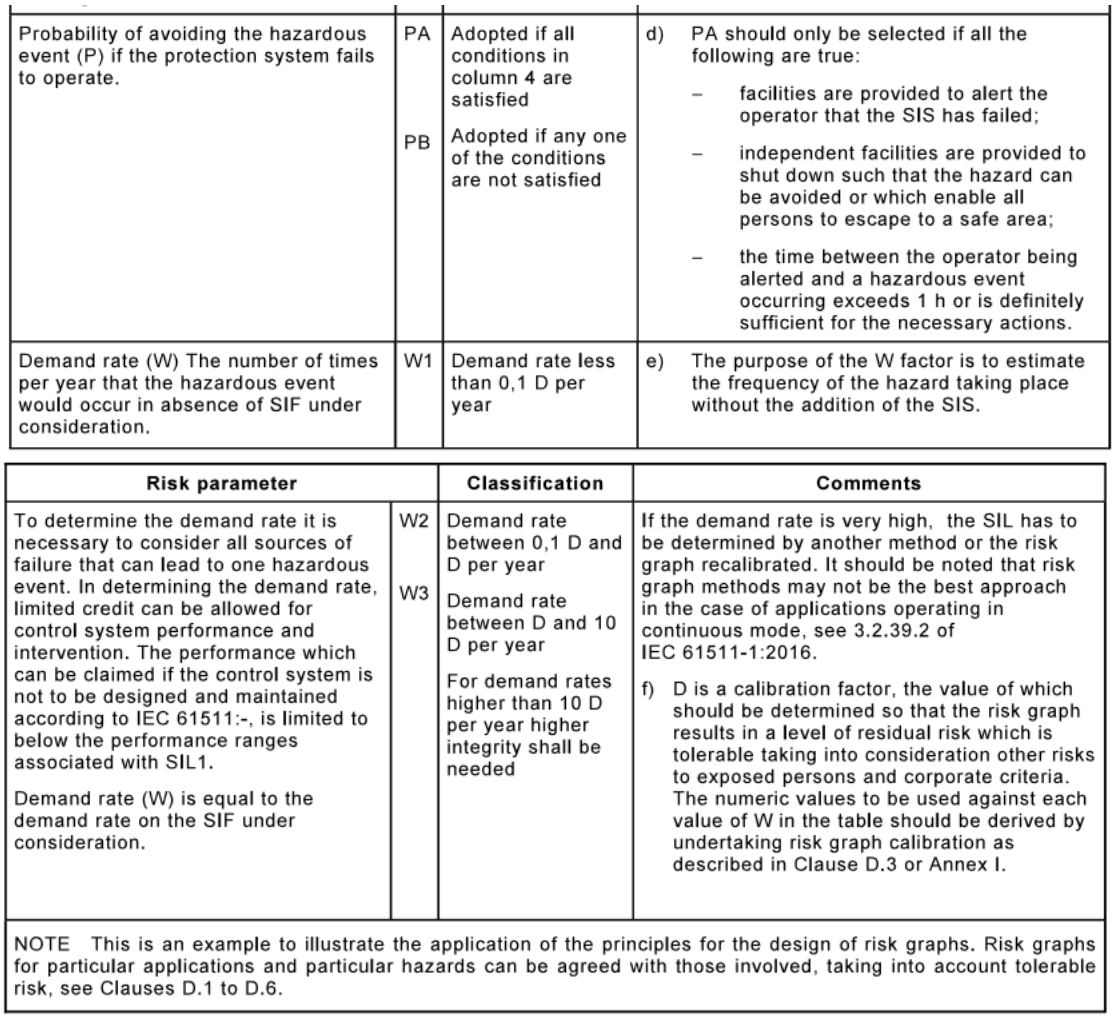
Appendix C

Calibrated Risk Graph Category



Risk parameter		Classification	Comments
Consequence (C) Number of fatalities	CA	Minor injury	a) The classification system has been developed to deal with injury and death to people.
This can be calculated by determining the numbers of people present when the area exposed to the hazard is occupied and multiplying by the vulnerability to the identified hazard.	CB	Range 0,01 to 0,1	b) For the interpretation of CA, CB, CC and CD, the consequences of the accident and normal healing should be taken into account.
	CC	Range >0,1 to 1,0	
The vulnerability is determined by the nature of the hazard being protected against. The following factors can be used: V = 0,01 Small release of flammable or toxic material V = 0,1 Large release of flammable or toxic material V = 0,5 As above but also a high probability of catching fire or highly toxic material V = 1 Rupture or explosion	CD	Range >1,0	
Occupancy (F) This is calculated by determining the proportional length of time the area exposed to the hazard is occupied during a normal working period.	FA	Rare to more frequent exposure in the hazardous zone. Occupancy less than 0,1	c) See comment a) above.
NOTE 1 If the time in the hazardous area is different depending on the shift being operated then the maximum should be selected. NOTE 2 It is only appropriate to use FA where it can be shown that the demand rate is random and not related to when occupancy could be higher than normal. The latter is usually the case with demands which occur at equipment start-up or during the investigation of abnormalities.	FB	Frequent to permanent exposure in the hazardous zone	

Figure C.1: **Calibration of the General Purpose Risk Graph** (1/2) (IEC 61511 :2016)

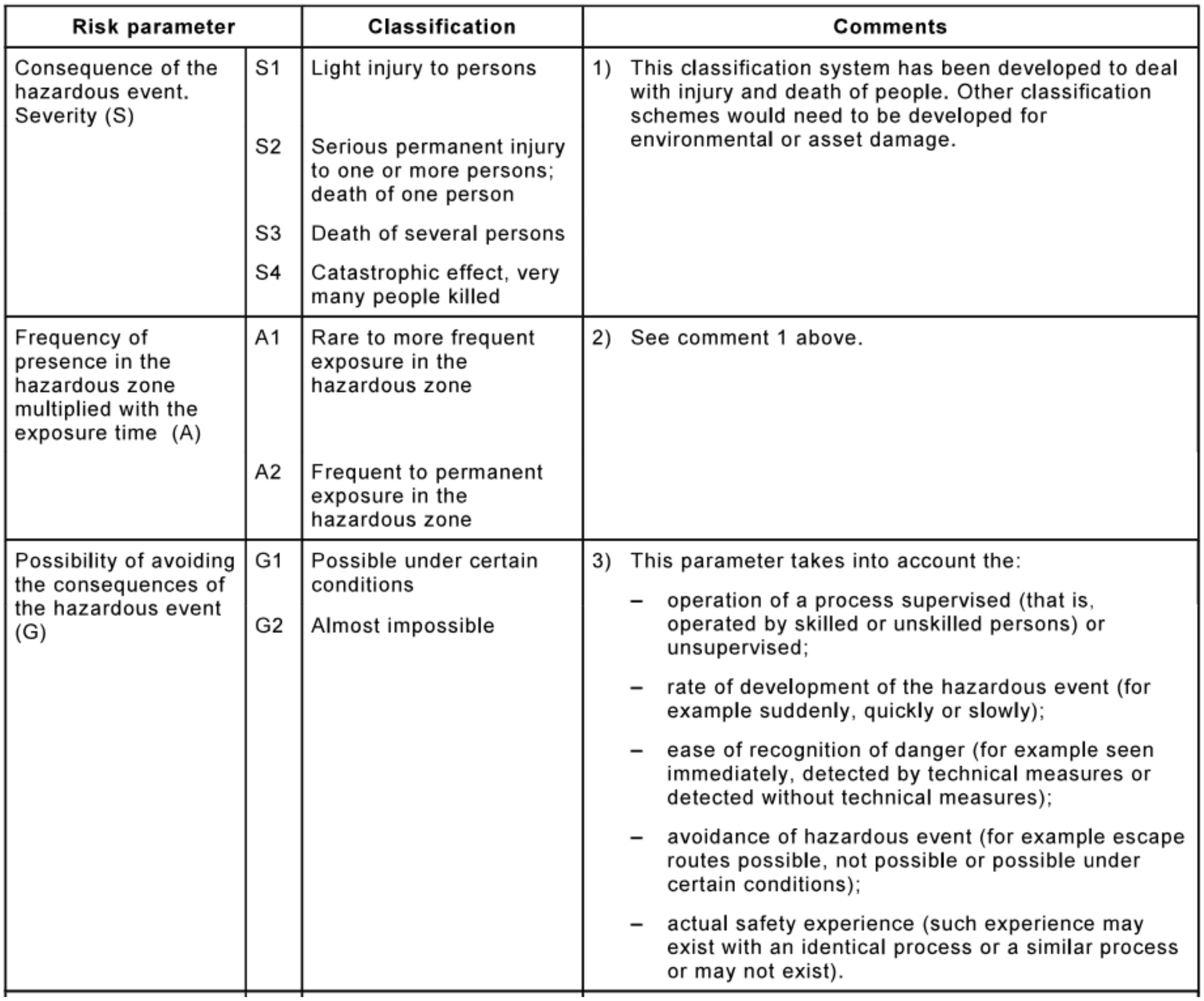


Risk parameter		Classification	Comments
Probability of avoiding the hazardous event (P) if the protection system fails to operate.	PA PB	Adopted if all conditions in column 4 are satisfied Adopted if any one of the conditions are not satisfied	d) PA should only be selected if all the following are true: – facilities are provided to alert the operator that the SIS has failed; – independent facilities are provided to shut down such that the hazard can be avoided or which enable all persons to escape to a safe area; – the time between the operator being alerted and a hazardous event occurring exceeds 1 h or is definitely sufficient for the necessary actions.
Demand rate (W) The number of times per year that the hazardous event would occur in absence of SIF under consideration.	W1	Demand rate less than 0,1 D per year	e) The purpose of the W factor is to estimate the frequency of the hazard taking place without the addition of the SIS.
To determine the demand rate it is necessary to consider all sources of failure that can lead to one hazardous event. In determining the demand rate, limited credit can be allowed for control system performance and intervention. The performance which can be claimed if the control system is not to be designed and maintained according to IEC 61511:-, is limited to below the performance ranges associated with SIL1. Demand rate (W) is equal to the demand rate on the SIF under consideration.	W2 W3	Demand rate between 0,1 D and D per year Demand rate between D and 10 D per year For demand rates higher than 10 D per year higher integrity shall be needed	If the demand rate is very high, the SIL has to be determined by another method or the risk graph recalibrated. It should be noted that risk graph methods may not be the best approach in the case of applications operating in continuous mode, see 3.2.39.2 of IEC 61511-1:2016. f) D is a calibration factor, the value of which should be determined so that the risk graph results in a level of residual risk which is tolerable taking into consideration other risks to exposed persons and corporate criteria. The numeric values to be used against each value of W in the table should be derived by undertaking risk graph calibration as described in Clause D.3 or Annex I.
NOTE This is an example to illustrate the application of the principles for the design of risk graphs. Risk graphs for particular applications and particular hazards can be agreed with those involved, taking into account tolerable risk, see Clauses D.1 to D.6.			

Figure C.2: **Calibration of the General Purpose Risk Graph** (2/2) (IEC 61511 :2016)

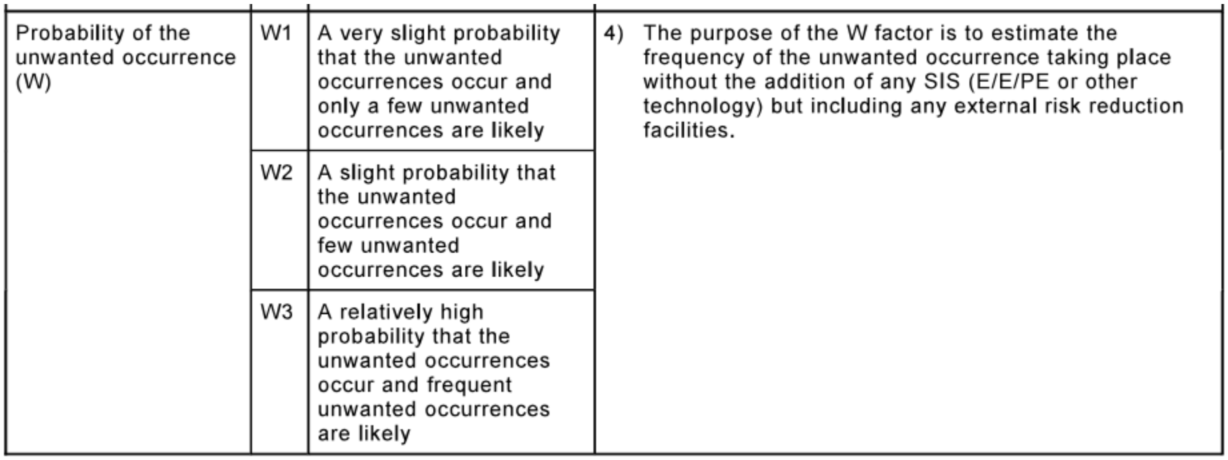
Appendix D

Risk Graph Category



Risk parameter		Classification	Comments
Consequence of the hazardous event. Severity (S)	S1	Light injury to persons	1) This classification system has been developed to deal with injury and death of people. Other classification schemes would need to be developed for environmental or asset damage.
	S2	Serious permanent injury to one or more persons; death of one person	
	S3	Death of several persons	
	S4	Catastrophic effect, very many people killed	
Frequency of presence in the hazardous zone multiplied with the exposure time (A)	A1	Rare to more frequent exposure in the hazardous zone	2) See comment 1 above.
	A2	Frequent to permanent exposure in the hazardous zone	
Possibility of avoiding the consequences of the hazardous event (G)	G1	Possible under certain conditions	3) This parameter takes into account the: – operation of a process supervised (that is, operated by skilled or unskilled persons) or unsupervised; – rate of development of the hazardous event (for example suddenly, quickly or slowly); – ease of recognition of danger (for example seen immediately, detected by technical measures or detected without technical measures); – avoidance of hazardous event (for example escape routes possible, not possible or possible under certain conditions); – actual safety experience (such experience may exist with an identical process or a similar process or may not exist).
	G2	Almost impossible	

Figure D.1: **Data of Risk Graph** (1/2) (IEC 61511 :2016)

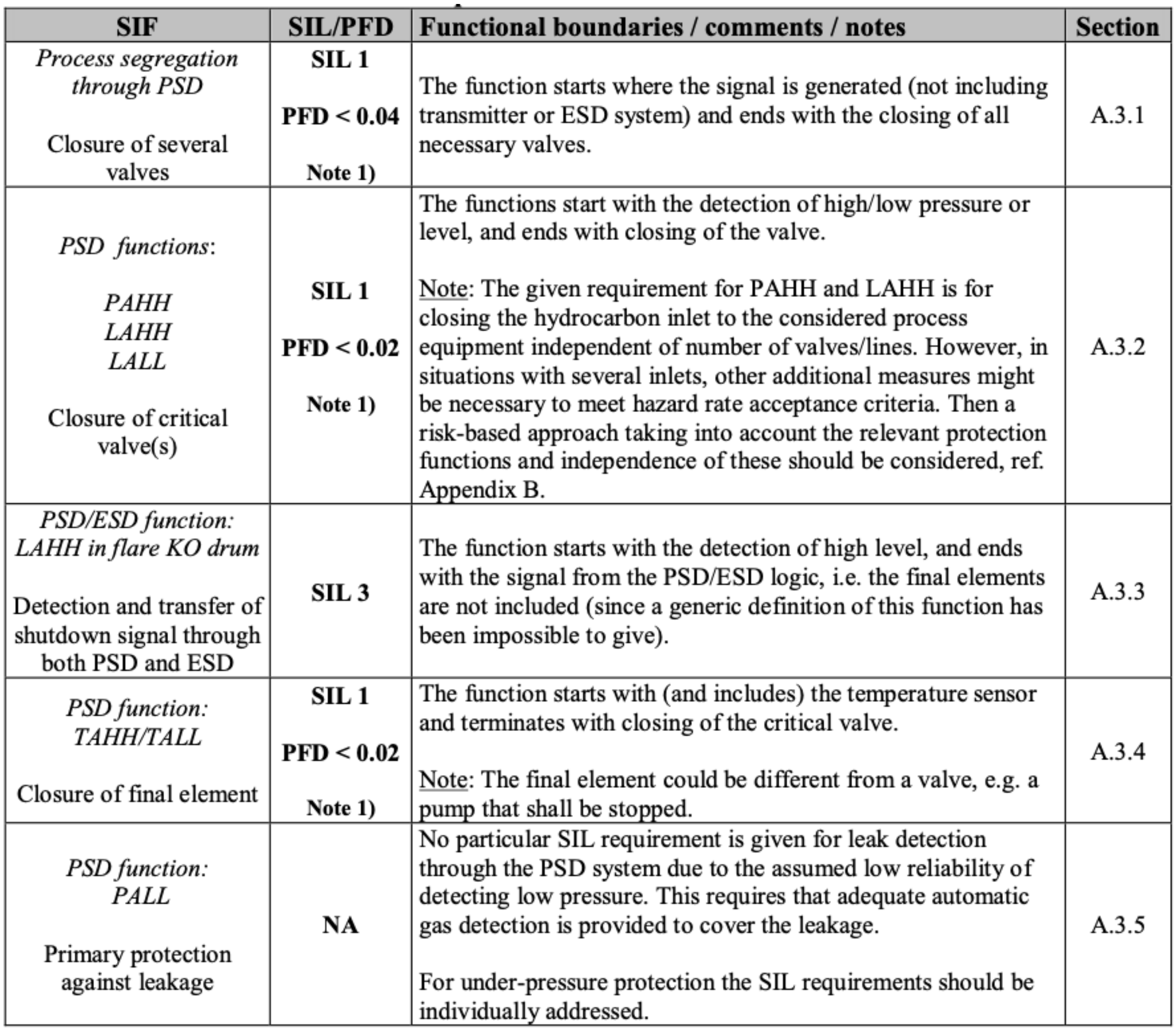


Probability of the unwanted occurrence (W)	W1	A very slight probability that the unwanted occurrences occur and only a few unwanted occurrences are likely	4) The purpose of the W factor is to estimate the frequency of the unwanted occurrence taking place without the addition of any SIS (E/E/PE or other technology) but including any external risk reduction facilities.
	W2	A slight probability that the unwanted occurrences occur and few unwanted occurrences are likely	
	W3	A relatively high probability that the unwanted occurrences occur and frequent unwanted occurrences are likely	

Figure D.2: **Data of Risk Graph** (2/2) (IEC 61511 :2016)

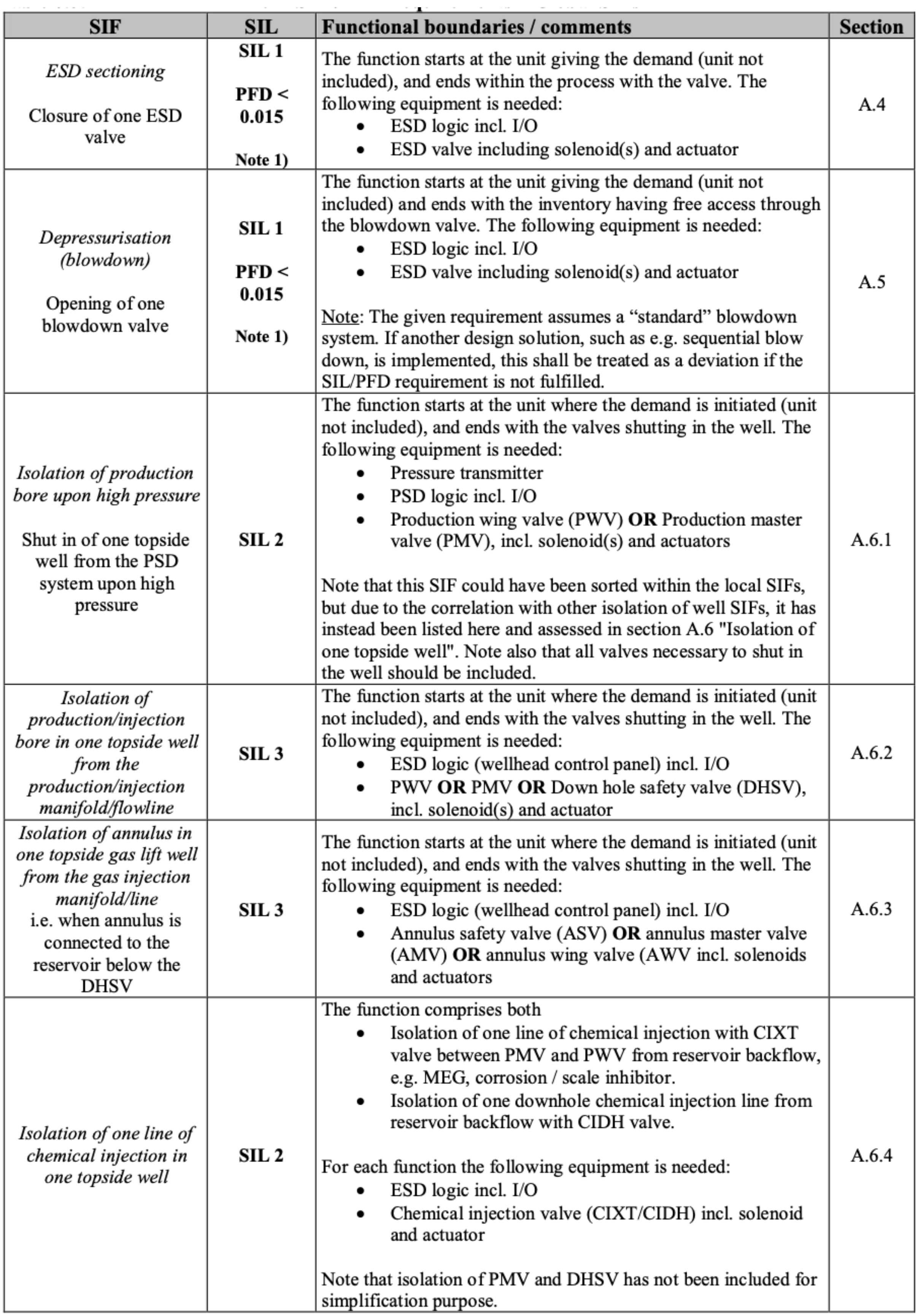
Appendix E

Minimum SIL Requirements from NOG 070



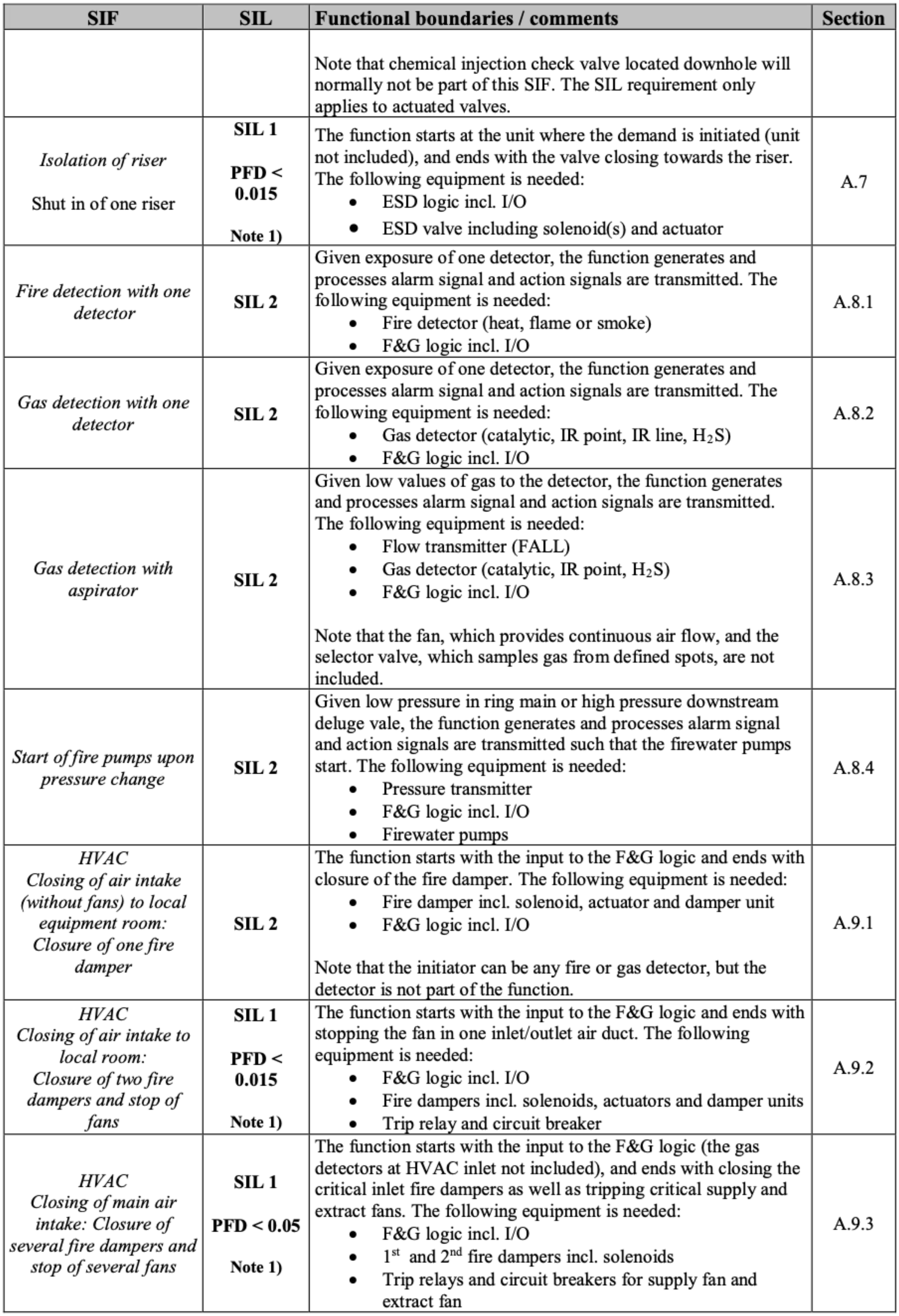
SIF	SIL/PFD	Functional boundaries / comments / notes	Section
Process segregation through PSD Closure of several valves	**SIL 1** **PFD < 0.04** **Note 1)**	The function starts where the signal is generated (not including transmitter or ESD system) and ends with the closing of all necessary valves.	A.3.1
PSD functions: *PAHH* *LAHH* *LALL* Closure of critical valve(s)	**SIL 1** **PFD < 0.02** **Note 1)**	The functions start with the detection of high/low pressure or level, and ends with closing of the valve. Note: The given requirement for PAHH and LAHH is for closing the hydrocarbon inlet to the considered process equipment independent of number of valves/lines. However, in situations with several inlets, other additional measures might be necessary to meet hazard rate acceptance criteria. Then a risk-based approach taking into account the relevant protection functions and independence of these should be considered, ref. Appendix B.	A.3.2
PSD/ESD function: LAHH in flare KO drum Detection and transfer of shutdown signal through both PSD and ESD	**SIL 3**	The function starts with the detection of high level, and ends with the signal from the PSD/ESD logic, i.e. the final elements are not included (since a generic definition of this function has been impossible to give).	A.3.3
PSD function: TAHH/TALL Closure of final element	**SIL 1** **PFD < 0.02** **Note 1)**	The function starts with (and includes) the temperature sensor and terminates with closing of the critical valve. Note: The final element could be different from a valve, e.g. a pump that shall be stopped.	A.3.4
PSD function: PALL Primary protection against leakage	**NA**	No particular SIL requirement is given for leak detection through the PSD system due to the assumed low reliability of detecting low pressure. This requires that adequate automatic gas detection is provided to cover the leakage. For under-pressure protection the SIL requirements should be individually addressed.	A.3.5

Figure E.1: **Minimum SIL Requirements - Local SIFs** (GL 070:2018)



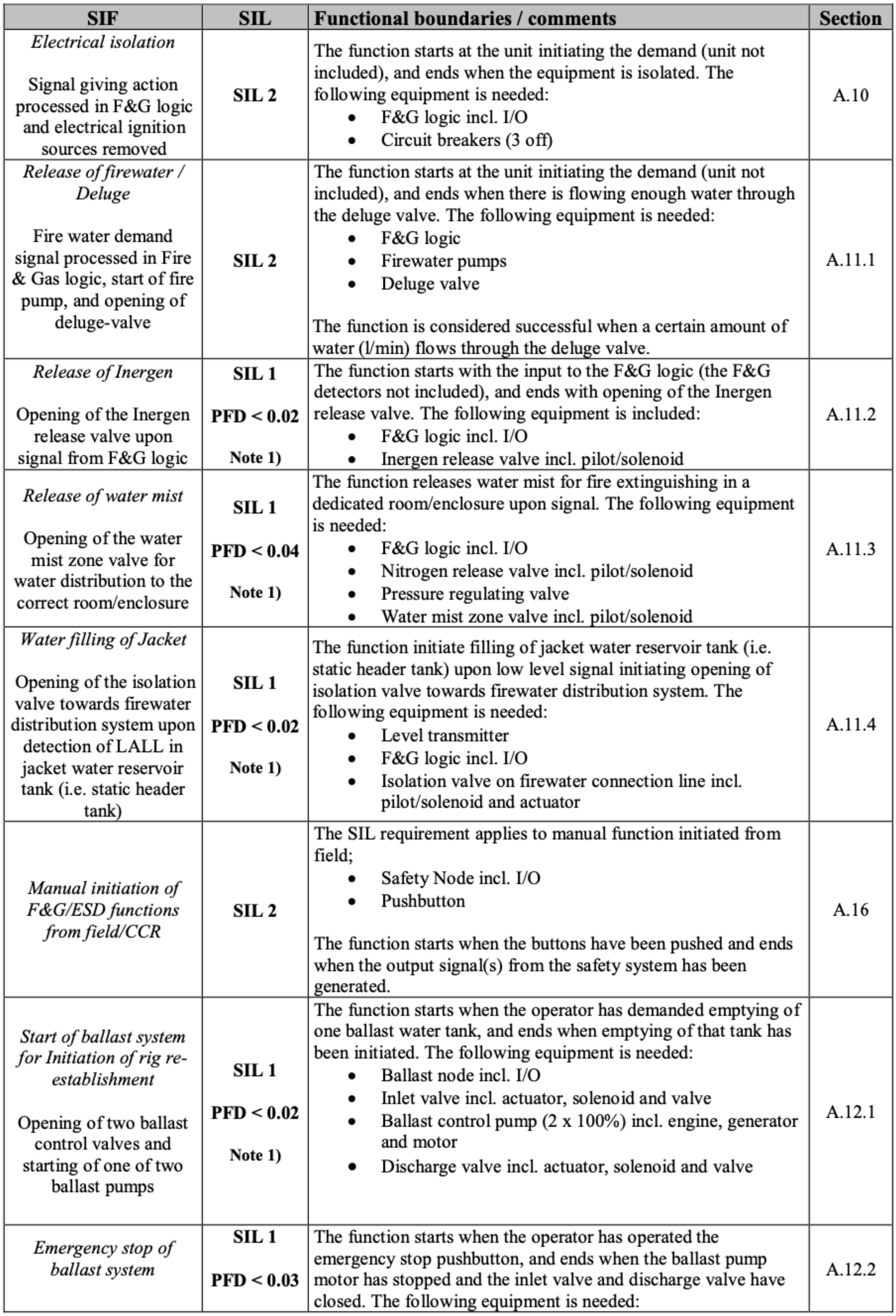
SIF	SIL	Functional boundaries / comments	Section
ESD sectioning Closure of one ESD valve	**SIL 1** **PFD < 0.015** **Note 1)**	The function starts at the unit giving the demand (unit not included), and ends within the process with the valve. The following equipment is needed: • ESD logic incl. I/O • ESD valve including solenoid(s) and actuator	A.4
Depressurisation (blowdown) Opening of one blowdown valve	**SIL 1** **PFD < 0.015** **Note 1)**	The function starts at the unit giving the demand (unit not included) and ends with the inventory having free access through the blowdown valve. The following equipment is needed: • ESD logic incl. I/O • ESD valve including solenoid(s) and actuator Note: The given requirement assumes a "standard" blowdown system. If another design solution, such as e.g. sequential blow down, is implemented, this shall be treated as a deviation if the SIL/PFD requirement is not fulfilled.	A.5
Isolation of production bore upon high pressure Shut in of one topside well from the PSD system upon high pressure	**SIL 2**	The function starts at the unit where the demand is initiated (unit not included), and ends with the valves shutting in the well. The following equipment is needed: • Pressure transmitter • PSD logic incl. I/O • Production wing valve (PWV) **OR** Production master valve (PMV), incl. solenoid(s) and actuators Note that this SIF could have been sorted within the local SIFs, but due to the correlation with other isolation of well SIFs, it has instead been listed here and assessed in section A.6 "Isolation of one topside well". Note also that all valves necessary to shut in the well should be included.	A.6.1
Isolation of production/injection bore in one topside well from the production/injection manifold/flowline	**SIL 3**	The function starts at the unit where the demand is initiated (unit not included), and ends with the valves shutting in the well. The following equipment is needed: • ESD logic (wellhead control panel) incl. I/O • PWV **OR** PMV **OR** Down hole safety valve (DHSV), incl. solenoid(s) and actuator	A.6.2
Isolation of annulus in one topside gas lift well from the gas injection manifold/line i.e. when annulus is connected to the reservoir below the DHSV	**SIL 3**	The function starts at the unit where the demand is initiated (unit not included), and ends with the valves shutting in the well. The following equipment is needed: • ESD logic (wellhead control panel) incl. I/O • Annulus safety valve (ASV) **OR** annulus master valve (AMV) **OR** annulus wing valve (AWV incl. solenoids and actuators	A.6.3
Isolation of one line of chemical injection in one topside well	**SIL 2**	The function comprises both • Isolation of one line of chemical injection with CIXT valve between PMV and PWV from reservoir backflow, e.g. MEG, corrosion / scale inhibitor. • Isolation of one downhole chemical injection line from reservoir backflow with CIDH valve. For each function the following equipment is needed: • ESD logic incl. I/O • Chemical injection valve (CIXT/CIDH) incl. solenoid and actuator Note that isolation of PMV and DHSV has not been included for simplification purpose.	A.6.4

Figure E.2: **Minimum SIL Requirements - Global SIFs** (1/3) (GL 070:2018)



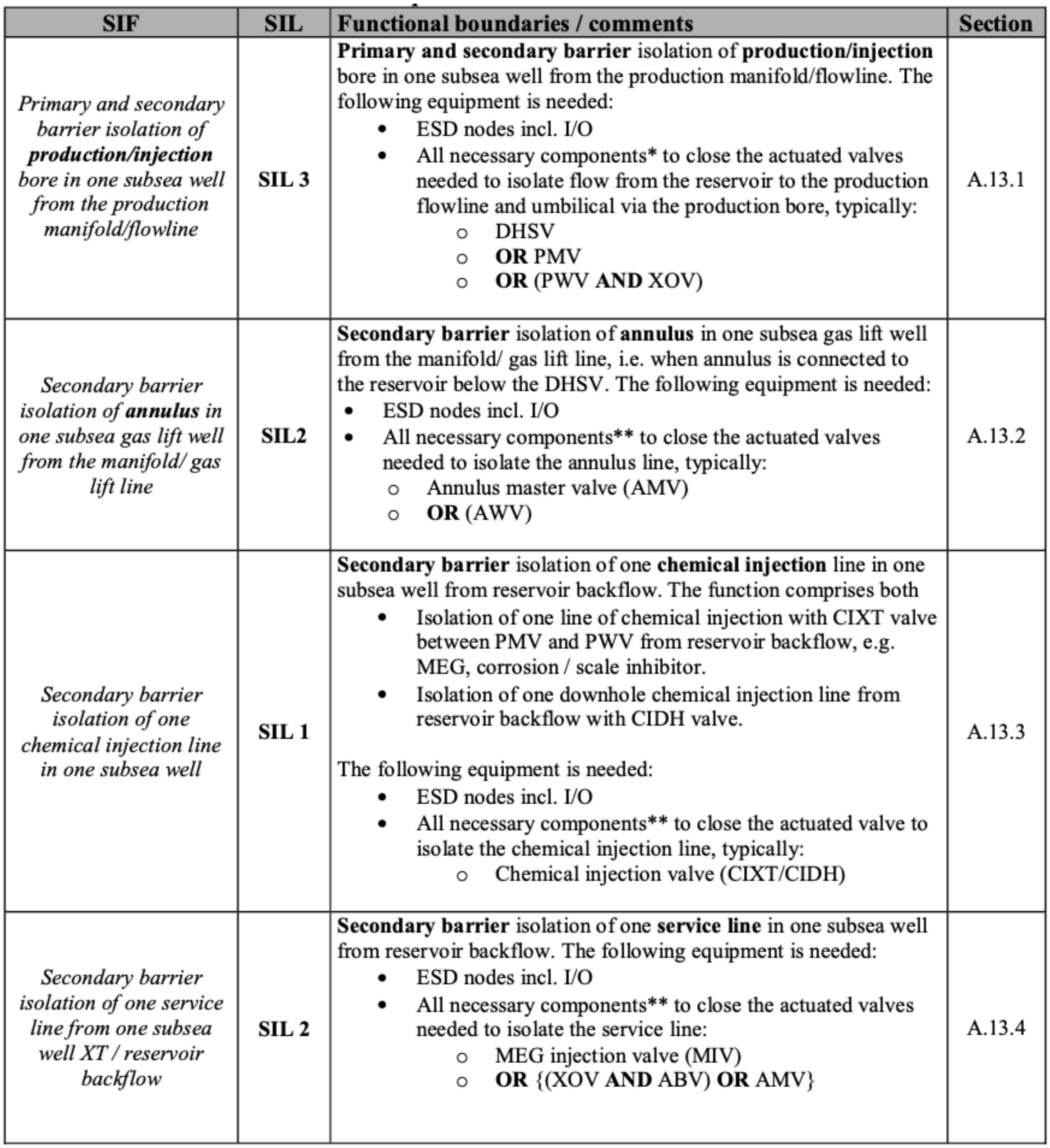
SIF	SIL	Functional boundaries / comments	Section
		Note that chemical injection check valve located downhole will normally not be part of this SIF. The SIL requirement only applies to actuated valves.	
Isolation of riser Shut in of one riser	**SIL 1** **PFD < 0.015** **Note 1)**	The function starts at the unit where the demand is initiated (unit not included), and ends with the valve closing towards the riser. The following equipment is needed: • ESD logic incl. I/O • ESD valve including solenoid(s) and actuator	A.7
Fire detection with one detector	**SIL 2**	Given exposure of one detector, the function generates and processes alarm signal and action signals are transmitted. The following equipment is needed: • Fire detector (heat, flame or smoke) • F&G logic incl. I/O	A.8.1
Gas detection with one detector	**SIL 2**	Given exposure of one detector, the function generates and processes alarm signal and action signals are transmitted. The following equipment is needed: • Gas detector (catalytic, IR point, IR line, H_2S) • F&G logic incl. I/O	A.8.2
Gas detection with aspirator	**SIL 2**	Given low values of gas to the detector, the function generates and processes alarm signal and action signals are transmitted. The following equipment is needed: • Flow transmitter (FALL) • Gas detector (catalytic, IR point, H_2S) • F&G logic incl. I/O Note that the fan, which provides continuous air flow, and the selector valve, which samples gas from defined spots, are not included.	A.8.3
Start of fire pumps upon pressure change	**SIL 2**	Given low pressure in ring main or high pressure downstream deluge vale, the function generates and processes alarm signal and action signals are transmitted such that the firewater pumps start. The following equipment is needed: • Pressure transmitter • F&G logic incl. I/O • Firewater pumps	A.8.4
HVAC *Closing of air intake (without fans) to local equipment room: Closure of one fire damper*	**SIL 2**	The function starts with the input to the F&G logic and ends with closure of the fire damper. The following equipment is needed: • Fire damper incl. solenoid, actuator and damper unit • F&G logic incl. I/O Note that the initiator can be any fire or gas detector, but the detector is not part of the function.	A.9.1
HVAC *Closing of air intake to local room: Closure of two fire dampers and stop of fans*	**SIL 1** **PFD < 0.015** **Note 1)**	The function starts with the input to the F&G logic and ends with stopping the fan in one inlet/outlet air duct. The following equipment is needed: • F&G logic incl. I/O • Fire dampers incl. solenoids, actuators and damper units • Trip relay and circuit breaker	A.9.2
HVAC *Closing of main air intake: Closure of several fire dampers and stop of several fans*	**SIL 1** **PFD < 0.05** **Note 1)**	The function starts with the input to the F&G logic (the gas detectors at HVAC inlet not included), and ends with closing the critical inlet fire dampers as well as tripping critical supply and extract fans. The following equipment is needed: • F&G logic incl. I/O • 1st and 2nd fire dampers incl. solenoids • Trip relays and circuit breakers for supply fan and extract fan	A.9.3

Figure E.3: **Minimum SIL Requirements - Global SIFs** (2/3) (GL 070:2018)



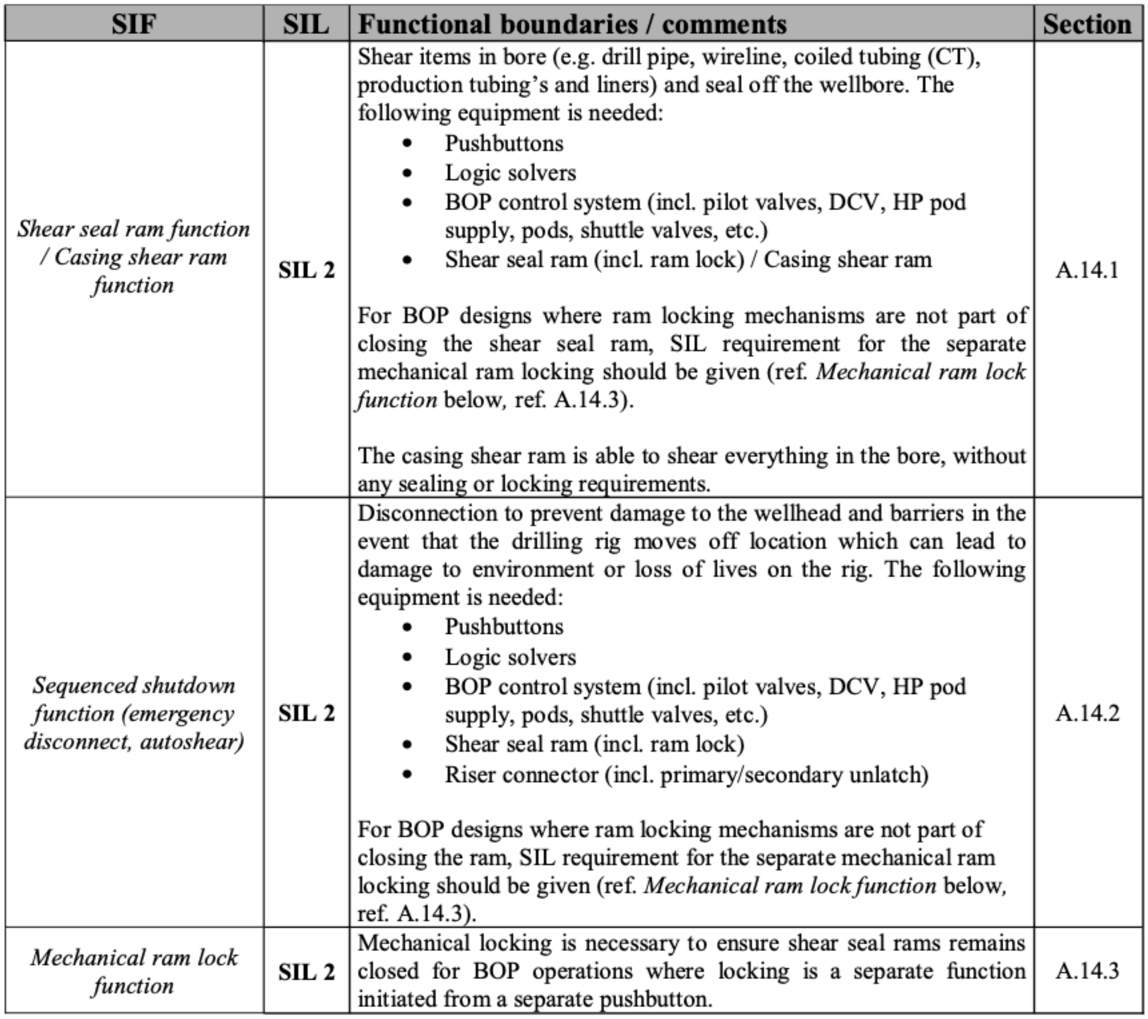
SIF	SIL	Functional boundaries / comments	Section
Electrical isolation Signal giving action processed in F&G logic and electrical ignition sources removed	**SIL 2**	The function starts at the unit initiating the demand (unit not included), and ends when the equipment is isolated. The following equipment is needed: • F&G logic incl. I/O • Circuit breakers (3 off)	A.10
Release of firewater / Deluge Fire water demand signal processed in Fire & Gas logic, start of fire pump, and opening of deluge-valve	**SIL 2**	The function starts at the unit initiating the demand (unit not included), and ends when there is flowing enough water through the deluge valve. The following equipment is needed: • F&G logic • Firewater pumps • Deluge valve The function is considered successful when a certain amount of water (l/min) flows through the deluge valve.	A.11.1
Release of Inergen Opening of the Inergen release valve upon signal from F&G logic	**SIL 1** **PFD < 0.02** **Note 1)**	The function starts with the input to the F&G logic (the F&G detectors not included), and ends with opening of the Inergen release valve. The following equipment is included: • F&G logic incl. I/O • Inergen release valve incl. pilot/solenoid	A.11.2
Release of water mist Opening of the water mist zone valve for water distribution to the correct room/enclosure	**SIL 1** **PFD < 0.04** **Note 1)**	The function releases water mist for fire extinguishing in a dedicated room/enclosure upon signal. The following equipment is needed: • F&G logic incl. I/O • Nitrogen release valve incl. pilot/solenoid • Pressure regulating valve • Water mist zone valve incl. pilot/solenoid	A.11.3
Water filling of Jacket Opening of the isolation valve towards firewater distribution system upon detection of LALL in jacket water reservoir tank (i.e. static header tank)	**SIL 1** **PFD < 0.02** **Note 1)**	The function initiate filling of jacket water reservoir tank (i.e. static header tank) upon low level signal initiating opening of isolation valve towards firewater distribution system. The following equipment is needed: • Level transmitter • F&G logic incl. I/O • Isolation valve on firewater connection line incl. pilot/solenoid and actuator	A.11.4
Manual initiation of F&G/ESD functions from field/CCR	**SIL 2**	The SIL requirement applies to manual function initiated from field; • Safety Node incl. I/O • Pushbutton The function starts when the buttons have been pushed and ends when the output signal(s) from the safety system has been generated.	A.16
Start of ballast system for Initiation of rig re-establishment Opening of two ballast control valves and starting of one of two ballast pumps	**SIL 1** **PFD < 0.02** **Note 1)**	The function starts when the operator has demanded emptying of one ballast water tank, and ends when emptying of that tank has been initiated. The following equipment is needed: • Ballast node incl. I/O • Inlet valve incl. actuator, solenoid and valve • Ballast control pump (2 x 100%) incl. engine, generator and motor • Discharge valve incl. actuator, solenoid and valve	A.12.1
Emergency stop of ballast system	**SIL 1** **PFD < 0.03**	The function starts when the operator has operated the emergency stop pushbutton, and ends when the ballast pump motor has stopped and the inlet valve and discharge valve have closed. The following equipment is needed:	A.12.2

Figure E.4: **Minimum SIL Requirements -Global SIFs** (3/3) (GL 070:2018)



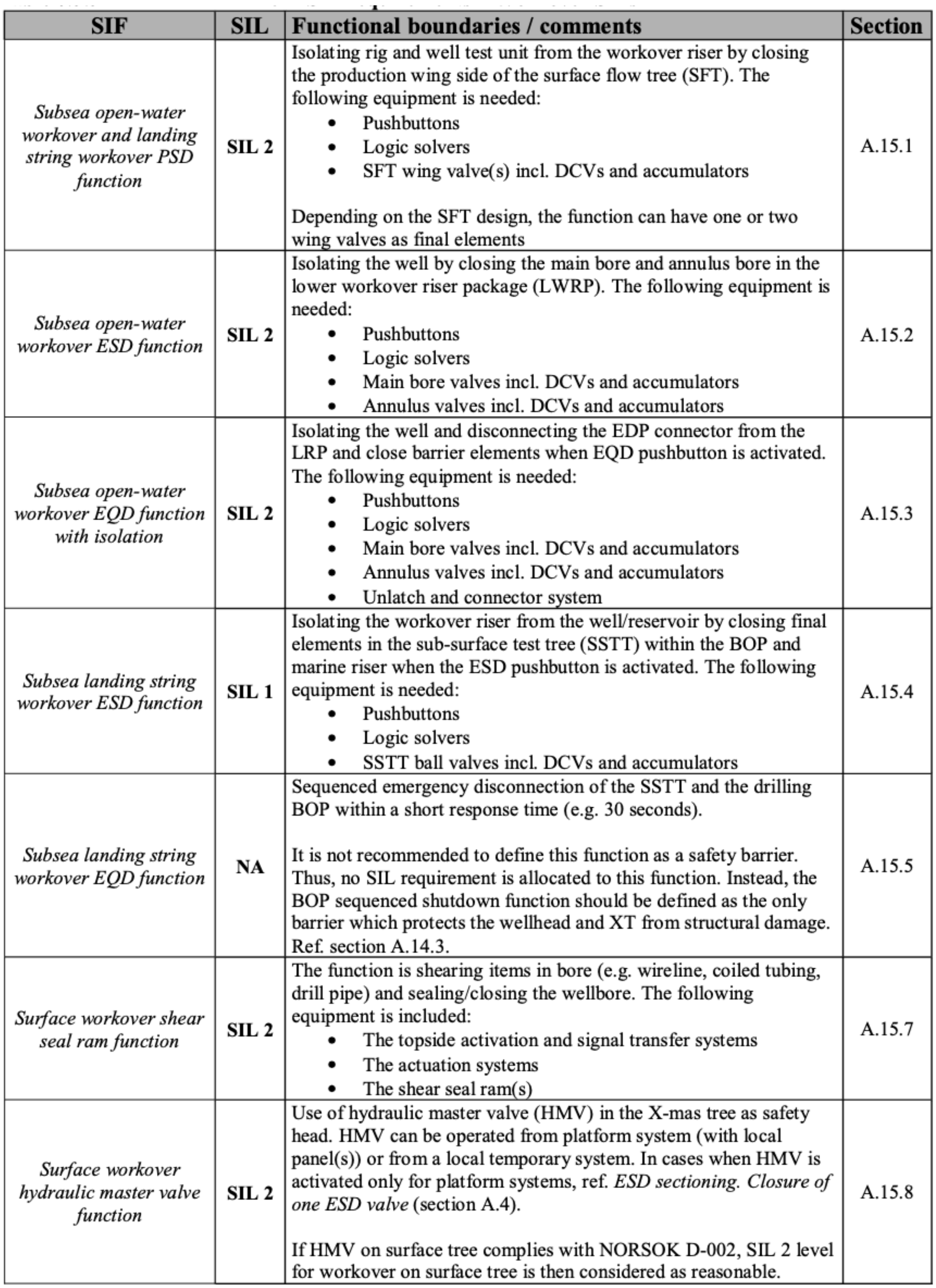
SIF	SIL	Functional boundaries / comments	Section
Primary and secondary barrier isolation of ***production/injection*** *bore in one subsea well from the production manifold/flowline*	**SIL 3**	**Primary and secondary barrier** isolation of **production/injection** bore in one subsea well from the production manifold/flowline. The following equipment is needed: • ESD nodes incl. I/O • All necessary components* to close the actuated valves needed to isolate flow from the reservoir to the production flowline and umbilical via the production bore, typically: o DHSV o **OR** PMV o **OR** (PWV **AND** XOV)	A.13.1
Secondary barrier isolation of ***annulus*** *in one subsea gas lift well from the manifold/ gas lift line*	**SIL2**	**Secondary barrier** isolation of **annulus** in one subsea gas lift well from the manifold/ gas lift line, i.e. when annulus is connected to the reservoir below the DHSV. The following equipment is needed: • ESD nodes incl. I/O • All necessary components** to close the actuated valves needed to isolate the annulus line, typically: o Annulus master valve (AMV) o **OR** (AWV)	A.13.2
Secondary barrier isolation of one chemical injection line in one subsea well	**SIL 1**	**Secondary barrier** isolation of one **chemical injection** line in one subsea well from reservoir backflow. The function comprises both • Isolation of one line of chemical injection with CIXT valve between PMV and PWV from reservoir backflow, e.g. MEG, corrosion / scale inhibitor. • Isolation of one downhole chemical injection line from reservoir backflow with CIDH valve. The following equipment is needed: • ESD nodes incl. I/O • All necessary components** to close the actuated valve to isolate the chemical injection line, typically: o Chemical injection valve (CIXT/CIDH)	A.13.3
Secondary barrier isolation of one service line from one subsea well XT / reservoir backflow	**SIL 2**	**Secondary barrier** isolation of one **service line** in one subsea well from reservoir backflow. The following equipment is needed: • ESD nodes incl. I/O • All necessary components** to close the actuated valves needed to isolate the service line: o MEG injection valve (MIV) o **OR** {(XOV **AND** ABV) **OR** AMV}	A.13.4

Figure E.5: **Minimum SIL Requirements - Subsea SIFs** (1/2) (GL 070:2018)



SIF	SIL	Functional boundaries / comments	Section
Shear seal ram function / Casing shear ram function	**SIL 2**	Shear items in bore (e.g. drill pipe, wireline, coiled tubing (CT), production tubing's and liners) and seal off the wellbore. The following equipment is needed: • Pushbuttons • Logic solvers • BOP control system (incl. pilot valves, DCV, HP pod supply, pods, shuttle valves, etc.) • Shear seal ram (incl. ram lock) / Casing shear ram For BOP designs where ram locking mechanisms are not part of closing the shear seal ram, SIL requirement for the separate mechanical ram locking should be given (ref. *Mechanical ram lock function* below, ref. A.14.3). The casing shear ram is able to shear everything in the bore, without any sealing or locking requirements.	A.14.1
Sequenced shutdown function (emergency disconnect, autoshear)	**SIL 2**	Disconnection to prevent damage to the wellhead and barriers in the event that the drilling rig moves off location which can lead to damage to environment or loss of lives on the rig. The following equipment is needed: • Pushbuttons • Logic solvers • BOP control system (incl. pilot valves, DCV, HP pod supply, pods, shuttle valves, etc.) • Shear seal ram (incl. ram lock) • Riser connector (incl. primary/secondary unlatch) For BOP designs where ram locking mechanisms are not part of closing the ram, SIL requirement for the separate mechanical ram locking should be given (ref. *Mechanical ram lock function* below, ref. A.14.3).	A.14.2
Mechanical ram lock function	**SIL 2**	Mechanical locking is necessary to ensure shear seal rams remains closed for BOP operations where locking is a separate function initiated from a separate pushbutton.	A.14.3

Figure E.6: **Minimum SIL Requirements - Subsea SIFs** (2/2) (GL 070:2018)

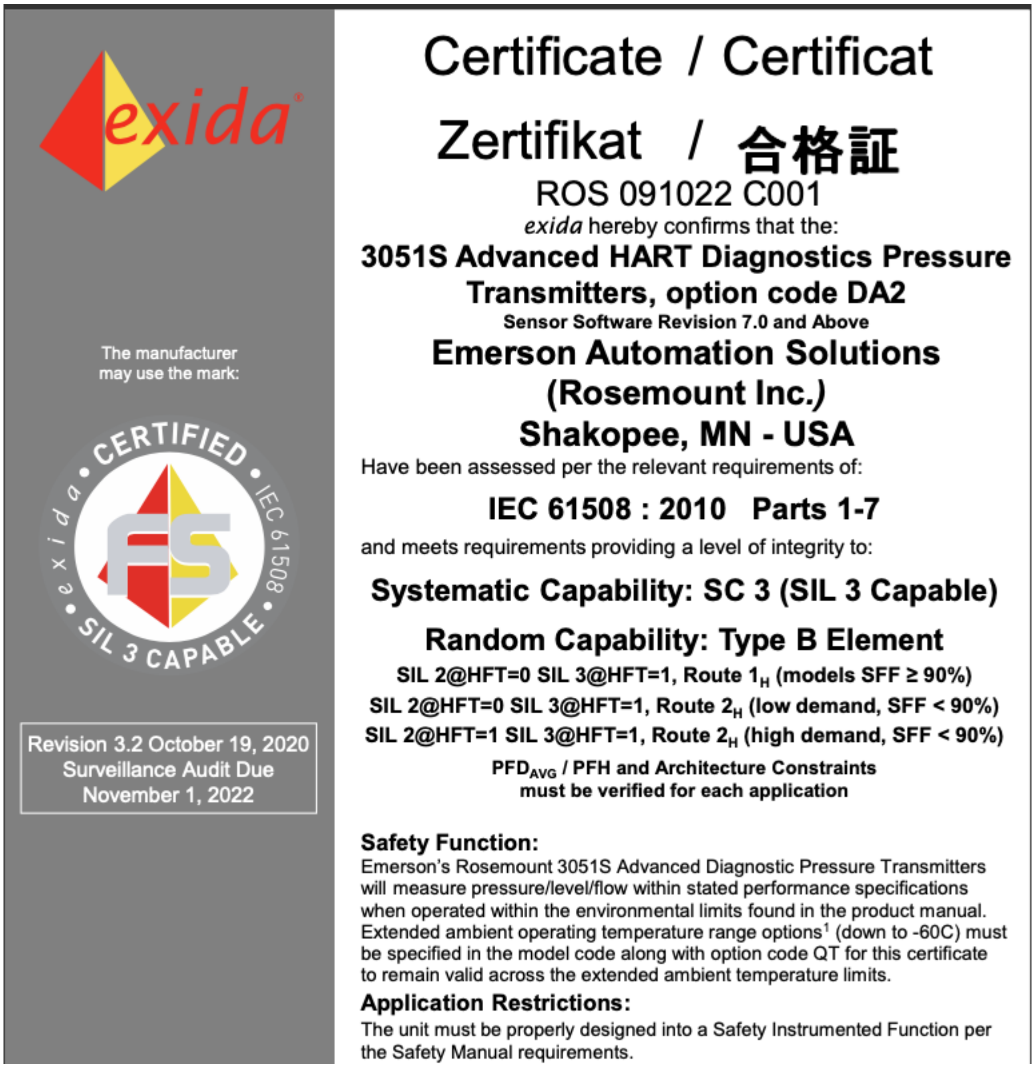


SIF	SIL	Functional boundaries / comments	Section
Subsea open-water workover and landing string workover PSD function	**SIL 2**	Isolating rig and well test unit from the workover riser by closing the production wing side of the surface flow tree (SFT). The following equipment is needed: • Pushbuttons • Logic solvers • SFT wing valve(s) incl. DCVs and accumulators Depending on the SFT design, the function can have one or two wing valves as final elements	A.15.1
Subsea open-water workover ESD function	**SIL 2**	Isolating the well by closing the main bore and annulus bore in the lower workover riser package (LWRP). The following equipment is needed: • Pushbuttons • Logic solvers • Main bore valves incl. DCVs and accumulators • Annulus valves incl. DCVs and accumulators	A.15.2
Subsea open-water workover EQD function with isolation	**SIL 2**	Isolating the well and disconnecting the EDP connector from the LRP and close barrier elements when EQD pushbutton is activated. The following equipment is needed: • Pushbuttons • Logic solvers • Main bore valves incl. DCVs and accumulators • Annulus valves incl. DCVs and accumulators • Unlatch and connector system	A.15.3
Subsea landing string workover ESD function	**SIL 1**	Isolating the workover riser from the well/reservoir by closing final elements in the sub-surface test tree (SSTT) within the BOP and marine riser when the ESD pushbutton is activated. The following equipment is needed: • Pushbuttons • Logic solvers • SSTT ball valves incl. DCVs and accumulators	A.15.4
Subsea landing string workover EQD function	**NA**	Sequenced emergency disconnection of the SSTT and the drilling BOP within a short response time (e.g. 30 seconds). It is not recommended to define this function as a safety barrier. Thus, no SIL requirement is allocated to this function. Instead, the BOP sequenced shutdown function should be defined as the only barrier which protects the wellhead and XT from structural damage. Ref. section A.14.3.	A.15.5
Surface workover shear seal ram function	**SIL 2**	The function is shearing items in bore (e.g. wireline, coiled tubing, drill pipe) and sealing/closing the wellbore. The following equipment is included: • The topside activation and signal transfer systems • The actuation systems • The shear seal ram(s)	A.15.7
Surface workover hydraulic master valve function	**SIL 2**	Use of hydraulic master valve (HMV) in the X-mas tree as safety head. HMV can be operated from platform system (with local panel(s)) or from a local temporary system. In cases when HMV is activated only for platform systems, ref. *ESD sectioning. Closure of one ESD valve* (section A.4). If HMV on surface tree complies with NORSOK D-002, SIL 2 level for workover on surface tree is then considered as reasonable.	A.15.8

Figure E.7: **Minimum SIL Requirements - Workover SIFs** (GL 070:2018)

Appendix F

Equipment SIL Certificates



exida
CERTIFIED
exida
IEC 61508
SIL 3 CAPABLE
FS

The manufacturer
may use the mark:

Revision 3.2 October 19, 2020
Surveillance Audit Due
November 1, 2022

Certificate / Certificat

Zertifikat / 合格証

ROS 091022 C001

exida hereby confirms that the:

3051S Advanced HART Diagnostics Pressure Transmitters, option code DA2

Sensor Software Revision 7.0 and Above

Emerson Automation Solutions
(Rosemount Inc.)
Shakopee, MN - USA

Have been assessed per the relevant requirements of:

IEC 61508 : 2010 Parts 1-7

and meets requirements providing a level of integrity to:

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type B Element

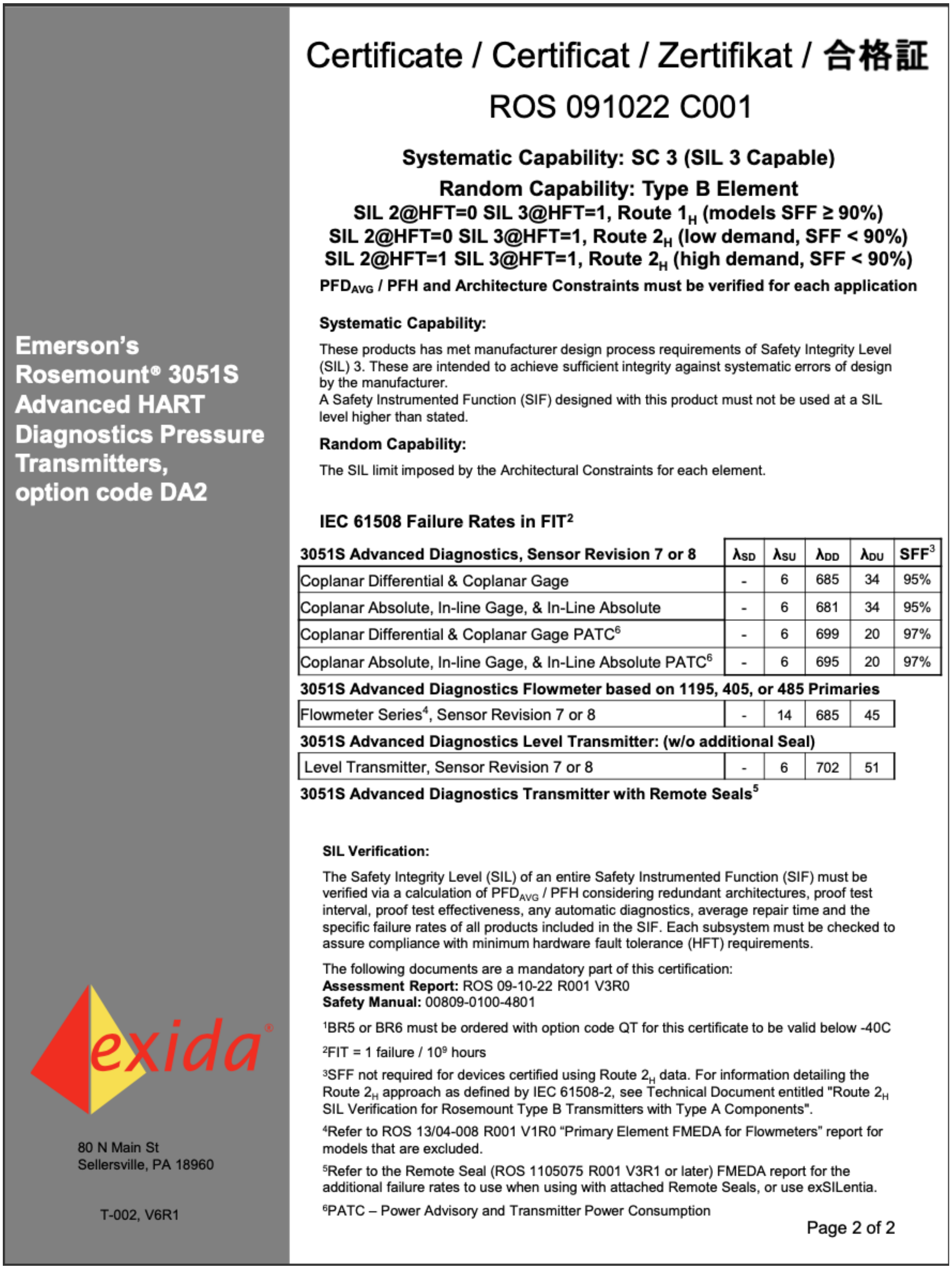
SIL 2@HFT=0 SIL 3@HFT=1, Route 1_H (models SFF ≥ 90%)
SIL 2@HFT=0 SIL 3@HFT=1, Route 2_H (low demand, SFF < 90%)
SIL 2@HFT=1 SIL 3@HFT=1, Route 2_H (high demand, SFF < 90%)

PFD_{AVG} / PFH and Architecture Constraints
must be verified for each application

Safety Function:
Emerson's Rosemount 3051S Advanced Diagnostic Pressure Transmitters will measure pressure/level/flow within stated performance specifications when operated within the environmental limits found in the product manual. Extended ambient operating temperature range options[1] (down to -60C) must be specified in the model code along with option code QT for this certificate to remain valid across the extended ambient temperature limits.

Application Restrictions:
The unit must be properly designed into a Safety Instrumented Function per the Safety Manual requirements.

Figure F.1: **Equipment SIL Certificate - Sensor** (1/2) (Exida)



Emerson's Rosemount® 3051S Advanced HART Diagnostics Pressure Transmitters, option code DA2

Certificate / Certificat / Zertifikat / 合格証

ROS 091022 C001

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type B Element

SIL 2@HFT=0 SIL 3@HFT=1, Route 1_H (models SFF ≥ 90%)

SIL 2@HFT=0 SIL 3@HFT=1, Route 2_H (low demand, SFF < 90%)

SIL 2@HFT=1 SIL 3@HFT=1, Route 2_H (high demand, SFF < 90%)

PFD$_{AVG}$ / PFH and Architecture Constraints must be verified for each application

Systematic Capability:

These products has met manufacturer design process requirements of Safety Integrity Level (SIL) 3. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer.
A Safety Instrumented Function (SIF) designed with this product must not be used at a SIL level higher than stated.

Random Capability:

The SIL limit imposed by the Architectural Constraints for each element.

IEC 61508 Failure Rates in FIT[2]

3051S Advanced Diagnostics, Sensor Revision 7 or 8	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF[3]
Coplanar Differential & Coplanar Gage	-	6	685	34	95%
Coplanar Absolute, In-line Gage, & In-Line Absolute	-	6	681	34	95%
Coplanar Differential & Coplanar Gage PATC[6]	-	6	699	20	97%
Coplanar Absolute, In-line Gage, & In-Line Absolute PATC[6]	-	6	695	20	97%
3051S Advanced Diagnostics Flowmeter based on 1195, 405, or 485 Primaries					
Flowmeter Series[4], Sensor Revision 7 or 8	-	14	685	45	
3051S Advanced Diagnostics Level Transmitter: (w/o additional Seal)					
Level Transmitter, Sensor Revision 7 or 8	-	6	702	51	
3051S Advanced Diagnostics Transmitter with Remote Seals[5]					

SIL Verification:

The Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) must be verified via a calculation of PFD$_{AVG}$ / PFH considering redundant architectures, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failure rates of all products included in the SIF. Each subsystem must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements.

The following documents are a mandatory part of this certification:
Assessment Report: ROS 09-10-22 R001 V3R0
Safety Manual: 00809-0100-4801

[1] BR5 or BR6 must be ordered with option code QT for this certificate to be valid below -40C

[2] FIT = 1 failure / 10^9 hours

[3] SFF not required for devices certified using Route 2_H data. For information detailing the Route 2_H approach as defined by IEC 61508-2, see Technical Document entitled "Route 2_H SIL Verification for Rosemount Type B Transmitters with Type A Components".

[4] Refer to ROS 13/04-008 R001 V1R0 "Primary Element FMEDA for Flowmeters" report for models that are excluded.

[5] Refer to the Remote Seal (ROS 1105075 R001 V3R1 or later) FMEDA report for the additional failure rates to use when using with attached Remote Seals, or use exSILentia.

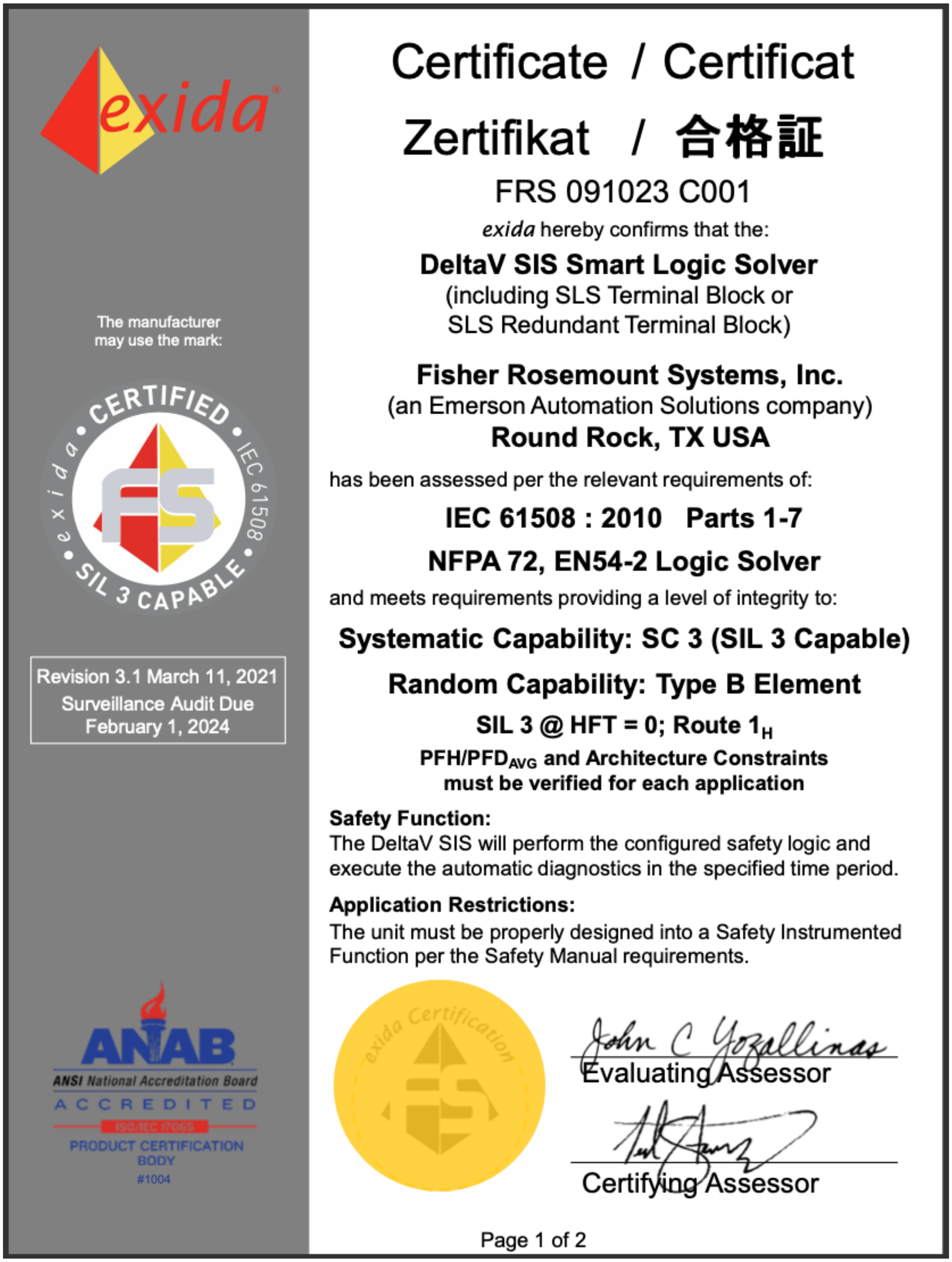
[6] PATC – Power Advisory and Transmitter Power Consumption

80 N Main St
Sellersville, PA 18960

T-002, V6R1

Page 2 of 2

Figure F.2: **Equipment SIL Certificate - Sensor** (2/2) (Exida)



exida

The manufacturer may use the mark:

CERTIFIED • IEC 61508 • SIL 3 CAPABLE • exida

Revision 3.1 March 11, 2021
Surveillance Audit Due
February 1, 2024

ANAB
ANSI National Accreditation Board
ACCREDITED
ISO/IEC 17065
PRODUCT CERTIFICATION BODY
#1004

Certificate / Certificat
Zertifikat / 合格証

FRS 091023 C001

exida hereby confirms that the:

DeltaV SIS Smart Logic Solver
(including SLS Terminal Block or
SLS Redundant Terminal Block)

Fisher Rosemount Systems, Inc.
(an Emerson Automation Solutions company)
Round Rock, TX USA

has been assessed per the relevant requirements of:

IEC 61508 : 2010 Parts 1-7

NFPA 72, EN54-2 Logic Solver

and meets requirements providing a level of integrity to:

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type B Element

SIL 3 @ HFT = 0; Route 1_H

PFH/PFD$_{AVG}$ and Architecture Constraints must be verified for each application

Safety Function:
The DeltaV SIS will perform the configured safety logic and execute the automatic diagnostics in the specified time period.

Application Restrictions:
The unit must be properly designed into a Safety Instrumented Function per the Safety Manual requirements.

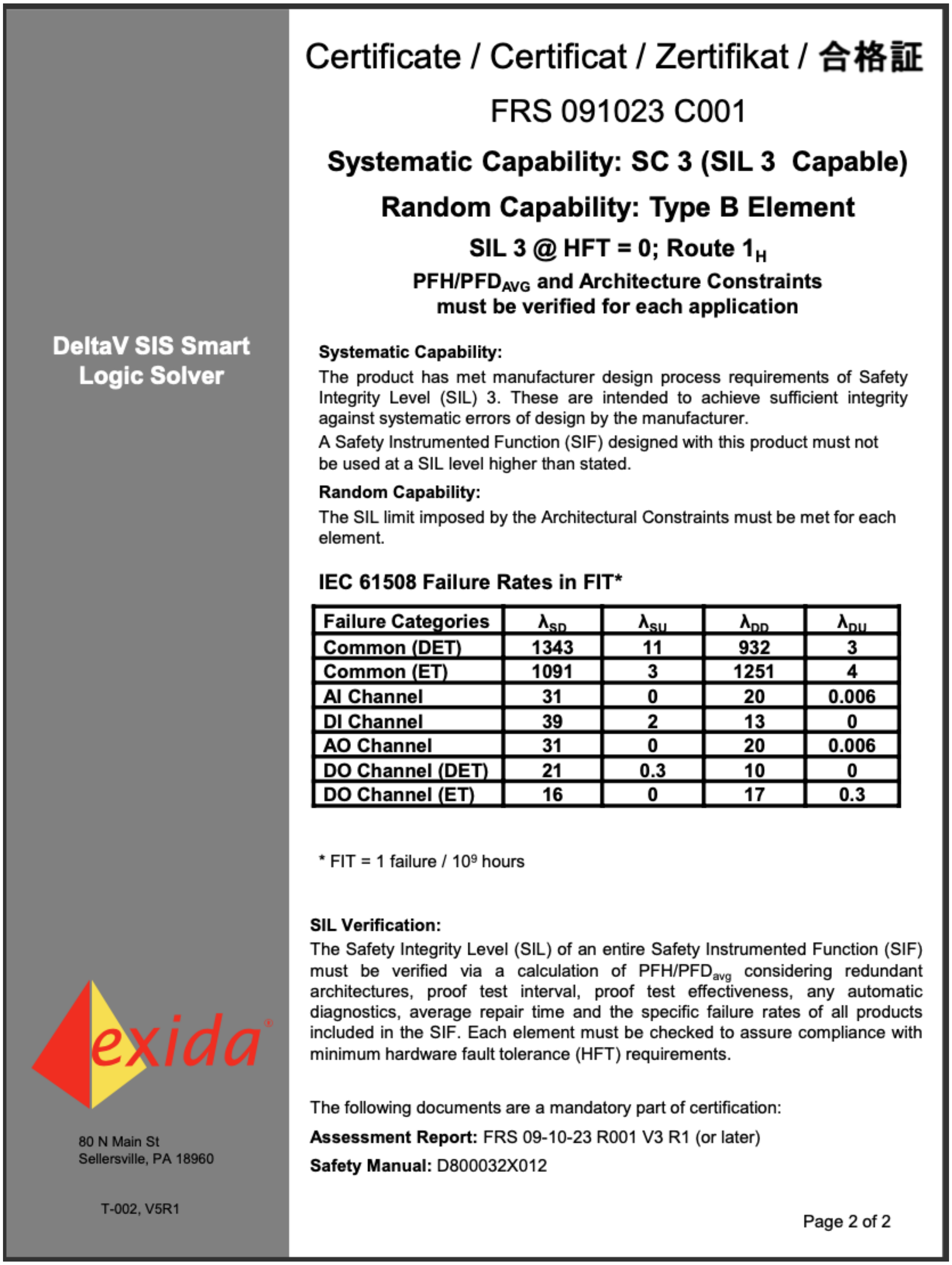
exida Certification

John C Yozallinas
Evaluating Assessor

Certifying Assessor

Page 1 of 2

Figure F.3: **Equipment SIL Certificate - Logic Solver** (1/2) (Exida)



DeltaV SIS Smart Logic Solver

Certificate / Certificat / Zertifikat / 合格証

FRS 091023 C001

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type B Element

SIL 3 @ HFT = 0; Route 1_H

PFH/PFD_{AVG} and Architecture Constraints must be verified for each application

Systematic Capability:

The product has met manufacturer design process requirements of Safety Integrity Level (SIL) 3. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer.

A Safety Instrumented Function (SIF) designed with this product must not be used at a SIL level higher than stated.

Random Capability:

The SIL limit imposed by the Architectural Constraints must be met for each element.

IEC 61508 Failure Rates in FIT*

Failure Categories	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}
Common (DET)	1343	11	932	3
Common (ET)	1091	3	1251	4
AI Channel	31	0	20	0.006
DI Channel	39	2	13	0
AO Channel	31	0	20	0.006
DO Channel (DET)	21	0.3	10	0
DO Channel (ET)	16	0	17	0.3

* FIT = 1 failure / 10^9 hours

SIL Verification:

The Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) must be verified via a calculation of PFH/PFD_{avg} considering redundant architectures, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failure rates of all products included in the SIF. Each element must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements.

The following documents are a mandatory part of certification:

Assessment Report: FRS 09-10-23 R001 V3 R1 (or later)

Safety Manual: D800032X012

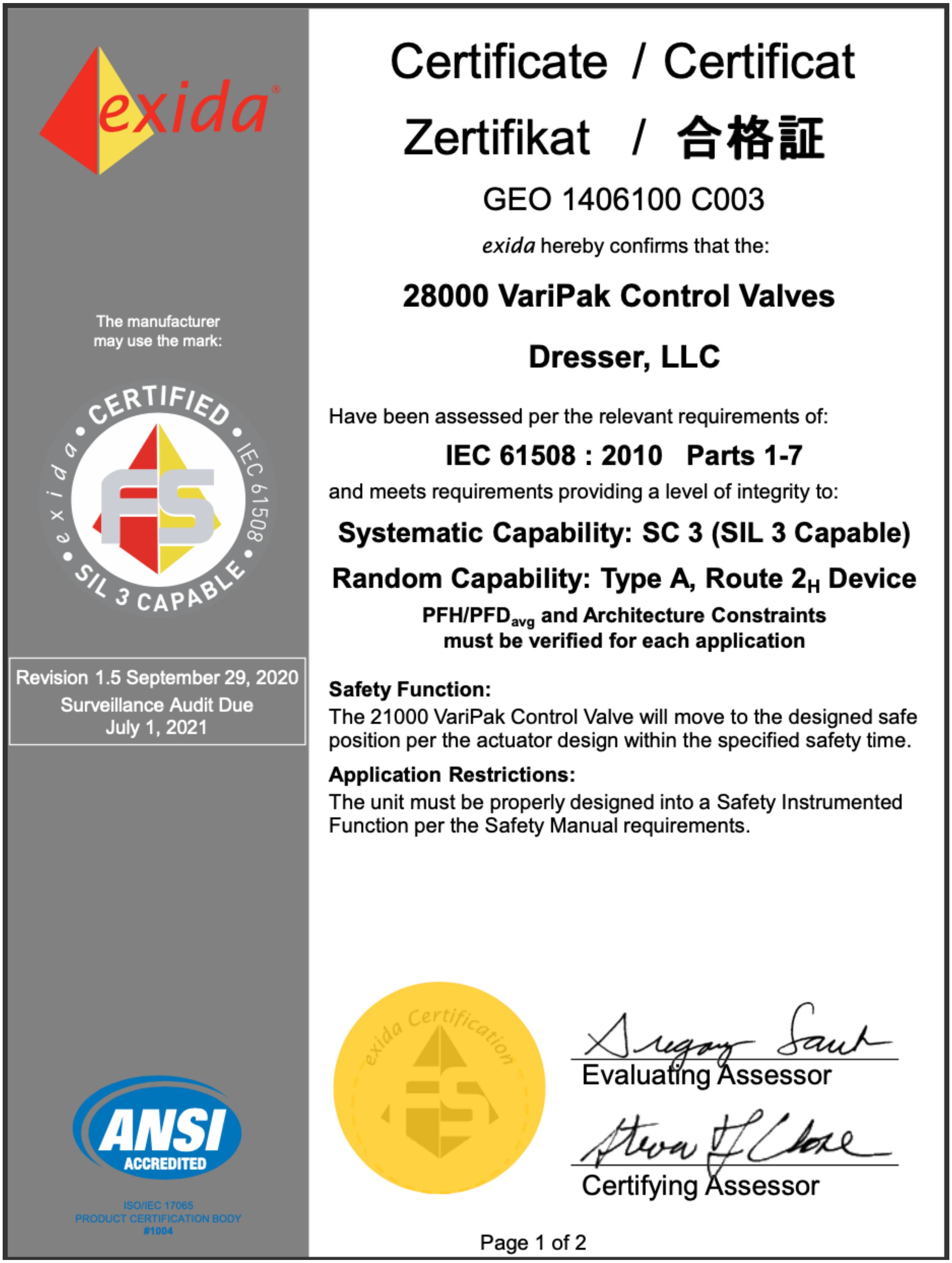
exida®

80 N Main St
Sellersville, PA 18960

T-002, V5R1

Page 2 of 2

Figure F.4: **Equipment SIL Certificate - Logic Solver** (2/2) (Exida)



exida

The manufacturer
may use the mark:

CERTIFIED • IEC 61508 • SIL 3 CAPABLE • exida

Revision 1.5 September 29, 2020
Surveillance Audit Due
July 1, 2021

ANSI ACCREDITED

ISO/IEC 17065
PRODUCT CERTIFICATION BODY
#1004

Certificate / Certificat

Zertifikat / 合格証

GEO 1406100 C003

exida hereby confirms that the:

28000 VariPak Control Valves

Dresser, LLC

Have been assessed per the relevant requirements of:

IEC 61508 : 2010 Parts 1-7

and meets requirements providing a level of integrity to:

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type A, Route 2_H Device

PFH/PFD$_{avg}$ and Architecture Constraints must be verified for each application

Safety Function:

The 21000 VariPak Control Valve will move to the designed safe position per the actuator design within the specified safety time.

Application Restrictions:

The unit must be properly designed into a Safety Instrumented Function per the Safety Manual requirements.

exida Certification

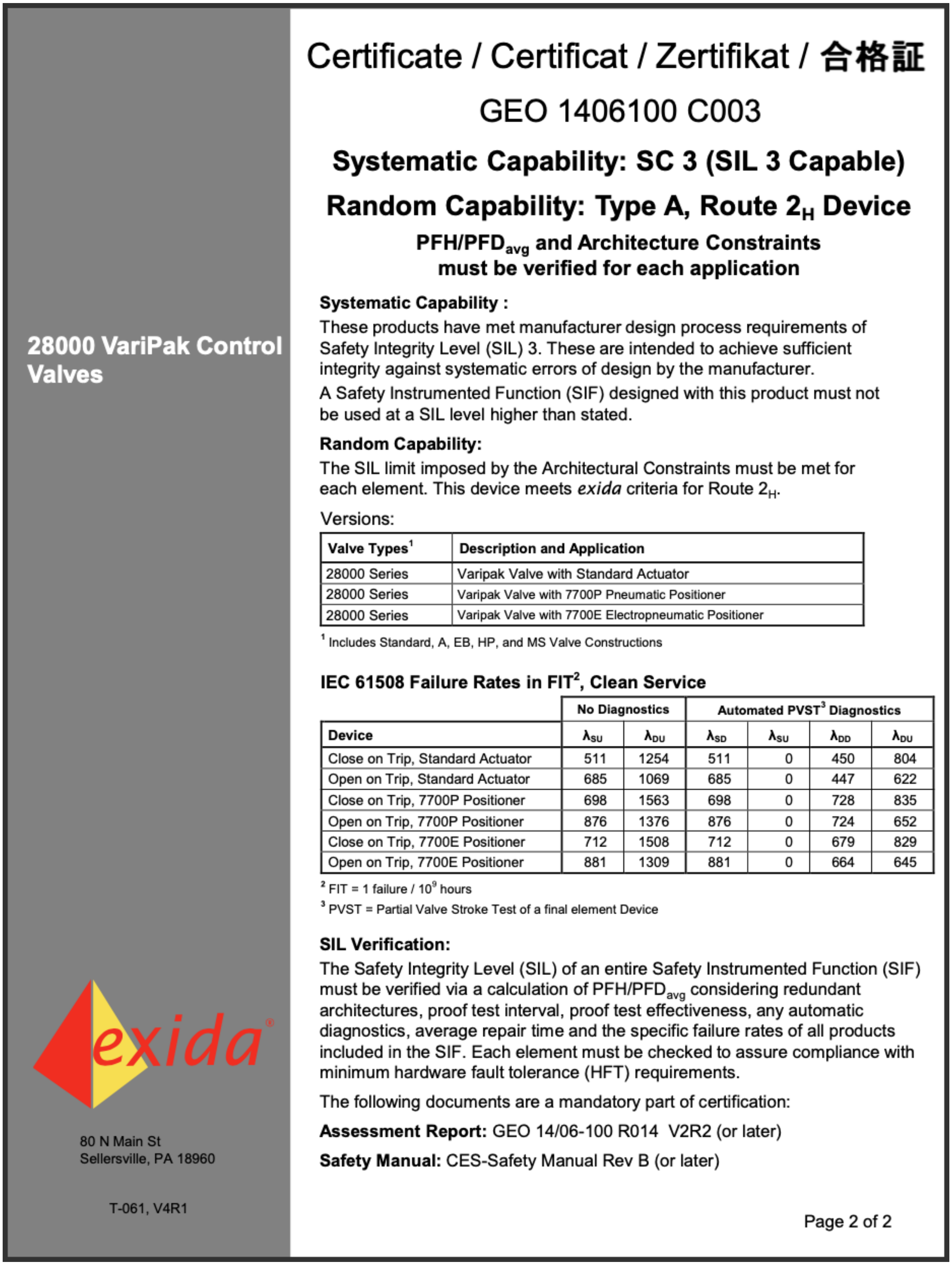
Gregory Sauk

Evaluating Assessor

Certifying Assessor

Page 1 of 2

Figure F.5: **Equipment SIL Certificate - Valve** (1/2) (Exida)



Certificate / Certificat / Zertifikat / 合格証

GEO 1406100 C003

Systematic Capability: SC 3 (SIL 3 Capable)

Random Capability: Type A, Route 2_H Device

PFH/PFD_{avg} and Architecture Constraints must be verified for each application

28000 VariPak Control Valves

Systematic Capability :

These products have met manufacturer design process requirements of Safety Integrity Level (SIL) 3. These are intended to achieve sufficient integrity against systematic errors of design by the manufacturer.

A Safety Instrumented Function (SIF) designed with this product must not be used at a SIL level higher than stated.

Random Capability:

The SIL limit imposed by the Architectural Constraints must be met for each element. This device meets *exida* criteria for Route 2_H.

Versions:

Valve Types[1]	Description and Application
28000 Series	Varipak Valve with Standard Actuator
28000 Series	Varipak Valve with 7700P Pneumatic Positioner
28000 Series	Varipak Valve with 7700E Electropneumatic Positioner

[1] Includes Standard, A, EB, HP, and MS Valve Constructions

IEC 61508 Failure Rates in FIT[2], Clean Service

	No Diagnostics		Automated PVST[3] Diagnostics			
Device	λ_{SU}	λ_{DU}	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}
Close on Trip, Standard Actuator	511	1254	511	0	450	804
Open on Trip, Standard Actuator	685	1069	685	0	447	622
Close on Trip, 7700P Positioner	698	1563	698	0	728	835
Open on Trip, 7700P Positioner	876	1376	876	0	724	652
Close on Trip, 7700E Positioner	712	1508	712	0	679	829
Open on Trip, 7700E Positioner	881	1309	881	0	664	645

[2] FIT = 1 failure / 10^9 hours

[3] PVST = Partial Valve Stroke Test of a final element Device

SIL Verification:

The Safety Integrity Level (SIL) of an entire Safety Instrumented Function (SIF) must be verified via a calculation of PFH/PFD_{avg} considering redundant architectures, proof test interval, proof test effectiveness, any automatic diagnostics, average repair time and the specific failure rates of all products included in the SIF. Each element must be checked to assure compliance with minimum hardware fault tolerance (HFT) requirements.

The following documents are a mandatory part of certification:

Assessment Report: GEO 14/06-100 R014 V2R2 (or later)

Safety Manual: CES-Safety Manual Rev B (or later)

exida®

80 N Main St
Sellersville, PA 18960

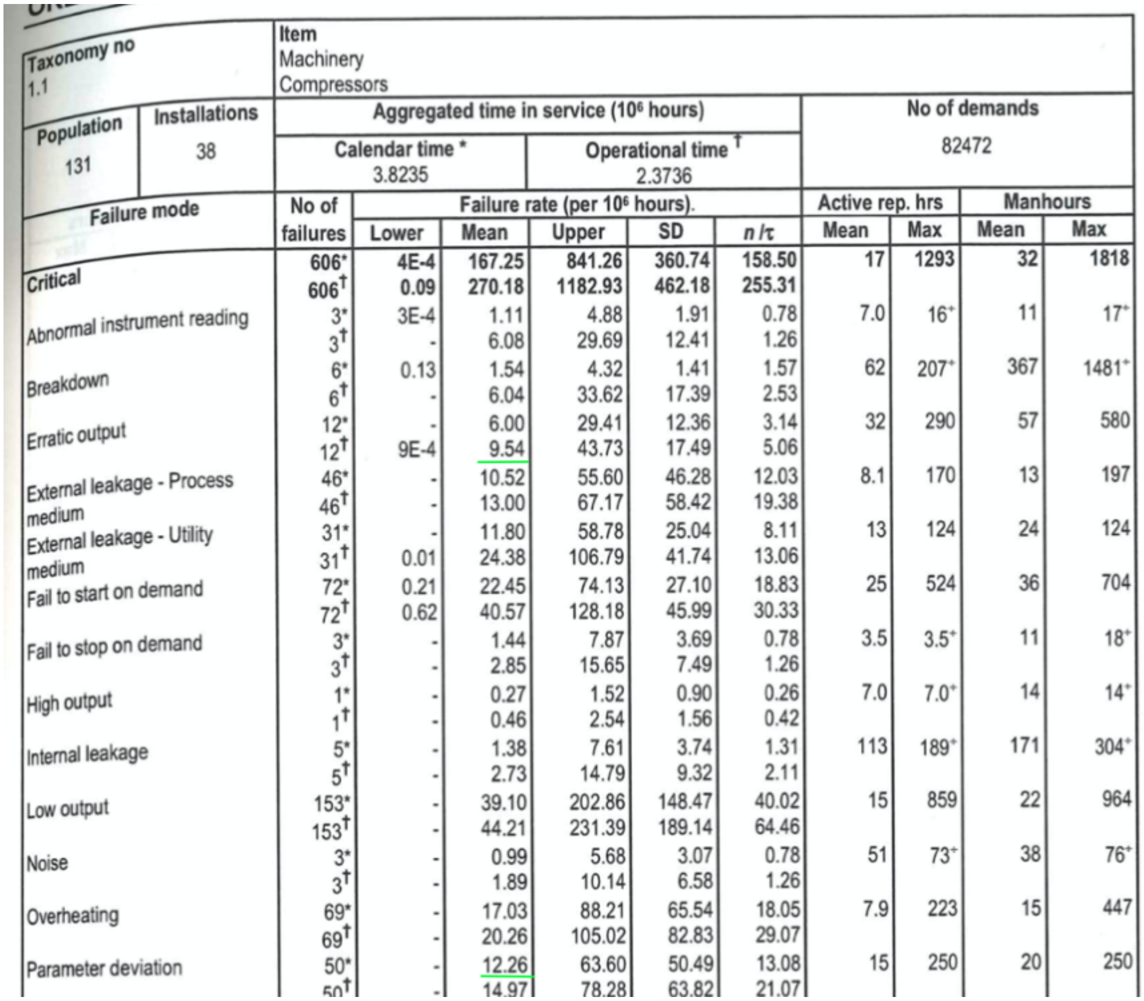
T-061, V4R1

Page 2 of 2

Figure F.6: **Equipment SIL Certificate - Valve** (2/2)(Exida)

Appendix G

Compressor Data



Taxonomy no 1.1		Item Machinery Compressors	
Population 131	Installations 38	Aggregated time in service (10^6 hours) Calendar time * 3.8235 Operational time † 2.3736	No of demands 82472

Failure mode	No of failures	Failure rate (per 10^6 hours).					Active rep. hrs		Manhours	
		Lower	Mean	Upper	SD	n/τ	Mean	Max	Mean	Max
Critical	606*	4E-4	167.25	841.26	360.74	158.50	17	1293	32	1818
	606†	0.09	270.18	1182.93	462.18	255.31				
Abnormal instrument reading	3*	3E-4	1.11	4.88	1.91	0.78	7.0	16+	11	17+
	3†	-	6.08	29.69	12.41	1.26				
Breakdown	6*	0.13	1.54	4.32	1.41	1.57	62	207+	367	1481+
	6†	-	6.04	33.62	17.39	2.53				
Erratic output	12*	-	6.00	29.41	12.36	3.14	32	290	57	580
	12†	9E-4	9.54	43.73	17.49	5.06				
External leakage - Process medium	46*	-	10.52	55.60	46.28	12.03	8.1	170	13	197
	46†	-	13.00	67.17	58.42	19.38				
External leakage - Utility medium	31*	-	11.80	58.78	25.04	8.11	13	124	24	124
	31†	0.01	24.38	106.79	41.74	13.06				
Fail to start on demand	72*	0.21	22.45	74.13	27.10	18.83	25	524	36	704
	72†	0.62	40.57	128.18	45.99	30.33				
Fail to stop on demand	3*	-	1.44	7.87	3.69	0.78	3.5	3.5+	11	18+
	3†	-	2.85	15.65	7.49	1.26				
High output	1*	-	0.27	1.52	0.90	0.26	7.0	7.0+	14	14+
	1†	-	0.46	2.54	1.56	0.42				
Internal leakage	5*	-	1.38	7.61	3.74	1.31	113	189+	171	304+
	5†	-	2.73	14.79	9.32	2.11				
Low output	153*	-	39.10	202.86	148.47	40.02	15	859	22	964
	153†	-	44.21	231.39	189.14	64.46				
Noise	3*	-	0.99	5.68	3.07	0.78	51	73+	38	76+
	3†	-	1.89	10.14	6.58	1.26				
Overheating	69*	-	17.03	88.21	65.54	18.05	7.9	223	15	447
	69†	-	20.26	105.02	82.83	29.07				
Parameter deviation	50*	-	12.26	63.60	50.49	13.08	15	250	20	250
	50†	-	14.97	78.28	63.82	21.07				

Figure G.1: **Compressor Failure Data** (ORE [2009])

Bibliography

IEC 61508 :2010. Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1-7. Standard, International Electrotechnical Commission, Geneva, Apr 2010.

David J Smith. Safety critical systems handbook : a straightforward guide to functional safety : Iec 61508 (2010 edition) and related standards, including process iec 61511, machinery iec 62061 and iso 13849, 2011.

E.W. Singleton. The application of control valves to compressor anti-surge systems. URL https://www.valve-world.net/pdf/vw00ff_control_kentintrol.pdf.

API RP 17V :2015. Recommended Practice for Analysis, Design, Installation, and Testing of Safety Systems for Subsea Applications. Standard, American Petroleum Institute, Washington DC, Feb 2015.

IEC 61511 :2016. Safety instrumented systems for the process industry sector – Part 1-3. Standard, International Electrotechnical Commission, Geneva, Feb 2016.

GL 070:2018. 070 - Norgweian Oil and Gas - Application of IEC 61508 and 61511 in the Norwegian Petroleum Industry (Recommended SIL Requirements). Standard, Norwegian Oil and Gas Association, Stavanger, Jun 2018.

Oreda : offshore reliability data handbook : Vol. 1 : Topside equipment, 2009.

H Kim, M.A Lundteigen, A Hafver, F.B Pedersen, G Skofteland, C Holden, and S.J Ohrem. Application of systems-theoretic process analysis to a subsea gas compression system. In *Safety and Reliability - Safe Societies in a Changing World - Proceedings of the 28th International European Safety and Reliability Conference, ESREL 2018*, pages 1467–1476, 2018. ISBN 0815386826.

ISO 31000 :2018. Risk management - Guidelines. Standard, International Organization for Standardization, Geneva, Feb 2018.

IEC 31010 :2019. Risk management - Risk assessment techniques. Standard, International Electrotechnical Commission, Geneva, Jun 2019.

Marvin Rausand. *Risk Assessment: Theory, Methods, and Applications*. Statistics in practice. John Wiley Sons, Incorporated, Somerset, 1 edition, 2011. ISBN 9780470637647.

Yiliu Liu and Marvin Rausand. Reliability assessment of safety instrumented systems subject to different demand modes. 24(1):49–56, 2011. ISSN 0950-4230.

International Electrotechnical Commission EIV(192-03-01). Electropedia: The world's online electrotechnical vocabulary (eiv 192-03-01). URL https://www.electropedia.org/iev/iev.nsf/display?openform&ievref=192-03-01.

ISO/TR 12489 :2013. Petroleum, petrochemical and natural gas industries - Reliability modelling and calculation of safety systems. Standard, European Committee for Standardization, Brussels, Jan 2016.

EN 50126 :2017. Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1-3. Standard, European Committee for Electrotechnical Standardization, Brussels, Oct 2017.

IEC 62061 :2015. Safety of machinery - Functional safety of safety-related electrical, electronic, and programmable electronic control systems. Standard, International Electrotechnical Commission, Geneva, Jun 2015.

ISO 26262 :2018. Road vehicles - Functional safety – Parts 1-10. Standard, International Organization for Standardization, Geneva, Dec 2018.

IEC 61513 :2011. Nuclear power plants - Instrumentation and control important to safety - General requirements for systems. Standard, International Electrotechnical Commission, Geneva, Aug 2011.

Yijing Ren, Laibin Zhang, Yingchun Ye, Wei Liang, and Hedeng Yang. Reliability assessment of anti-surge control system in centrifugal compressor. In *2012 Fourth International Conference on Computational and Information Sciences*, pages 1240–1243, 2012. doi: 10.1109/ICCIS.2012.218.

A Almasi. Latest techniques and practical notes on anti-surge systems for centrifugal compressors. *Australian journal of mechanical engineering*, 10(1):81–90, 2012. ISSN 1448-4846.

Yong Bai and Qiang Bai. *Subsea Engineering Handbook*. Elsevier Science Technology, Oxford, 2010. ISBN 1856176894.

Layer of protection analysis : simplified process risk assessment. A CCPS concept book. Center for Chemical Process Safety of the American Institute of Chemical Engineers, New York, 2001. ISBN 0816908117.

Ronald J Willey. Layer of protection analysis. *Procedia engineering*, 84:12–22, 2014. ISSN 1877-7058.

Denise Chastain-Knight. Confirming the safety instrumented system layer of protection. *Process safety progress*, 39(1):n/a, 2019. ISSN 1547-5913.

Marvin Rausand. System reliability theory : models, statistical methods, and applications, 2004.

Marvin Rausand. *Reliability of Safety-Critical Systems: Theory and Applications*, volume 9781118112724. John Wiley Sons, Incorporated, Somerset, 2014. ISBN 9781118112724.

Man Energy Solutions (MAN). New heights below sea level. URL https://www.man-es.com/oil-gas/solutions/subsea-compression.

PDS Method :2013. Reliability Prediction Method for Safety Instrumented Systems. Standard, SINTEF, Trondheim, May 2013.

Arthur M Dowell III. Layer of protection analysis for determining safety integrity level. *ISA Transactions*, 37(3):155–165, 1998. ISSN 0019-0578. doi: https://doi.org/10.1016/S0019-0578(98)00018-4. URL https://www.sciencedirect.com/science/article/pii/S0019057898000184.

NTNU
Norwegian University of
Science and Technology