Funnel Risk Graph Method in the Design of Integrated Control and Safety System

Submitted in fulfilment of the requirements of the degree of

Doctor of Philosophy

(Electrical and Electronic Engineering)

College of Engineering and Science

VICTORIA UNIVERSITY
MELBOURNE AUSTRALIA

Angelito 'Allan' Gabriel

MBA(Hons), BS(CompEng), BS(MechEng), FIEAust 3244705, CPEng, NPER, RPEQ,
TUV FSEng 5125/12, IEEE Member

February 2018

To my beloved wife *ANNIE*, my prince *CHARLES* and my parents for their understanding, supports and most of all, love.

Abstract

With the emergence of oil and gas industries such as the LNG industry in Australia, e.g., the Chevron's US$54B Gorgon and Wheatstone projects, Inpex's US$34B Ichthys, Shell's US$12.6B Prelude FLNG, Origin's $24.7B APLNG's projects, to name a few, and other related industries, it is inevitable that these industries need to utilise risk analysis techniques during the development and application of their Safety Instrumented System (SIS), in order to efficiently and safely conduct its business, and for industry compliance. Currently, evaluation and design of integrated control and safety systems (ICSS), particularly the SIS are often cumbersome, time consuming and complex considering a lot of Standards and Regulations to follow. These systems are mission and safety-critical systems such that the development and execution must be carefully planned and traceable to certain Standards and Regulations but needs to be cost-efficient.

To address this impending concern, this research project will focus on the development of an application of a more cost-effective, simplified and enhanced approach for the design and evaluation of Safety Instrumented Systems (SIS) called the Funnel Risk Graph Method (FRGM). Although risk graph methods are commonly used in industries, the FRGM is unique in a way that the approach is presented as a screening tool or initial pass, before a more detailed analysis is carried out. Instead of subjecting all Safety Instrumented Function (SIF) one-by-

one to a much complex traditional assessment process, the FRGM is used as a funnel. If the assessed safety-related system received Safety Integrity Level (SIL) allocation of greater than SIL 2 during the initial pass then a semi-quantitative or a quantitative method as a ‘final pass’ should be conducted, or the multi-disciplinary assessment team reached an agreement to justify the ‘second pass’ or pose a high Equipment Under Control (EUC) risk. Based on the preliminary results, it is expected that significant economic benefits can be achieved. Likewise, compliance will become more practicable and standards more useful, resulting to an equal degree of functional safety as compared to the traditional approach yet resource utilisation is efficient.

Further testing and analyses will be conducted to quantify the benefits of FRGM. Real-life case studies utilizing industrial SIS devices will be presented to demonstrate the benefits of this approach. In contrast with other complex schemes commonly used for safety assessment, the proposed FRGM gives benefits such that it is straightforward in steps and resource-efficient. While safety is aimed at protecting the systems from accidental failures to eliminate or minimize hazards, security is focused on protecting the systems from deliberate malicious attacks. They share the same goal – protecting the SIS from failing. Industry cybersecurity has become more critical these days, and to address such concern, risk assessment for the cybersecurity of SIS is proposed to be integrated in the assessment process using a proposed framework, as part of the enhanced process.

Declaration

"I, Angelito Gabriel, declare that the PhD thesis entitled 'Funnel Risk Graph Method in the Design of Integrated Control and Safety System' is no more than 100,000 words in length including quotes and exclusive of tables, figures, appendices, bibliography, references and footnotes. This thesis contains no material that has been submitted previously, in whole or in part, for the award of any other academic degree or diploma. Except where otherwise indicated, this thesis is my own work"

14 February 2018

Signature

Date

Acknowledgements

My first, and most earnest, acknowledgement in my doctoral studies must go to my respected supervisors, Associate Professor Dr. Juan Shi and Dr. Cagil Ozansoy for countless discussions, invaluable guidance and support, and for encouraging me throughout my doctoral studies. I am indebted to these two lovely persons for their advice and directions which has enabled me not only to complete this research but also to become a better researcher. I would also like to sincerely thank Professor Akhtar Kalam, Dr. Horace King and Professor Aladin Zayegh for their constructive guidance and supports during this journey. I would like to thank Ms. Elizabeth Smith for her continuous assistance and guidance throughout my studies.

I would also like to thank the staff of Graduate Research Office specially Ms. Nadia Itaywi for processing my applications. I would also like to express my sincere gratitude to the entire members of staff of the College of Engineering and Science, Victoria University and all those who provided me with the needed assistance while doing this research.

Published papers during the author's candidature

All of the research results reported in this thesis have been published as academic articles in referred journals or have been submitted as academic papers to referred journals. A list of published papers are:

Published Journal Papers

1) A. Gabriel, "Design and Evaluation of Safety Instrumented Systems: A Simplified and Enhanced Approach," in *IEEE Access*, vol. 5, pp. 3813-3823, 2017. doi: 10.1109/ACCESS.2017.2679023.
2) A. Gabriel, J. Shi and C. Ozansoy, "A Proposed Alignment of the National Institute of Standards and Technology Framework with the Funnel Risk Graph Method," in *IEEE Access*, vol. 5, pp. 12103-12113, 2017. doi: 10.1109/ACCESS.2017.2718568.

3) A. Gabriel, J. Shi, C. Ozansoy, “Developments in SIL Determination and Calculation,” in Elsevier, Reliability Engineering and System Safety, vol. 177. pp. 148-161, September 2018. doi: 10.1016/j.ress.2018.04.028

The contents of some of the chapters have been adopted from the published papers. The detailed list of the included papers in each chapter is given in the table below.

Chapter No.	Publication Title	Publication Details	Publication Status
2	Developments in SIL Determination and Calculation	Elsevier Journal of Reliability Engineering and System Safety	Available in the Elsevier Journal of Reliability Engineering and System Safety
3	Design and Evaluation of Safety Instrumented Systems: A Simplified and Enhanced Approach	IEEE Access	Available in *IEEEXplore*
5	A Proposed Alignment of the National Institute of Standards and Technology Framework with the Funnel Risk Graph Method	IEEE Access	Available in *IEEEXplore*

List of Abbreviations

AC	Architectural Constraints
BBN	Bayesian Belief Networks
BoD	Basis of Design
BOP	Blowout Preventer
BPCS	Basic Process Control System
CCF	Common Cause Failure
CIUM	Control Input Unit Module
COUM	Control Output Unit Module
CPT	Conditional Probability Tables
CTMC	Continuous Time Markov Chains
CSMS	Cybersecurity Management System
C&E	Cause & Effect Diagram
DBN	Dynamic Bayesian Network
DD	Dangerous Detected
DDMR	Double Dual Modular Redundancy
DP	Differential Pressure
DTS	De-energized to Safe
DU	Dangerous Undetected

DVC	Digital Valve Controller
EA	Event Assessment
EMA	Enhanced Markov Analysis
ETS	Energized to Safe
FACT	Failure-Attack-CounTermeasure
FBN	Fuzzy Bayesian Network
FE	Final Element
FEED	Front End Engineering Design
FER	Field Equipment Room
FGS	Fire and Gas System
FMEDA	Failure Mode, Effects, and Diagnostic Analysis
FRGM	Funnel Risk Graph Method
FSMP	Functional Safety Management Plan
FTA	Fault Tree Analysis
FFTA	Fuzzy Fault Tree Analysis
GDM	General Dependency Model
GPFDF	Generalised PFD Formula
HAZOP	Hazard and Operability
HARA	Hazard Analysis and Risk Assessment

HIPS	High Integrity Protective System
HRM	Hybrid Relation Model
HMI	Human Machine Interface
ICS	Industrial Control System
ICSS	Integrated Control and Safety System
IS	Intrinsically Safe
ISA	International Society of Automation
IEC	International Electrotechnical Commission
IPL	Independent Protection Layer
KooN	K-out-of-N architecture
LNG	Liquefied Natural Gas
LOPA	Layers of Protection Analysis
LVCB	Low Voltage Circuit Breaker
MA	Markov Analysis
MC	Maintenance Capability
MCS	Monte Carlo Simulation
MDBN	Multiphase Dynamic Bayesian Network
MF	Membership Functions
MOC	Management of Change

MOS	Maintenance Override Switch
MRST	Minimum Resource Spanning Trees
MT	Mission Time
MTTFS	Mean Time to Failure Safe
MTTR	Mean Time to Repair
MTSR	Mean Time to System Restoration
MUnT	Mean Unavailable Time
NEC	Network Enabled Capability
NIST	National Institute of Standards and Technology
NSSR	No Standard Safety Requirement
NR	Not Recommended
O&M	Operations and Maintenance
PCS	Process Control System
P&ID	Piping and Instrumentation Diagram
PFD	Probability of Failure on Demand
PFD_{avg}	Probability of Failure on Demand Average Range

PHA	Process Hazard Analysis
PL	Protection Layer
PLC	Programmable Logic Controllers
PRA	Probabilistic Risk Assessment
PROBIST	Probability Binary State
PSA	Process Safety Analysis
PST	Partial Stroke Testing
PTC	Proof Test Coverage
PTI	Proof Test Interval
PV	Process Variable
PVST	Partial Valve Stroke Test
RBD	Reliability Block Diagram
RRF	Risk Reduction Factor
SD	Safe Detected
SCP	Screw Pluggable
SERH	Safety Equipment Reliability Handbook
SFF	Safe Failure Fraction – Ratio of the (total safe failure rate of a subsystem plus the dangerous detected failure rate of the subsystem) to the total failure rate of the subsystem.

SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SILver	SIL Verification
SIS	Safety Instrumented System
SM	Switching Markov
SME	Subject Matter Expert
SOA	Safety Objective Analysis
SoS	System of Systems
SOV	Solenoid Valve
SPP	Spring Pluggable
SU	Safe Undetected
ST	Spurious Trip: A failure of an SIS related system or component resulting in an unwarranted process shutdown.
SRS	Safety Requirements Specification
SSDVR	SIF SIL Design Verification Report
TMR	Triple Modular Redundancy
TSO	Tight Shutoff
TUV	Technischer Uberwachungsverein

List of Symbols

3σ criterion	Triangular Fuzzy Number
$\tilde{A}$	Fuzzy Number
$A_L^{(\alpha)}$	Left-end-point of the fuzzy interval
$A_R^{(\alpha)}$	Right-end-point of the fuzzy interval
B_{10}	Cycles in usable life (failure rate value)
β	Common Cause Failure Fraction
β_D	Detected common cause failure fraction
C	Consequence
E	Extensive
f	Frequency
λ_S	Transition rate to safe state
λ_{de}	Demand rate
$\boldsymbol{\lambda}_{SD}$	Safe detected failure rate
$\boldsymbol{\lambda}_{SU}$	Safe undetected failure rate
$\boldsymbol{\lambda}_{DD}$	Dangerous detected failure rate
$\boldsymbol{\lambda}_{DU}$	Dangerous undetected failure rate
$\boldsymbol{\lambda}_D(=\boldsymbol{\lambda}_{DU}+\boldsymbol{\lambda}_{DD})$	Dangerous failure rate
μ_{DD}	DD- repair rate
μ_{DU}	DU- repair rate

$\mu_{\tilde{A}}^{(x)}$	Membership Function of Fuzzy Number
μ_S	Restoration rate
μ_{de}	Demand duration rate
m	Renewal rate
M	Minor
N	Number of Total Time Slices
P	Probability
R	Risk
S	Serious
V	Vulnerability factor
W	Demand

Table of Contents

List of Figures

List of Tables

“Imagination is more important than knowledge...”

— Albert Einstein (1879 - 1955)

Chapter 1 - Introduction

Integrated Control and Safety Systems (ICSS) are considered the heart of any industrial plant. Dependability to ICSS is very important because systems failure might endanger human life, lead to significant property loss, or cause extensive environmental damage. In oil and gas, such as the LNG industry [1], petrochemical and process industries, Safety Instrumented Systems (SIS) are implemented to safely '*secure liquid inside the pipe*' or keep a process under control from hazardous processes, and ensure that the instrumentation for functional safety is in place. These mission and safety-critical systems prevent physical harm to personnel and/or damage to company property or the environment. In the event that a hazardous process condition is sensed by the ICSS, a safe state will then be executed by the SIS. Moreover, in the event of a SIS failure, the SIS is expected to force the process into its fail-safe condition, i.e., the condition where the presence of harm is eliminated [2]. As oil and gas industries have been one of the major sources of energy, its existence is inevitable in the decades to come, despite of the risks associated with it. It is in absolute certainty that these industries need to utilize ICSS to safely and effectively conduct their business. Learning from the past, understanding these constraints and making contributions are paramount in this research project. Take for example the oil platform Piper Alpha, which was destroyed by a gas leak in July 1988, and is still the worst offshore oilfield disaster to date (in terms of human life lost). Design and evaluation of ICSS, in particular the SIS are often

cumbersome, time consuming and complex [3, 4, 5, 6, 7, 8, 9] considering a bunch of Standards and Regulations to follow. Therefore, new optimised approaches to the design and evaluation of ICSS will be fundamental to this research work. An application of a more cost-effective, simplified and enhanced approach called the Funnel Risk Graph Method (FRGM), for the design and evaluation of SIS will be investigated in this project. Like other computers, ICSS is also vulnerable to cyber-attacks, recent news about serious security incidents such as *WannaCry* [10] ransomware affecting the whole world are heard more often. Therefore, an evaluation of the impact of the cybersecurity vulnerabilities will also be considered in this project.

This chapter provides an overview of the research reported in this thesis. Previous research progresses were reviewed and the motivation for the work is presented. The objectives of the research are identified and the main scientific contributions made through this research are highlighted.

1.1 Motivation and Background

In oil and gas, petrochemical and process industries, SIS is implemented to safely *'secure liquid inside the pipe'* or keep a process under control from hazardous processes, and ensure that the instrumentation for functional safety is in place [1]. These mission and safety-critical systems are designed to prevent physical harm to personnel and/or damage to company property or the environment. In the event that a hazardous process condition is sensed by the

ICSS then a safe state will be executed by the SIS. Moreover, in the event of SIS failure, the SIS is expected to force the process into its fail-safe condition, i.e., the condition where the presence of harm is eliminated [1]. For instance, a control valve moves to its fail-open or fail-close condition depending on the SIS design. The ultimate objective of designing SIS is to comply with the requirements of Safety Integrity Level (SIL). As identified by risk analysis of the related process, a SIS is designed against the SIL [1]. Reference [2] requires Probability of Failure on Demand (PFD), which is a requirement of the SIS design. In process industry sector, a more detailed application of SIS is included in [3]. The requirements of SIL must be reflected by the design of the SIS. The architecture of SIS including field devices and systems need to be selected properly to enable safety function as designed. Hardware Fault Tolerance (HFT), as one of the architectural constraints is also examined in this paper. One of the ways to approach SIS issues is suggested by [2] and, for SIS concerning the process industries, by [3]. These international standards [2, 3] refer to safety system for electric, electronic and programmable electronic systems. Specifically, these international standards set criteria and management guidelines from the '*cradle*' or the first phase of the project until the '*grave*', which is the end of life of the product. When these international standards are strictly followed, it is often than not, leads to allocation of more resources and time in the safety assessment phase, as such the application is often complicated [4-9]. Furthermore, none of the standards are able to provide both a stand-alone safety lifecycle framework and the guidelines necessary for the realization of a diverse range of safety system applications and

technologies that are likely to be encountered in industries such as in mining or industrial plant [10]. Given the complexity of process industries, mining and other plant, SIL and Performance Level (PL) allocation should be performed via a quantitative or semi-quantitative methodology where practicable [1]. The size of instrumentation, SIS, project risk assessments yield a large number of hazards, many of which require further consideration and allocation of SIL's or PL's to safety-related systems. In such cases, it may be impracticable to apply a semi-quantitative or quantitative approach due to the substantial amount of time and resources involved. An optimised method for SIS design starts from the assessment phase.

All the aforementioned reasons have motivated us to investigate the current gaps between the existing methodologies and challenges involved in the design and evaluation of ICSS, particularly the SIS through the introduction of FRGM.

1.2 Objective and Scope of the Thesis

1.2.1 General Objective

The aim of this thesis is to explore a more cost-effective, simplified and enhanced approach for the design and evaluation of SIS through the FRGM. Safety Integrity Level (SIL) and Performance Level (PL) allocation for process, mining and other related industries require deeper level of analysis. Adopting the SIL allocation process to the concept of risk reduction is shown in **Figure 1.1.** For

each of the Equipment Under Control (EUC) risks are identified, the level of risk is calculated or estimated and then one or more risk reduction measures are designated. The objective of this risk management approach is to apply sufficient risk reduction measures against the EUC risk such that the “actual risk reduction” exceeds the “necessary risk reduction” to achieve an acceptable “tolerable risk”.

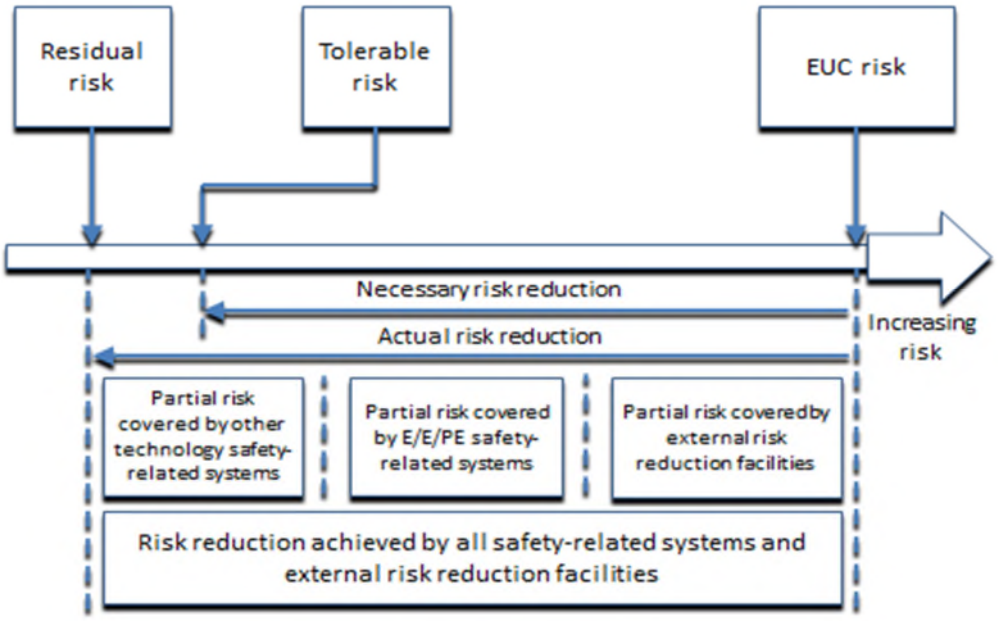


Fig. 1.1. Risk Reduction General Concept

Based on this concept, this research project’s main aim is to develop and apply an optimised approach for the design and evaluation of ICSS using the FRGM method shown in **Figure 1.2** [10-12] (*FRGM is the proposed approach in evaluation of ICSS that aims to reduce costs in the early stage of the design process*).

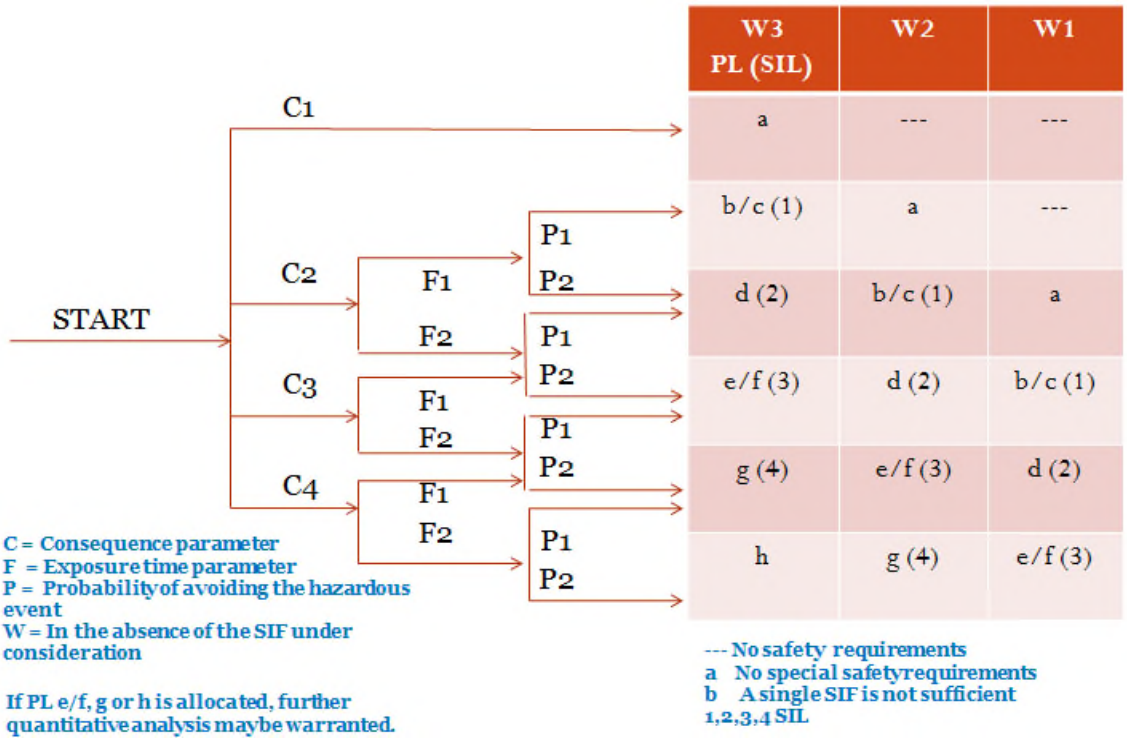


Fig. 1.2. Funnel Risk Graph Method

1.2.2 Specific Objectives:

Real-life industrial scenarios will be analysed to prove the advantage of FRGM over the traditional approach. The specific objectives of this project are to:

1. Develop the framework of the FRGM approach by aligning to the phases of the safety lifecycle as a ‘funnel’;
2. Present case study analyses to prove the advantages of FRGM over the traditional approach;
3. Carry out an evaluation of FRGM, comparing it to the traditional method to show that;

- FRGM will result in equal functional safety;
- FRGM requires few number of steps required and time taken, thus achieving economic benefit.

4. Analyse different kinds of SIF with resulting SIL;
5. Cybersecurity consideration using FRGM.

1.3 Main Contributions to Knowledge

This research strives to address the issues faced by the oil & gas and related industries regarding the evaluation and design of ICSS, particularly the SIS. Big or small players in the industry, cannot escape from the fact that they need to utilise ICSS in their business operations. Traditionally, in designing ICSS, all SIF must undergo quantitative or semi-quantitative analyses consuming a lot of resources. In this research work, an application of a more cost-effective, simplified and enhanced approach called FRGM for the design and evaluation of SIS will be explored in reference to the functional safety standards. FRGM will be discussed in-depth in *Chapter 3*. Based on the preliminary results, it is expected that the project will result in significant economic benefits, more practicable compliance with results in equal degree of functional safety as compared to the traditional approach. To prove the effectiveness of this approach, comparative analyses are presented in *Chapters 3 and 4*. The proposed approach will also consider cybersecurity as an important component of the assessment in *Chapter 5*. Specifically, my main contribution can be summarised as follows, I have:

- Developed the FRGM as a novel approach to determine SIL ratings. The FRGM approach can be applied to filter lower SIL ratings and the result as target or required SIL. By utilising this technique, a lot of resources can be saved. Potential cost savings were presented in *Chapters 3 and 4* for different applications;
- Presented several case studies and compared results of FRGM with traditional method to show accuracy of FRGM. The application of FRGM was presented in *Chapter 3* involving 3 SIFs. These 3 SIFs were involved in a process of transporting and handling solids through a conveyor belt. They are designed to disable any movement of the conveyor belt and its associated equipment during emergency or metal detection. Potential hazards may involve fatalities, injuries or equipment damage. Another real-life case study was presented In *Chapter 4* utilising LNG Plant A. The Plant is one of the biggest LNG plants in the world with an estimated gas resource of 50 trillion cubic feet;
- Presented cost benefit analyses of FRGM. All of the case studies presented in this research demonstrated potential cost savings to prove the effectiveness of the FRGM approach. The 3 SIFs in *Chapter 3*, which involves a process of transporting and handling solids through a conveyor belt, generated a potential savings of $976,500. The LNG Plant A in *Chapter 4* yielded a total cost reduction of $3,906,000 out of four (4) multidisciplinary personnel which conducts the safety

assessment. This was based on 3,000 SIFs, total reduction of 2.167 hours and average salary rate of $150/hour;

- Conducted SIL calculations and verifications for SIFs in the LNG Plant A using exSILentia software and compared results with FRGM to prove accuracy of the proposed FRGM approach. Achieved SIL ratings were verified for 16 SIF loops in *Chapter 4.* It is shown in Table 4.1 that all 16 loops achieved their respective SIL targets. SIF 064LZ-0011 LL even exceeded the achieved SIL from 1 to 2;
- Developed the novel National Institute of Standards and Technology (NIST) + FRGM framework for the integration of SIS and cybersecurity. It has been recognised by the research community [13-21], the industry, as well as the International Society of Automation (ISA) [22] that there is a need of such alignment between safety and security, in which this research work was also striving to address;
- Presented a case study using the NIST + FRGM framework for a SIF in the LNG Plant A. SIF 064FZ-0567 LL from LNG Plant A was explored and re-analysed to illustrate the proposed integrated NIST + FRGM in *Chapter 5*. The objective is to demonstrate how SIL assessment would be impacted in the consideration of cyber security threats. The result showed that the SIF has low cybersecurity risk with SIL rating of SIL 1. The primary advantage of this integrated approach is that it ensures all risks (cybersecurity and safety) are considered.

Secondarily, optimising the evaluation process into a unified approach would mean significant cost benefit.

1.4 Organisation of the Thesis

This thesis is presented in six Chapters. The organisation of the remaining Chapters is as follows:

Chapter 2 provides literature reviews of past and ongoing research work. Pros and cons of those methodology were compared and contradicted. Various SIL determination and calculation methods are compared as per criteria of relevant qualifying factors. This Chapter compared advantages and disadvantages of reviewed methods from complexity, accuracy and cost-effectiveness perspectives.

Chapter 3 focuses on the development of FRGM which was based on the Phase 5: Safety Requirements Allocation. This was based on the 16-phase IEC61508 [2] safety lifecycle with the inclusion of IEC62061 [23], IEC61511 [3], ISO13849 [24] and AS4024.1 [25] as a combined safety lifecycle process [10]. The qualities of FRGM being more cost-effective and simplified is explored in this Chapter. Comparative analyses between FRGM and LOPA (and other traditional methods) are also presented. The FRGM only takes 3 steps while LOPA takes 13 steps. An estimated cost savings of $976,500 is calculated for 3,000 SIFs with the presented case study example.

Chapter 4 provides quantitative analyses for the SIFs used in the LNG Plant A Process Unit 6400 (PU6400). This Chapter demonstrates SIL calculations performed for each SIF loop that were assigned a SIL target of SIL 1 or greater. Calculations are based on the actual hardware selected for the Sensor, the Logic Solver and the Final Element. The software for performing SIL calculations is exSILentia coupled with the latest reliability database SERH, then results compared against FRGM. Considering the factors such as number of hours reduced using FRGM, salary per hour and the number of personnel conducting the assessment, potential savings can be achieved at around $3,906,000 using the FRGM when the entire SIFs of the LNG Plant A are evaluated.

Chapter 5 this complementary chapter is dedicated to an integrated and optimised evaluation framework for ICSS and related subsystems considering cybersecurity and safety. This can be achieved by the alignment of the cybersecurity framework formulated by the National Institute of Standards and Technology (NIST) with safety and security standards ISA84 (IEC 61511) and ISA99 (IEC 62443), and the novel Funnel Risk Graph Method (FRGM). The need of such alignment between safety and security has been recognised by the research community, the industry, as well as the International Society of Automation (ISA). The framework is called NIST + FRGM.

Chapter 6 summarises the research work and presents the conclusions drawn from the study along with some recommendations for possible future research opportunities.

Chapter 2 - Developments in SIL Determination and Verification

2.1 Introduction

Recent developments in technology and the move towards efficient utilisation of resources have inspired researchers and practitioners to come up with cost-effective approaches to Safety Integrity Level (SIL) determination and verification, as the current methods are too cumbersome and time-consuming. The bottom line is meeting the organisation's safety requirements in an economical manner regardless of methodology employed yet without sacrificing accuracy. This Chapter presents a review of various target SIL determination and calculation methods in the life cycle of Safety Instrumented Systems (SIS). Various SIL determination and calculation methods are compared as per criteria of relevant qualifying factors. Advantages and disadvantages of each method are briefly discussed. The key outcome of this review is that the qualitative funnel risk graph method (FRGM) can be used as a funnel technique to assess lower SIL ratings whilst more complex methods are applied on higher SILs with caution.

IEC 61508 [2] and IEC 61511 [3] are two standards used to measure the SIL of a SIS in the related industries such as oil, gas, chemicals and electricity [26]. SIL is a concept that was introduced during the development of IEC 61508

[2], which is a measure of the confidence with which the system can be expected to perform their safety function. SIL is the measure that indicates the importance of Safety Instrumented Function (SIF), as described in IEC 61508-6 [27]. **Figure 2.1** shows the block diagram of SIS Subsystems and **Figure 2.2** shows an example of SIS, which generally consists of three Subsystems: *sensor*, *logic solver* and *final element*. The sensor subsystem detects the onset of possible hazardous situations, the logic solver subsystem decides what to do by evaluating the information from the sensor subsystem, and the final element subsystem takes action through control valves, safety valves, circuit breakers, among others.

A SIF is designed to respond to a specific hazardous event and implements an action. Bringing to safe state is the task for demand mode SIFs. Continuous mode SIFs 'maintain' plant in safe state. Demand mode SIF bring equipment under control (EUC) into a safe state. Each SIF is defined with a SIL according to the risk reduction level that is required from that function. The SIL has a discrete four-level scale, where SIL 1 is the minimum safety requirement and SIL 4 is the most stringent. These levels are used to specify the safety integrity requirements for the safety functions performed by safety systems. The target SIL is a criterion indicating whether a SIS should meet the safety requirements, derived from risk assessment. The actual SIL indicates that the SIS can perform its safety function after SIL verification. There are three different approaches in SIL determination [28], i.e., qualitative, quantitative and semi quantitative.

Several methods under these approaches can be used and have their advantages and disadvantages. SIL assignment during design of SIS from database based on experience was explored by Wang et al. [29].

Functional safety refers to SIS that implements SIF. SIL targets must first be determined, and later verified or validated. SIS are widely used in the process industry to protect humans, the environment, and material assets against hazardous events, such as an explosion due to high pressure or product spillage due to high tank level.

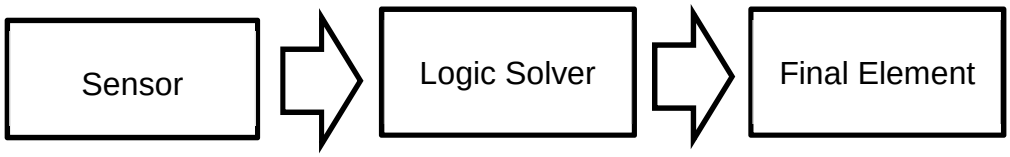


Fig. 2.1. Block diagram of SIS subsystems.

Fig. 2.2. Example of SIS subsystems.

The SIS must fulfil certain safety requirements to provide a specified level of risk reduction. Many standards and guidelines have been developed, which define the SIF requirements and how the SIL should be determined and its requirements should be fulfilled. There are a few governing standards for

functional safety such as IEC 61513 (Nuclear power plants), IEC 62061 (Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems, based on EN 61508), ISO 13849-1 (Safety of machinery - Safety-related parts of control systems. Non-technology dependent standard for control system safety of machinery), IEC 62304 (Medical device software), EN 50128 (Railway industry specific – Software safety), EN 50129 (Railway industry specific – system safety in electronic systems), EN 50495 (Safety devices related to explosion risks), NASA Safety Critical Guidelines, ISO 26262 (Road vehicles functional safety), EUROCAE ED-12B European Airborne Flight Safety Systems among others. However, IEC 61508 [2] is the most common of these standards, which is a generic standard specifying the functional safety requirements for SIS. The IEC 61508 [2] also serves as the overarching mother standard for the development of industry-specific safety standards such as IEC 61511 [3] for the process industry and IEC 62061 [23, 30] for machinery systems. SIS have been used for many years to perform SIF in the process industries. If SIS is to be effectively used for SIF, it is essential that SIS achieves certain minimum standards and performance levels. IEC 61511 [3] standard addresses the application of SIS for the process industries. It also requires a process hazard and risk assessment to be carried out to enable the specification for SIS to be derived.

The objective of functional safety management is to identify the management activities that are necessary to ensure the functional safety

objectives are met [3]. They are implemented by Integrated Control and Safety Systems (ICSS), which are usually operating in a computer network using wired and/or wireless communication technologies. Risk managers may use SIF together with several other risk reduction measures to control risk exposure. The target level of risk reduction for each SIF is determined to ensure that the overall risk to personnel is as low as reasonably practicable.

This Chapter presents a review of SIL determination and validation methods. SIL determination is the front-end engineering aspect to set the target SIL on each of a given SIF, while SIL verification is the validation process to ensure if the achieved target SIL can be achieved, using preferred methods. There are several calculation techniques described in the IEC 61508-7 [2] standard to verify the SIL for the systems comprised of programmable electronic and automation components. It was noted that the application of each one of these methods might be cumbersome depending on the different approaches that the analyst may take.

This Chapter is organized as follows: Section 2.2 discusses SIL approaches, Section 2.3 explores selective SIL target determination methods, Section 2.4 explores research interests in Bayesian networks (BNs) and dynamic Bayesian networks (DBNs), Section 2.5 discusses techniques in SIL calculation, Section 2.6 summarises and reviews different selected target SIL determination and calculation methods, and finally, Section 2.7 concludes the Chapter.

2.2 SIL approaches

IEC 61508 [31] standard is the generic approach for all safety lifecycle activities for systems comprised of electrical and/or electronic and/or programmable electronic components (electrical/electronic/ programmable electronic systems (E/E/PES) that are designed to perform safety functions. This integrated approach has been utilised such that a rational and consistent technical policy be developed for all electrically-based safety-related systems.

The overall safety lifecycle of IEC 61508 [2] is shown in **Figure 2.3** [2]. IEC 61508 [31] standard has the following functions:

- When E/E/PESs are used to perform safety functions, they consider all relevant overall E/E/PES and software safety lifecycle phases.
- It has been developed in a way that it is comprehensive; that is the framework is sufficiently robust and far-reaching to accommodate for future developments.
- As an overarching standard, it enables application sector international standards, dealing with safety-related E/ E/ PESs, to be developed, which enables to have both safety and economic benefits.
- It provides a method for the development of the safety requirements specification (SRS) necessary to achieve the required functional safety for E/E/PE safety-related systems.

- It uses SIL for specifying the target level of safety integrity for the safety functions to be implemented by the E/E/PE safety-related systems.
- In the determination of the SIL requirements, it adopts a risk-based approach.
- It has sets of numerical target failure measures for E/E/PE safety-related systems which are linked to the SIL.
- On the target failure measures, it sets the lower limit in a dangerous mode of failure, which can be claimed for a single E/E/PE safety-related system; for E/E/PE safety-related systems operating in:

(1) A low demand mode of operation, the lower limit is set at an average probability of failure of 10^{-5} to perform its design function on demand,

(2) A high demand or continuous mode of operation, the lower limit is set at a probability of a dangerous failure of 10^{-9} per hour;

- It adopts a broad range of principles, techniques and measures to achieve functional safety for E/E/PE safety-related systems, but does not use the concept of fail-safe.

For the process industries, IEC 61511 [3] is to be used. It addresses the application of SIS. It requires a process hazard and risk assessment to be carried out to enable the specification for SIS to be derived. IEC 61511 has two concepts

which are fundamental to its application; safety lifecycle and SIL. It addresses SIS, which are based on the use of E/E/PES technology. Where other technologies are used for logic solvers, the basic principles of this standard should be applied. IEC 61511 also addresses the SIS sensors and final elements regardless of the technology used. IEC 61511 is process industry specific within the framework of IEC 61508 [2]. There are key differences between IEC 61511 [3] and IEC 61508 [2] and these differences are enumerated in **Tables 2.1** and **2.2** based on the comparison of IEC 61511 to IEC 61508.

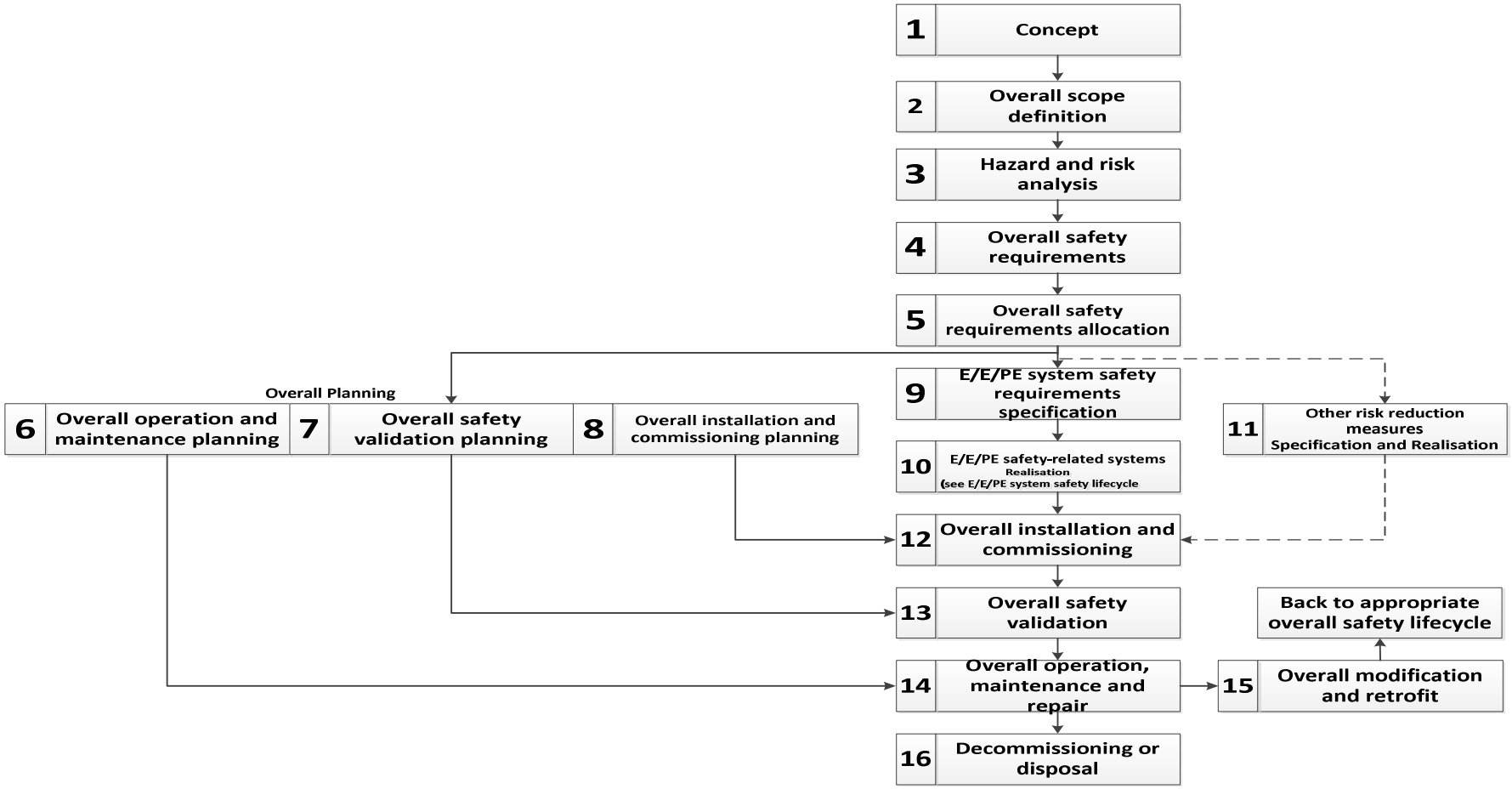


Fig. 2.3. Overall safety life cycle by IEC 61508 [2].

Table 2.1. Organizational differences [2, 3].

IEC 61508	IEC 61511	Comment
Part 1	Part 1	IEC 61508-1, -2, -3 and -4 have been combined into IEC 61511-1
Part 2	Part 2	Included in IEC 61511-1
Part 3	Part 3	Included in IEC 61511-1
Part 4	Part 4	Included in IEC 61511-1
Part 5	Part 5	Included in IEC 61511-3
Part 6	Part 6	Guidelines for IEC 61511-1
Part 7	Part 7	Informative references included in each part as annexes

Table 2.2 Terminology [2, 3].

IEC 61508-4	IEC 61511-1	Comment
E/E/PE safety related system	SIS	IEC 61508 refers to E/E/PE safety systems while IEC 61511 refers to safety instrumented systems
PES	SIS	IEC 61508 “PES” includes sensors and final control elements, while IEC 61511 uses the term SIS.
Process control system	Basic process control system	Basic process control system is a global term for the process sector.
EUC	Process	IEC 61508 refers to EUC (equipment under control) while IEC 61511 refers to process.
Safety function	SIF	IEC 61508 safety function implemented by E/E/PES, other technology safety related system, or external risk reduction facilities. IEC 61511 SIF is implemented solely by SIS.

2.3 Selective target SIL determination methods

SIL determination refers to the activity of selecting the required SIL for a SIF. SIL determination is usually done after the risk assessment has been performed and the SIFs required have been defined. Qualitative and quantitative techniques can be used to evaluate the risk associated to a process. After the risk has been evaluated, the necessary SIF needs to be identified then implement it on a SIS to achieve the desired safety level, and verify that the SIS configuration meets the required SIL. The IEC 61508 [2] provides a method for the development of the SRS necessary to achieve the required functional safety for

E/E/PE safety-related systems. It uses SIL for specifying the target of safety integrity for safety functions, adopts a risk-based approach for SIL determination and sets numerical target failure measures, which are linked to the SIL.

In the field of ICSS, research on SIL determination has attracted considerable attention and thus, we have enumerated, discussed and compared various selected techniques.

Risk graph method is one of the frequently-used methods when determining target SIL [32]. It is intended to be simple and conservative [33]. The risk graph considers likelihood, consequence, occupancy and probability of personnel avoiding hazards while hazard matrices consider only likelihood and consequence of an event. These four parameters used in risk graph are combined to indicate the level of unmitigated risks. Risk graph method is a qualitative method that enables SIL determination from a knowledge of the risk factors associated with the EUC and the EUC control system [2]. Risk graph is based on the following equation as shown in Eq. (1.1):

$$R = f\ x\ C \qquad (1.1)$$

Where R is the risk with no safety-related systems in place;

f, is the frequency of the hazardous event with no safety-related systems in place, and;

C, is the consequence of the hazardous event.

The frequency of the hazardous event is made up of three influencing factors such as frequency of, and exposure time in; the possibility of avoiding the

hazardous event and the probability of the hazardous event taking place without the addition of any safety-related systems. With this, four risk parameters were produced:

- C: consequence parameter of the hazardous event;
- F: frequency of and exposure time parameter in the hazardous zone;
- P: Probability of avoiding the hazardous event and;
- W: Demand rate in the absence of the SIF under consideration.

The Funnel Risk Graph Method (FRGM) [34, 35] is based on the risk graph method, which was explored by Gabriel et al. [34, 35], and presented in **Figure 2.4**.

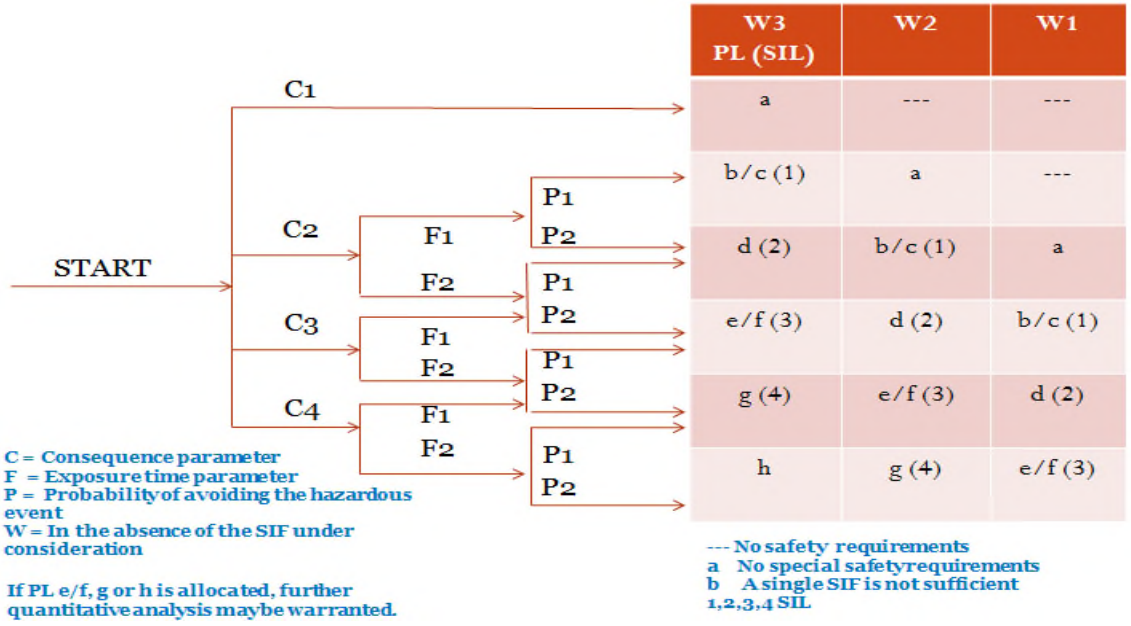


Fig. 2.4. The Funnel Risk Graph Method (FRGM)

Table 2.3 shows the comparative differences between the traditional quantitative methods such as Fault Tree Analysis (FTA) and semi-quantitative method Layers of Protection Analysis (LOPA), as compared to the proposed FRGM approach at say 10,000* SIFs (example only). Per our simulations, cost reduction is realized by the number of hours spent by a multi-disciplinary team. The coarser or less accurate assessment of risk using the FRGM is not a concern as it is used as a funnel from a broad range of SIL 0 to SIL 2. **Table 2.4** shows the sensitivity analysis with varying inputs.

Table 2.3. Comparison between traditional methods and FRGM.

Criteria	Standard Methods (LOPA, FTA)	FRGM	Time Reduction	Cost Reduction ($100/hr. rate)
Time & Cost Reduction	Approximately 2.5 hours per SIF x 10,000 = 25,000 hours	Approx. 20 minutes per SIF x 10,000 SIF = 3,333 hours	21,667 hours	$2,166,667
Steps Involved	13 steps for LOPA	3- step process		
Pros	More accurate assessment of risk.	Straight forward, resource- efficient		
Cons	Requires a lot of resources	Coarser or less accurate assessment of risk		

Table 2.4. Benefit calculation and sensitivity analysis.

Standard Method, hrs.	FRGM, hrs.	Reduction, hrs.	Rate, $/hr.	Cost savings, $
2	0.33	1.67	150	2,500,000
2	0.33	1.67	130	2,166,667
1	0.33	0.67	150	1,000,000
1	0.33	0.67	130	866,667
0.75	0.33	0.42	150	625,000

* 10,000 SIFs were used to easily demonstrate the advantages of FRGM and the difference using LOPA.

Chang et al. [32] presented an uncertainty analysis for target SIL determination and discussed its application in the offshore industry. The work presented aimed to identify uncertainty sources in SIL determination methods, specifically the risk graph method. As shown in **Figure 2.5**, there are two classifications of uncertainty:

(1) Randomness due to natural variability of system (aleatory) and,

(2) Imprecision due to lack of knowledge on the system (epistemic) [36].

Based on the definitions of uncertainty, various target SIL determination methods can be classified as possibly affected by aleatory/epistemic, parameter/model/known completeness/unknown completeness uncertainty, based on the characteristics of each method. The result of the classification is shown in **Table 2.5**. The authors [32] proposed procedures for uncertainty analysis in SIL determination by using three distinct approaches. These include the non-probabilistic Fuzzy Set approach, probabilistic Monte Carlo simulation (MCS), and a combination of non-probabilistic and probabilistic MCS and the Fuzzy Set approaches. The key feature of the work [32] is the fact that it investigated the effect of uncertainties, the fuzzy set approach and MCS in its application to the risk graph method and OLF 070 (SIL Table from Norwegian Oil Industry Association, Norwegian: *Oljeindustriens Landsforening*, OLF) minimum SIL requirement, respectively. The fuzzy set approach was used to evaluate the risk graph method, a combination of MCS and fuzzy set approach was used for the LOPA, and finally the OLF 70 minimum SIL Table was evaluated using the

MCS. All methods showed reliable results, with the MCS and fuzzy set approach applied to LOPA showing advantages of less uncertainty than the fuzzy set approach, given there is sufficient information available.

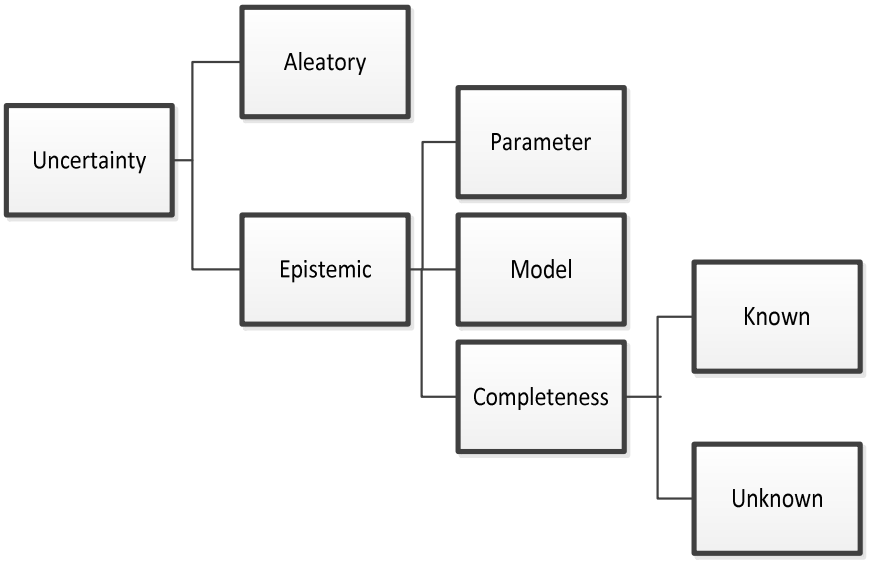


Fig. 2.5. Uncertainty classification [32].

Khalil et al. [37] proposed a cascaded fuzzy-LOPA model for SIL determination for certain hazardous scenarios and at different frequencies of occurrence in the natural gas industry. The authors developed two fuzzy models. One was developed to determine the severity of each scenario which involved checking the impact of each scenario on safety and economical aspects for the company. The second model was used to determine the SIL requirement based on the risk. The models were developed by means of a distinct fuzzy logic model, the Mamdani [38] model and MATLAB was used to simulate the results.

Table 2.5. Uncertainty sources and their classification, in SIL determination methods [32].

Method	Characteristics of Model	Uncertainty sources	Completeness/Randomness
Risk Graph	• 4 key categorised parameters combination & propagation a. Consequence b. Frequency or Demand rate c. P_{fail} to avoid hazardous event d. Occupancy • Strongly dependent on analyst' experience and knowledge	• Categorisation of parameters: linguistic ambiguity a. Number of categories b. Ranges of parameter values for each category • Inconsistent consensus: subjectivity a. Subjectivity: different teams, different results b. Competence gap between teams	• No aleatory • Epistemic a. Known/unknown completeness b. Model c. No parameter
LOPA	• Assume multiple independent protection layer mode: Onion model • Determine enabling events or conditions from the initiating event • Quantify effectiveness of an independent protection layer in terms of its PFD	• Independent protection layers a. Identification of IPLs b. PFD values for each IPL • Inconsistent consensus (for qualitative parameter, C) a. Subjectivity: different teams, different results b. Competence gap	• No aleatory • Epistemic a. Known/unknown completeness b. Model c. No parameter
Minimum SIL	• Calculation method: o Reliability Block Diagram (RBD) • Dependent on both SIF boundary and voting configurations of each element	• Parameter values a. Various reliability database b. Difference between vendor data and generic database • Plant-specific conditions: Validity of typical SIF	• No aleatory • Epistemic a. Known/unknown completeness b. Model c. No parameter

Table 2.6 shows the SIL ratings with the corresponding average probability of dangerous failure on demand (PFDavg) and Risk Reduction Factor (RRF). NSSR "No Standard Safety Requirement" could be considered as no SIL required while

NR “Not Recommended” means there is nothing capable of reducing the risk to acceptable limits. The introduced model was tested at moderate and high-risk levels controlled in its practical limits using SIF. The results showed that the proposed cascaded model and conventional models gave the same results in two experiments, and the proposed cascaded model only gave better SIL results in one single experiment.

Table 2.6. PFD and RRF for each SIL rating [37].

SIL	Probability of failure on demand average range (PFD_{AVG})	Risk Reduction Factor (RRF)
NSSR	10^{-1} to 1	1 to 10
1	10^{-2} to 10^{-1}	10 to 100
2	10^{-3} to 10^{-2}	100 to 1,000
3	10^{-4} to 10^{-3}	1,000 to 10,000
4	10^{-5} to 10^{-4}	10,000 to 100,000
NR	10^{-6} to 10^{-5}	100,000 to 1,000,000

Kim et al. [31] proposed an evaluation method for hardware SIL determination by using hazard analysis and risk assessment (HARA) and failure modes, effects and diagnostic analysis (FMEDA). The safety assessment of SIS was evaluated in two phases; defining the safety requirements using HARA, and evaluating the SIL for hardware and software. The hardware SIL evaluation was conducted as an eight-step process based on FMEDA that can be used to evaluate hardware SILs for reliability verification. This process defined the components of the SIS subsystems, failure modes, and failure effects. A failure mechanism distribution and failure rate were assigned to each component, and the safety mode was determined, as well as the detectability of each failure mode. The case study was the flame scanner system using HARA and FMEDA, where

the safety requirement of the flame scanner was determined using the risk graph method. As a result, the safety requirement of the flame scanner system was defined as SIL 2. The hardware SIL was also determined to be SIL 2 from the combined architectural constraints.

Ding et al. [39] proposed an approach for SIL determination based on system degradation by using reliability block diagram (RBD). From the perspective of system degradation, any failed channel in a multi-channel system will cause degradation of the system. This approach discusses the RBD of several classical safety architectures and explores the formula of PFD and Mean unavailable time (MUnTs), also based on the degradation processes. The key idea of the method proposed was to perform RBD analysis and calculation of average *PFD* at each stage of system degradation, caused by failures of redundant channels. The method was applied to several classical redundant architectures of safety related systems, and could make the SIL verification process simpler.

Dutuit et al [40] proposed PFD evaluation method in relationship with SIL of SIS by introducing fault tree models. They focused on the periodically tested components, which according to their study, must be elaborated to perform realistic computations of PFD and SIL. The specific problems raised by the assessment of SIL, which restricts the use of the formula proposed in the standard was raised. Time-dependent behavior of the system unavailability in addition to its average value was also considered. Using a simple pressure

protection system, results were obtained by means of the FTA against those obtained by means of stochastic Petri nets. The results provided by the *Aralia Workshop* software were compared with those obtained by means of MCS based on Petri Net models. These comparisons showed that results obtained by means of FTA were almost identical to those obtained by the more elaborated methods.

Nait-Said et al. [41] proposed several modified risk graph methods to improve flexibility and reduce the subjective uncertainty. **Figure 2.6** [41] is the overall procedure of fuzzy safety integrity assessment. To assess risk parameters, calibration may be made by varying risk parameter values. The proposed version of risk graph uses fuzzy rule-based-risk graph, which has main advantages of:

(1) Preservation of the four parameters used in the standard risk graph and can be adapted easily to improved risk graphs;

(2) Fuzzy scales with fuzzy linguistic values used to assess risk parameters and calibration of the model may be made by varying risk parameters values.

The results were numerical values of risk reduction factor, which can be compared directly with those given by quantitative methods such as LOPA and semi-quantitative methods such as FTA.

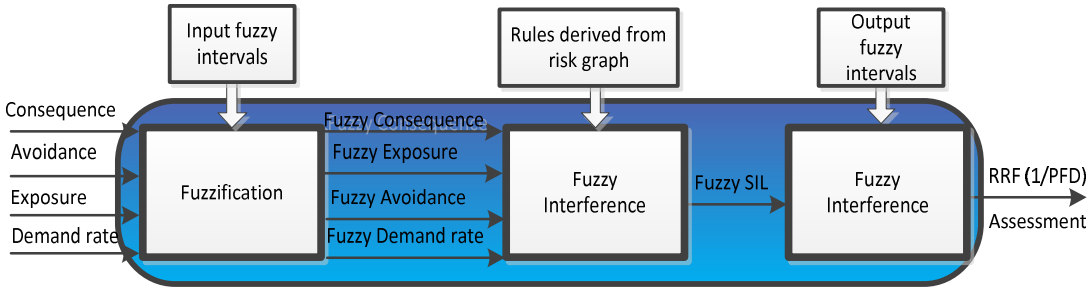


Fig. 2.6. Overall procedure of fuzzy safety integrity assessment [41].

Shu et al. [42] proposed a simplified method for SIL determination for complex SIS by conducting Markov Analysis (MA) on each channel of the MooN architecture and combining the results. MA shows great advantages in flexibility and ability to describe the time-dependent PFD. However, similar to other studies, the size of the Markov models increases explosively as systems become complex. For instance, using the commonly used MooN architecture shown in **Table 2.7** [42], with N number of channels increasing, the number of possible intermediate states in the architecture would also become bigger. In effect, the size of the matrix model becomes uncontrollable. In terms of the concern about the common cause failure (CCF), the proposed solution was to introduce the multi-β factor model in different MooN configuration. The effect of the CCF model is necessary to combine the failure probabilities of all channels in a MooN configuration. The results have proven that the simplified approach can simplify Markov modelling without loss of accuracy if a proper CCF model is adopted.

A similar study had been conducted by Knegtering and Brombacher [43], wherein they attempted to break down the SIS architecture and developed the micro Mark model. Their model divided the whole Markov model into small ones according to RBD and combined the results on the assumption of independent events. Unfortunately, the impact of CCF was ignored in their model, which appears to be inaccurate making modelling results suspicious.

Table 2.7. The size of the matrix model in reference [41].

Type of MooN	Size of matrix model
1oo1	4-by-4
1oo2	7-by-7
2oo2*	13-by-13
2oo3	23-by-23
3oo4*	54-by-54
6oo6*	204-by-204

A SIL determination method based on Markov model processes were explored by Pilch [44]. This is the generalised equations, based on [2] for calculating the PFD which considers CCF. Sallak et al. [45] proposed a fuzzy probabilistic method for SIL determination of SIS considering the uncertainty of failure rates of its components. The concept can be explained using **Figure 2.7**, which was based on conventional fault tree analysis utilizing probabilistic approach [30, 46, 47]. A fuzzy number $\tilde{A}$ can be expressed using Eq. (1.2):

$$\widetilde{\mathrm{A}} \rightarrow \left[\mathrm{A}_L^{(\alpha)},\ \mathrm{A}_R^{(\alpha)}\right], \quad 0 \leq \alpha \leq 1. \qquad (1.2)$$

The symbols $\mathrm{A}_L^{(\alpha)}$ and $\mathrm{A}_R^{(\alpha)}$ denote $\mu_{\widetilde{A}}^{(x)}$left-end-point and right-end-point of this interval. For any fuzzy number $\widetilde{A}$ which has the membership function $\mu_{\widetilde{A}}^{(x)}$, an interval bounded by two points at each α -level (0 ≤ α ≤ 1) can be obtained using the α-cut method.

This fuzzy probabilities based approach to evaluate the SIS PFD and the SIL was applied to a process example from the technical report ISA-TR84.00.02-2002 [48] and compared to a conventional probabilistic approach. The results justify the effectiveness of the proposed methodology in evaluating the SIL of the SIS. The proposed method recommends a guidance on reducing the SIL uncertainty

based on a fuzzy probabilistic importance measure which is used to identify the SIS critical components. It was further highlighted by the authors that the issues of maintenance and repair strategies into the fuzzy probabilistic approach should be considered to perform the trade-off between the maintenance cost and the required SIL for the SIS.

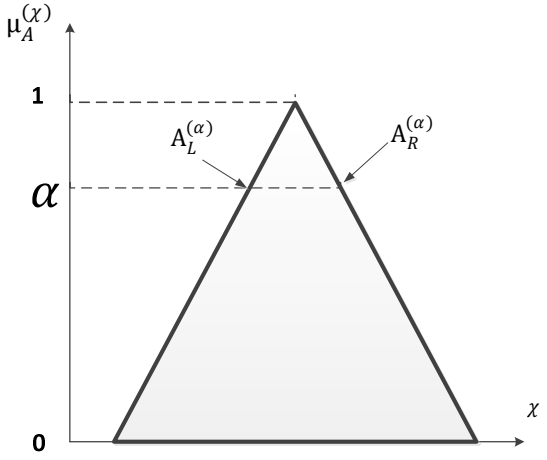


Fig. 2.7. Fuzzy probabilistic approach concept [45].

Jahanian [49] conducted a detailed analysis and derived a universal form of PFD formula called the Generalised PFD Formula (GPFDF) for K-out-of-N (KooN) systems using the same structure of PFD elements utilized by the standards [2]. While there have been other studies on IEC 61508 formulas and the simplified KooN equations [50-59], none have proposed an inclusive generalized form of IEC 61508 formulas to duplicate all the specific combinations covered by the standard. Thus, the GPFDF approach can be used as a determination method to all KooN combinations. The GPFDF was verified by

using specific K and N values and reproducing the specific formulas given in IEC 61508.6-2011 for ordinary combinations of 1oo1, 1oo2, 2oo2, 2oo3 and 1oo3. The proposed GPFDF equation can be expressed using Eq. (1.3):

$$PFD_{KooN} = \prod_{i=1}^{n-k+1} (n-i+1)\ ((1-\beta)\ \lambda_{DU} + (1-\beta_D)\lambda_{DD})(\frac{\lambda_{DU}}{\lambda_D}\left(\frac{\tau}{i+1} + PTT + MRT\right) + \frac{\lambda_{DU}}{\lambda_D} MTTR + \beta\lambda_{DU}\left(\frac{\tau}{2} + PTT + MRT\right) + \beta_D\lambda_{DD})MTTR \quad (1.3)$$

This proposal was applied into a real-life example and the result was verified against both IEC 61508 and the simplified formula. A simplified configuration of the real-life example is shown in **Figure 2.8.** The case study was a single gas burner with one set of double block and vent valves to isolate the fuel gas, and five flame outlets where each outlet was monitored by one flame scanner. Using this example, they have proven that by using GPFDF, you can get the same result as per IEC 61508. The unique work that the authors have conducted was that they have replicated an inclusive generic form of the standard [2] formulas for all possible combinations covered by the same standard. On the practical side, the advantage of this approach is that they can be used in calculating PFD for every K-out-of-N architecture.

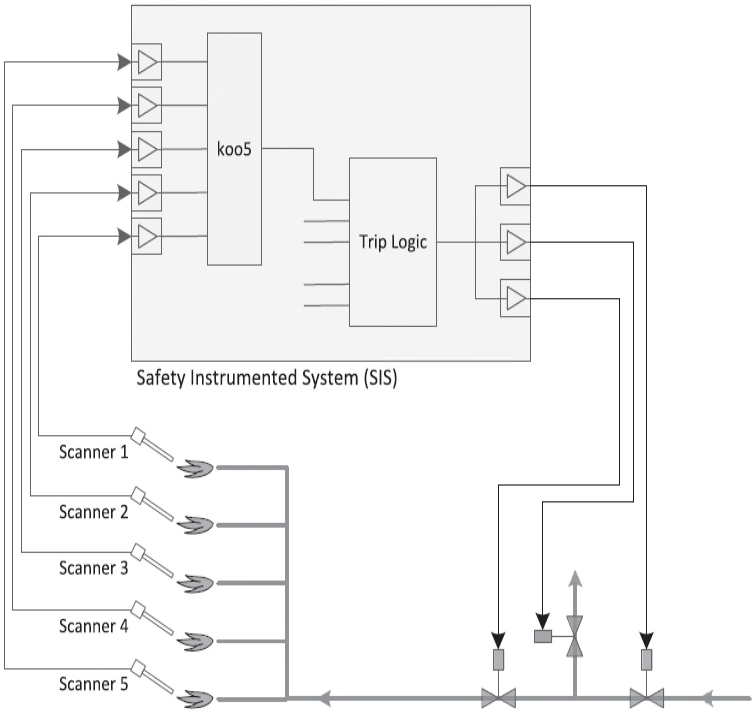


Fig. 2.8. Example using a single burner with five outlets [49].

On the same vein, Chebila et al. [60] explored generalized analytical expressions for SIS performance measures, specifically the PFD_{AVG} and PFH. They have developed a set of simplified and generalized expressions for PFD_{AVG} and PFH for any KooN architecture, considering Partial Stroke Testing (PST) and CCF.

Ouache et al. [61] studied a new model for SIS in a quantitative assessment approach. Specifically, they have proposed a three-step mathematical model to compute the PFD of SISs and used Bowtie method to conduct the safety analysis of several scenarios by determining the PFD of safeguards. The sequence of work comprised:

(1) KHALFI (Characteristics of Hazard Analysis based on Logic Frequency Initiative) mathematical model to compute the real PFD at any geographical location considering environmental factors such as temperature, humidity, pressure, wind speed and time which can affect PFD.

(2) Probability binary state (PROBIST) was used to calibrate precisely the values of PFD.

(3) Bowtie method was incorporated for evaluating the PFD of safeguards where new classification for SIL is proposed.

Simulink was used to facilitate the automatic computation and analysis in the proposed model. The atmospheric elements were determined to be significant for consideration to attain the best reliability in the calculation of PFD. They have also proposed to extend the SIL classification up to SIL 10 with corresponding PFD and PFH as shown in **Table 2.8**.

Mechri et al. [62] proposed a SIL determination method using a holistic approach for modeling the unavailability of SIS by using switching Markov chains. The influence of several parameters on the performance of SIS, such as CCF, imperfect and partial proof testing was considered in the model. Markov chains modelling is one of the approaches mentioned in IEC 61511 [3]. It is more applicable for use in systems with repairable components at constant failure and restoration rates [63, 64]. The authors argued that switching Markov chains is preferred over the conventional Markov because SIS are periodically tested, thus

the unavailability of the SIS can be computed by summing the probabilities of being in states *j* at each time *t*, as given in Eq. (1.4):

$$PFD(t) = \sum_j Pj\ (t) \tag{1.4}$$

Table 2.8. Reliability of extended safety integrity level [61].

SIL	PFD	Safety Availability (SA) (%)	PFH
SIL 1	[$5 \cdot 10^{-1}$ 1]	[50 0]	[$5 \cdot 10^{-6}$ $1 \cdot 10^{-5}$]
SIL 2	[$1 \cdot 10^{-1}$ $5 \cdot 10^{-1}$]	[90 50]	[$1 \cdot 10^{-6}$ $5 \cdot 10^{-6}$]
SIL 3	[$5 \cdot 10^{-2}$ $1 \cdot 10^{-1}$]	[95 90]	[$5 \cdot 10^{-7}$ $1 \cdot 10^{-6}$]
SIL 4	[$1 \cdot 10^{-2}$ $5 \cdot 10^{-2}$]	[99 95]	[$1 \cdot 10^{-7}$ $5 \cdot 10^{-7}$]
SIL 5	[$5 \cdot 10^{-3}$ $1 \cdot 10^{-2}$]	[99.5 99]	[$5 \cdot 10^{-8}$ $1 \cdot 10^{-7}$]
SIL 6	[$1 \cdot 10^{-3}$ $5 \cdot 10^{-3}$]	[99.9 99.5]	[$1 \cdot 10^{-8}$ $5 \cdot 10^{-8}$]
SIL 7	[$5 \cdot 10^{-4}$ $1 \cdot 10^{-3}$]	[99.95 99.9]	[$5 \cdot 10^{-9}$ $1 \cdot 10^{-8}$]
SIL 8	[$1 \cdot 10^{-4}$ $5 \cdot 10^{-4}$]	[99.99 99.995]	[$1 \cdot 10^{-9}$ $5 \cdot 10^{-9}$]
SIL 9	[$5 \cdot 10^{-5}$ $1 \cdot 10^{-4}$]	[99.995 99.99]	[$5 \cdot 10^{-10}$ $1 \cdot 10^{-9}$]
SIL 10	[$1 \cdot 10^{-5}$ $5 \cdot 10^{-5}$]	[99.999 99.995]	[$1 \cdot 10^{-10}$ $5 \cdot 10^{-10}$]

The basic concept of the switching Markov chain was further explained and modeled using a *one-out-of-one* (1oo1) architecture as shown in **Figure 2.9** and switching states in **Table 2.9**. Using this simple SIS example, the switching Markov chains start from the initial state 1, with a detected failure rate λ_{DD} to transition as state 2. When a failure is detected and the repair starts, the rate of repair is μ_{DD}. For the undetected failure, it can occur at rate λ_{DU} and signified as transition states from 1 to 3.

The advantage of this approach is that it can be utilised to a more complex safety system, with cumbersome analysis as a downside. Modelling complex systems make the number of states of the Markov model exponentially large. As an example, the proposed modelling approach was applied to a high integrity

protection system of a chemical reactor, as a complex system. Unfortunately, safe failures were not considered in this work.

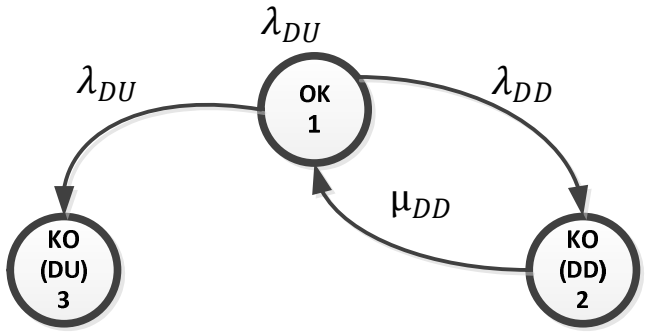


Fig. 2.9. Switching Markov model of 1oo1 architecture [62].

Table 2.9. States and description of switching Markov model [62].

States	Description
1	OK
2	Detected failure
3	Undetected failure

Baghei [65] proposed the 3-Parameter SPW technique: A new method for evaluation of target SIL. This modification to risk graph parameters aims to add more flexibility and reduces their subjective uncertainties while keeping the method simple. The three parameters, namely severity (S), hazard avoidance probability (P), and demand rate (W) were used instead of the former four parameters (consequence - C, exposure - F, probability of avoiding the hazard - P, demand rate W). The author dropped the exposure parameter F on the premise that a scenario with consequence parameter of C_B and exposure parameter of F_B behaves just like a scenario with consequence parameter of C_C and exposure parameter of F_A regardless of the values of parameters P and W.

Mathematically, the correlation between consequence and exposure parameters are given as in Eq. (1.5) and Eq. (1.6):

$$C_B F_B = C_C F_A \tag{1.5}$$

Similarly, it can be shown that on the risk graph as:

$$C_C F_B = C_D F_A \tag{1.6}$$

We can now combine the exposure frequency parameter (F) with consequence parameter (C) and a new severity parameter, S, is defined that shows overall consequence severity of hazardous event, starting from Eq. (1.7).

Therefore, S = 0 denoted by S_0, equals C_A on risk graph, S = 1 shown as S_1 equals $C_B F_A$ and so on, i.e.:

$$S_0 = C_A \tag{1.7}$$

$$S_1 = C_B F_A \tag{1.8}$$

$$S_2 = C_B F_B = C_C F_A \tag{1.9}$$

$$S_3 = C_C F_B = C_D F_A \tag{2.0}$$

$$S_4 = C_C F_B \tag{2.1}$$

Continuing the same logic, it is observed that:

$$S_1 P_B = S_2 P_A \tag{2.2}$$

$$S_2 P_B = S_3 P_A \tag{2.3}$$

$$S_3 P_B = S_4 P_A \tag{2.4}$$

However, the problem with removing the *exposure* parameter is that the result may not be more reflective of the risk assessment of the actual process hazard condition. The risk assessment team would not be able to calibrate the risk graph

based on a fit for purpose scenario. For example, a plant operator who has an 8-hour exposure (F) to hazard is different to an operator who does his routine daily checks and exposes himself in the hazard only for a few minutes. Analysing the comparative results of SPW, it appears that the conventional risk graph method showed SIL3 while SPW is SIL2 (0.015). These contradicting results cast doubts in utilising this method as safety of personnel, damage to property and the environment is at stake.

2.4 Bayesian Networks (BNs) and Dynamic Bayesian Networks (DBNs)

Several researchers were attracted in utilizing the emerging BNs and DBNs. The following studies conducted using BNs and DBNs as regard to SIL determination, system reliability, safety and risk evaluation.

Cai et al. [66] proposed a novel multiphase dynamic BN (MDBN) methodology for the determination of SIL. The MDBN for SIL determination focuses on theoretical proof test, proof test interval phase, proof test phase. The purpose of the test was to uncover covert failures that can cause dangerous failures which cannot be detected using normal diagnostics method. In conducting proof testing, the device first needs to be put out of service.

Then, visual inspection should be performed followed by calibration and a series of simulation tests. Similarly, the operation in proof test phase can be modelled using DBN according to the actual conditions. The DBN for proof test

interval phase and DBN for proof test phase are integrated to form the MDBN as shown in **Figure 2.10** [66].

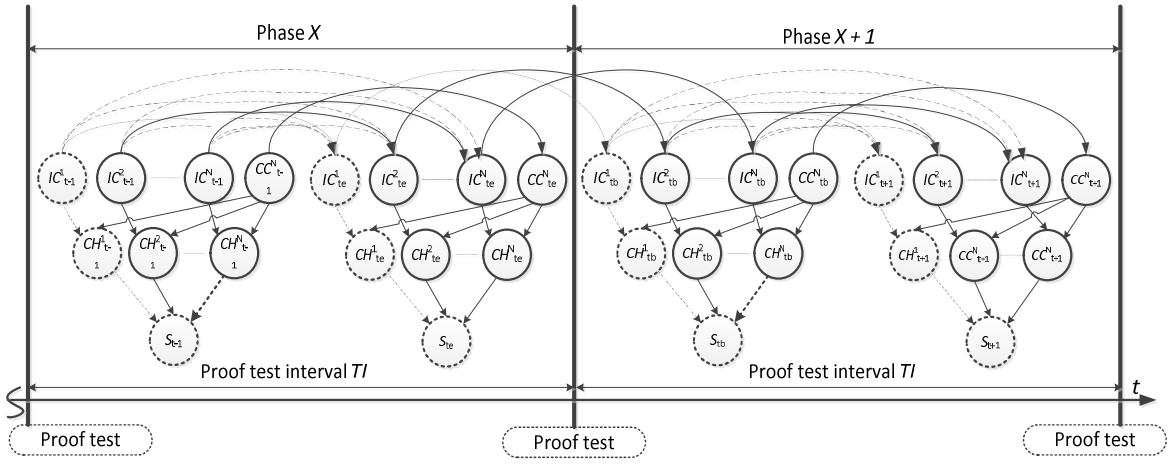


Fig. 2.10. Schematic diagram of MDBN for SIL determination [66].

Using Markov state transition diagram of five states, namely, DU, DD, NS, SD and SU, the conditional probability relationships of independent cause (IC) failure and common cause (CC) failure nodes in proof test phase are determined as shown in **Figure 2.11** [66]. In each node, eight variables, namely, ζ, δ, θ, σ, α, ε, μ and γ, are used to describe the transition probabilities of states θ, μ, ζ, and δ. The transition rates from DU, DD, SD and SU to NS, respectively. σ, ε, α and γ are the transition rate factors from DU to DU, SU to SU, NS to SU and NS to DU, respectively. **Table 2.10** shows the conditional probability tables (CPTs) of IC failure and CC failure nodes in proof test phase as derived from the transition diagram in **Figure 2.11** [66]. Aside from the fact that this method is complex, the determination of SIL of SIS is only operating in a low demand mode. No example was presented using a real-life SIF device.

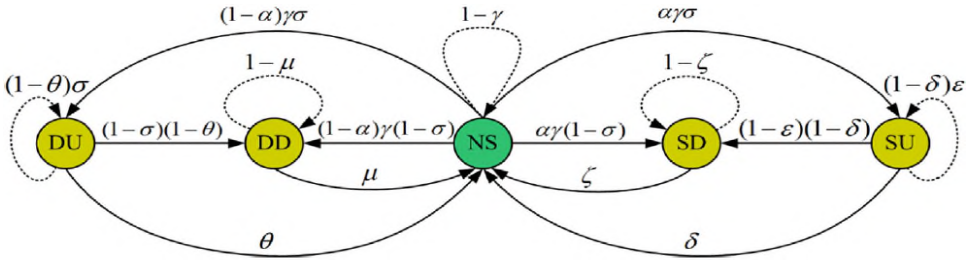


Fig. 2.11. State transition diagram of IC and CC nodes in proof test phase [66].

Table 2.10. State transition CPTs of IC and CC nodes in proof test phase [66].

Before proof test	After proof test				
	NS	**SD**	**SU**	**DD**	**DU**
NS	$1 - \gamma$	$\propto \gamma\,(1-\ \sigma)$	$\propto \gamma\,\sigma$	$(1-\propto)\gamma(1-\sigma)$	$(1-\propto)\gamma\sigma$
SD	ζ	$1-\zeta$	O	O	O
SU	δ	$(1-\delta)(1-\varepsilon)$	$(1-\delta)\varepsilon$	O	O
DD	μ	O	O	$1-\mu$	O
DU	θ	O	O	$(1-\theta)(1-\varepsilon)$	$(1-\theta)\varepsilon$

Tsilipanos et al. [67] proposed a BN-modeled system of systems (SoS) framework for the reliability evaluation of telecommunication networks. The authors employed a hybrid scheme – a combination of HazOp (hazard and operability analysis) and FTA. Further enhancement was the application of the BN model coupled with sensitivity analysis to solve complex probability queries. The proposed model can also estimate the impact of residual mishap risks or other unknown events. The SoS emergent behavior and model were applied in the case of a fiber–to–the-curb VDSL telecommunications network.

Doguc et al. [68] proposed an automated approach for the reliability assessment of grid systems by using BN, which require no prior information of

the grid system structure. This approach is based on a data-mining algorithm, the $\kappa 2$, to discover the grid system structure from raw historical system data, that allows to find minimum resource spanning trees (MRST) within the grid and then uses BN to model the MRST and estimate grid service reliability. The components in the grid is a very large set, which takes advantage of this proposal since it does not need to consider them all. It stops when it finds all possible MRSTs, which usually requires considering only a small subset of the components in the grid system. Also, experimental analysis of the performance and accuracy of the proposed method are provided. It is shown that the proposed method discovers the MRSTs in less time than the method that uses genetic algorithm and provides very accurate reliability values. Moreover, the proposed method will be very useful for system and reliability engineers, since it is fully automated, does not rely on assumptions and does not require prior knowledge of the grid system structure.

Jiang et al. [69] proposed BN-based probabilistic model, named the hybrid relation model (HRM), for the reliability evaluation of programmable logic controller (PLC) systems. The complexity of PLC system reliability analysis arises in handling the complex relations among the hardware components and the embedded software. Different embedded software types will lead to different arrangements of hardware executions and different system reliability quantities. The proposed approach is a novel probabilistic HRM model for the reliability analysis of PLC systems**.** It is based upon the execution logic of the embedded

software and the distribution of the hardware components. With the computational mechanism of the BN, the HRM handles the failure probabilities of the hardware components as well as the complex relations caused by the execution logic of the embedded software. The hardware components were mapped to the corresponding HRM nodes and embed the failure probabilities of the hardware components into the well-defined conditional probability distribution tables of the HRM nodes. Authors claimed that the experimental results demonstrated the accuracy of the said model.

Zhang et al. [70] proposed a fuzzy-BN-based systemic decision support method for safety risk analysis under uncertainty in tunnel construction. Interestingly, we can learn from the application of the tunnel construction project as it is highly complicated and with large potential risks. Fuzzy BN (FBN) has been utilised to explore the relationships between tunnel-induced damage and its influential variables relying on the risk and hazards criteria. The authors have adopted the so-called "3σ criterion" to calculate the characteristic values of a triangular fuzzy number in the probability fuzzification process, and the α-weighted valuation method was adopted for defuzzification. Pros and cons between FBN and fuzzy fault tree analysis (FFTA) as risk analysis tools was also conducted. The holistic FBN methodology had many limitations and future potential works in developing an expert system technique would make the approach manageable.

Daemi and Ebrahimi [71] proposed a BN-based reliability evaluation method for composite power systems with emphasis on the importance of degree sequence of components in consideration of load variation and weather conditions. The weather conditions and load level variation in construction and implementation of the BN associated with the composite power systems was considered. The geographical division model was used to model weather conditions in various regions of the given power system and different sections of overhead transmission lines.

Innal et al. [72] proposed new generic formulations of their related performance indicators, i.e. PFDavg, PFH, PFSavg and STR, as valid formulae for any KooN architectures. There will be huge consequences when SIS fails and this proposal considers the safety of the monitored system (SIS safety integrity) and the production availability due to false trips (SIS operational integrity). This is a more realistic approach as operational aspects are plugged into the equation. These new formulations allow designers and engineers to assess SIS, which is acceptable for any KooN configurations unlike dedicated standards which only provides formulae for some KooN architectures.

Baraldi et al. [73] applied BN to handle the uncertainty problems of human reliability analysis (HRA) and compared it with fuzzy expert system. Furthermore, the work analysed and compared two expert systems, based on Bayesian Belief Networks (BBN) and fuzzy logic. The study included the analysis of the five

groups of BBN applications. These groups of BBN applications include the following:

- Modelling of organizational factors,
- Analysis of the relationships among failure influencing factors,
- BBN-based extensions of existing HRA methods,
- Dependency assessment among human failure events, and
- Assessment of situation awareness.

The study showed that BBN approach should be preferred in all cases characterized by quantifiable uncertainty in the input, since it provides a satisfactory representation of the uncertainty and its output is directly interpretable for use within process safety analysis (PSA). Typically, HRA models, which are part of the overall PSA model, are utilised to make decisions with risk-relevant implications. All assumptions in the development of the model may undergo review and acceptance by regulatory bodies. In this respect, the acceptance of BBN applications for HRA in terms of validation and verification must be supported by relevant authorities.

O'Connor and Mosleh [74] explored a general dependency model (GDM) that utilised BN to model the probabilistic dependencies for analysis of common causes failures (CCF) and dependent failures in system risk and reliability assessments. Three parameters for each failure cause were introduced to show the relationship to physical attributes of the system being modeled, i.e., cause

condition probability, component fragility, and coupling factor strength. The paper also demonstrates the development and use of the GDM in traditional applications of Probabilistic Risk Assessments (PRA), and for Event Assessments (EA) and Significance Determination (SD). An example was presented to show how to build and quantify the GDM using similar inputs to that of current CCF methodologies. The work also presented how the GDM can adjust to uncertain evidence, asymmetrical components and coupling factor strength. Furthermore, the work provided insight into the change in propensity of a system to adopt CCF based on actual system features.

Cai et al. [75-77] proposed BN-based reliability evaluation methods in consideration of CCF, imperfect coverage and intermittent faults. They also recommended DBN-based real-time reliability evaluation methodology for industrial systems. Architectures such as the Triple Modular Redundancy (TMR) and Double Dual Modular Redundancy (DDMR) control systems for subsea Blowout Preventer (BOP) were presented as a case study example. The reliability of subsea BOP control systems were evaluated at any given time. The difference between posterior and prior probabilities of each single component given the system failure was obtained using the proposed BN network models. It is interesting to note that the results showed that the DDMR control system has a little higher reliability than the TMR system. The authors suggested that to improve the reliability of subsea BOP control systems, the component failure rates should be reduced for TMR systems for ethernet switch, PLC and human

machine interface (HMI), whereas the failure rates of ES and PC should be reduced for DDMR system. In terms of the recovery mechanism of PLC, HMI, ethernet switch and subsystems should be given more attention for TMR and DDMR control systems, respectively. For future works, fault-tolerant control systems shall be examined in the light of perfect and imperfect repairs and preventive maintenance.

Ramírez and Utne [78] proposed DBN-based evaluation method of life extension for ageing repairable systems. The model has three main applications:

- Assessing and selecting optimal decision alternatives for the life extension at present time, based on historical data;
- Identifying and minimizing the factors that have a negative impact on the system performance, and;
- Reassessing and optimizing the decision alternatives during operation throughout the life extension period, based on updating the model with new operational data gathered.

With respect to the life extension duration, the criteria for selecting the best alternative was attained by analysing and predicting the system performance. Factors that need to be considered in decision making are costs, safety and unavailability. Example presented was the life extension of a firewater pump. In this case study, the application of the DBN model was applied in operation of the said firewater pump for more than 26 years. This approach is not only applicable

for life extension of a component but also justification for ageing systems whose life is not going to be extended.

Flammini et al. [79] presented both a failure model for KooN architecture based on BN and a maintenance model based on continuous time Markov chains. These were combined to a compositional multi formalism modeling approach to analyse the effect of imperfect maintenance on system safety. Based on the result of the study, the use of different formalisms support for an easy and effective representation of the hazardous failure model. Specifically, the issue of evaluating the impact of imperfect maintenance on system safety has been addressed by solving a multi formalism compositional model including a BN failure model and a continuous time Markov chain maintenance model. The single formalism approach could appear less complex with respect to multi formalism approach. Furthermore, the researchers proposed a BN-based method to evaluate the trustworthiness of 2oo3 decision fusion mechanisms in multi-sensor applications [80].

Weber and Theilliol [54] studied a solution to control an over actuated system that was structured as a typical consecutive KooN: F system. BN was applied on circular and linear typical consecutive KooN: F system to estimate its reliability and provide the parameters to distribute the control efforts among the redundant set of actuators. Specifically, in the example, the reliability of consecutive-*2*-out-of-*5*: F system to linear and circular structure was presented. Diagnosis with inspections scenario was also realised to compute the on-line

functioning probabilities of each actuator with the BN model. Research showed that the graphical aspect of BN is very noteworthy because it formalises the model by coupling a generic model structure with simple parameter matrices, and the inference computes the reliability of actuators according to evidences.

2.5 Techniques in SIL calculation

In reliability assessment of SRS, SIL verification plays a critical role. After the target SIL has been determined, then SIL verification or validation must take place. In order to achieve the required SIL for the safety functions, IEC 61508 adopts an overall safety lifecycle as the technical framework of safety-related systems. One of the necessary procedures of the overall safety lifecycle is the SIL verification, which verifies whether the PFDavg of designed safety-related system meets the required failure measure. The SIL of safety-related system can be verified by reliability quantitative analysis techniques presented in the IEC 61508-6 [27] or ISA-TR84.00.02 [81]. They are both performance-based standards that focus on the SIL [82]

Summers [30] narrated view points on ISA TR84.0.02. The author recommends the use of simplified equations (SE) and FTA due to their cost effectiveness. Since ISA-TR84.0.02 [30] only provides guidance (not a mandatory requirement) on how to calculate the SIL of a SIS and not for specific steps, engineers and designers need to do their due diligence in gathering further information for their respective industry needs. Other quantitative techniques

include RBD [83, 84], Markov Analysis (MA) [27],[85],[86], Fault Tree Analysis (FTA) [27],[87] failure mode and effects analysis (FMEA) [88], SE [27], hybrid techniques [89], MCS [84, 90], Petri nets, etc.

Guo and Yang [91] explored the flexibility of automated MA modelling as compared to manual technique, which is a fallible exercise. Although MA is powerful, it tends to become complex and time-consuming because the size of the MA model exponentially increases with respect to the complexity of the system. Authors recommendation was to break SIS into subsystems, incorporating restorations and CCF into the framework, so they can be easily managed and then automate the MA modelling to save time. This technique post many concerns as the assumptions are significant such as:

1. Failure rate and diagnostic coverage for all the channels in a voted group are the same;
2. Constant failure rates and repair rates;
3. All the components made up of the SIS operate successfully in the initial state of SIS;
4. Only single normal failure (non-CCF) can occur per unit of time;
5. Only one set of multiple failures caused by common cause can occur per unit of time;
6. Single normal failure and CCF cannot occur in the same unit of time;
7. All the safe failure states of a group are handled as one representative state;

8. Degraded operations are considered e.g., detected failures can be repaired without interrupting other parts of the system;
9. In the event of a spurious trip, the system will be restored to its initial state.

The above assumptions clearly occur only in a perfect world and does not reflect the actual complexities of the actual world. Zhang et al. [50] also studied PFD_G calculations by applying the MA model and using the mathematical relationship between system unavailability and system failure frequency. However, most results obtained were also different from those in IEC 61508-6. The discrepancies in the calculation of given t_{CE}; t_{GE} and t^1_{GE} for 1oo2, 1oo2D and 2oo3 system architectures are presented in **Table 2.11** [50].

Table 2.11. Comparison among equivalent mean down times for the three system architectures [50].

System	t_{CE}, t_{GE} and t^1_{GE} obtained by Markov model	t_{CE}, t_{GE} and t^1_{GE} given in IEC 61508-6
1oo2 2oo3	$t_{CE} = (\lambda_{DU}/\lambda_D)(T_1/3+MTTR) + (\lambda_{DD}/\lambda_D)\,MTTR$ $t_{GE} = ½\,[(\lambda_{DU}/\lambda_D)(T_1/3+MTTR) + (\lambda_{DD}/\lambda_D)\,MTTR]$	$t_{CE} = (\lambda_{DU}/\lambda_D)(T_1/2+MTTR) + (\lambda_{DD}/\lambda_D)\,MTTR$ $t_{GE} = (\lambda_{DU}/\lambda_D)(T_1/3+MTTR) + (\lambda_{DD}/\lambda_D)\,MTTR$
1oo2D	$t^1_{CE} = (\lambda_{DU}/\lambda)(T_1/3+MTTR) + (\lambda_{DD}/\lambda)\,MTTR$, $\lambda = \lambda_{DD} + \lambda_{DU} + \lambda_{SD}$ $t^1_{GE} = \lambda_{DU}(T_1/3+MTTR) + (\lambda_{DD}/\lambda_{SD})\,MTTR / 2(\lambda_{DU} + \lambda_{DD} + \lambda_{SD})$	$t^1_{CE} = (\lambda_{DU}/\lambda)(T_1/2+MTTR) + (\lambda_{DD}/\lambda)\,MTTR$, $\lambda = \lambda_{DD} + \lambda_{DU} + \lambda_{SD}$ $t^1_{GE} = \lambda_{DU}(T_1/3+MTTR) + (\lambda_{DD}/\lambda_{SD})\,MTTR / (\lambda_{DU} + \lambda_{DD} + \lambda_{SD})$

Innal [92] as part of the Ph.D. work, studied PFD_G calculations and got the same formula as mentioned in IEC 61508 [2]. This was conducted by using a continuous Markov model to approximate the exact Markov model.

In addition, the author has also explored other approaches to calculate PFD_G. The author has reviewed that the underlying behavior of any KooN architecture made up of periodically tested components, was not Markov, but piecewise Markov. It has been verified that the average unavailability of these architectures, calculated via a multi-phase model, could be approximated by the asymptotic unavailability of a classic Markov model. An approach based on piecewise Markov models or their derived models has been presented to enable the author to work back to the analytical formula. A simple SIS was utilised to verify that the average unavailability of any KooN architecture could be approximated by the asymptotic unavailability of a classic Markov model calculated via a multi-phase model. The SFF has been examined as well in relation to the expected SIL value in consideration with the proposal submitted by Jean-Pierre Signoret, the Reliability Engineer (TOTAL) and Examiner of the author [92]. The author further examined that the SFF is irrelevant and should not constrain the probabilistic determination of the SIL. It is also interesting to note that the findings about the overall risk reduction factor, as a result from an association of several protection layers, is not obtained by simply multiplying the individual risk factors, as opposed to the majority of the papers published.

Jin et al. [93] gave a common approach covering both low and high-demand modes of operation and obtained results close to IEC 61508-6 [27] by using the Markov model. Normally, SIS are divided into two modes, low and high demand modes. IEC 61508 [2] differentiates between two modes of SIS operation as: low-demand and high-demand. The classification of operational modes was based on two criteria:

(1) Frequency that the SIS is expected to operate when demanded, and

(2) Expected time that a failure may remain unrevealed, considering the functional test frequency.

IEC 61508 [2] discusses a SIS operating in the high demand or continuous mode (operating as a continuous control function) if the demand rate is greater than once per year, or greater than twice the frequency of functional tests. In high demand or continuous mode of operation, the lower limit is set at a probability of a dangerous failure of 10^{-9} per hour. It is important to identify high demand scenarios and then apply the correct calculation. The use of a low demand approach is conservative that leads to more cost allocation. Using a high demand calculation gives a more appropriate assessment with a lower SIL requirement [94].

Figure 2.12 illustrates the Markov transition diagram for the examined system for corresponding system states shown in **Table 2.12** and transition rates shown in **Table 2.13**. The model has six system states, 0,1, ... ,5, where state 5 is the initial state and state 0 represents the hazardous event/state. If the SIS is

not the last protection layer, the hazardous event is a demand for the next barrier. State 5 is the normal operating state, where the SIS is available and there is no demand for the activation of the SIS. State 4 shows the safe state, where no hazardous event can happen. This is achieved after a spurious trip. State 3 is where the SIS is responding to a demand. In state 2, there is no demand for the SIS yet the SIS has a DD-failure. State 1 and state 2 are similar, but the SIS has DU instead of DD-failure. State 0 is the renewal state or the hazardous event, where the SIS has a DU- or DD- failure and there is a demand for the activation of the SIS.

It is assumed that the system satisfies the Markov property, and that all transition rates are constant in time. The problem with this study is that the failure rates and repair rates were assumed to be the same in the various operating states in on-demand and non-demand states, thus the DD and DU repair times are exponentially distributed. In the actual application, these rates are often varying, but according to a view from Bukowski [95], this assumptions can give a reasonable accuracy.

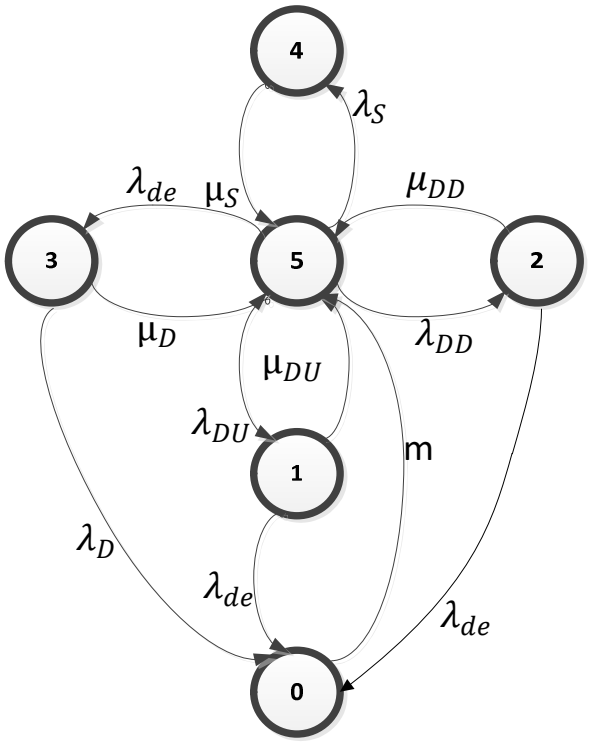


Fig. 2.12. Markov transition diagram [93].

Table 2.12. System states [93].

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

Table 2.13. System states [93].

Transition rate	Description
λ_S	Transition rate to safe state
μ_S	Restoration rate
λ_{de}	Demand rate
μ_{de}	Demand duration rate
λ_{DD}	DD- failure rate
μ_{DD}	DD- repair rate
λ_{DU}	DU- failure rate
μ_{DU}	DU- repair rate
$\lambda_D (= \lambda_{DU} + \lambda_{DD})$	Dangerous failure rate
M	Renewal rate

The work discussed in [93] has further explored the study in a real-world application utilising a single pressure transmitter, wherein the authors concluded that the Markov model gives very accurate results, both for low-demand and high-demand mode. They have claimed that all the main results will also be applicable for a more complex multi-component SIS.

Dutuit et al. [40] presented a methodology to assess the PFD_G by means of Fault Trees and got similar results compared to the results obtained by means of MCS based on a Petri net model. The focus on the study was on a low demand rate. It has been highlighted that the Petri net models, even for simple systems, are quite complex to design and to maintain. That is the reason why Fault Tree models are preferable, however, raised several specific problems. A common mistake exists in calculating the top event probability from average values of components' unavailability. The more the system is redundant, the more the result is non-conservative. In reference [2], the distributions for periodically tested components into Fault Tree models were factored in to calculate accurately the average PFD. The concerns raised by the assessment of SIL, which restrict the use of the formulae proposed in the standard. It was further examined that concerns about the fact that SIL should be assessed by considering the time-dependent behaviour of the system unavailability in addition to its average value. Using a simple pressure protection system, the results obtained by means of the FTA were compared against those obtained by means of stochastic Petri nets with predicates.

Goble and Brombacher [96] introduced the FMEA technique to calculate the diagnostic coverage (DC) used in PFD_G. Although this is not a SIL calculation method, however, it would be helpful to mention this method of estimating the DC. A FMEA is a bottom up technique that is very effective in identifying critical component failures in a Programmable Electronic Systems (PES). Since DCS are one of the major advantages of a safety PLC, the ability to measure and evaluate it plays an important role in both safety and availability. The study was conducted using an extended FEMEA [97-99] and fault injection testing [52, 100, 101]. The measure of DC called the "Coverage Factor" was defined as the probability (a number from 0 to 1). As an example, the authors have utilised a PES input circuit specially designed to detect potentially dangerous failures using reference diagnostics and local comparison between two circuits. The safe coverage factor for the circuit was calculated using Eq. (2.5) by taking the total safe detected failure rate and dividing by the total safe failure rate [96]:

$$C^S = \frac{\sum_{all\ components} \lambda^{SD}_{component\ i}}{\sum_{all\ components} \lambda^{SD}_{component\ i} + \sum_{all\ components} \lambda^{SU}_{component\ i}} \qquad (2.5)$$

The dangerous coverage factor can be calculated using Eq. (2.6):

$$C^D = \frac{\sum_{all\ components} \lambda^{DD}_{component\ i}}{\sum_{all\ components} \lambda^{DD}_{component\ i} + \sum_{all\ components} \lambda^{DU}_{component\ i}} \qquad (2.6)$$

Oliveira [102] introduced a generalized equation for PFD_G calculations to any KooN architecture by using simplified equation technique. Using ISA

TR84.00.02-2002 document, simplified equations for PFD evaluation were explored. The results obtained by the generalized equation were close to those of the numerical model and comparison were also made with analytical equations in IEC 61508-6. Verlinden et al. [89] presented a hybrid model which was a combination of RBD and Markov model. Specifically, as applied to a nuclear reactor safety shutdown system, they have explored a tandem of dynamic state space based continuous time Markov chains (CTMC) model and system level static RBD-formalism approach as shown in **Figures 2.13 & 2.14**. They have emphasized that the Markov has major drawbacks. These dynamic models are the exponential growth of the state space as a function of the number of components, known as the state space explosion [43, 103, 104]. The construction of models for complex systems vary rapidly becomes difficult and prone to errors. They have considered the effects of maintenance into the model, such as periodic tests and repairs.

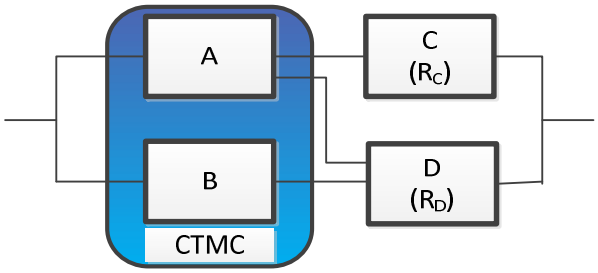


Fig. 2.13. Hybrid model; System level RBD [89].

As shown in the study, the hybrid model easily allows detection of the measurement front-end as the main factor to system unavailability. It was

observed that the PFD increases rapidly with the corresponding increase in the periodic test interval. The probability of operator error was not considered in the simulation thus, the current hybrid model does not allow optimization of the test interval. Challenges post by determining the optimal surveillance test intervals has been discussed and treated by several studies [104-107], using various techniques for single as well as for multiple (RAMS + C) optimization criteria [89].

Rouvroye and Brombacher [108], Rouvroye and Bliek [109] and Bukowski [110] compared techniques such as FMEA, parts count analysis, RBD, Hybrid, FTA and analysis by experts. They have indicated that MA and enhanced MA techniques can cover most aspects of the system's safety-related behaviour except the uncertainty and sensitivity analysis. It is commonly known that MA is a more complicated approach unless one gained expertise of MA which can be obtained [91].The result from [108] of the calculations of PFD_{avg} for techniques such as parts count, RBD, Hybrid IEC, Hybrid SIN, FTA, MA and enhance MA (EMA) are presented in **Fig. 15** [108]. The comparison of analysis techniques on a number of aspects are summarised in **Table 2.14** [108]. MA covers most aspects for quantitative safety evaluation. Aspects not covered by MA are uncertainty analysis and sensitivity analysis.

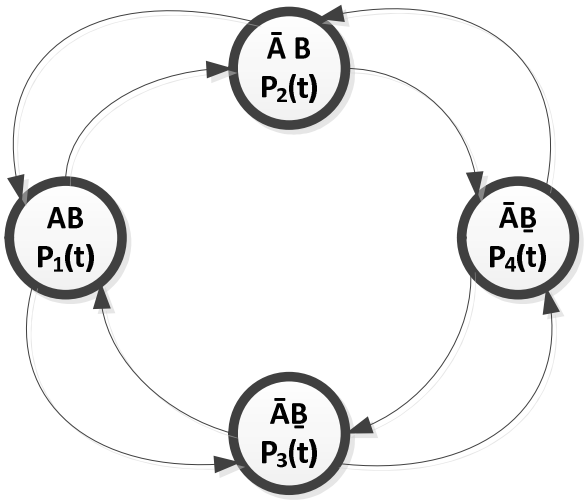


Fig. 2.14. Hybrid model; Sub-level CTMC [89].

These aspects are included in the EMA technique. Parts count analysis and reliability block diagrams lead to pessimistic results. The hybrid techniques and the FTA also lead to pessimistic results compared to the MA. Authors suggested to use EMA technique due to its large coverage. EMA gives a range of values for the probability of failure on demand thus including the effects of uncertainty. The main conclusion of the calculation results is that different analysis techniques may lead to different SIL even when using the same set of data.

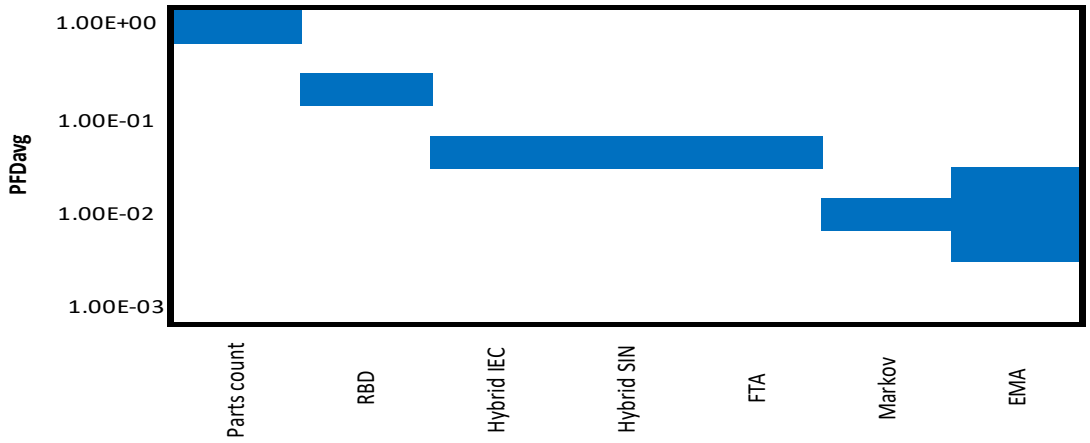


Fig. 2.15. Plotted calculation results [108].

Table 2.14. Comparison of analysis techniques [108].

	Safety ranking / comparison	Probability of dangerous failure	Availability prediction	Trip rate prediction	Effects of redundancy	Common cause failures	Systematic failures	Effect of diagnostics	Effects of on-line test and repair	Effects of off-line test and repairs	Time/sequence depended sequence aspects	Effects of uncertain data
Expert analysis	X	X	X		X	X	X	X				
FMEA	X				X		X	X				
Parts count analysis	X	X	X									
RBD	X	X	X		X	X	X					
FTA	X	X	X	X	X	X		X	X	X		
Hybrid techniques	X	X	X	X	X	X	X	X	X	X		
MA	X	X	X	X	X	X	X	X	X	X	X	
EMA	X	X	X	X	X	X	X	X	X	X	X	X

2.6 Summary and review of different selected target SIL determination and calculation method

2.6.1 Evaluation of target SIL determination methods

Risk graph method has the advantage of being less complex and cost-effective as analysts need to consider only the four risk parameters, namely; C, consequence of the hazardous event, F, frequency of, and exposure time in, the hazardous zone, P, possibility of failing to avoid the hazardous event and W, probability of the unwanted occurrence, to determine SIL [2]. Due to its qualitative nature, it is not as accurate as compared to quantitative method.

The FRGM [34] has more advantage compared with traditional methods. Comparative analysis against traditional methods was presented and FRGM showed better results. Benefit sensitivity calculation was presented with varying inputs to prove further advantage of FRGM over traditional methods. Due to its qualitative nature, it is not as accurate as compared to quantitative method. However, it is proposed to use this method in lower SILs and conduct quantitative or semi-quantitative method for higher SILs [34, 35] with caution.

The advantage of LOPA is its accuracy as the analysis encompasses different disciplines of a plant to determine if there are sufficient independent protection layers (IPLs) against an accident scenario. An IPL is a device, system or action that is capable of preventing a scenario from proceeding to its undesired consequence. The effectiveness of an IPL is quantified in terms of its probability

of failure on demand. The typical IPLs considered in the process design phase are basic process control systems (BPCSs), critical alarms and human intervention, SIFs, physical protection, and emergency response systems [32]. The risk assessment is thorough and conducted by a multi-disciplinary team (i.e., operator, engineer, manufacturing management, process control engineer, instrument/electrical maintenance person, risk analysis specialist) to determine a SIL, and thus it is accurate. The disadvantage is its practicality and complexity as the method starts with tedious data developed in the HazOp analysis and accounts for each identified hazard. Also, documenting the initiating cause and the protection layers that prevent or mitigate the hazard. The total amount of risk reduction can then be determined and the need for more risk reduction analysed, if additional risk reduction is required, and if it is to be provided in the form of a SIF [3].

Cascaded fuzzy LOPA requires construction of two models; the severity fuzzy-model and the cascaded fuzzy model to determine SIL rating. The disadvantage of this method is its complexity. The theoretical idea of using fuzzy-LOPA method to determine SIL rating has not been applied in real world application before and thus, the accuracy is not proven and tested. The advantage of this proposed method, according to simulations [37], is that the results presented comparable output obtained using the traditional LOPA. Fuzzy-based models are reliable and could be readjusted for sensitivity analysis to obtain the most accurate results.

A FMEDA is an extension of the well-proven FMEA technique, and it can be used on electrical or mechanical products. It combines standard FMEA

techniques with extensions to identify online diagnostic techniques. It is a technique recommended to generate failure rates for each important category (safe detected, safe undetected, dangerous detected, and dangerous undetected) in safety models [96]. This method is complex and not cost-effective as the hardware SIL evaluation requires an eight-step process. This process defines the components of the SIS subsystems, failure modes, and failure effects. A failure mechanism distribution and failure rate are assigned to each component, and the safety mode is determined, as well as the detectability of each failure mode. As the process is thorough, it has an advantage of being accurate.

The advantages of RBD techniques [111] are straightforward and intuitional, thus less complex and practical [39]. As a disadvantage, further study needs to be conducted to improve the accuracy of RBD and solutions to minimize the effects of common cause failures in actual applications. Another disadvantage is that RBD models do not take repairs into account, however, repairs of known failures can be carried out.

FTA techniques have advantages such as a clear graphical representation of the system. Available mathematical models for numerous modes of operation (i.e., repairable, non-repairable, and stand-by). Results can directly indicate key contributors to system unavailability. Consideration of sensitivity cases for modifications to system components, architecture, and component testing intervals. Easy conversion of system model for evaluation of nuisance trip rates. Publicly available software tools for performing FTA. For the disadvantages, FTA has the inability to address partially failed states and time-dependent failure rates, as well as the requirement for training of the analyst. FTA assumes that a device

is in only one of two states – working or failed. This does not allow for the consideration of functioning, but damaged states. Furthermore, the specific problems raised by the assessment of SIL, which restrict the use of the formula proposed in the standard was raised [40]. The focused on the periodically tested components, which according to their study [40], must be elaborated to perform realistic computations of PFD and SIL.

MA demonstrates numerous advantages in terms of flexibility and ability to describe the time-dependent PFD [42]. A comparison of different techniques shows that Markov analysis covers most aspects for quantitative safety evaluation [108]. Aspects not covered by Markov analysis are uncertainty analysis and sensitivity analysis. These aspects are included in the Enhanced Markov Analysis technique. However, as a disadvantage, similar to other studies, the size of the Markov models increases explosively as systems become complex [42].

The fuzzy probabilities based approach to evaluate the SIS PFD and the SIL [45] has the advantage of being more accurate in certain situations where there is uncertainty on reliability parameters of SIS components. This complex method uses fuzzy set theory as a new approach to evaluate the confidence level of the SIL determination when failure rates of SIS components are uncertain. Fuzzy set theory has been used in many engineering domains including risk and safety assessment wherein fuzzy numbers used by fuzzy sets exploit an uncertain quantity such as a basic event. As a disadvantage, the issues of maintenance and repair strategies into the fuzzy probabilistic approach should be

considered to perform the trade-off between the maintenance cost and the required SIL for the SIS, which makes it impractical to apply in real world cases.

Reliability model, when utilised on uncertain events can give the advantage of having more accurate results. The three-step process ensures that the new mathematical model captures the best reliability in calculation of PFD. It has the disadvantage of being complex as it involves several multifaceted steps and modelling. Its application may be implemented on higher SILs to realise its cost-effectiveness.

The advantage of Switching Markov [62] chain approach is that it can be utilised to a more complex safety system, with cumbersome analysis as a downside. The method is more applicable for use in systems with repairable components at constant failure and restoration rates [63, 64]. The influence of several parameters on the performance of SIS, such as common cause failure (CCF), imperfect and partial proof testing was considered in the model, making the method accurate in this regard.

The 3-Parameter SPW [65] technique is based on the Risk Graph method and has an inherent advantage of being non-complex, cost-effective and flexible. It is simple to use and can be used as full qualitative or semi-qualitative yielding the same results. However, as a disadvantage, the problem with removing the *exposure* parameter is that the result may not be more reflective of the risk assessment of the actual process hazard condition. Furthermore, as shown in the example [65], upon analysing the comparative results of SPW, it appears that there was discrepancies. The conventional Risk Graph method resulted in SIL3 while the SPW method resulted in SIL2 (0.015). These contradicting results cast

doubts in utilising this method as safety of personnel, damage to property and the environment is at stake.

MDBN is a novel method which has an advantage of being accurate as it can uncover covert failures that can cause dangerous failures, which cannot be detected using normal diagnostic methods. Proof test interval phase and proof test phase are modelled separately using DBN and integrated to form the MDBN [66]. Aside from being complex, the disadvantage of this approach is that the presented determination methodology can only be used in a low demand mode.

Based on the criteria of complexity, accuracy and cost-effectiveness, **Table 2.15** shows the comparison among methods. Note that these ratings were purely based on the authors' perspective. Complexity can be defined as the difficulty of use of the particular method in a real-world application. The more stars, the less complex.

Table 2.15. Comparison of selected target SIL determination methods.

Selected target SIL determination methods	Complexity	Accuracy	Practicality /Cost-effective
Risk graph	*****	**	****
FRGM	*****	****	*****
LOPA	**	*****	**
Cascaded fuzzy- LOPA	*	**	**
FMEDA	***	*****	***
RBD	***	*	***
FTA	***	*****	***
MA/EMA	*	****	**
Fuzzy probabilistic	**	****	**
Reliability model	*	****	**
Switching Markov Chain	**	****	***
3-Parameters SPW technique	*****	*	*****
MDBN	**	****	**

*****more stars preferred

Accuracy is the precision of results obtained, mainly derived from complex inputs and various considerations. The more stars, the more accurate. Cost-

effectiveness can be deduced from the time spent in evaluation of SIFs, i.e., the cost of qualified engineers/analysts/operators to do SIL evaluation. The more stars, the more cost-effective.

2.6.2 Evaluation of SIL calculation methods

The SE technique has its advantage of being straightforward in determining the PFDavg for the Subsystems: sensor (FS), logic solver (LS) and final element (FE). Once the individual PFDs for each input, logic solver, output and support system are known, these PFDs are simply summed for the PFD_{SIS} as shown in Eq (2.7);

$$PFD_{SIS} = \Sigma PFD_{FS} + \Sigma PFD_{LS} + \Sigma PFD_{FE} + \Sigma PFD_{SS} \quad (2.7)$$

Since the SE used for calculating the PFDavg were initially derived from Markov models, unfortunately, the simplification of the models resulted in some limitations. Furthermore, unlike Markov models, this method does not handle time dependent failures or sequence dependent failures as one of its disadvantages. Moreover, due to these limitations, this method should not be used to analyze programmable logic solvers.

Hybrid model [89] is a combination of RBD and Markov model. It is a tandem of dynamic state space based continuous time Markov chains (CTMC) model and system level static RBD-formalism approach. The main advantage is that the hybrid model easily allows detection of the measurement front-end as the main factor to system unavailability. However, due to inherent characteristics of the Markov model, it has major drawbacks in terms of complexity and cost-

effectiveness. These dynamic models is the exponential growth of the state space as a function of the number of components, known as the state space explosion [43, 103, 104]. The construction of models for complex systems vary rapidly becomes difficult and prone to errors. Moreover, the probability of operator error was not considered in the simulation thus, the current hybrid model does not allow optimization of the test interval sacrificing its accuracy.

MCS [90] method provides professional tool for SIL verification in complex safety systems, as an advantage. Disadvantages are that systems with static components (i.e., components in which the reliability does not change with time) cannot be simulated. With this characteristic, most of the reliability optimization and allocation techniques cannot be applied.

Stochastic Petri net with predicates advantage is its extended computational power making it accurate in complex systems. Moreover, another advantage of these Petri nets is their ability to perform modular models. On the downside, Petri net models, even for simple systems, are quite complex to design and to maintain. That is the reason why Fault Tree models are preferable between the two.

Based on the criteria of complexity, accuracy and cost-effectiveness, **Table 2.16** shows the comparison among different methods. Complexity can be defined as the difficulty of use of the particular method in a real-world application. The more stars, the less complex. Accuracy is the precision of results obtained, mainly derived from complex inputs and various considerations. The more stars, the more accurate. Cost-effectiveness can be deduced from the time spent in

evaluation of SIFs, i.e., the cost of qualified engineers/analysts/operators to do SIL evaluation. The more stars, the more cost-effective.

Table 2.16. Comparison of selected SIL calculation methods.

Selected Calculation Methods	Complexity	Accuracy	Practicality/Cost-effective
SE	*****	*	****
FTA	***	*****	***
RBD	***	*	***
MA	*	****	**
FMEA	****	*****	***
Hybrid	*	***	*
MCS	**	***	**
Stochastic Petri nets	*	****	**

*****more stars preferred

2.7 Discussion and Conclusion

This Chapter has reviewed and summarised various selected target SIL determination and calculation methodologies. A comparison of different methods has been presented using well-defined criteria. This Chapter compared advantages and disadvantages of reviewed methods from complexity, accuracy and cost-effectiveness perspectives. The risk graph method has gained wide attention due to its simplicity and easy-to-use features [33-35, 65]. Based on simulations presented in this Chapter using the risk graph-based FRGM and comparing to other traditional methods such as LOPA, the FRGM yields more advantages in terms of cost-reduction and ease of use. Therefore, the FRGM can be proposed to be used as a funnel to determine lower SIL rating and practice more rigor at higher SIL.

These inherent characteristics of the risk graph method of being coarser and less accurate are not much of a concern as it is proposed to be used as a filter

only from a broad range of lower SILs. A lot of resources can be saved utilising this approach [34, 35] as discussed in this work. For higher SILs, which requires greater degree of functional safety, extra care must be exercised, and more accurate method must be employed. Careful calibration against the company's risk matrix must be conducted to ensure the accuracy of the FRGM.

Chapter 3 - Development of the Funnel Risk Graph Method (FRGM)

3.1 Introduction

The international standard IEC 61508 [2] addresses the requirements for safety related systems based on electrical, electronic and programmable electronic technology. This is a generic document, non-specific to any industry and relevant to a wide range of different sectors. The international standard IEC 61511 [3] was created as a derivation of IEC 61508 [2] to cover specifically the process industry. The standard ISA-TR84.00.01 [112] later adopted the standard IEC 61511 [3] in its entirety with some minimal modifications. Therein, any reference to IEC 61511 [3] is equivalent to ISA-TR84.00.01 [112] and vice versa.

The SIS of a SIF is independent from the plant control functions performed by the Basic Process Control System (BPCS). A SIF is a safety protective function implemented by a SIS, and composed of any combination of sensors, logic solver and final elements (e.g. valves). A SIF must achieve a specific level of integrity, represented by the SIL. Per IEC 61511 [3], definition of any SIFs must be based on a previous risk assessment. The risk assessment would determine the current level of risk presented by the facility. This would be compared against a tolerable risk level. The gap between the actual risk level and the tolerable risk is the required level of risk reduction as shown in **Figure 3.1,** also called the Risk Reduction Factor (RRF). The RRF is the relation of the actual risk presented by

the facility and the risk that must be achieved as a target based on the acceptance criteria: RRF = Actual Risk / Tolerable Target Risk.

An important consideration is that the tolerable risk level to be used as baseline for risk assessment must be set by each individual organization specific to each process or facility as their Corporate Risk Criteria.

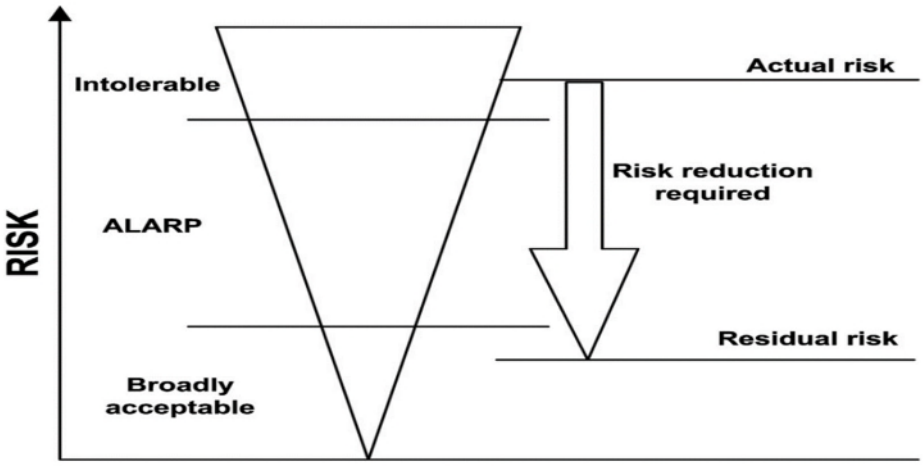
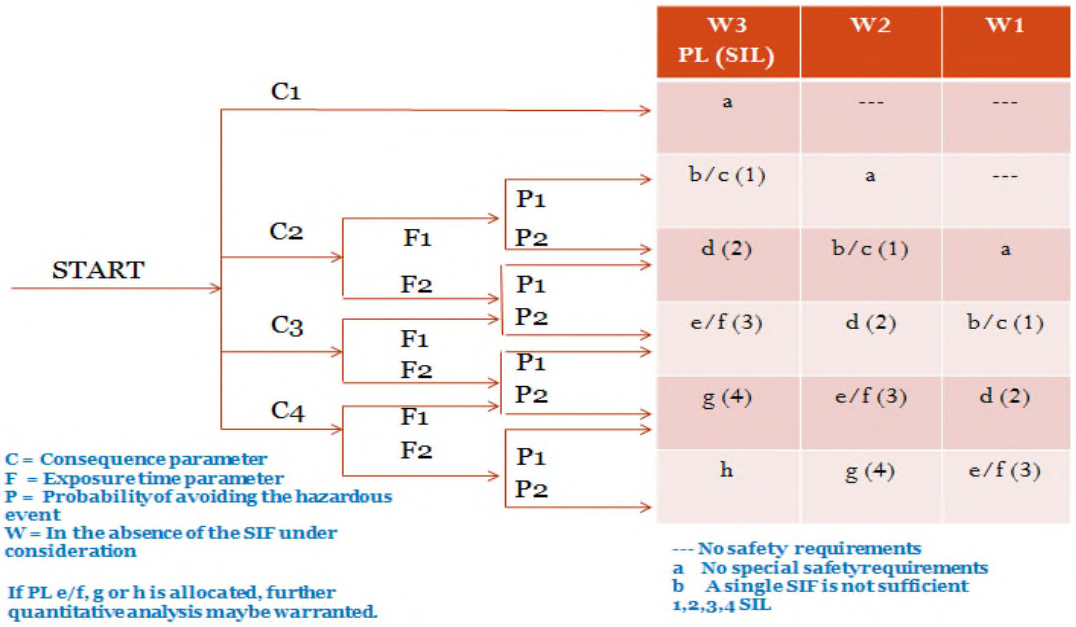


Fig. 3.1. Risk reduction factor concept.

As defined in IEC 61511 [3], SIL is a widely used safety performance measure for SIF. The standard IEC 61511 [3] suggests several methods for SIL determination, ranging from fully quantitative methods to fully qualitative methods. The use of multi-disciplinary-team collaboration is required to evaluate large number of safety functions during plant design and the need to integrate multidisciplinary design and operation knowledge to achieve effective risk reduction. There are different methods to determine and verify SIL [2, 3, 6, 28-34, 37, 39-42, 48, 58, 65, 66, 79, 83, 85, 87, 88, 90, 94, 108, 109, 113, 114]. Two widely used methods in the Oil & Gas industry for SIL determination are Risk Graphs and Layer of Protection Analysis (LOPA) [33]. Each of these methods has their own advantages and disadvantages. The simplicity and cost-effectiveness of Risk Graphs makes them convenient for screening a large

number of safety functions, specifically for lower SILs. Risk Graphs are still widely used as a stand-alone method. This can make Risk Graphs useful as a first screening pass prior to using LOPA. LOPA allows the required risk reduction to be incorporated into the SIL values with higher precision. This enables a more detailed consideration of the available protection layers and leaves an objective traceable record of the decision-making process.

Although Risk Graphs method can provide the same level of SIL determination rigor as LOPA [34, 35], one must exercise extra precaution in evaluating higher SILs. Thus, we introduce the Funnel Risk Graph Method (FRGM) in this chapter, and its development as shown in **Figure 3.2**. Furthermore, this chapter will also explore the cost-effectiveness and simplicity of the risk graph-based FRGM; the results were verified to show that it does not sacrifice its accuracy.



W3 PL (SIL)	W2	W1
a	---	---
b/c (1)	a	---
d (2)	b/c (1)	a
e/f (3)	d (2)	b/c (1)
g (4)	e/f (3)	d (2)
h	g (4)	e/f (3)

Fig. 3.2. Funnel Risk Graph Method [34]

The FRGM is a SIL assessment methodology based on Risk Graphs qualitative approach in reference to functional safety standards [2]. Traditionally, in designing SIS, all SIF, depending on the designers' preference, must undergo quantitative, semi-quantitative or qualitative analyses consuming a lot of resources.

Section 3.2 deals with the relationship between the safety lifecycle and the FRGM. Section 3.3 shows the equivalence of SIL, PL and CAT. Section 3.4 discusses the calibration of the FRGM approach. Section 3.5 discusses the application of FRGM to case study involving 3 SIFs while Section 3.6, using LOPA. Section 3.7 compares the FRGM and other traditional methods. Finally, Section 3.8 concludes the Chapter.

3.2 Safety Lifecycle and the FRGM

The 16 phase IEC 61508 [2] safety lifecycle with the inclusion of IE C62061 [23], IEC 61511 [3], ISO 13849 [24] and AS 4024.1 [25] as a combined safety lifecycle process [10] aims to establish safety requirements for plant, considering the specific circumstances and risks (e.g., environmental, operational, etc.) associated with its use and maintenance until the end of the life of the plant.

Table 3.1 shows the phases of the safety lifecycle that should be driven by the end-user to ensure that the safety requirements are appropriate for the specific application. Phases 6-7 and 13-16 are phases of the safety lifecycle should be driven by the end-user to ensure that the safety requirements are adequately implemented and maintained. Phases 8-12 are responsibilities that may be assigned to other organisation, however, it remains the end-user's

responsibility to ensure that the other organisation complies with the requirements of those phases:

Table 3.1. – Phases of the safety lifecycle

Phase Sequence	Phase Description
1	Concept
2	Scope
3	Hazard and Risk Analysis
4	Overall Safety Requirements
5	Safety Requirements Allocation
9	Safety Requirements Specification
6	Operation and Maintenance Planning
7	Safety Validation Planning
13	Safety Validation
14	Operations and Maintenance
15	Modification and Retrofit
16	Decommissioning
8	Installation and Commissioning Planning
10	E/E/PE Safety-related Systems Realisation
11	Other Risk Reduction Measures Specification and Realisation
12	Installation and Commissioning

The proposed method focuses on *Phase 5: Safety Requirements Allocation* using the FRGM as shown in **Figure 3.2**, which was based on IEC 61508 [2] in reference to the general scheme described in IEC 61511 [3] but characterized as a "*funnel*" approach. Typically, a medium-sized plant is comprised of thousands of Safety Instrumented Functions (SIF). Instead of subjecting all SIF one-by-one to a much complex (semi-quantitative or quantitative) assessment process, the FRGM (qualitative) is aimed to use as a funnel or an "*initial pass*". If the assessed safety-related systems received SIL allocation of greater than SIL2 (or greater than SIL1, depending on company risk profile) during the "*initial pass*" then a semi-quantitative or a quantitative method as a "*final pass*" should be conducted, or the multi-disciplinary assessment team reached an agreement to justify the

“second pass”, or pose a high EUC risk. Doing so would mean significant savings in resources as presented later in this Chapter.

The responsibility for performing a SIL/PL allocation should not be passed off to the designers as they may not have sufficient specific information to do this. The multi-disciplinary site personnel should perform a risk assessment based on their specific application of the EUC, determine the safety functions and SIL/PL on the basis of their notion of ‘tolerable risk’, and then communicate this to the designer through Safety Requirements Specifications (SRS). This methodology utilizes several parameters. It illustrates the level of the hazardous situation in the event that the SIS fails or become unavailable.

3.3 The Equivalence of SIL and PL

Table 3.2 shows the corresponding equivalence between the ISO 13849 [24] Performance Level (PL a, b, c, d and e) and IEC 61508 [2] / IEC 62061 [23] Safety Integrity Levels (SIL 1, 2 and 3) that has been depicted in issues of ISO 13849-1, since 2006 [10]. The PL concept is used to describe five (5) classes of safety integrity – PLa, b, c, d and e. PLa describes the lowest level of safety integrity and PLe describes the highest. The PL concept only takes account of ‘high’ and ‘continuous’ demand modes of operation of safety-related systems. The Probability of Dangerous Failure Per Hour (PFH) is a measure of safety integrity for ‘high’ and ‘continuous’ demand safety functions. The maximum PFH’s allowable for each SIL are also described in **Table 3.2.**

3.4 The Equivalence of SIL and CAT

The Safeguarding Category (CAT) concept is used to describe five (5) classes of safety integrity – CATB, 1, 2, 3 and 4. CATB describes the lowest level of safety integrity and CAT4 describes the highest. The CAT concept does not classify the demand modes of operation of safety-related systems. Unlike SILs and PLs, CATs do not have numerical probability of failure targets.

Table 3.2. – Equivalence of PL's and SIL's

Performance Level (PL) ISO 13849	Probability of Dangerous Failure per Hour (PFH)	Equivalent Safety Integrity Level (SIL) IEC 61508 / IEC 61511
a	$10^{-5} \leq PFH < 10^{-4}$	No SIL (or <SIL1)
b	$3x10^{-6} \leq PFH < 10^{-5}$	SIL 1
c	$10^{-6} \leq PFH < 3x10^{-6}$	SIL 1
d	$10^{-7} \leq PFH < 10^{-6}$	SIL 2
e	$10^{-8} \leq PFH < 10^{-7}$	SIL 3

However, CATs are defined by qualitative requirements on system architecture and fault behaviour. The detailed requirements are listed in AS 4024.1501 [115] Clause 7 and are summarised as follows:

- **CATB**: The safety-related parts shall be designed, constructed, selected, assembled and combined in accordance with relevant standards, using 'basic safety principles'[2] [116].

[2] 'Basic safety principles', 'well-tried components' and 'well-tried safety principles' are defined in AS 4024.1502 Appendices A to D.

- **CAT1**: The requirements of CATB and, the safety-related parts shall be designed and constructed using ‘well-tried components’ and ‘well-tried safety principles’.
- **CAT2**: The requirements of CATB, the use of ‘well-tried safety principles’ and, the safety function shall be checked at suitable intervals by the control system.
- **CAT3**: The safety-related parts shall be designed so that a single fault does not lead to loss of the safety function. Where reasonably practicable single faults shall be detected at, or before, the next demand on the safety function.
- **CAT4**: The safety-related parts shall be designed so that a single fault does not lead to loss of the safety function. Single faults shall be detected at or before the next demand on the safety function.

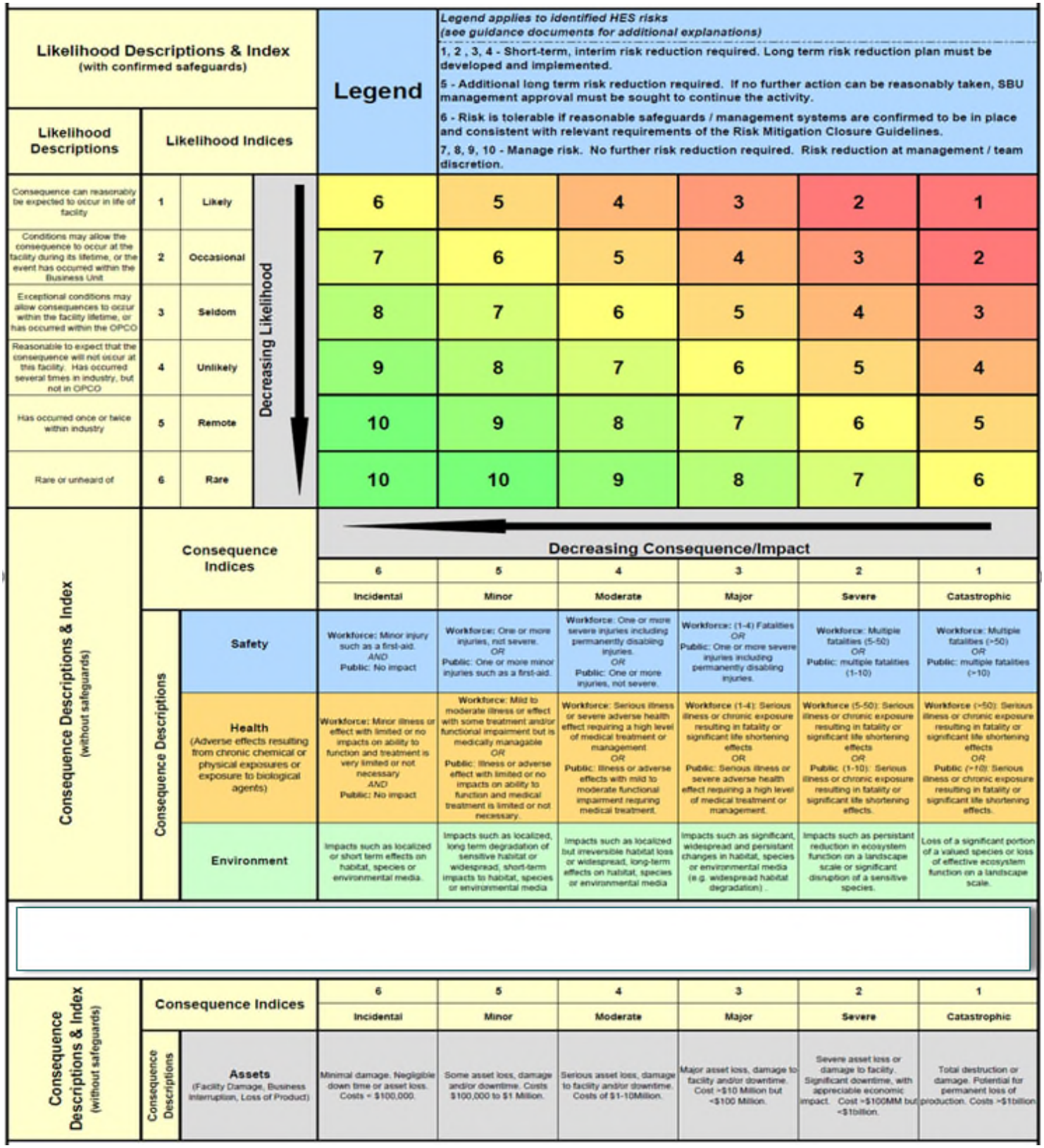
Table 3.3 shows the equivalence between the AS 4024.1 [25] machinery safeguarding categories (CATB, 1 2, 3 and 4) and IEC 61508 [2] / IEC 62061 [23] SIL [2, 10] (SIL 1, 2 and 3).

Table 3.3. – Equivalence of SIL’s and CAT’s

Category (CAT) AS4024	Hardware Fault Tolerance (HWFT)	Safety Failure (SFF)	Maximum SIL Claim Limit according to the architectural constraints IEC 61508/ IEC 61511
1	0	SFF< 60%	No SIL (or <SIL1)
2	0	60%≤ SFF < 90%	SIL 1
3	1	SFF< 60%	SIL 1
	1	60%≤ SFF < 90%	SIL 2
4	>1	60%≤ SFF < 90%	SIL 3
	1	SFF ≥90%	SIL 3

3.5 Calibration of the FRGM

Calibration process of the FRGM is essential. Primarily, the purpose of calibration is to align the SIL chosen within the bounds of corporate risks. An example of corporate risk matrix is shown in **Figure 3.3**. Calibration also considers other risks' sources, for verification purposes and to describe the parameters in the light of corporate context. Decision makers in the organization are responsible for allocating quantifiable values to risk graph parameters. It is the discretion of the management how they classify the risk parameters according to what their experts believe. Different organization foresees risk differently but in general, there are many forms of commonality among them. **Table 3.4** is an example of calibration for chemical processes. For the case study in this Chapter, the calibration of the FRGM against the corporate matrix is shown in **Table 3.5**. It was collaboratively decided that for Consequence C1 represents minor injury, C2 for serious injury, C3 for permanent disability or one fatality and C4 for multiple fatalities. For Exposure Parameter (F), the F1 represents rare to frequent exposure while F2 denotes permanent exposure or almost permanent exposure. For Avoidance Parameter (P), P1 signifies that the avoidance is possible under certain conditions while for P2, avoidance is impossible or almost impossible. Finally, for the Demand Parameter (W), there are three categories; W3, the function is demanded more than once per year, W2, the function is demanded less than once per year but more than once per 10 years and W1, the function is demanded less than once per 10 years. For our case study utilising 3 SIFs, they all have high demand, which is W3 because it is a conveyor safety system that requires safety function to be demanded more than once per year.



Likelihood Descriptions & Index (with confirmed safeguards)			Legend	Legend applies to identified HES risks (see guidance documents for additional explanations)
				1, 2, 3, 4 - Short-term, interim risk reduction required. Long term risk reduction plan must be developed and implemented.
				5 - Additional long term risk reduction required. If no further action can be reasonably taken, SBU management approval must be sought to continue the activity.
				6 - Risk is tolerable if reasonable safeguards / management systems are confirmed to be in place and consistent with relevant requirements of the Risk Mitigation Closure Guidelines.
				7, 8, 9, 10 - Manage risk. No further risk reduction required. Risk reduction at management / team discretion.

Likelihood Descriptions	Likelihood Indices		Decreasing Likelihood						
Consequence can reasonably be expected to occur in life of facility	1	Likely		6	5	4	3	2	1
Conditions may allow the consequence to occur at the facility during its lifetime, or the event has occurred within the Business Unit	2	Occasional		7	6	5	4	3	2
Exceptional conditions may allow consequences to occur within the facility lifetime, or has occurred within the OPCO	3	Seldom		8	7	6	5	4	3
Reasonable to expect that the consequence will not occur at this facility. Has occurred several times in industry, but not in OPCO	4	Unlikely		9	8	7	6	5	4
Has occurred once or twice within industry	5	Remote		10	9	8	7	6	5
Rare or unheard of	6	Rare		10	10	9	8	7	6

Consequence Descriptions & Index (without safeguards)			Consequence Indices	Decreasing Consequence/Impact					
				6	5	4	3	2	1
				Incidental	Minor	Moderate	Major	Severe	Catastrophic
	Consequence Descriptions	Safety		Workforce: Minor injury such as a first-aid. AND Public: No impact	Workforce: One or more injuries, not severe. OR Public: One or more minor injuries such as a first-aid.	Workforce: One or more severe injuries including permanently disabling injuries. OR Public: One or more injuries, not severe.	Workforce: (1-4) Fatalities OR Public: One or more severe injuries including permanently disabling injuries.	Workforce: Multiple fatalities (5-50) OR Public: multiple fatalities (1-10)	Workforce: Multiple fatalities (>50) OR Public: multiple fatalities (>10)
		Health (Adverse effects resulting from chronic chemical or physical exposures or exposure to biological agents)		Workforce: Minor illness or effect with limited or no impacts on ability to function and treatment is very limited or not necessary AND Public: No impact	Workforce: Mild to moderate illness or effect with some treatment and/or functional impairment but is medically managable OR Public: Illness or adverse effect with limited or no impacts on ability to function and medical treatment is limited or not necessary.	Workforce: Serious illness or severe adverse health effect requiring a high level of medical treatment or management OR Public: Illness or adverse effects with mild to moderate functional impairment requring medical treatment.	Workforce (1-4): Serious illness or chronic exposure resulting in fatality or significant life shortening effects OR Public: Serious illness or severe adverse health effect requiring a high level of medical treatment or management.	Workforce (5-50): Serious illness or chronic exposure resulting in fatality or significant life shortening effects OR Public (1-10): Serious illness or chronic exposure resulting in fatality or significant life shortening effects.	Workforce (>50): Serious illness or chronic exposure resulting in fatality or significant life shortening effects OR Public (>10): Serious illness or chronic exposure resulting in fatality or significant life shortening effects.
		Environment		Impacts such as localized or short term effects on habitat, species or environmental media.	Impacts such as localized, long term degradation of sensitive habitat or widespread, short-term impacts to habitat, species or environmental media	Impacts such as localized but irreversible habitat loss or widespread, long-term effects on habitat, species or environmental media	Impacts such as significant, widespread and persistant changes in habitat, species or environmental media (e.g. widespread habitat degradation) .	Impacts such as persistant reduction in ecosystem function on a landscape scale or significant disruption of a sensitive species.	Loss of a significant portion of a valued species or loss of effective ecosystem function on a landscape scale.

Consequence Descriptions & Index (without safeguards)			Consequence Indices	6	5	4	3	2	1
				Incidental	Minor	Moderate	Major	Severe	Catastrophic
	Consequence Descriptions	Assets (Facility Damage, Business Interruption, Loss of Product)		Minimal damage. Negligible down time or asset loss. Costs < $100,000.	Some asset loss, damage and/or downtime. Costs $100,000 to $1 Million.	Serious asset loss, damage to facility and/or downtime. Costs of $1-10Million.	Major asset loss, damage to facility and/or downtime. Cost >$10 Million but <$100 Million.	Severe asset loss or damage to facility. Significant downtime, with appreciable economic impact. Cost >$100MM but <$1billion.	Total destruction or damage. Potential for permanent loss of production. Costs >$1billion

Fig. 3.3. Example of corporate risk matrix.

Table 3.4. – Typical Pattern of Calibration using the FRGM

Risk Parameter		Classification
Consequence (C) Total number of fatalities. Can be quantified by counting the number of people exposed multiply by the Vulnerability factor. Vulnerability factor is determined by the nature of the hazard being protected against. V = 0.01 Toxic or flammable material in small amount of release. V = 0.1 Toxic or flammable material in large amount of release. V = 0.5 Toxic or flammable material in large amount of release but also a high probability of potential fire or highly toxic material. V = 1 Explosion or rupture.	C_A C_B C_C C_D	Minor injury Range 0.01 to 0.1 Range > 0.1 to 1.0 Range > 1.0
Occupancy (F) Calculated by the length of time exposed to hazard during the normal working hour.	F_A F_B	Use F_A if the exposure to the hazardous environment is infrequent to more frequent. Usually it is considered less than 0.1 occupancy Use F_B if the exposure to the hazardous environment is frequent to permanent.
Probability (P) Pertains to the chance of preventing the hazardous situation in the event that the protection system stops to operate.	P_A P_B	Use P_A if all conditions in column 4 are met. Use P_B if all the conditions stated are not met.
Demand rate (W) Is the rate that the hazardous situation would happen without considering the presence of the SIF. All sources of failure should be considered in identifying the demand rate (W)	W_1 W_2 W_3	Use W_1 if W (Demand rate) is less than 0.1 D/year. Use W_2 if W (Demand rate) is between 0.1D and D/year. Use W_3 if W (Demand rate) is between D and 10D/year. If W (Demand rate) is greater than 10D/ year then higher integrity is required.

Table 3.5. – Calibration of FRGM

C (Consequence) Parameter	Description
C1	Minor injury (non-permanent)
C2	Serious injury (non-permanent)
C3	Permanent disability or fatality
C4	Multiple fatalities
F (Exposure) Parameter	**Description**
F1	Rare to frequent exposure
F2	Permanent exposure or almost permanent exposure
P (Avoidance) Parameter	**Description**
P1	Avoidance is possible under certain conditions (e.g., independent facilities are provided to alert exposed persons, independent facilities are provided to shutdown the plant, danger is easily recognised and there is sufficient time for persons to escape the hazard, or actual safety experience indicates that avoidance is possible)
P2	Avoidance is not possible or is almost impossible
W (Demand) Parameter	**Description**
W3	Function is demanded more than once per year
W2	Function is demanded less than once per year but more than once per 10 years
W1	Function is demanded less than once per 10 years.

3.6 Application of FRGM to case study involving 3 SIFs

In order to show the simplicity and effectiveness of the FRGM approach, an example of a process system involving a conveyor safety system with three SIFs is presented in block diagram **Figure 3.4.**

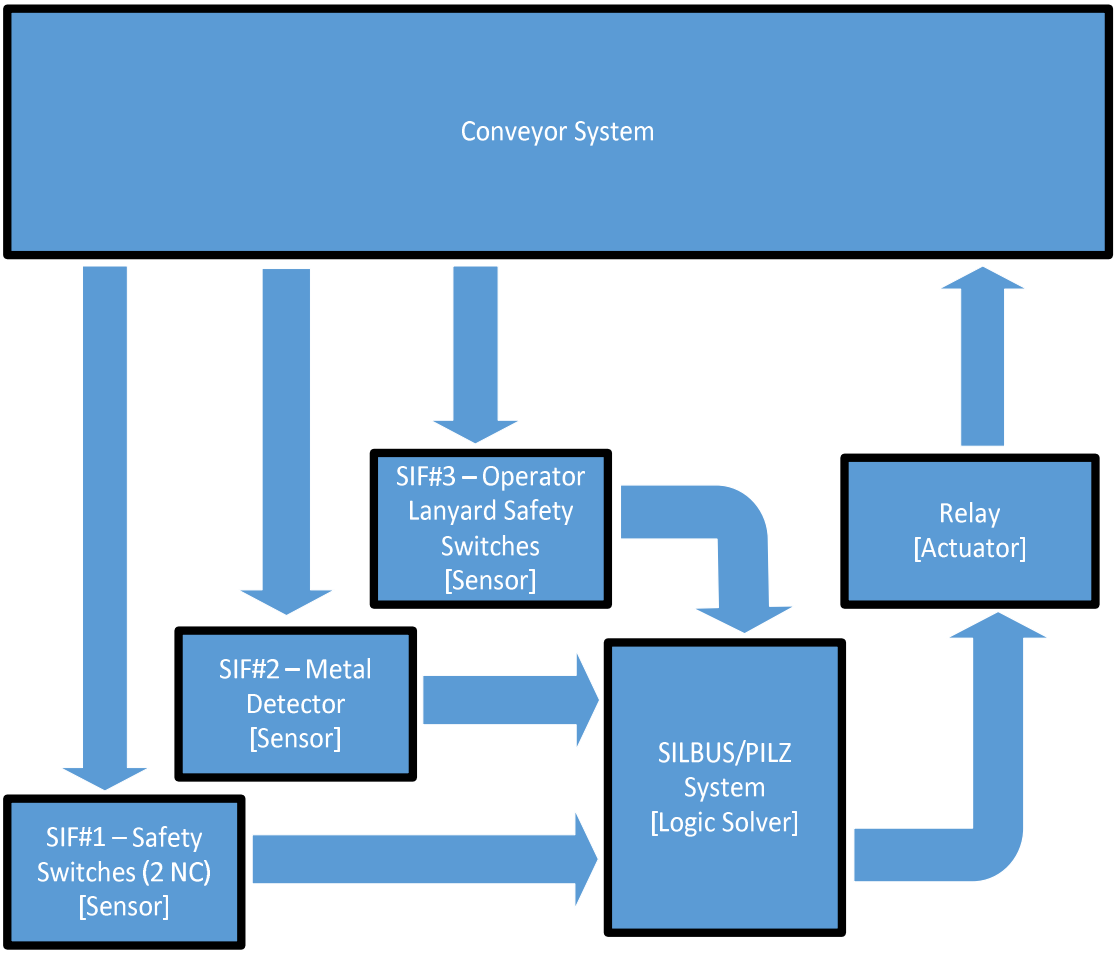


Fig. 3.4. Block Diagram of Conveyor Safety System

3.6.1 SIF#1 (A100), SIF#2 (M100) and SIF#3 (A200) analyses

The process involves transporting and handling of solids through a conveyor belt. All SIF is designed to disable any movement of the conveyor belt and its associated equipment during emergency or metal detection. Failure to do so may lead to fatalities, injuries or equipment damage.

SIF#1 (A100) as shown in **Figure 3.5** is a **C112 conveyor belt gate** interlock safety system, which comprised of two identical switches. When

activated during emergency, the actuator (plastic slide plate) needs to press the limit switches, which in turn will activate the emergency stop. Emergency situations e.g., operator caught in between, conveyor belt failures, etc. SIF#1 should be activated (pulled). Another function of this SIF is to enable safe cleaning operations of metal particles by unwanted conveyor belt movement. Obviously, failure of this SIF may lead to fatalities, injuries and/or equipment damage. The safety switch activation is done via pulling the trip cable or from a broken trip cable i.e., total loss of tension on it. The two Normally-Close (NC) switches in SIF#1 (A100) are connected in series; opening of the contacts of any of the two switches will activate the SILBUS/PILZ relay system [117] and trips the conveyor as shown in schematic diagram in **Figure 3.6.** A beacon light is also connected to indicate switch activation as shown in **Figure 3.5.**

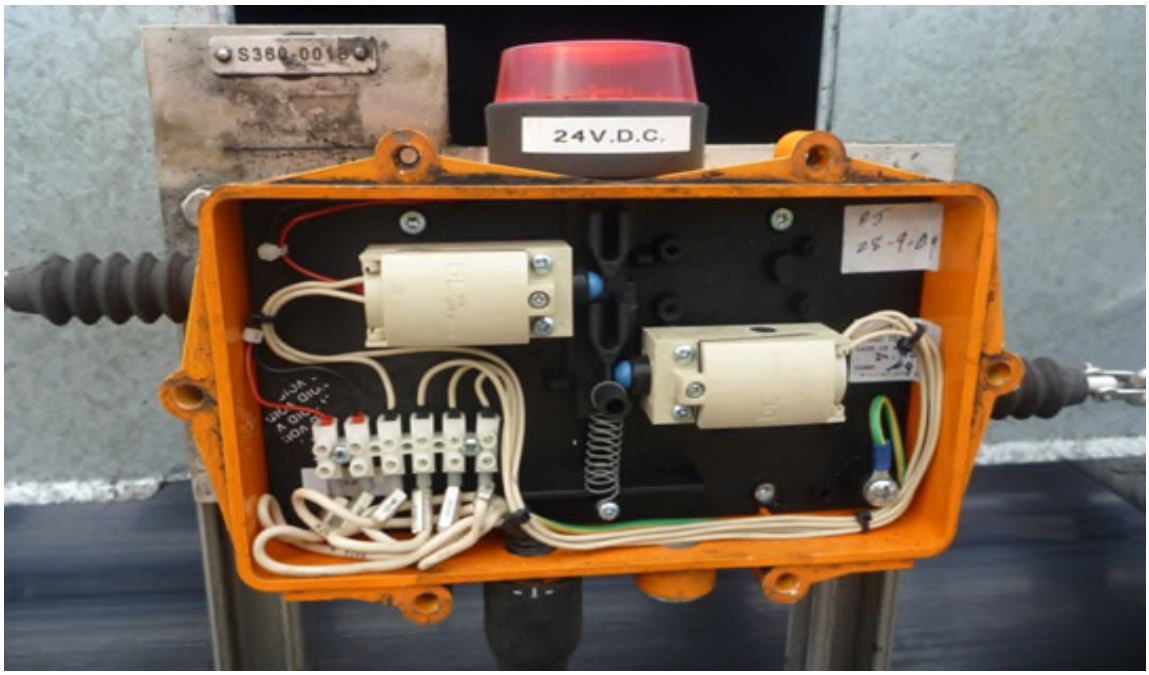


Fig. 3.5. SIF#1 (A100) - Safety Switches

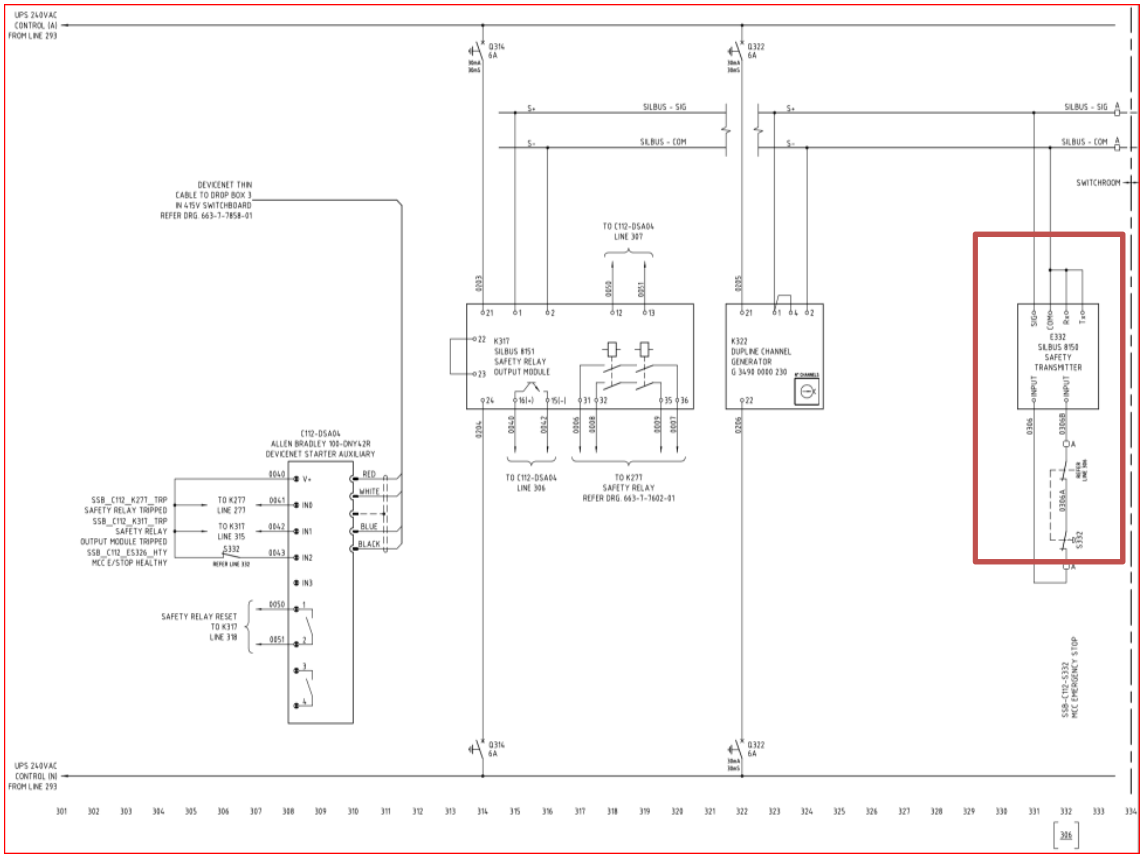


Fig. 3.6. SIF#1 (A100) – Schematic Diagram showing SILBUS transmitter

SIF#2 (M100) as depicted in **Figure 3.7**, is **metal detector** device that is used to sense any unwanted presence of metal in the conveyor belt and eventually disable conveyor movement. Metal detectors are used to detect tramp metal pieces from the raw material coming on the conveyor belt. Metal detectors are used to prevent damage to the processing machinery like crushers, cutting machines, cutters, mills, rollers, saws, presses, chippers and other processing machinery. Metal detectors are almost required in the plants like cement, sand and gravel, plastics, wood and timber, tobacco, tea, clay, chemicals. Typically, in a normal operating conveyor system, there are unwanted metals that goes with the raw material e.g., coal, minerals, etc. These unwanted magnetic particles like metal cans, bolts, pieces of loose metals, can damage the conveyor system. Thus,

metal detectors are necessary to prevent damage to the equipment. **Figure 3.7** shows an example [118] of metal detector as SIF#2 (M100).

Fig. 3.7. SIF#2 (M100) – Metal Detector [118]

SIF#3 (A200) is **operator lanyard** safety switches, which have similar function to SIF#1 (A100). However, the difference is that the risk is located near

the operator station, where permanent exposure or almost permanent exposure is evident. **Figure 3.8** shows an example [119] of metal detector as SIF#3 (A200).

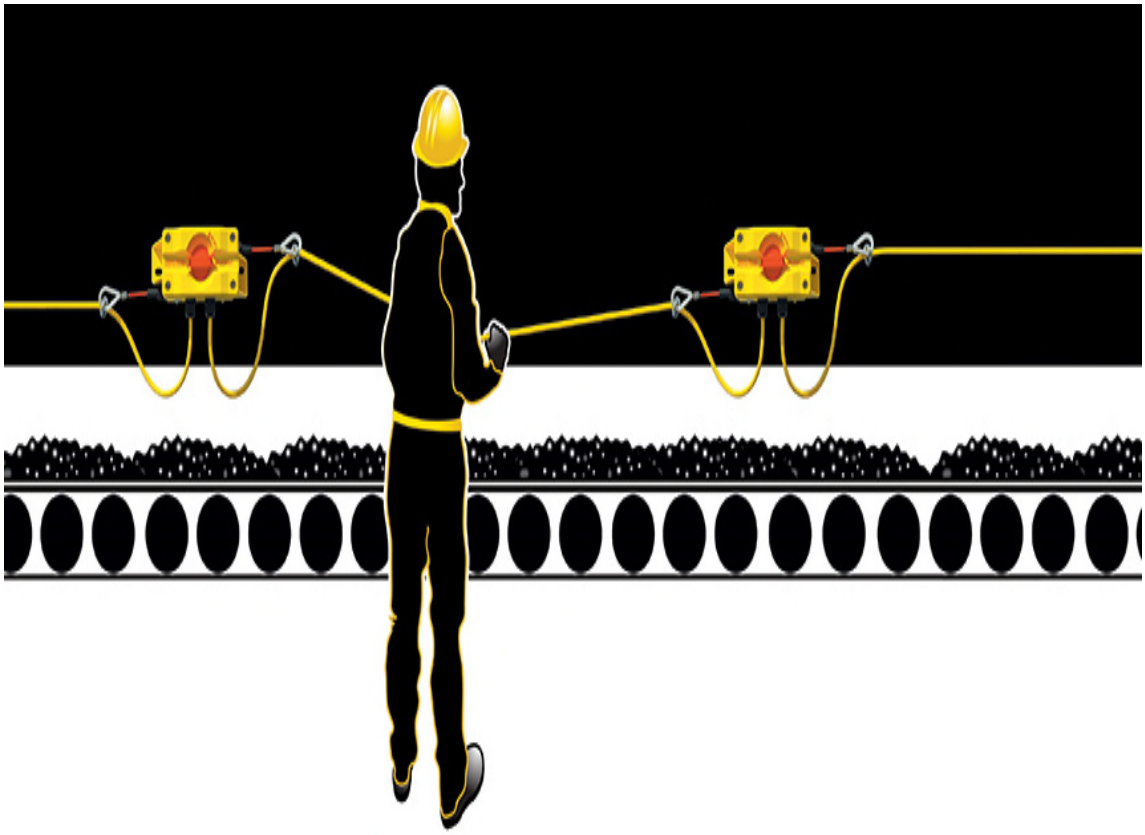


Fig. 3.8. SIF#3 (A200) - Safety Switches [119]

The FRGM process starts from the collaborative risk assessment [2] conducted by a team of multi-disciplinary personnel, which was composed of process control engineer, process specialist, safety specialist, control room and field operators. During the collaborative risk assessment, the company risk matrix was calibrated against the FRGM. Calibration is a must, primarily to align the SIL chosen within the bounds of corporate risks. Calibration also covers other sources of risks, for verification purposes and to describe the parameters within the confines of corporate environment.

Figure 3.5 above, shows the photo of the safety switch - SIF#1 (A100) and was evaluated using the proposed FRGM. **Figure 3.9** shows the step procedure for conducting the FRGM to SIF#1 (A100). The FRGM serves as an "*initial pass*" before going into a much complex assessment process, if required.

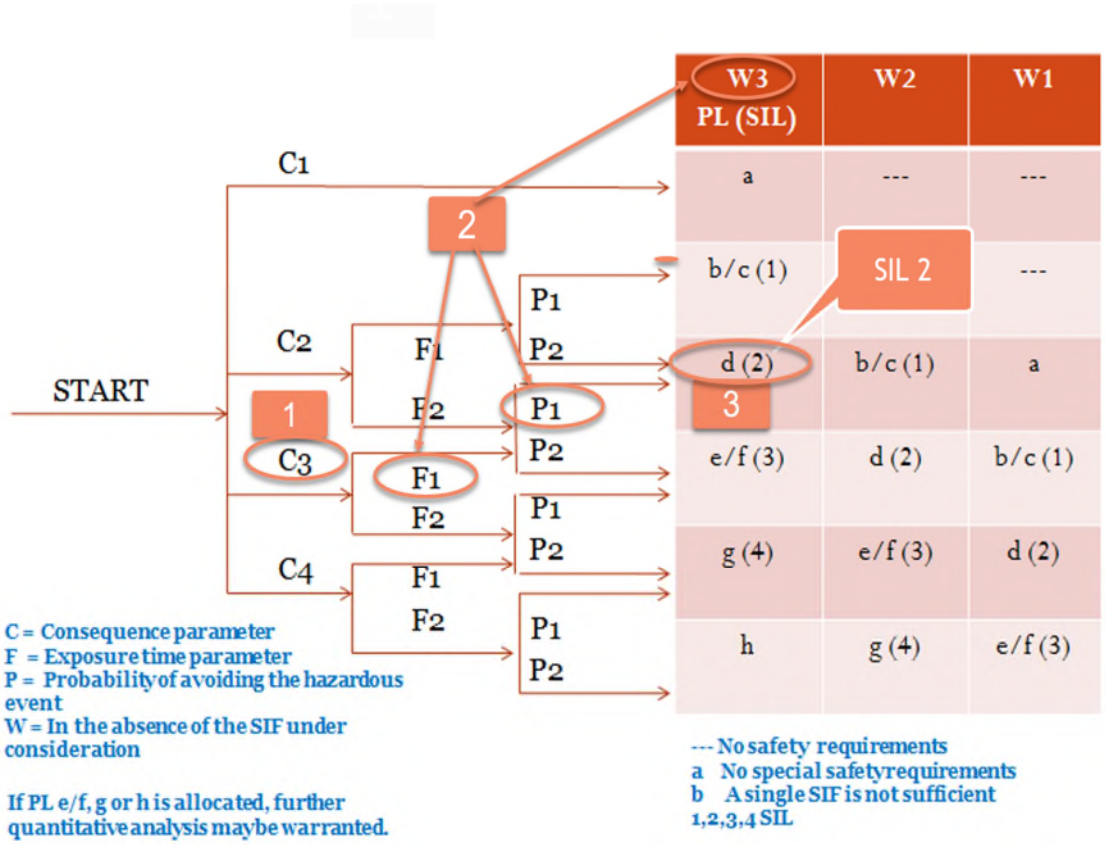


Fig. 3.9. FRGM straightforward steps using SIF#1 (A100) – SIL 2

For **SIF#1 (A100) C112 conveyor belt gate**, these are the simple steps to conduct FRGM:

Step 1: Select one parameter (Consequence C3 parameter was selected as shown in **Figure 3.9**). C3 – permanent disability or fatality;

Step 2: Chosen parameters are then linked to other parameters (Exposure F1, Probability P1, and Demand W3 as shown in **Figure 3.9**). F1 – rare to frequent exposure, P1 – avoidance is possible under certain conditions, W3 – function is demanded more than once per year;

Step 3: Resolve the SIL allocated to the SIF as shown in **Figure 3.9**.

In this case, it was easily evaluated that the SIL for SIF#1 (A100) is **SIL 2** as shown in **Figure 3.9**. Since this is only SIL 2, it can be used as the assessed SIL. As the calibration of FRGM dictates that the result from SIL2 and below can be used as the assess SIL then it can be used as the determined required (target) SIL. However, if the assessed safety-related system received SIL allocation of greater than SIL 2, during the "*initial pass*" then a semi-quantitative or a quantitative method as a "*final pass*" should be conducted.

For **SIF#2 (M100) metal detector**, these are the simple steps to conduct FRGM:

Step 1: Select one parameter (Consequence C2 parameter was selected as shown in **Figure 3.10**). C2 – serious injury (non-permanent);

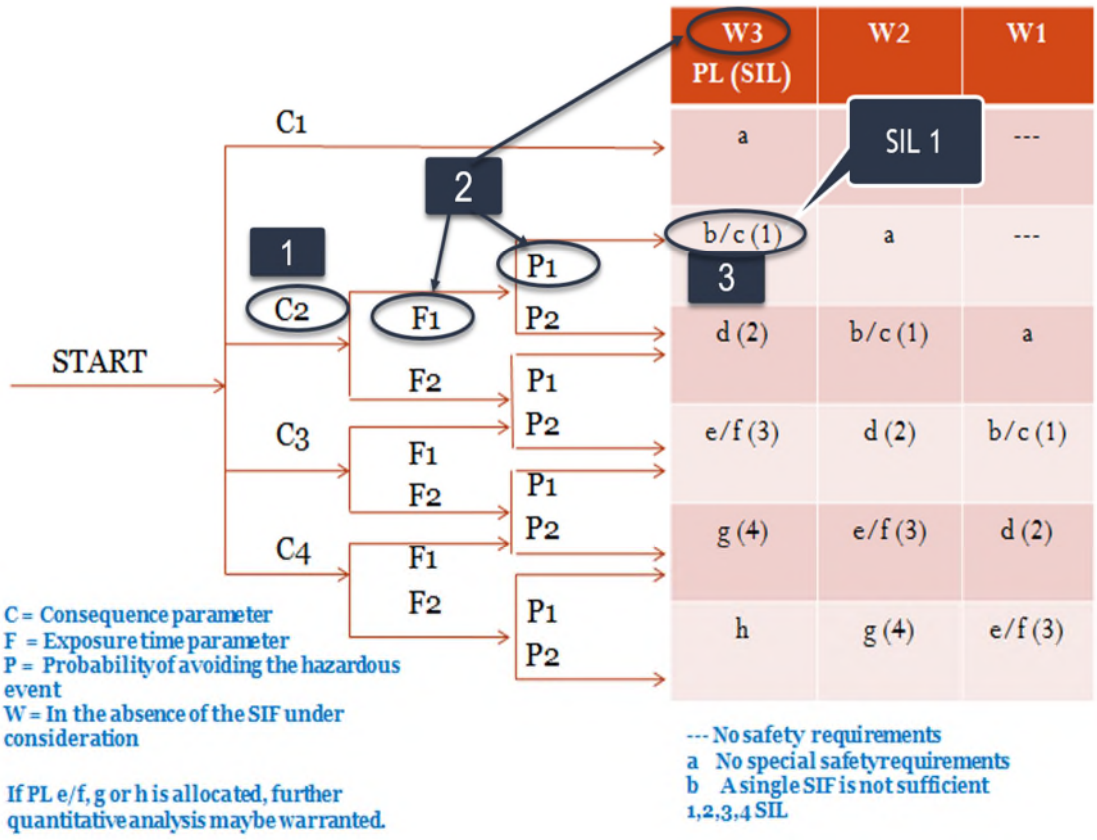


Fig. 3.10. FRGM straightforward steps using SIF#2 (M100) – SIL 1

Step 2: Chosen parameters are then linked to other parameters (Exposure F1, Probability P1, and Demand W3 as shown in **Figure 3.10**). F1 – rare to frequent exposure, P1 – avoidance is possible under certain conditions, W3 – function is demanded more than once per year;

Step 3: Resolve the SIL allocated to the SIF as shown in **Figure 3.10**.

In this case, it was easily evaluated that the SIL for SIF#2 (M100) is **SIL 1** as shown in **Figure 3.10**. Since this is only SIL 1, it can be used as the assessed SIL. As the calibration of FRGM dictates that the result from SIL2 and below can be used as the assess SIL then it can be used as the determined required (target) SIL.

For **SIF#3 (A200) Operator lanyard safety switches**, these are the simple steps to conduct FRGM:

Step 1: Select one parameter (Consequence C3 parameter was selected as shown in **Figure 3.11**). C3 – permanent disability or fatality;

Step 2: Chosen parameters are then linked to other parameters (Exposure F2, Probability P1, and Demand W3 as shown in **Figure 3.11**). F2 – permanent exposure or almost permanent exposure, P1 – avoidance is possible under certain conditions, W3 – function is demanded more than once per year;

Step 3: Resolve the SIL allocated to the SIF as shown in **Figure 3.11**.

In this case, it was easily evaluated that the SIL for SIF#3 (A200) is **SIL 3** as shown in **Figure 3.11**. In this case, since this is SIL 3, it is justified that it will undergo a more complex process such as quantitative methodology.

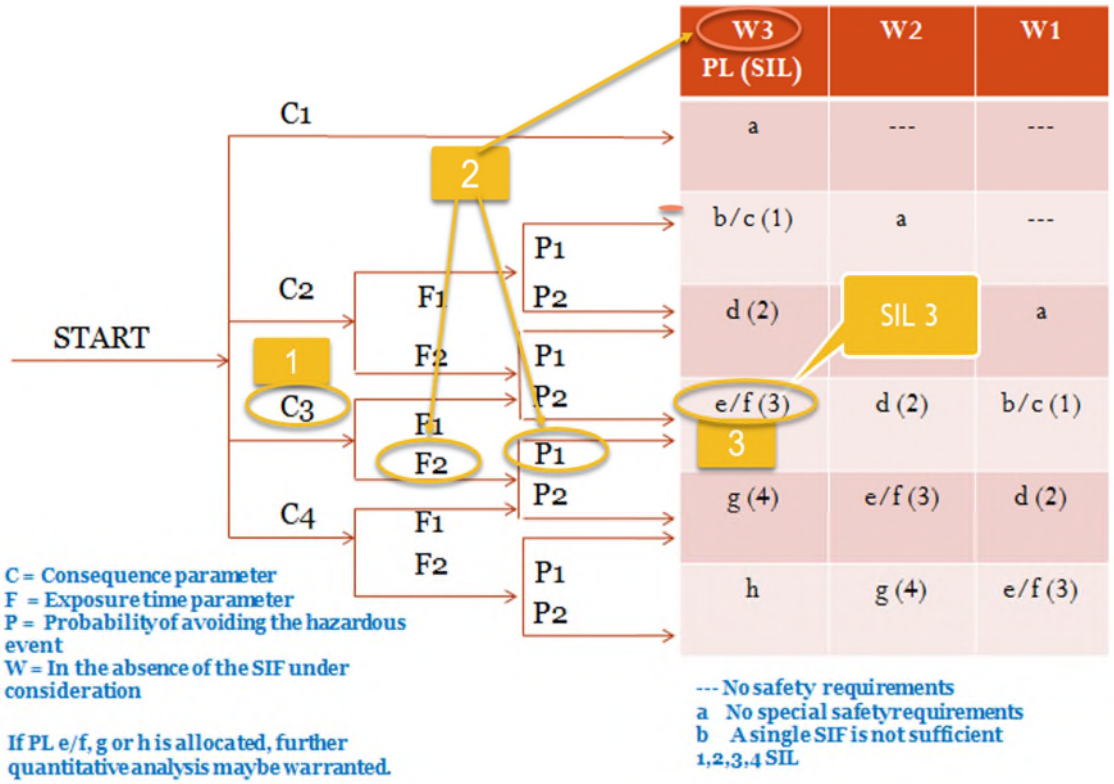


Fig. 3.11. FRGM straightforward steps using SIF#3 (A200) – SIL 3

Furthermore, at the discretion of the multi-disciplinary assessment team, they can come into an agreement to justify the "*final pass*" even though the outcome of FRGM is SIL 2 or less. Further justification for a final pass also includes those SIFs that are involved in preventing or mitigating high consequence events and which are the only risk control against a risk.

In summary, using the FRGM, which was calibrated against the corporate risk matrix, the summary result of safety risk assessment is shown in **Table 3.6**. SIL 2 is required for SIF#1 (A100), SIL 1 for SIF#2 (M100) and SIL 3 for SIF#3 (A200). SIL 2 is equivalent to PL d and CAT 3 with PFH between $10^{-7} \leq$ and $< 10^{-6}$, SIL 1 is equivalent to PL b/c and CAT 2 with PFH between $3x10^{-6} \leq$ and $< 10^{-5}$, while SIL 3 is equivalent to PL e/f and CAT 4 with PFH between $10^{-8} \leq$ and $< 10^{-7}$, per **Tables 3.2** and **3.3**.

Table 3.6. – Summary of Risk Assessment and Allocations using FRGM for SIF#1, SIF#2 and SIF#3

SIF Identifier	SIF Description & Function	Allocations (C, F, P, W)				PL	SIL	CAT
SIF#1 (A100)	C112 Conveyor Belt Gate Interlock Safety Switches	C3	F1	P1	W3	d	2	3
SIF#2 (M100)	M100 Metal Detector	C2	F1	P1	W3	b/c	1	2
SIF#3 (A200)	A200 Operator Lanyard Safety Switches	C3	F2	P1	W3	e/f	3	4

3.6.2 Application of LOPA to case study involving 3 SIFs

Using the same 3 SIFs, the LOPA method has been applied. Using the LOPA method, we arrive with the same safety function results as compared using FRGM as shown in **Table 3.7.**

The LOPA method [3] commences with data acquired during hazard identification and accounts for each identified hazard by documenting the initiating cause and the protection layers that prevent or mitigate the hazard.

Table 3.7. – Summary of Risk Assessment and Allocations using LOPA [3] for 3 SIFs

#	1	2	3	4	5	6	7	8	9	10	11	12	13
	Impact event	Severity level	Initiating cause	Initiation likelihood	General process	BPCS	Alarms	Additional mitigation.	IPL additional	Intermediate likelihood	SIF integrity	Mitigated event	Notes
SIF#1 – A100	Permanent disability or fatality	Serious	Loss of tension	0.1	0.1	0.1	0.1	0.1	Machine guards	10^{-7}	**10^{-2} SIL2**	10^{-9}	Lanyard switch non-SIL rated
SIF#2 – M100	Serious injury (non-permanent)	Minor	Sensor failure	0.01	0.1	0.1	0.1	0.1	Machine guards	10^{-8}	**10^{-1} SIL1**	10^{-9}	Sensor requires regular cleaning
SIF#3 – A200	Permanent disability or fatality	Extensive	Loss of tension	0.1	0.1	0.1	0.1	0.5	Machine guards	5×10^{-7}	**10^{-3} SIL3**	5×10^{-10}	Lanyard switch non-SIL rated

The total amount of risk reduction can then be determined and the need for more risk reduction analysed. If additional risk reduction is needed and if it is to be provided in the form of a SIF, the LOPA methodology allows the determination of the appropriate SIL for the SIF.

A risk model should be constructed that manages risk across all processes, units, and all their operating modes for a facility in order to use LOPA [2, 3] for SIL determination. The risk model should assign the following attributes to hazard scenarios: process, process unit, operating mode, consequence type, consequence severity, and consequence receptor. Other attributes may be assigned, such as hazard type and receptor location. Appropriate summations of risk can then be made and the estimates compared with compatible risk tolerance criteria. If the criteria are not met, those scenarios that contribute most risk can be identified and adjustments made, for example, the addition of SIFs or an increase in the SILs of existing SIFs.

A step-by-step approach for performing the analysis is described below and the result is presented in **Table 3.7**:

1. Prepare data developed in the Hazard and Operability (HAZOP) analysis and accounts for each identified hazard by documenting the initiating cause and the protection layers that prevent or mitigate the hazard. These include consequence, consequence severity, cause, cause frequency, existing safeguards and recommended new safeguards. Steps should be guided by a LOPA-trained person.

2. Prepare LOPA with the required information such as impact event, severity level, initiating cause, initiating likelihood, protection layers and required additional mitigation.
3. Impact event. Using the LOPA report sheet [3], enter each impact event description determined from the HAZOP.
4. Severity Level. Enter severity levels of Minor (M), Serious (S), or Extensive (E).
5. Initiating cause. List all of the initiating causes of the impact event.
6. Initiation likelihood. Enter likelihood values of the initiating causes occurring, in the events per year. The experience of the team is very important in determining the initiating cause of likelihood.
7. Protection layers. List multiple Protection Layers (PLs) that are normally provided in the process industry. Each protection layer consists of a grouping of equipment and/or administrative controls that function in concert with the other layers. **Table 3.8** shows a typical protection layer (prevention and mitigation) Probability of Failure on Demand (PFD).

Table 3.8. – Typical Protection Layer Probability of Failure on Demand

Protection layer	PFD
Control loop	1.0×10^{-1}
Human performance (trained, no stress)	1.0×10^{-2} to 1.0×10^{-4}
Human performance (under stress)	0.5 to 1.0
Operator response to alarms	1.0×10^{-1}
Vessel pressure rating above maximum challenge from internal and external pressure sources	10^{-4} or better, if vessel integrity is maintained (that is, corrosion is understood, inspections and maintenance is performed on schedule)

8. Additional mitigation. Determine the appropriate PFD for all additional mitigation layers such as pressure relief devices, dikes, restricted access, etc.
9. Independent Protection Layers (IPL). List protection layers that meet the criteria of IPL [3].
10. Intermediate event likelihood. Calculated by multiplying the initiating likelihood by the PFD of the protection layers and mitigating layers. If the intermediate event likelihood is less than the corporate criteria for events of this severity level, additional PLs are not required. Further risk reduction should, however, be applied if economically appropriate. If the intermediate event likelihood is greater than the corporate criteria for events of this severity level, additional mitigation is required.
11. SIF integrity level. If a new SIF is needed, the required integrity level can be calculated by dividing the corporate criteria for this severity level of event by the intermediate event likelihood.
12. Mitigated event likelihood. The mitigated event likelihood is now calculated by multiplying intermediate event likelihood and SIF integrity level. This continues until the team has calculated mitigated event likelihood for each impact event that can be identified.
13. Total risk. The last step is to add up all the mitigated event likelihood for serious and extensive impact events that present the same hazard.

3.7 Comparison between FRGM and LOPA (and other traditional methods)

In previous above sections, we have demonstrated the SIL determination for 3 SIFs using FRGM and LOPA. The summary of the results for SIL determination using FRGM and LOPA is shown below in **Table 3.9**. It is evidently clear that both methods yield the same results. In terms of steps taken to complete the assessment, the FRGM only takes 3 steps while LOPA takes 13 steps. The three (3) steps to the proposed FRGM approach are as follows and LOPA as mentioned in Section 3.5:

***Step** 1.* Select one parameter (say Consequence C2 parameter) from **Figure 3.2**;

***Step** 2.* Link Chosen parameters to other parameters (i.e. Exposure, Probability, Demand W);

***Step** 3.* Resolve the SIL allocated to the SIF.

For example, Consequence C2, Frequency F1, Probability P1 with demand W3 would yield a SIL1. But if the Probability changes to P2 with the same condition, then SIL2 is allocated. The FRGM approach can also be utilized to enable assessment of SIS where the potential consequences include severe environmental impact or property loss.

Table 3.9. – Summary of Results using FRGM and LOPA for SIF#1, SIF#2 and SIF#3

SIF Identifier	SIF Description & Function	FRGM SIL	LOPA SIL
SIF#1 (A100)	C112 Conveyor Belt Gate Interlock Safety Switches	2	2
SIF#2 (M100)	M100 Metal Detector	1	1
SIF#3 (A200)	A200 Operator Lanyard Safety Switches	3	3

The main difference with this proposed technique is that, instead of jumping into costly and time-consuming methods (semi-quantitative or quantitative), all SIF will first undergo FRGM (qualitative), which usually takes only a few minutes for each SIF to collaborate with a multi-disciplinary team with calibrated parameters. Only those SIFs which falls under the following category, which typically around 5% of the total SIF, will undergo a quantitative or semi-quantitative method:

- SIF with SIL allocation of more than SIL2, i.e., SIL 3 during the FRGM "*initial pass*".
- Did not achieve a satisfactory level of consensus within the multi-disciplinary team during the "*initial pass*".
- Pose a high EUC risk.

In terms of time reduction and consequent cost-savings, **Table 3.10** shows the comparative differences between the standard semi-quantitative methods such as LOPA [2, 120, 121], quantitative methods such as Fault Tree Analysis (FTA) [30, 40, 87, 122] and Event Tree Analysis (ETA), as compared with the proposed FRGM approach at typically 3,000 SIFs. Cost reduction is realised by the number of hours spent by a multi-disciplinary team. Pros and cons using the proposed FRGM approach as compared to the standard approach are shown in the same **Table 3.9.** From the past experiences of the author in the industry, it is known that one would spend around 2.5 hours per SIF. A reasonable estimate for the FRGM analysis per SIF would be 20 minutes, justified by the author by timing himself during the application of the FRGM methods to the case studies. The salary rate of $150/hour was based on random current survey. The coarser

or less accurate assessment of risk using the FRGM is not a concern as it is used as a funnel from a broad range of SIL 0 to SIL 2.

Table 3.10. – Comparison between FRGM and Traditional Standard Methods

Criteria	Traditional Standard Methods (LOPA, FTA, ETA)	FRGM	Time Reduction, hours	Cost Reduction ($150/hr. rate)
Time & Cost Reduction	Approximately 2.5 hours per SIF x 3,000 SIF = 7,500 hours	Approx. 20 minutes per SIF x 3,000 SIF = 990 hours	6,510 hrs.	$976,500
Steps Involved	13 steps for LOPA	3-step process		
Pros	More accurate assessment of risk.	Straight forward, resource- efficient		
Cons	Requires a lot of resources	Coarser or less accurate assessment of risk		

As observed by the author, in a typical process plant, approximately 95% or more of the SIF falls on SIL 2 or under and an estimated 5% or less falls on SIL 3 or above. Interestingly, the same safety function can be achieved using any of the methodology as shown in **Table 3.9.** A lot of resources can be saved using the simple FRGM. For example, if the Consequence parameter is C1 (calibrated as minor injury) then it is easily determined to be no special safety requirement using the FRGM that only takes a few minutes. Similarly, if we have a Consequence C2, Frequency F1 and either of any Probabilities or Demand W then we will arrive into a maximum SIL 2.

Furthermore, **Table 4.0** shows the sensitivity analyses of varying the number of hours spent utilising the traditional methods and applying different salary rates. The benefit calculation of using FRGM as opposed to using LOPA is shown in **Table 3.11.** We can obviously see that FRGM poses economic benefits assuming around 3,000 SIFs used.

Table 3.11. Benefit calculation and sensitivity analysis for 3,000 SIFs.

Traditional Standard Method, hrs.	FRGM, hrs.	Reduction, hrs.	Rate, $/hr.	Cost savings, $
2.5	0.33	2.17	150	$ 976,500
2.5	0.33	2.17	130	$ 846,300
2	0.33	1.67	150	$ 751,500
2	0.33	1.67	130	$ 651,300
1	0.33	0.67	150	$ 301,500
1	0.33	0.67	130	$ 261,300
0.75	0.33	0.42	150	$ 189,000
0.75	0.33	0.42	130	$ 163,800

3.8 Conclusion

Oil & gas and related heavy industries, big or small players, cannot escape from the fact that they need to utilize ICSS in their business operations. Traditionally, in designing ICSS, all SIF must undergo quantitative or semi-quantitative analyses consuming a lot of resources. Given the complexity of process industries, SIL and PL allocation should be performed via a quantitative or semi-quantitative methodology. However, as emphasized, it may be impracticable to apply a semi-quantitative or quantitative approach due to the substantial amount of time and resources involved, thus FRGM approach is proposed.

In this Chapter, an application of a more cost-effective, simplified and enhanced approach called FRGM for the design and evaluation of SIS has been explored. The proposed simplified approach is a Funnel Risk Graph Method (FRGM) in reference to functional safety standards. Based on the results presented, it is expected that the project will results in significant economic benefits, more practicable compliance and result in equal degree of functional safety as compared with the traditional approach. The work in this Chapter has

proposed the use of the FRGM approach as a funnel method to filter lower SILs. In comparison to LOPA and other traditional methods, it has shown significant benefits. To prove the effectiveness of this approach, comparative analyses between FRGM and LOPA (and other traditional methods) were also presented. The FRGM only takes 3 steps while LOPA takes 13 steps. An estimated cost savings of $ 976,500 was calculated for 3,000 SIFs as presented in **Tables 3.10** and **3.11**.

FRGM is a qualitative method based in [2, 3, 34, 35]. This method is based on qualitative knowledge of the likelihood and consequences of hazardous events, as well as the number of layers of protection available. It is based on the assumption that each added protection layer provides a risk reduction of one order of magnitude. The FRGM is presented in **Figure 3.2.** The factors used in the matrix are:

- Severity rating.
- Likelihood of the hazardous event.
- Number of independent protection layers for the specific hazardous event.

The simplicity of FRGM makes it convenient for screening a large number of SIFs. This can make FRGM useful as a first screening pass prior to using quantitative or semi-quantitative methods.

Chapter 4 - Quantitative Analyses: SIF SIL Design Calculations & Verifications

4.1 Introduction

A lot of resources can be saved using the FRGM approach as opposed to using traditional methods for lower SILs. This can be proven and verified using quantitative analyses, which will be demonstrated in this Chapter. Specifically, Chapter 4 shows SIL calculations performed for each SIF loop with a SIL target of SIL 1 or greater. Calculations are based on the actual hardware selected for the Sensor, the Logic Solver and the Final Element. In this study, the software used to perform SIL calculations was exSILentia version 3.3.0.906 coupled with the latest reliability database SERH. The exSILentia® integrated Safety Lifecycle Engineering Tool is a powerful aid for any engineer involved in safety lifecycle tasks such as SIL selection, Safety Requirements Specification, and SIL verification [123].

SIL targets for SIF loops were assigned during Process Hazard Analysis/Safety Objective Analysis (PHA/SOA) studies. A process hazard analysis (PHA) (or process hazard evaluation) is a set of organized and systematic assessments of the potential hazards associated with an industrial process. A PHA provides information intended to assist managers and employees in making decisions for improving safety and reducing the consequences of unwanted or unplanned releases of hazardous chemicals. A

PHA is directed toward analysing potential causes and consequences of fires, explosions, releases of toxic or flammable chemicals and major spills of hazardous chemicals, and it focuses on equipment, instrumentation, utilities, human actions, and external factors that might impact the process [124].

There are varieties of methodologies that can be used to conduct a PHA, including but not limited to: Checklist, What if?, What if?/Checklist, hazard and operability study, failure mode and effects analysis and those methods discussed in *Chapter 2* of this thesis. PHA methods are qualitative in nature. The selection of a methodology to use depends on a number of factors, including the complexity of the process, the length of time a process has been in operation and if a PHA has been conducted on the process before, and if the process is unique, or industrially common. Other methods such as layer of protection analysis (LOPA) [121] or fault tree analysis (FTA) [87] may be used after a PHA if the PHA team could not reach a risk decision for a given scenario.

SIL calculations have been performed for each Safety Instrumented Function (SIF) loop that has been assigned a SIL target of SIL 1 or greater. Calculations are based on the actual hardware selected for the Sensor, the Logic Solver and the Final Element.

The software for performing SIL calculations is exSILentia coupled with the latest reliability database SERH.

The result of these calculations will show that the same safety function can be attained as compared to using the FRGM approach. As mentioned in previous chapters, the FRGM is a SIL assessment methodology based on Risk Graphs qualitative approach in reference to functional safety standards [2, 3].

Traditionally, in designing SIS, all SIF, depending on the designers' preference, must undergo quantitative, semi-quantitative or qualitative analyses consuming a lot of resources. However, using FRGM, cost savings can be realised in a significant scale.

4.2 Scope – Process Unit 6400

For the purpose of this study, selected SIFs were taken and performed SIL calculations in one of the process units of an LNG plant, which we named as the *LNG Plant A Process Unit 6400* (PU6400). The Plant is one of the biggest LNG plants in the world. The PU6400 system's main function is for waste water collection, treatment and disposal. It has an estimated gas resource of 50 trillion cubic feet. It has subsea infrastructure for the production, gathering and transport of reservoir fluids from various locations to the main island. The gas processing facility is located on an island. Operating and maintenance activities and processes have been developed to ensure these values are protected. The LNG Plant A consists of three production field, a nominal natural gas liquefaction plant with supporting utility, unloading/loading and storage facilities. It has domestic gas plant, utilities area, which includes PU6400, supporting infrastructure and tie-ins for future expansion of the LNG trains. Due to the complexity of the system, this Chapter will only deal with the PU6400.

4.3 Analysis of SIL Calculations/Verifications

The outcomes of the PHA/SOA revalidation process in LNG Plant A PU6400 are shown in **Table 4.1**. The process of calculations is not shown in this study. The achieved SIL for each 16 SIF loops as shown in **Table 4.1.** The FRGM approach is also used to determine the required SIL and the result is shown in **Table 4.2.** The SIL verification results for all SIF loops in PU6400 are provided with varying level of detail in **Appendix A** to **Appendix C**.

Table 4.1. Summary of Safety Instrumented Functions for PU6400

SIF Name	Target (Determine required SIL)		FRGM (Used to determine the required SIL)		Achieved	Time Reduction	Cost Reduction ($150/hr. rate)
	SIL	Hours	SIL	Hours	SIL	Hours	$
064FZ-0567 LL	1	2.5	1	0.33	1	2.167	325
064FZ-0568 LL	1	2.5	1	0.33	1	2.167	325
064FZ-0602 LL	1	2.5	1	0.33	1	2.167	325
064FZ-0603 LL	1	2.5	1	0.33	1	2.167	325
064FZ-0821 LL	1	2.5	1	0.33	1	2.167	325
064FZ-0831 LL	1	2.5	1	0.33	1	2.167	325
064FZ-0852 LL	1	2.5	1	0.33	1	2.167	325
064LZ-0011 LL	1	2.5	1	0.33	2	2.167	325
064LZ-0511 HH	1	2.5	1	0.33	1	2.167	325
064LZ-0511 LLL	1	2.5	1	0.33	1	2.167	325

SIF Name	Target (Determine required SIL)		FRGM (Used to determine the required SIL)		Achieved	Time Reduction	Cost Reduction ($150/hr. rate)
	SIL	Hours	SIL	Hours	SIL	Hours	$
064LZ-0541 LL	1	2.5	1	0.33	1	2.167	325
064LZ-0712 LL	2	2.5	2	0.33	2	2.167	325
064PDZ-0733 +HH	1	2.5	1	0.33	1	2.167	325
064PDZ-0733 -HH	1	2.5	1	0.33	1	2.167	325
064PDZ-0830 HH	1	2.5	1	0.33	1	2.167	325
064XS-0020	1	2.5	1	0.33	1	2.167	325

The IEC 61511 Compliance Report in **Appendix C** shows details of the selected SIF SIL verification results.

For all SIF functions considered in this study, the verification tool has estimated the same SIL level that was identified by the FRGM method. The FRGM determination graphs for selected SIFs are shown in **Appendix D, Figures D.1** and **D.2,** and further explained below:

For SIF 064FZ-0567 LL, these are the simple steps to conduct FRGM:

Step 1: Select one parameter (Consequence C2 parameter was selected as shown in **Appendix D, Figure D.1**). C2 – serious injury (non-permanent);

Step 2: Chosen parameters are then linked to other parameters (Exposure F1, Probability P1, and Demand W3 as shown in **Appendix D, Figure D.1**). F1 – rare to frequent exposure, P1 – avoidance is possible under certain conditions, W3 – function is demanded more than once per year;

Step 3: Resolve the SIL allocated to the SIF as shown in **Appendix D, Figure D.1**.

In this case, it was easily evaluated that the SIL for SIF 064FZ-0567 LL is **SIL 1** as shown in **Appendix D, Figure D.1**. Since this is only SIL 1, it can be used as the assessed SIL. As the calibration of FRGM dictates that the result from SIL2 and below can be used as the assess SIL then it can be used as the determined required (target) SIL.

For SIF 064LZ-0712 LL, these are the simple steps to conduct FRGM:

Step 1: Select one parameter (Consequence C3 parameter was selected as shown in **Appendix D, Figure D.2**). C3 – permanent disability or fatality;

Step 2: Chosen parameters are then linked to other parameters (Exposure F1, Probability P1, and Demand W3 as shown in **Appendix D, Figure D.2**). F1 – rare to frequent exposure, P1 – avoidance is possible under certain conditions, W3 – function is demanded more than once per year;

Step 3: Resolve the SIL allocated to the SIF as shown in **Appendix D, Figure D.2**.

In this case, it was easily evaluated that the SIL for SIF#1 (A100) is **SIL 2** as shown in **Appendix D, Figure D.2**. Since this is only SIL 2, it can be used as the assessed SIL. As the calibration of FRGM dictates that the result from SIL2 and below can be used as the assess SIL then it can be used as the determined required (target) SIL. However, if the assessed safety-related system received SIL allocation of greater than SIL 2, during the "*initial pass*" then a semi-quantitative or a quantitative method as a "*final pass*" should be conducted.

The results using the FRGM approach are also presented in **Table 4.1** using the process recently demonstrated and described in *Chapter 3*.

The FRGM is the proposed approach in evaluation of ICSS that aims to reduce costs in the early stage of the design process. This method is based on qualitative knowledge of the likelihood and consequences of hazardous events, as well as the number of layers of protection available. It is based on the assumption that each added protection layer provides a risk reduction of one order of magnitude. The FRGM is presented in **Figure 3.2** of *Chapter 3*. The simplicity of FRGM makes it convenient for screening a large number of SIFs. **Table 4.1** also shows the comparative differences between the standard method(s) and FRGM used in Target SIL determination. From the past experiences of the author in the industry, it is known that one would spend around 2.5 hours per SIF. A reasonable estimate for the FRGM analysis per SIF would be 20 minutes (0.33 hour) per person, justified by the author by timing himself during the application of the FRGM methods to the case studies. Typically, at a minimum, there are about four (4) multidisciplinary personnel which conducts the safety assessment. This includes representatives from Process Engineering, Maintenance, Operations, ICSS Engineering and Health & Safety Engineering. The average salary rate of $150/hour was based on random current survey. Furthermore, on a bigger scale (not only PU6400), considering the entire SIFs of the LNG Plant A, which has around 3,000 number of SIFs, the cost reduction on this instance can be realised as shown in **Table 4.2.** Furthermore, the same safety function can be achieved using FRGM, thus not sacrificing accuracy.

Table 4.2. Summary Cost Reduction Entire LNG Plant A SIFs

No. of SIFS	Target SIL Determination (traditional), hrs./person	FRGM, hr./person	Total Time Reduction. hrs./person	Total number of persons	Cost Reduction ($150/hr. rate/person)	Group Total Cost Reduction
3,000	2.5	0.33	2.167	4	$ 976,500	$ 3,906,000

4.4 SIFs Involved and Description

The following are the 16 SIFs involved in this study and the description of their specific functions.

4.4.1 064FZ-0567 LL

On Low Low flow from discharge of water disposal pump as detected by 064FZ-0567, trip water disposal pump via 064UZR-6601. The hazard is level control failure. Consequence is that the control system will speed up running pump. Level in the tank will decrease; if the level is lost, then it will cause a damage to running downstream pump. Impact on ability to dispose of LNG plant produced water. Furthermore, there is a potential shutdown of LNG plant.

4.4.2 064FZ-0568 LL

On Low Low flow from discharge of water disposal pump as detected by 064FZ-0568, trip water disposal pump via 064UZR-6701. The hazard is level control failure. Consequence is that the control system will speed up running pump. Level in the tank will decrease; if level is lost, then damage to running downstream pump. Impact on ability to

dispose of LNG plant produced water. Furthermore, there is a potential shutdown of LNG plant.

4.4.3 064FZ-0602 LL

On Low Low flow from discharge of water disposal pump as detected by 064FZ-0602, trip water disposal pump via 064UZR-6801. The hazard is level control failure. Consequence is that the control system will speed up running pump. Level in the tank will decrease; if the level is lost, then it will cause a damage to running downstream pump. Impact on ability to dispose of LNG plant produced water. Furthermore, there is a potential shutdown of LNG plant.

4.4.4 064FZ-0603 LL

On Low Low flow from discharge of water disposal pump as detected by 064FZ-0603, trip water disposal pump via 064UZR-6901. The hazard is level control failure. Consequence is that the control system will speed up running pump. Level in the tank will decrease; if level is lost, then damage to running downstream pump. Impact on ability to dispose of LNG plant produced water. Furthermore, there is a potential shutdown of LNG plant.

4.4.5 064FZ-0821 LL

On Low Low flow from discharge of membrane filtrate pumps as detected by 064FZ-0821, trip both pumps via 064UZR-7901/2. Hazard is control system failure (filtrate isolation valve). Consequence is a potential to damage pumps. Potential impact on LNG production due to inability to treat wastewater.

4.4.6 064FZ-0831 LL

On Low Low discharge flow from membrane recirculation pumps as detected by 064FZ-0831, trip both pumps via 064UZR-9201/2. Hazard is valve from tank to membrane recirculation pump closed in error. Consequence is a potential to damage both pumps and inability to treat wastewater with impact on LNG production.

4.4.7 064FZ-0852 LL

On Low Low discharge flow from membrane backwash pumps as detected by 064FZ-0852, trip both pumps via 064UZR-7801/2. Hazard is valve on backwash pump suction closed in error. Consequence is a potential damage to both pumps. Without backwash, pressure will build up and the ability to treat wastewater will be impacted. In long term, potential impact on LNG production.

4.4.8 064LZ-0011 LL

On Low Low level in tank as detected by 064LZ-0011, trip Slop Oil pump via 064UZR-0201 & close 064UZV-0202. Hazard is reduced or loss of level in tank. Consequence is a possibility of pump cavitation. Possible pump damage, seal leak, hydrocarbon release, fire and possible personnel exposure.

4.4.9 064LZ-0511 HH

On High High level in flow equalisation tank as detected by 064LZ0511, trip both transfer pumps via 064UZR-5001/2. Hazard is pump out full sump. Consequence is a potential overflow to Class 1 drains that may affect the environment.

4.4.10 064LZ-0511 LLL

On Low Low Low level in flow equalisation tank as detected by 064LZ0511, trip both wastewater transfer pumps via 064UZR-5701/2. Hazard is both pumps running due to manual initiation of second pump. Consequence is that the level in tank will decrease. Pumps will run dry, with potential damage to both. Overflows will occur at sources. Therefore, potential impact on LNG production due to requirement to evacuate.

4.4.11 064LZ-0541 LL

On Low Low level in lift station as detected by 064LZ-0541, trip both transfer pumps via 064UZR-5001/2. Hazard is control failure such that pumps do not turn off. Consequence is that when the lift station level reduces, pumps run dry. There is a potential damage to both of the pumps. Inability to dispose of wastewater leads to the potential requirement to evacuate and to shutdown LNG Plant.

4.4.12 064LZ-0712 LL

On Low Low level in tank as detected by 064LZ-0712, trip both membrane recirculation pumps via 064UZR-9201/2. Hazard is drain / sample valves open in error leading to empty tank. Consequences are potential damage to membrane recirculation pumps and inability to treat wastewater and disruption of routine operations.

4.4.13 064PDZ-0733 +HH

On High High forward differential pressure across membranes as detected by 064PDZ-0733, trip both membrane filtrate pumps via 064UZR-7901/2. Hazard is blocked membranes due to insufficient cleaning / backwash. Consequence is that fouling or collapsing of membranes.

4.4.14 064PDZ-0733 -HH

On High High reverse differential pressure across membranes as detected by 064PDZ-0733, both trip membrane backwash pumps via 064UZR-7801/2. Hazards are blocked membranes due to insufficient cleaning / backwash and both backwash pumps running. Consequence is fouling or collapsing of membranes.

4.4.15 064PDZ-0830 HH

On High High differential pressure across strainer as detected by 064PDZ-0830, trip both membrane recirculation pumps via 064UZR-9201/2. Hazard is strainer blocked on feed to membrane skid. Consequence is a potential damage to membrane recirculation pumps. Potential impact on LNG production due to inability to treat wastewater.

4.4.16 064XS-0020

Pump not running closes 064UZV-0202, which will prevent reverse flow into tank. Hazard is reverse flow from condensate header and/or condensate storage tank. Consequence is a potential for reverse flow from condensate header due to other unit pumping through header or reverse flow due to static head in condensate storage tank. Possible

to overflow tank. Possible tank damage, release of hydrocarbon. Possible personnel exposure.

4.5 Calculation Basis

This SIL verification was based on unit 6400 Waste Water Collection, Treatment and Disposal System. Modelling was performed in accordance with the following specifications and guidance on:

- SIF modelling requirements.
- Applicable project and Australian standards.
- Project exSILentia version requirements and settings.
- Acceptable results.
- Sensor, Logic Solver and Final Element Reliability Data.

4.6 SIS Logic Solver

It was assumed that the SIS is implemented and maintained in accordance with the requirements of the associated Product Safety Manual [125] for the highest SIL of all SIFs implemented in the SIS.

The SIS logic solver selected for all the SIFs within this process unit was a *"Yokogawa ProSafe-RS Redundant [Certified SIL: 3]"* [126].

4.7 Field Equipment

Unless specified otherwise, all sensors and final elements were assumed to be fail-safe.

All SIF transmitters were covered from direct sunlight in order for the reliability data utilised in the SIF SIL calculation to be valid. If unshaded and environmental conditions are such that a transmitter is subjected to a temperature range outside the range considered in the SIL certification, the SIL calculation were done utilising the recommended ‘derated’ failure rate specified in the certification report for that transmitter.

Where equipment data sheets were not available, or the listed equipment of a type not present in the exSILentia software’s reliability database or the specification for SIF SIL verification calculation, generic database components have instead been used to model the related SIFs.

4.8 Sensor Elements

For sensors 064FZ-0567 LL, 064FZ-0568 LL, 064FZ-0602 LL & 064FZ-0603 LL external comparison is utilized taking credit for the comparison between the SIS sensor and its respective PCS sensor in order to achieve the SIL 1 architectural constraint.

For sensors 064FZ-0821/31/52, 'Generic Flow Transmitter - Mag Meter' is selected in exSILentia as the Manufacturer/Model; Yokogawa AXF050C is not available in the exSILentia SERH data base.

For sensors 064LZ-0511, 064LZ-0712, 064PDZ-0733 and 064PDZ-0830 remote seal is selected in exSILentia.

For sensor 064LZ-0712, MOC-B-31-PCS-0066 specifies that a comparison block will be configured between 064LZ-0712 and 064LC-0711. External comparison has been implemented in this calculation in order to achieve the SIL 2 architectural constraint.

Motor running feedback signal 064GBZ-6601 within SIF 064FZ-0567 LL, has been modelled utilising user defined data for a MCC Motor Contactor - Siemens (SIRIUS 3RT Series), (see **Attachment 2**).

Motor running feedback signal 064GBZ-6701 within SIF 064FZ-0568 LL, has been modelled utilising user defined data for a MCC Motor Contactor - Siemens (SIRIUS 3RT Series), (see **Attachment 2**).

Motor running feedback signal 064GBZ-6801 within SIF 064FZ-0602 LL, has been modelled utilising user defined data for a MCC Motor Contactor - Siemens (SIRIUS 3RT Series), (see **Attachment 2**).

Motor running feedback signal 064GBZ-6901 within SIF 064FZ-0603 LL, has been modelled utilising user defined data for a MCC Motor Contactor - Siemens (SIRIUS 3RT Series), (**see Attachment 2**).

Motor running feedback signals 064GBZ-0851/2 within SIF 064FZ-0852 LL, have been modelled utilising user defined data for a MCC Motor Contactor - Siemens (SIRIUS 3RT Series), (**see Attachment 2**).

Motor running feedback signals 064GBZ-0821/2 within SIF 064FZ-0821 LL, have been modelled utilising user defined data for a MCC Motor Contactor - Siemens (SIRIUS 3RT Series), (see **Attachment 2**).

Motor running feedback signals 064GBZ-0831/2 within SIF 064FZ-0831 LL, have been modelled utilising user defined data for a MCC Motor Contactor - Siemens (SIRIUS 3RT Series), (see **Attachment 2**).

For sensor 064LZ-0541, 'Generic Level Transmitter' is selected in exSILentia as the Manufacturer/Model; Flygt LTU-701 is not available in the exSILentia SERH data base. APCS SI132-61110 signal isolator is modelled using ‘Generic Isolated Switch Amplifier’ as device specific failure rate data is not available. Novaris SL36 signal line protector is modelled using ‘Generic Intrinsic Safety Barrier’ as device specific failure rate data is not available.

Motor running feedback signal 064XS-0020 within SIF 064XS-0020 has been modelled utilising failure rate data for a generic relay over failure rate data for the MCC Contactor, DTT (ABB Axx-30 Series), as this is the more conservative approach.

4.8.1 Valves

Partial Valve Stroke Testing was not applied in the modelling of any valve within this unit.

For 064UZV-0202: Shutdown valve has been modelled utilising Exida SERH data for Cameron Type 31 in the SIL calculations instead of the TUV certificate values for Cameron B and BT series ball valves.

Bifold VBP volume booster’s useful life is 10 to 15 years based on clean air and an ambient temperature average of 40 deg. C. as per Exida FMEDA report BIF 09/10-25 R001, Version V1, Revision R1.

ASCO Solenoid valve series 327 useful life is approximately 10 years as per Exida IEC 61508 Function Safety Assessment report ASC 09-04-59 R003 V1 R3 61508 Assessment, Version V1, Revision R3.

4.8.2 Electrical Loads

064UZR-0201 - Pump trip modelled utilising user defined reliability data for a MCC Contactor, DTT (ABB Axx-30 Series), (see **Attachment 2**).

064UZR-5001/2, Pump trip modelled utilising exSILentia SERH data for a ‘Generic MCC - interrupt function 10 < HP <= 100’.

064UZR-5701/2 - Pump trip modelled utilising user defined reliability data for a MCC Contactor, DTT (Siemens SIRIUS 3RT Series), (see **Attachment 2**).

064UZR-6601 - Pump trip modelled utilising user defined reliability data for a MCC Contactor, DTT (Siemens SIRIUS 3RT Series), (see **Attachment 2**).

064UZR-6701 - Pump trip modelled utilising user defined reliability data for a MCC Contactor, DTT (Siemens SIRIUS 3RT Series), (see **Attachment 1**).

064UZR-6801 - Pump trip modelled utilising user defined reliability data for a MCC Contactor, DTT (Siemens SIRIUS 3RT Series), (see **Attachment 1)**.

064UZR-6901 - Pump trip modelled utilising user defined reliability data for a MCC Contactor, DTT (Siemens SIRIUS 3RT Series), (see **Attachment 1**).

064UZR-7801/2 - Pump trip modelled utilising user defined reliability data for a MCC Contactor, DTT (Siemens SIRIUS 3RT Series), (see **Attachment 1**); and a Safety Relay, DTT (Phoenix PSR-SCP-24DC/ESP4/2X1/1X2), (see **Attachment 3**).

064UZR-7901/2 - Pump trip modelled utilising user defined reliability data for a MCC Contactor, DTT (Siemens SIRIUS 3RT Series), (see **Attachment 1**); and a Safety Relay, DTT (Phoenix PSR-SCP-24DC/ESP4/2X1/1X2), (see **Attachment 3**).

064UZR-9201/2 - Pump trip modelled utilising user defined reliability data for a MCC Contactor, DTT (Siemens SIRIUS 3RT Series), (see **Attachment 1**); and a Safety Relay, DTT (Phoenix PSR-SCP-24DC/ESP4/2X1/1X2), (see **Attachment 3**).

064UZR-9601/2 - Pump trip modelled utilising user defined reliability data for a MCC Contactor, DTT (Siemens SIRIUS 3RT Series), (see **Attachment 1**); and a Safety Relay, DTT (Phoenix PSR-SCP-24DC/ESP4/2X1/1X2), (see **Attachment 3**).

4.9 Reliability Data

4.10 SERH

The primary and preferred source of device reliability data for SIL verification calculations was the latest version of the exSILentia SERH database. SERH database 2017.1.03 was current at the time the calculations presented in this study.

4.11 User Defined

Reliability data entered manually into exSILentia (i.e. not sourced from SERH), was referred to as User Defined data. When such data was used in a

calculation, reference to the data source(s) shall be provided with supporting comments to justify the use and choice of this external data.

4.12 Conclusion

This Chapter proves that results using the FRGM and exSILentia software are the same as summarised in **Table 4.1**. SIL calculations were performed for each Safety Instrumented Function (SIF) loop that has been assigned a SIL target of SIL 1 or greater. SIL targets for Safety Instrumented Function (SIF) loops were assigned during PHA/SOA studies.

Detailed SIL calculations were presented for PU6400 with target and achieved SILs using exSILentia, coupled with the latest reliability database SERH. Calculations were based on the actual hardware selected for the Sensor, the Logic Solver and the Final Element.

Results from FRGM approach were compared with the same SIFs. Cost reduction were realised initially for process unit 6400. The work in this Chapter has proposed the use of the FRGM approach as a funnel method to filter lower SILs. In comparison to the result form exSILentia, it has shown significant benefits. Therefore, considering the entire LNG Plant A, which has around 3,000 SIFs, a potential significant cost savings for the team can be achieved using FRGM to the tune of around $3,906,000.

Appendix A - SILVER SUMMARY REPORT

Project Name LNG Plant A
Unit / Process Area 6400 - Wastewater

SIF Tag 064FZ-0567 LL

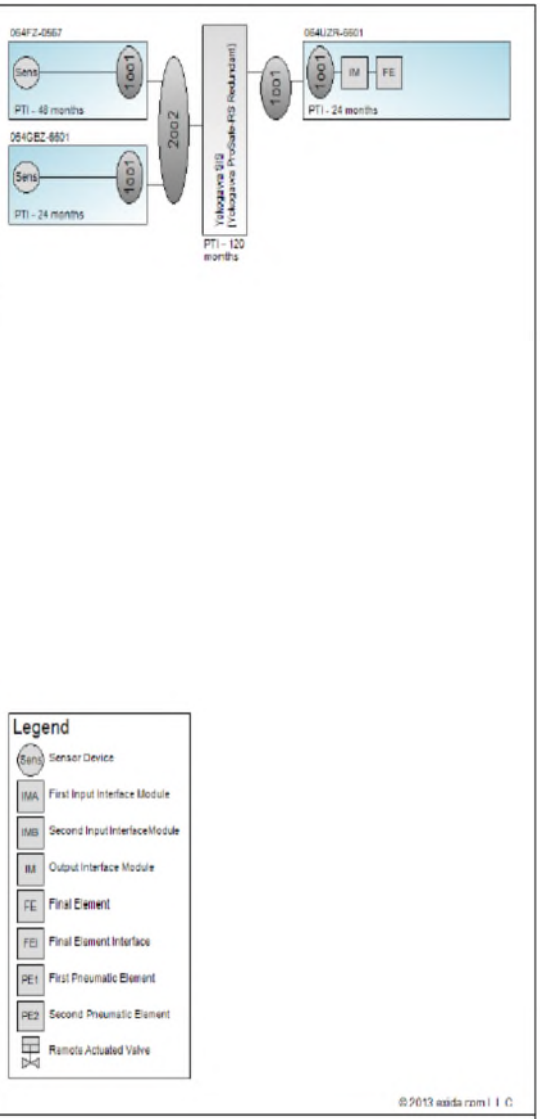
SIF Description On Low Low flow from discharge of Water Disposal Pump 0P-6429A as detected by 064FZ-0567, trip Water Disposal Pump 0P-6429A via 064UZR-6601.

SIF Reference SILver: RE01, RE05, RE14, RE30, RE42, RE53, RE57, RE59, RE60, RE61, RE62, RE76, RE101, RE102

Responsible PH
Analysis Date 25 Jun 2017
Mission Time 15 years

Safety Instrumented Function Performance	
Target SIL	**1**
Target RRF	**10**
Achieved SIL	**1**
PFDavg	1.42E-02
SIL (PFDavg)	1
SIL (Arch. Constraints IEC 61508:2000)	1
SIL (Systematic Capability)	-
Achieved RRF	70
MTTFS (years)	84.75

	PFDavg	MTTFS	SILac
Sensor Part	1.27E-02	4251.57	1
Logic Solver Part	3.95E-04	297.12	3
Final Element Part	1.18E-03	121.98	3



Remarks: The SIF operates in Low demand mode.

Field Equipment MCI: 2 – Good repair – 90% Logic Solver MCI: 2 – Good repair – 90%.

Asset gap of 2 being accepted in asset scenarios therefore target is SIL 1 for 064FZ-0567 LL, 064FZ-0568 LL, 064FZ-0602 LL & 064FZ-0603 LL. In Safety scenario IPLs 064FC-0561, 064FC-0563, 064FC-0600 & 064FC-0601 are claimed as PCS1 therefore target is SIL1 for 064FZ-0567 LL, 064FZ-0568 LL, 064FZ-0602 LL & 064FZ-0603 LL.

1) Sensor Element:

a) External comparison with 064FC-0561 is implemented to meet SIL 1 architectural constraint.

b) The failure rate data for the impulse line has been doubled because there are two tapping points.

c) Running feedback signal 064GBZ-6601 has been modelled utilising the failure rate data for the MCC Motor Contactor - Siemens (SIRIUS 3RT Series) in 064UZR-6601.

2) Final Element:

a) User defined PFD data utilised to model the Safety Relay, DTT (Phoenix PSR-SCP-24DC/FSP/1X1/1X2). See attachment 2 of the SSDVR for failure rate data.

b) MCC Contactor, DTT (Siemens SIRIUS 3RT Series) Failure Rate Data has been calculated in accordance with IEC 62061 Par. 6.7.8.2.1 Note 2 [1]. See attachment 3 of the SSDVR for more detail.

Fig. A.1. Silver Summary Report for 064FZ-0567 LL

Project Name LNG Plant A

Unit / Process Area 6400 - Wastewater

SIF Tag 064FZ-0568 LL

SIF Description On Low Low flow from discharge of Water Disposal Pump 0P-6429B as detected by 064FZ-0568, trip Water Disposal Pump via 064UZR-6701.

SIF Reference SILver: RE01, RE05, RE15, RE31, RE43, RE53, RE57, RE59, RE60, RE61, RE62, RE78, RE101, RE102

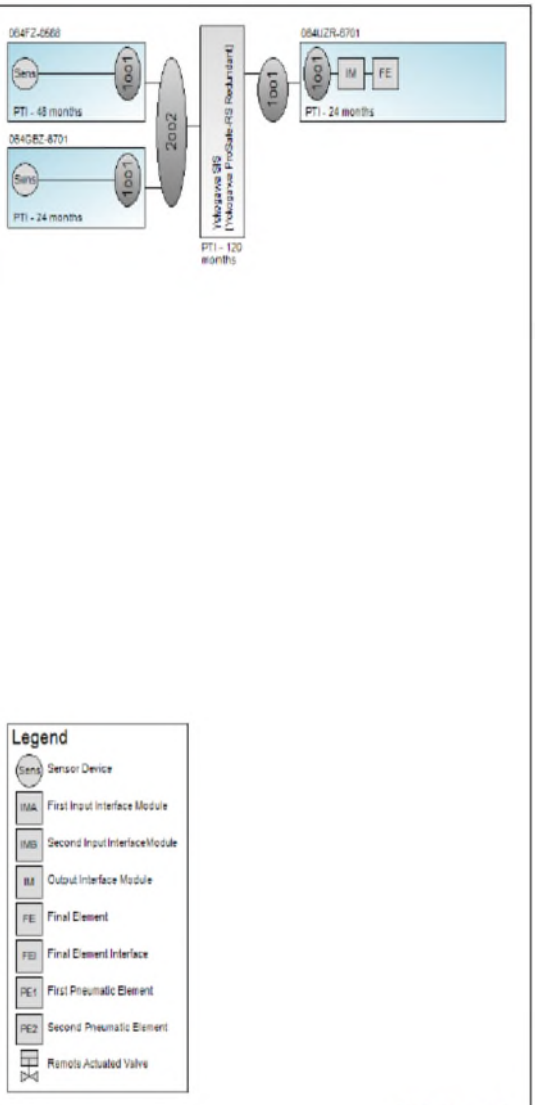
Responsible PH

Analysis Date 25 Jun 2017

Mission Time 15 years

Safety Instrumented Function Performance	
Target SIL	**1**
Target RRF	**10**
Achieved SIL	**1**
PFDavg	1.42E-02
SIL (PFDavg)	1
SIL (Arch. Constraints IEC 61508:2000)	1
SIL (Systematic Capability)	-
Achieved RRF	70
MTTFS (years)	84.75

	PFDavg	MTTFS	SILac
Sensor Part	1.27E-02	4251.57	1
Logic Solver Part	3.95E-04	297.12	3
Final Element Part	1.18E-03	121.98	3



Remarks: The SIF operates in Low demand mode.

Field Equipment MCI: 2 – Good repair – 90% Logic Solver MCI: 2 – Good repair – 90%.

Asset gap of 2 being accepted in asset scenarios therefore target is SIL 1 for 064FZ-0567 LL, 064FZ-0568 LL, 064FZ-0602 LL & 064FZ-0603 LL. In Safety scenario IPLs 064FC-0561, 064FC-0563, 064FC-0600 & 064FC-0601 are claimed as PCS1 therefore target is SIL1 for 064FZ-0567 LL, 064FZ-0568 LL, 064FZ-0602 LL & 064FZ-0603 LL.

1) Sensor Element:

a) External comparison with 064FC-0563 is implemented to meet SIL 1 architectectural constraint.

b) The failure rate data for the impulse line has been doubled because there are two tapping points.

c) Running feedback signal 064GBZ-6701 has been modelled utilising the failure rate data for the MCC Motor Contactor - Siemens (SIRIUS 3RT Series) in 064UZR-6701.

2) Final Element:

a) User defined PFD data utilised to model the Safety Relay, DTT (Phoenix PSR-SCP-24DC/FSP/1X1/1X2). See attachment 2 of the SSDVR for failure rate data.

b) MCC Contactor, DTT (Siemens SIRIUS 3RT Series) Failure Rate Data has been calculated in accordance with IEC 62061 Par. 6.7.8.2.1 Note 2 [1]. See attachment 3 of the SSDVR for more detail.

Fig. A.2. Silver Summary Report for 064FZ-568 LL

Project Name LNG Plant A

Unit / Process Area 6400 - Wastewater

SIF Tag 064FZ-0602 LL

SIF Description On Low Low flow from discharge of Water Disposal Pump 0P-6429C as detected by 064FZ-0602, trip Water Disposal Pump via 064UZR-6801.

SIF Reference SILver: RE01, RE06, RE16, RE32, RE44, RE53, RE57, RE59, RE60, RE61, RE62, RE79, RE101, RE102

Responsible PH

Analysis Date 25 Jun 2017

Mission Time 15 years

Safety Instrumented Function Performance	
Target SIL	**1**
Target RRF	**10**
Achieved SIL	**1**
PFDavg	1.42E-02
SIL (PFDavg)	1
SIL (Arch. Constraints IEC 61508:2000)	1
SIL (Systematic Capability)	-
Achieved RRF	70
MTTFS (years)	84.75

	PFDavg	MTTFS	SILac
Sensor Part	1.27E-02	4251.57	1
Logic Solver Part	3.95E-04	297.12	3
Final Element Part	1.18E-03	121.98	3

Remarks: The SIF operates in Low demand mode.

Field Equipment MCI: 2 – Good repair – 90% Logic Solver MCI: 2 – Good repair – 90%.

Asset gap of 2 being accepted in asset scenarios therefore target is SIL 1 for 064FZ-0567 LL, 064FZ-0568 LL, 064FZ-0602 LL & 064FZ-0603 LL. In Safety scenario IPLs 064FC-0561, 064FC-0563, 064FC-0600 & 064FC-0601 are claimed as PCS1 therefore target is SIL1 for 064FZ-0567 LL, 064FZ-0568 LL, 064FZ-0602 LL & 064FZ-0603 LL.

1) Sensor Element:

a) External comparison with 064FC-0600 is implemented to meet SIL 1 architectectural constraint.

b) The failure rate data for the impulse line has been doubled because there are two tapping points.

c) Running feedback signal 064GBZ-6801 has been modelled utilising the failure rate data for the MCC Motor Contactor - Siemens (SIRIUS 3RT Series) in 064UZR-6801.

2) Final Element:

a) User defined PFD data utilised to model the Safety Relay, DTT (Phoenix PSR-SCP-24DC/FSP/1X1/1X2). See attachment 2 of the SSDVR for failure rate data.

b) MCC Contactor, DTT (Siemens SIRIUS 3RT Series) Failure Rate Data has been calculated in accordance with IEC 62061 Par. 6.7.8.2.1 Note 2 [1]. See attachment 3 of the SSDVR for more detail.

Fig. A.3. Silver Summary Report for 064FZ-0602 LL

Project Name LNG Plant A

Unit / Process Area 6400 - Wastewater

SIF Tag 064FZ-0603 LL

SIF Description On Low Low flow from discharge of Water Disposal Pump 0P-6429D as detected by 064FZ-0603, trip Water Disposal Pump via 064UZR-6901.

SIF Reference SILver: RE01, RE06, RE17, RE33, RE45, RE53, RE57, RE59, RE60, RE61, RE62, RE80, RE101, RE102

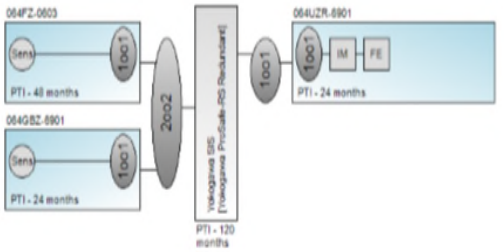
Responsible PH

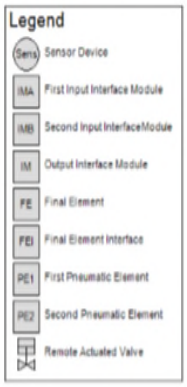
Analysis Date 25 Jun 2017

Mission Time 15 years

Safety Instrumented Function Performance	
Target SIL	**1**
Target RRF	**10**
Achieved SIL	**1**
PFDavg	1.42E-02
SIL (PFDavg)	1
SIL (Arch. Constraints IEC 61508:2000)	1
SIL (Systematic Capability)	-
Achieved RRF	70
MTTFS (years)	84.75

	PFDavg	MTTFS	SILac
Sensor Part	1.27E-02	4251.57	1
Logic Solver Part	3.95E-04	297.12	3
Final Element Part	1.18E-03	121.98	3





Remarks: The SIF operates in Low demand mode.

Field Equipment MCI: 2 – Good repair – 90% Logic Solver MCI: 2 – Good repair – 90%.

Asset gap of 2 being accepted in asset scenarios therefore target is SIL 1 for 064FZ-0567 LL, 064FZ-0568 LL, 064FZ-0602 LL & 064FZ-0603 LL. In Safety scenario IPLs 064FC-0561, 064FC-0563, 064FC-0600 & 064FC-0601 are claimed as PCS1 therefore target is SIL1 for 064FZ-0567 LL, 064FZ-0568 LL, 064FZ-0602 LL & 064FZ-0603 LL.

1) Sensor Element:

a) External comparison with 064FC-0601 is implemented to meet SIL 1 architectectural constraint.

b) The failure rate data for the impulse line has been doubled because there are two tapping points.

c) Running feedback signal 064GBZ-6901 has been modelled utilising the failure rate data for the MCC Motor Contactor - Siemens (SIRIUS 3RT Series) in 064UZR-6901.

2) Final Element:

a) User defined PFD data utilised to model the Safety Relay, DTT (Phoenix PSR-SCP-24DC/FSP/1X1/1X2). See attachment 2 of the SSDVR for failure rate data.

b) MCC Contactor, DTT (Siemens SIRIUS 3RT Series) Failure Rate Data has been calculated in accordance with IEC 62061 Par. 6.7.8.2.1 Note 2 [1]. See attachment 3 of the SSDVR for more detail.

Fig. A.4. Silver Summary Report for 064FZ-0603 LL

Project Name	LNG Plant A
Unit / Process Area	6400 - Wastewater
SIF Tag	064FZ-0821 LL
SIF Description	On Low Low flow from discharge of Membrane Filtrate Pumps 0A-6430-P3A/B as detected by 064FZ-0821, trip both pumps via 064UZR-7901/2.
SIF Reference	SILver: RE02, RE09, RE18, RE36, RE37, RE46, RE58, RE59, RE81, RE82, RE101, RE102, RE104, RE77
Responsible	PH, CST
Analysis Date	25 Jun 2017
Mission Time	15 years

Safety Instrumented Function Performance	
Target SIL	**1**
Target RRF	**10**
Achieved SIL	**1**
PFDavg	3.96E-02
SIL (PFDavg)	1
SIL (Arch. Constraints IEC 61508:2000)	1
SIL (Systematic Capability)	-
Achieved RRF	25
MTTFS (years)	225.47

	PFDavg	MTTFS	SILac
Sensor Part	3.70E-02	2178.57	1
Logic Solver Part	3.95E-04	293.27	3
Final Element Part	2.32E-03	1765.83	3

Remarks: The SIF operates in Low demand mode.

Field Equipment MCI: 2 – Good repair – 90% Logic Solver MCI: 2 – Good repair – 90%.

1) Sensor Element:

a) Data sheet indicates transmitter is Yokogawa ADMAG AXF series. No FMEDA or certification found, so generic device used in SIF model.

b) In absence of a Safety Manual and that the only real verification check is a zero check, the Proof Test Coverage for the AXF series transmitter has been set to 25%.

2) Final Element:

a) User defined PFD data utilised to model the Safety Relay, DTT (Phoenix PSR-SCP-24DC/ESP4/2X1/1X2). See attachment 5 of the SSDVR for failure rate data.

b) MCC Contactor, DTT (Siemens SIRIUS 3RT Series) Failure Rate Data has been calculated in accordance with IEC 62061 Par. 6.7.8.2.1 Note 2 [1]. See attachment 3 of the SSDVR for more detail.

Fig. A.5. Silver Summary Report for 064FZ-0821 LL

Project Name LNG Plant A

Unit / Process Area 6400 - Wastewater

SIF Tag 064FZ-0831 LL

SIF Description On Low Low discharge flow from Membrane Recirc Pumps 0A-6430-P2A/B as detected by 064FZ-0831, trip both pumps via 064UZR-9201/2.

SIF Reference SILver: RE02, RE11, RE19, RE38, RE39, RE46, RE58, RE59, RE83, RE84, RE90, RE101, RE102, RE103, RE77

Responsible PH

Analysis Date 25 Jun 2017

Mission Time 15 years

Safety Instrumented Function Performance	
Target SIL	**1**
Target RRF	**10**
Achieved SIL	**1**
PFDavg	3.96E-02
SIL (PFDavg)	1
SIL (Arch. Constraints IEC 61508:2000)	1
SIL (Systematic Capability)	-
Achieved RRF	25
MTTFS (years)	225.47

	PFDavg	MTTFS	SILac
Sensor Part	3.70E-02	2178.57	1
Logic Solver Part	3.95E-04	293.27	3
Final Element Part	2.32E-03	1765.83	3

Remarks: The SIF operates in Low demand mode.

Field Equipment MCI: 2 – Good repair – 90% Logic Solver MCI: 2 – Good repair – 90%.

1) Sensor Element:

a) Data sheet indicates transmitter is Yokogawa ADMAG AXF series. No FMEDA or certification found, so generic device used in SIF model.

b) In absence of a Safety Manual and that the only real verification check is a zero check, the Proof Test Coverage for the AXF series transmitter has been set to 25%.

2) Final Element:

a) User defined PFD data utilised to model the Safety Relay, DTT (Phoenix PSR-SCP-24DC/ESP4/2X1/1X2). See attachment 5 of the SSDVR for failure rate data.

b) MCC Contactor, DTT (Siemens SIRIUS 3RT Series) Failure Rate Data has been calculated in accordance with IEC 62061 Par. 6.7.8.2.1 Note 2 [1]. See attachment 3 of the SSDVR for more detail.

Fig. A.6. Silver Summary Report for 064FZ-0831 LL

Project Name LNG Plant A

Unit / Process Area 6400 - Wastewater

SIF Tag 064FZ-0852 LL

SIF Description On Low Low discharge flow from Membrane Backwash Pumps 0A-6430-P4A/B as detected by 064FZ-0852, trip both pumps via 064UZR-7801/2.

SIF Reference SILver: RE02, RE12, RE20, RE34, RE35, RE46, RE58, RE59, RE85, RE86, RE90, RE101, RE102, RE77, RE105

Responsible PH

Analysis Date 25 Jun 2017

Mission Time 15 years

Safety Instrumented Function Performance	
Target SIL	**1**
Target RRF	**10**
Achieved SIL	**1**
PFDavg	3.96E-02
SIL (PFDavg)	1
SIL (Arch. Constraints IEC 61508:2000)	1
SIL (Systematic Capability)	-
Achieved RRF	25
MTTFS (years)	225.47

	PFDavg	MTTFS	SILac
Sensor Part	3.70E-02	2178.57	1
Logic Solver Part	3.95E-04	293.27	3
Final Element Part	2.32E-03	1765.83	3

Remarks: The SIF operates in Low demand mode.

Field Equipment MCI: 2 – Good repair – 90% Logic Solver MCI: 2 – Good repair – 90%.

1) Sensor Element:

a) Data sheet indicates transmitter is Yokogawa ADMAG AXF series. No FMEDA or certification found, so generic device used in SIF model.

b) In absence of a Safety Manual and that the only real verification check is a zero check, the Proof Test Coverage for the AXF series transmitter has been set to 25%.

2) Final Element:

a) User defined PFD data utilised to model the Safety Relay, DTT (Phoenix PSR-SCP-24DC/ESP4/2X1/1X2). See attachment 5 of the SSDVR for failure rate data.

b) MCC Contactor, DTT (Siemens SIRIUS 3RT Series) Failure Rate Data has been calculated in accordance with IEC 62061 Par. 6.7.8.2.1 Note 2 [1]. See attachment 3 of the SSDVR for more detail.

Fig. A.7. Silver Summary Report for 064FZ-0852 LL

Project Name LNG Plant A

Unit / Process Area 6400 - Wastewater

SIF Tag 064LZ-0011 LL

SIF Description On Low Low level in 0T-6405 as detected by 064LZ-0011, trip Slop Oil Pump 0P-6401 via 064UZR-0201 & close 064UZV-0202.

SIF Reference SILver: RE70, RE63, RE71, RE72, RE69, RE66, RE67, RE68, RE73, RE74, RE75, RE97, RE98, RE99, RE100, RE101, RE102

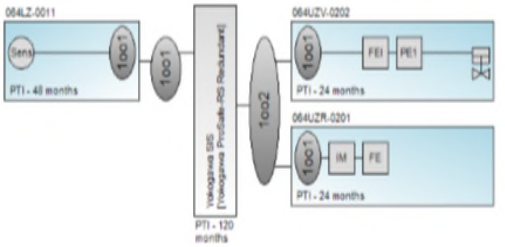
Responsible

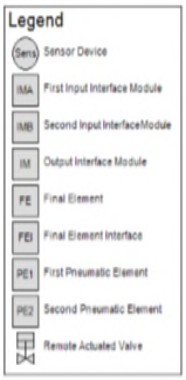
Analysis Date 25 Jun 2017

Mission Time 15 years

Safety Instrumented Function Performance	
Target SIL	**1**
Target RRF	**10**
Achieved SIL	**2**
PFDavg	4.48E-03
SIL (PFDavg)	2
SIL (Arch. Constraints IEC 61508:2000)	2
SIL (Systematic Capability)	-
Achieved RRF	223
MTTFS (years)	38.19

	PFDavg	MTTFS	SILac
Sensor Part	4.05E-03	111.82	2
Logic Solver Part	3.49E-04	378.33	3
Final Element Part	7.87E-05	68.49	4





Remarks: The SIF operates in Low demand mode.

Field Equipment MCI: 2 – Good repair – 90% Logic Solver MCI: 2 – Good repair – 90%.

1) Sensor Element:

a) As per G1-TE-J-0000-SPC0061 section 5.11 - A PTC of 50% is specified for the Rosemount 5300 Radar Level Transmitter.

2) Final Element:

a) 064UZR-0201 - User defined PFD data utilised to model the Safety Relay, DTT (Phoenix PSR-SCP-24DC/FSP/1X1/1X2). See attachment 2 of the SSDVR for failure rate data.

b) 064UZR-0201 - MCC Contactor, DTT (ABB Axx-30 Series) Failure Rate Data has been calculated in accordance with IEC 62061 Par. 6.7.8.2.1 Note 2 [1]. See attachment 4 of the SSDVR for more detail.

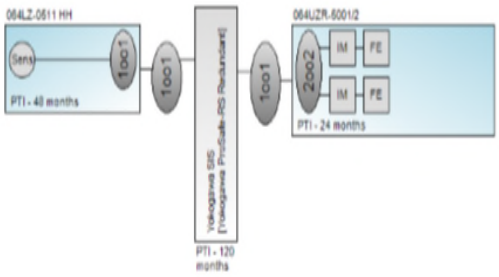
c) 064UZV-0202 - Modelled utilising exida SERH data for Cameron Type 31 ball valves in SIL calculations instead of the TUV certificate values for Cameron B and BT series ball valves.

d) 064UZV-0202 - Bifold VBP volume booster useful life is 10 to 15 years based on clean air and an ambient temperature average of 40 deg. C. as per Exida FMEDA report BIF 09/10-25 R001, Version V1, Revision R1.

e) 064UZV-0202 -Asco Solenoid valve series 327 useful life is approximately 10 years as per Exida IEC 61508 Function Safety Assessment report ASC 09-04-59 R003 V1 R3 61508 Assessment, Version V1, Revision R3.

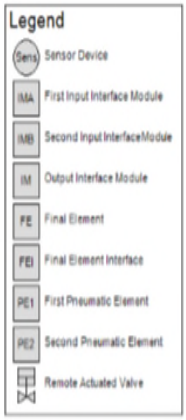
Fig. A.8. Silver Summary Report for 064LZ-0011 LL

Project Name	LNG Plant A
Unit / Process Area	6400 - Wastewater
SIF Tag	064LZ-0511 HH
SIF Description	On High High level in Flow Equalisation Tank 0T-6413 as detected by 064LZ-0511, trip both Construction Village Lift Station Transfer Pumps 0A-6431-P2A/B via 064UZR-5001/2.
SIF Reference	SILver: RE01, RE03, RE07, RE21, RE26, RE27, RE47, RE54, RE55, RE57, RE60, RE61, RE62, RE89, RE101, RE102, RE106
Responsible	PH
Analysis Date	25 Jun 2017
Mission Time	15 years



Safety Instrumented Function Performance	
Target SIL	**1**
Target RRF	**10**
Achieved SIL	**1**
PFDavg	2.44E-02
SIL (PFDavg)	1
SIL (Arch. Constraints IEC 61508:2000)	1
SIL (Systematic Capability)	-
Achieved RRF	41
MTTFS (years)	117.09

	PFDavg	MTTFS	SILac
Sensor Part	2.92E-03	249.98	1
Logic Solver Part	3.49E-04	378.33	3
Final Element Part	2.12E-02	527.15	2



Remarks: The SIF operates in Low demand mode.

Field Equipment MCI: 2 – Good repair – 90% Logic Solver MCI: 2 – Good repair – 90%.

1) Sensor Element:

a) Sensor process connection selected as per exida Assessment EJX Report: YEC 11/10-046 R004 - Adder for EJX Transmitter Differential Remote Seals, Normal Service, High Trip Application, Bolt-on Construction.

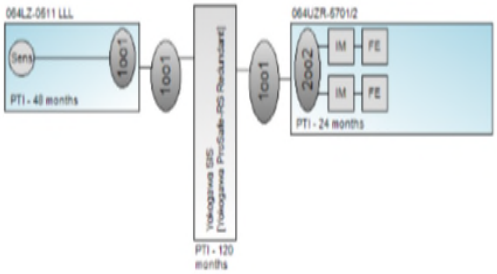
2) Final Element:

a) User defined PFD data utilised to model the Safety Relay, DTT (Phoenix PSR-SCP-24DC/FSP/1X1/1X2). See attachment 2 of the SSDVR for failure rate data.

b) Contactor is manufacturer/model Sprecher and Shuh/CA6-140-EI. As no failure rate data is available in the SERH data base for this model it is modelled as a Generic MCC Interrupt Function (10-100HP) based on motor size 94HP (70kW).

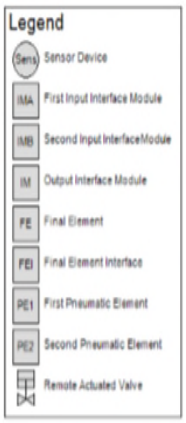
Fig. A.9. Silver Summary Report for 064LZ-0511 HH

Project Name	LNG Plant A
Unit / Process Area	6400 - Wastewater
SIF Tag	064LZ-0511 LLL
SIF Description	On Low Low Low level in Flow Equalisation Tank 0T-6413 as detected by 064LZ-0511, trip both Wastewater Transfer Pumps 0P-6426A/B via 064UZR-5701/2.
SIF Reference	SILver: RE01, RE03, RE04, RE21, RE28, RE29, RE47, RE56, RE57, RE60, RE61, RE62, RE91, RE92, RE59, RE101, RE102
Responsible	PH
Analysis Date	25 Jun 2017
Mission Time	15 years



Safety Instrumented Function Performance	
Target SIL	**1**
Target RRF	**10**
Achieved SIL	**1**
PFDavg	5.34E-03
SIL (PFDavg)	2
SIL (Arch. Constraints IEC 61508:2000)	1
SIL (Systematic Capability)	-
Achieved RRF	187
MTTFS (years)	136.38

	PFDavg	MTTFS	SILac
Sensor Part	2.73E-03	245.64	1
Logic Solver Part	3.49E-04	378.33	3
Final Element Part	2.27E-03	1617.88	3



Remarks: The SIF operates in Low demand mode.

Field Equipment MCI: 2 – Good repair – 90% Logic Solver MCI: 2 – Good repair – 90%.

1) Sensor Element:

a) Sensor process connection selected as per exida Assessment EJX Report: YEC 11/10-046 R004 - Adder for EJX Transmitter Differential Remote Seals, Normal Service, Low Trip Application, Bolt-on Construction.

2) Final Element:

a) User defined PFD data utilised to model the Safety Relay, DTT (Phoenix PSR-SCP-24DC/FSP/1X1/1X2). See attachment 2 of the SSDVR for failure rate data.

b) MCC Contactor, DTT (Siemens SIRIUS 3RT Series) Failure Rate Data has been calculated in accordance with IEC 62061 Par. 6.7.8.2.1 Note 2 [1]. See attachment 3 of the SSDVR for more detail.

Fig. A.10. Silver Summary Report for 064LZ-0511 LLL

Project Name LNG Plant A
Unit / Process Area 6400 - Wastewater

SIF Tag 064LZ-0541 LL

SIF Description On Low Low level in Construction Village Lift Station 0A-6431 as detected by 064LZ-0541, trip both Construction Village Lift Station Transfer Pumps 0A-6431-P2A/B via 064UZR-5001/2.

SIF Reference SILver: RE01, RE07, RE26, RE27, RE48, RE54, RE55, RE57, RE89, RE96, RE101, RE102

Responsible PH
Analysis Date 25 Jun 2017
Mission Time 15 years

Safety Instrumented Function Performance	
Target SIL	**1**
Target RRF	**10**
Achieved SIL	**1**
PFDavg	6.12E-02
SIL (PFDavg)	1
SIL (Arch. Constraints IEC 61508:2000)	2
SIL (Systematic Capability)	-
Achieved RRF	16
MTTFS (years)	36.84

	PFDavg	MTTFS	SILac
Sensor Part	4.06E-02	44.07	2
Logic Solver Part	2.43E-04	391	3
Final Element Part	2.12E-02	527.15	2

Remarks: The SIF operates in Low demand mode.

Field Equipment MCI: 2 – Good repair – 90% Logic Solver MCI: 2 – Good repair – 90%.

1) Sensor Element:

a) Datasheet identifies 064LZ-0541 as Flyght model LTU-701, not in exSILentia. No FMEDA data found. Generic level transmitter used instead. APCS SI132-61110 signal isolator is modelled using 'Generic Isolated Switch Amplifier' as device specific failure rate data is not available. Novaris SL36 signal line protector is modelled using 'Generic Intrinsic Safety Barrier' as device specific failure rate data is not available.

2) Final Element:

a) User defined PFD data utilised to model the Safety Relay, DTT (Phoenix PSR-SCP-24DC/FSP/1X1/1X2). See attachment 2 of the SSDVR for failure rate data.

b) Contactor is manufacturer/model Sprecher and Shuh/CA6-140-EI. As no failure rate data is available in the SERH data base for this model it is modelled as a Generic MCC Interrupt Function (10-100HP) based on motor size 94HP (70kW).

Fig. A.11. Silver Summary Report for 064LZ-0541 LL

Project Name LNG Plant A

Unit / Process Area 6400 - Wastewater

SIF Tag 064LZ-0712 LL

SIF Description On Low Low level in Post-Anoxic Tank 0A-6430-T3 as detected by 064LZ-0712, trip both Membrane Recirculation Pumps 0A-6430-P2A/B via 064UZR-9201/2.

SIF Reference SILver: RE02, RE08, RE11, RE22, RE38, RE39, RE50, RE58, RE59, RE60, RE61, RE62, RE83, RE84, RE90, RE77, RE101, RE102, RE103

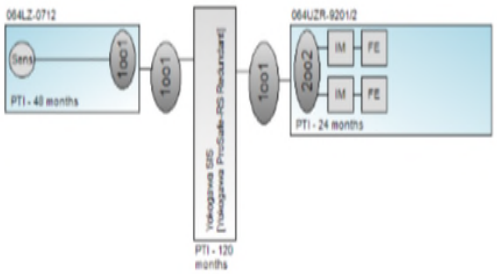
Responsible PH

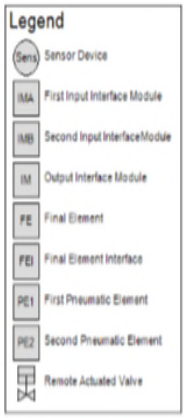
Analysis Date 25 Jun 2017

Mission Time 15 years

Safety Instrumented Function Performance	
Target SIL	**2**
Target RRF	**100**
Achieved SIL	**2**
PFDavg	3.76E-03
SIL (PFDavg)	2
SIL (Arch. Constraints IEC 61508:2000)	2
SIL (Systematic Capability)	-
Achieved RRF	266
MTTFS (years)	137.23

	PFDavg	MTTFS	SILac
Sensor Part	1.10E-03	245.24	2
Logic Solver Part	3.49E-04	378.33	3
Final Element Part	2.32E-03	1765.83	3





Remarks: The SIF operates in Low demand mode.

Field Equipment MCI: 2 – Good repair – 90% Logic Solver MCI: 2 – Good repair – 90%.

1) Sensor Element:

a) Sensor process connection selected as per exida Assessment EJX Report: YEC 11/10-046 R004 - Adder for EJX Transmitter Differential Remote Seals, Normal Service, Low Trip Application, Bolt-on Construction.

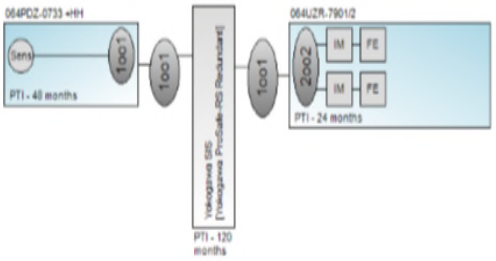
2) Final Element:

a) User defined PFD data utilised to model the Safety Relay, DTT (Phoenix PSR-SCP-24DC/ESP4/2X1/1X2). See attachment 5 of the SSDVR for failure rate data.

b) MCC Contactor, DTT (Siemens SIRIUS 3RT Series) Failure Rate Data has been calculated in accordance with IEC 62061 Par. 6.7.8.2.1 Note 2 [1]. See attachment 3 of the SSDVR for more detail.

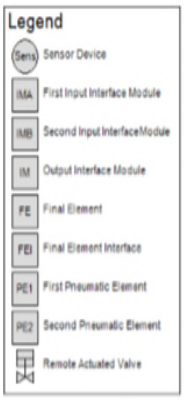
Fig. A.12. Silver Summary Report for 064LZ-0712 LL

Project Name	LNG Plant A
Unit / Process Area	6400 - Wastewater
SIF Tag	064PDZ-0733 +HH
SIF Description	On High High Forward Differential Pressure across Membranes 0A-6430-S1A..N as detected by 064PDZ-0733, trip both Membrane Filtrate Pumps 0A-6430-P3A/B via 064UZR-7901/2.
SIF Reference	SILver: RE02, RE10, RE09, RE23, RE36, RE37, RE49, RE58, RE59, RE60, RE61, RE62, RE81, RE82, RE90, RE77, RE101, RE102, RE104
Responsible	PH
Analysis Date	25 Jun 2017
Mission Time	15 years



Safety Instrumented Function Performance	
Target SIL	**1**
Target RRF	**10**
Achieved SIL	**1**
PFDavg	5.58E-03
SIL (PFDavg)	2
SIL (Arch. Constraints IEC 61508:2000)	1
SIL (Systematic Capability)	-
Achieved RRF	179
MTTFS (years)	138.7

	PFDavg	MTTFS	SILac
Sensor Part	2.92E-03	249.98	1
Logic Solver Part	3.49E-04	378.33	3
Final Element Part	2.32E-03	1765.83	3



Remarks: The SIF operates in Low demand mode.

Field Equipment MCI: 2 – Good repair – 90% Logic Solver MCI: 2 – Good repair – 90%.

1) Sensor Element:

a) Sensor process connection selected as per exida Assessment EJX Report: YEC 11/10-046 R004 - Adder for EJX Transmitter Differential Remote Seals, Normal Service, High Trip Application, Bolt-on Construction.

2) Final Element:

a) User defined PFD data utilised to model the Safety Relay, DTT (Phoenix PSR-SCP-24DC/ESP4/2X1/1X2). See attachment 5 of the SSDVR for failure rate data.

b) MCC Contactor, DTT (Siemens SIRIUS 3RT Series) Failure Rate Data has been calculated in accordance with IEC 62061 Par. 6.7.8.2.1 Note 2 [1]. See attachment 3 of the SSDVR for more detail.

Fig. A.13. Silver Summary Report for 064PDZ-0733 +HH

Project Name	LNG Plant A
Unit / Process Area	6400 - Wastewater
SIF Tag	064PDZ-0733 -HH
SIF Description	On High High Reverse Differential Pressure across Membranes 0A-6430-S1A..N as detected by 064PDZ-0733, both trip Membrane Backwash Pumps 0A-6430-P4A/B via 064UZR-7801/2.
SIF Reference	SILver: RE02, RE10, RE12, RE23, RE34, RE35, RE49, RE58, RE59, RE60, RE61, RE62, RE85, RE86, RE90, RE77, RE101, RE102, RE105
Responsible	PH
Analysis Date	25 Jun 2017
Mission Time	15 years

Safety Instrumented Function Performance	
Target SIL	**1**
Target RRF	**10**
Achieved SIL	**1**
PFDavg	5.39E-03
SIL (PFDavg)	2
SIL (Arch. Constraints IEC 61508:2000)	1
SIL (Systematic Capability)	-
Achieved RRF	186
MTTFS (years)	137.35

	PFDavg	MTTFS	SILac
Sensor Part	2.73E-03	245.64	1
Logic Solver Part	3.49E-04	378.33	3
Final Element Part	2.32E-03	1765.83	3

Remarks: The SIF operates in Low demand mode.

Field Equipment MCI: 2 – Good repair – 90% Logic Solver MCI: 2 – Good repair – 90%.

1) Sensor Element:

a) Sensor process connection selected as per exida Assessment EJX Report: YEC 11/10-046 R004 - Adder for EJX Transmitter Differential Remote Seals, Normal Service, Low Trip Application, Bolt-on Construction.

2) Final Element:

a) User defined PFD data utilised to model the Safety Relay, DTT (Phoenix PSR-SCP-24DC/ESP4/2X1/1X2). See attachment 5 of the SSDVR for failure rate data.

b) MCC Contactor, DTT (Siemens SIRIUS 3RT Series) Failure Rate Data has been calculated in accordance with IEC 62061 Par. 6.7.8.2.1 Note 2 [1]. See attachment 3 of the SSDVR for more detail.

Fig. A.14. Silver Summary Report for 064PDZ-0733 -HH

Project Name LNG Plant A

Unit / Process Area 6400 - Wastewater

SIF Tag 064PDZ-0830 HH

SIF Description On High High Differential Pressure across Strainer 064NT-7808 as detected by 064PDZ-0830, trip both Membrane Recirculation Pumps 0A-6430-P2A/B via 064UZR-9201/2.

SIF Reference SILver: RE02, RE11, RE24, RE38, RE39, RE49, RE58, RE59, RE60, RE61, RE62, RE83, RE84, RE90, RE77, RE101, RE102, RE103

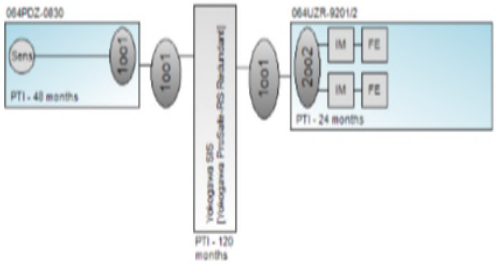
Responsible PH

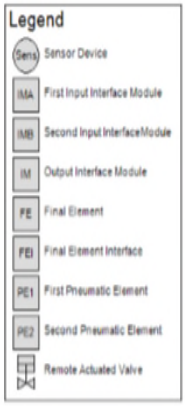
Analysis Date 25 Jun 2017

Mission Time 15 years

Safety Instrumented Function Performance	
Target SIL	**1**
Target RRF	**10**
Achieved SIL	**1**
PFDavg	5.76E-03
SIL (PFDavg)	2
SIL (Arch. Constraints IEC 61508:2000)	1
SIL (Systematic Capability)	-
Achieved RRF	174
MTTFS (years)	138.7

	PFDavg	MTTFS	SILac
Sensor Part	3.10E-03	249.98	1
Logic Solver Part	3.49E-04	378.33	3
Final Element Part	2.32E-03	1765.83	3





Remarks: The SIF operates in Low demand mode.

Field Equipment MCI: 2 – Good repair – 90% Logic Solver MCI: 2 – Good repair – 90%.

1) Sensor Element:

a) Sensor process connection selected as per exida Assessment EJX Report: YEC 11/10-046 R004 - Adder for EJX Transmitter Differential Remote Seals, Normal Service, High Trip Application, Bolt-on Construction.

2) Final Element:

a) User defined PFD data utilised to model the Safety Relay, DTT (Phoenix PSR-SCP-24DC/ESP4/2X1/1X2). See attachment 5 of the SSDVR for failure rate data.

b) MCC Contactor, DTT (Siemens SIRIUS 3RT Series) Failure Rate Data has been calculated in accordance with IEC 62061 Par. 6.7.8.2.1 Note 2 [1]. See attachment 3 of the SSDVR for more detail.

Fig. A.15. Silver Summary Report for 064PDZ-0830 HH

Project Name LNG Plant A

Unit / Process Area 6400 - Wastewater

SIF Tag 064XS-0020

SIF Description Pump not running closes 064UZV-0202, which will prevent reverse flow into 0T-6405

SIF Reference SILver: RE93, RE68, RE66, RE69, RE70, RE63, RE57, RE94, RE95, RE101, RE102

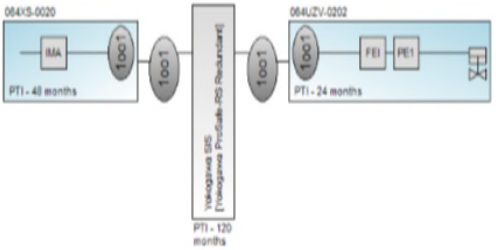
Responsible

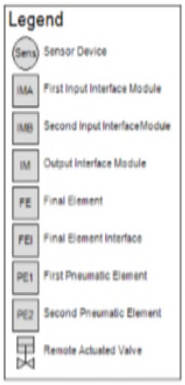
Analysis Date 25 Jun 2017

Mission Time 15 years

Safety Instrumented Function Performance	
Target SIL	**1**
Target RRF	**10**
Achieved SIL	**1**
PFDavg	6.42E-02
SIL (PFDavg)	1
SIL (Arch. Constraints IEC 61508:2000)	2
SIL (Systematic Capability)	-
Achieved RRF	16
MTTFS (years)	59.62

	PFDavg	MTTFS	SILac
Sensor Part	2.50E-02	130.1	2
Logic Solver Part	2.43E-04	394.58	3
Final Element Part	3.99E-02	152.64	2





Remarks: The SIF operates in Low demand mode.

Field Equipment MCI: 2 – Good repair – 90% Logic Solver MCI: 2 – Good repair – 90%.

1) Sensor Element:

a) Contactor auxiliary contact has been modelled utilising generic relay failure rate data over the MCC Contactor, DTT (ABB Axx-30 Series) failure rate data for more conservative approach.

b) Contactor auxiliary contact is a simple device, therefore a PTC of 50% is considered.

2) Final Element:

a) 064UZV-0202 - Modelled utilising exida SERH data for Cameron Type 31 ball valves in SIL calculations instead of the TUV certificate values for Cameron B and BT series ball valves.

b) 064UZV-0202 - Bifold VBP volume booster useful life is 10 to 15 years based on clean air and an ambient temperature average of 40 deg. C. as per Exida FMEDA report BIF 09/10-25 R001, Version V1, Revision R1.

c) 064UZV-0202 -Asco Solenoid valve series 327 useful life is approximately 10 years as per Exida IEC 61508 Function Safety Assessment report ASC 09-04-59 R003 V1 R3 61508 Assessment, Version V1, Revision R3.

Fig. A.16. Silver Summary Report for 064XS-0020

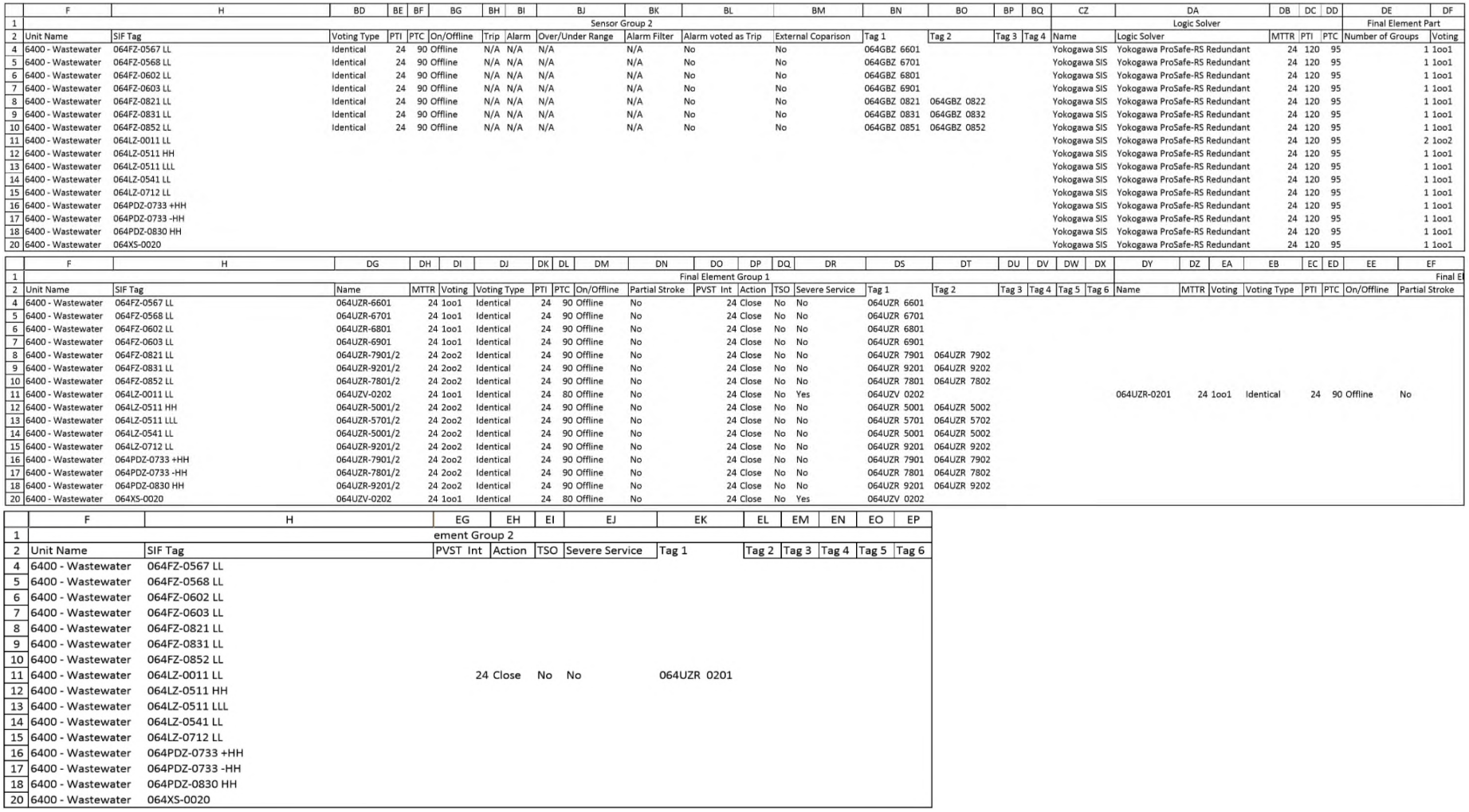
Appendix B: EXSILENTIA SILVER EXCEL EXPORT

	F	H	I	J	K	L	M	N
1			SIF Information					Overall SIF
2	Unit Name	SIF Tag	SIF Description	Required SIL	Required RRF	Achieved SIL	SIL PFDavg	Achieved RRF
4	6400 - Wastewater	064FZ-0567 LL	On Low Low flow from discharge of Water Disposal Pump 0P-6429A as detected by 064FZ-0567, trip Water Disposal Pump 0P-6429A via 064UZR-6601.	1	10	1	1	70
5	6400 - Wastewater	064FZ-0568 LL	On Low Low flow from discharge of Water Disposal Pump 0P-6429B as detected by 064FZ-0568, trip Water Disposal Pump via 064UZR-6701.	1	10	1	1	70
6	6400 - Wastewater	064FZ-0602 LL	On Low Low flow from discharge of Water Disposal Pump 0P-6429C as detected by 064FZ-0602, trip Water Disposal Pump via 064UZR-6801.	1	10	1	1	70
7	6400 - Wastewater	064FZ-0603 LL	On Low Low flow from discharge of Water Disposal Pump 0P-6429D as detected by 064FZ-0603, trip Water Disposal Pump via 064UZR-6901.	1	10	1	1	70
8	6400 - Wastewater	064FZ-0821 LL	On Low Low flow from discharge of Membrane Filtrate Pumps 0A-6430-P3A/B as detected by 064FZ-0821, trip both pumps via 064UZR-7901/2.	1	10	1	1	25
9	6400 - Wastewater	064FZ-0831 LL	On Low Low discharge flow from Membrane Recirc Pumps 0A-6430-P2A/B as detected by 064FZ-0831, trip both pumps via 064UZR-9201/2.	1	10	1	1	25
10	6400 - Wastewater	064FZ-0852 LL	On Low Low discharge flow from Membrane Backwash Pumps 0A-6430-P4A/B as detected by 064FZ-0852, trip both pumps via 064UZR-7801/2.	1	10	1	1	25
11	6400 - Wastewater	064LZ-0011 LL	On Low Low level in 0T-6405 as detected by 064LZ-0011, trip Slop Oil Pump 0P-6401 via 064UZR-0201 & close 064UZV-0202.	1	10	2	2	223
12	6400 - Wastewater	064LZ-0511 HH	On High High level in Flow Equalisation Tank 0T-6413 as detected by 064LZ-0511, trip both Construction Village Lift Station Transfer Pumps 0A-6431-P2A/B via 064UZR-5001/2.	1	10	1	1	41
13	6400 - Wastewater	064LZ-0511 LLL	On Low Low Low level in Flow Equalisation Tank 0T-6413 as detected by 064LZ-0511, trip both Wastewater Transfer Pumps 0P-6426A/B via 064UZR-5701/2.	1	10	1	2	187
14	6400 - Wastewater	064LZ-0541 LL	On Low Low level in Construction Village Lift Station 0A-6431 as detected by 064LZ-0541, trip both Construction Village Lift Station Transfer Pumps 0A-6431-P2A/B via 064UZR-5001/2.	1	10	1	1	16
15	6400 - Wastewater	064LZ-0712 LL	On Low Low level in Post-Anoxic Tank 0A-6430-T3 as detected by 064LZ-0712, trip both Membrane Recirculation Pumps 0A-6430-P2A/B via 064UZR-9201/2.	2	100	2	2	266
16	6400 - Wastewater	064PDZ-0733 +HH	On High High Forward Differential Pressure across Membranes 0A-6430-S1A..N as detected by 064PDZ-0733, trip both Membrane Filtrate Pumps 0A-6430-P3A/B via 064UZR-7901/2.	1	10	1	2	179
17	6400 - Wastewater	064PDZ-0733 -HH	On High High Reverse Differential Pressure across Membranes 0A-6430-S1A..N as detected by 064PDZ-0733, both trip Membrane Backwash Pumps 0A-6430-P4A/B via 064UZR-7801/2.	1	10	1	2	186
18	6400 - Wastewater	064PDZ-0830 HH	On High High Differential Pressure across Strainer 064NT-7808 as detected by 064PDZ-0830, trip both Membrane Recirculation Pumps 0A-6430-P2A/B via 064UZR-9201/2.	1	10	1	2	174
20	6400 - Wastewater	064XS-0020	Pump not running closes 064UZV-0202, which will prevent reverse flow into 0T-6405	1	10	1	1	16

	F	H	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG
1			Results				Part Results												SIF Parameters		
2	Unit Name	SIF Tag	Achieved PFDavg	SIL (Arch. Const.)	SIL Capability	MTTFS (Years)	SE PFDavg	SE MTTFS	SE SILAC	SE SysCap	LS PFDavg	LS MTTFS	LS SILAC	LS SysCap	FE PFDavg	FE MTTFS	FE SILAC	FE SysCap	MIssion Time (Years)	Startup Time (Hrs)	Demand Rate
4	6400 - Wastewater	064FZ-0567 LL	1.42E-02	1	N/A	84.75	1.27E-02	4251.57	1	N/A	3.95E-04	297.12	3	N/A	1.18E-03	121.98	3	N/A	15	24	Low Demand
5	6400 - Wastewater	064FZ-0568 LL	1.42E-02	1	N/A	84.75	1.27E-02	4251.57	1	N/A	3.95E-04	297.12	3	N/A	1.18E-03	121.98	3	N/A	15	24	Low Demand
6	6400 - Wastewater	064FZ-0602 LL	1.42E-02	1	N/A	84.75	1.27E-02	4251.57	1	N/A	3.95E-04	297.12	3	N/A	1.18E-03	121.98	3	N/A	15	24	Low Demand
7	6400 - Wastewater	064FZ-0603 LL	1.42E-02	1	N/A	84.75	1.27E-02	4251.57	1	N/A	3.95E-04	297.12	3	N/A	1.18E-03	121.98	3	N/A	15	24	Low Demand
8	6400 - Wastewater	064FZ-0821 LL	3.96E-02	1	N/A	225.47	3.70E-02	2178.57	1	N/A	3.95E-04	293.27	3	N/A	2.32E-03	1765.83	3	N/A	15	24	Low Demand
9	6400 - Wastewater	064FZ-0831 LL	3.96E-02	1	N/A	225.47	3.70E-02	2178.57	1	N/A	3.95E-04	293.27	3	N/A	2.32E-03	1765.83	3	N/A	15	24	Low Demand
10	6400 - Wastewater	064FZ-0852 LL	3.96E-02	1	N/A	225.47	3.70E-02	2178.57	1	N/A	3.95E-04	293.27	3	N/A	2.32E-03	1765.83	3	N/A	15	24	Low Demand
11	6400 - Wastewater	064LZ-0011 LL	4.48E-03	2	N/A	38.19	4.05E-03	111.82	2	N/A	3.49E-04	378.33	3	N/A	7.87E-05	68.49	4	N/A	15	24	Low Demand
12	6400 - Wastewater	064LZ-0511 HH	2.44E-02	1	N/A	117.09	2.92E-03	249.98	1	N/A	3.49E-04	378.33	3	N/A	2.12E-02	527.15	2	N/A	15	24	Low Demand
13	6400 - Wastewater	064LZ-0511 LLL	5.34E-03	1	N/A	136.38	2.73E-03	245.64	1	N/A	3.49E-04	378.33	3	N/A	2.27E-03	1617.88	3	N/A	15	24	Low Demand
14	6400 - Wastewater	064LZ-0541 LL	6.12E-02	2	N/A	36.84	4.06E-02	44.07	2	N/A	2.43E-04	391	3	N/A	2.12E-02	527.15	2	N/A	15	24	Low Demand
15	6400 - Wastewater	064LZ-0712 LL	3.76E-03	2	N/A	137.23	1.10E-03	245.24	2	N/A	3.49E-04	378.33	3	N/A	2.32E-03	1765.83	3	N/A	15	24	Low Demand
16	6400 - Wastewater	064PDZ-0733 +HH	5.58E-03	1	N/A	138.7	2.92E-03	249.98	1	N/A	3.49E-04	378.33	3	N/A	2.32E-03	1765.83	3	N/A	15	24	Low Demand
17	6400 - Wastewater	064PDZ-0733 -HH	5.39E-03	1	N/A	137.35	2.73E-03	245.64	1	N/A	3.49E-04	378.33	3	N/A	2.32E-03	1765.83	3	N/A	15	24	Low Demand
18	6400 - Wastewater	064PDZ-0830 HH	5.76E-03	1	N/A	138.7	3.10E-03	249.98	1	N/A	3.49E-04	378.33	3	N/A	2.32E-03	1765.83	3	N/A	15	24	Low Demand
20	6400 - Wastewater	064XS-0020	6.42E-02	2	N/A	59.62	2.50E-02	130.1	2	N/A	2.43E-04	394.58	3	N/A	3.99E-02	152.64	2	N/A	15	24	Low Demand

	F	H	AH	AI	AJ	AK	AL	AM	AN	AO	AP	AQ	AR	AS	AT	AU	AV	AW	AX	AY	AZ	BA	BB	BC
1			Sensor Part		Sensor Group 1																			
2	Unit Name	SIF Tag	Number of Groups	Voting	Name	MTTR	Voting	Voting Type	PTI	PTC	On/Offline	Trip	Alarm	Over/Under Range	Alarm Filter	Alarm voted as Trip	External Coparison	Tag 1	Tag 2	Tag 3	Tag 4	Name	MTTR	Voting
4	6400 - Wastewater	064FZ-0567 LL	2	2oo2	064FZ-0567	24	1oo1	Identical	48	25	Online	Low	Under	On	Off	Yes	Yes	064FZ 0567				064GBZ-6601	24	1oo1
5	6400 - Wastewater	064FZ-0568 LL	2	2oo2	064FZ-0568	24	1oo1	Identical	48	25	Online	Low	Under	On	Off	Yes	Yes	064FZ 0568				064GBZ-6701	24	1oo1
6	6400 - Wastewater	064FZ-0602 LL	2	2oo2	064FZ-0602	24	1oo1	Identical	48	25	Online	Low	Under	On	Off	Yes	Yes	064FZ 0602				064GBZ-6801	24	1oo1
7	6400 - Wastewater	064FZ-0603 LL	2	2oo2	064FZ-0603	24	1oo1	Identical	48	25	Online	Low	Under	On	Off	Yes	Yes	064FZ 0603				064GBZ-6901	24	1oo1
8	6400 - Wastewater	064FZ-0821 LL	2	2oo2	064FZ-0821	24	1oo1	Identical	48	25	Online	Low	Under	On	Off	Yes	No	064FZ 0821				064GBZ-0821/2	24	1oo2
9	6400 - Wastewater	064FZ-0831 LL	2	2oo2	064FZ-0831	24	1oo1	Identical	48	25	Online	Low	Under	On	Off	Yes	No	064FZ 0831				064GBZ-0831/2	24	1oo2
10	6400 - Wastewater	064FZ-0852 LL	2	2oo2	064FZ-0852	24	1oo1	Identical	48	25	Online	Low	Under	On	Off	Yes	No	064FZ 0852				064GBZ-0851/2	24	1oo2
11	6400 - Wastewater	064LZ-0011 LL	1	1oo1	064LZ-0011	24	1oo1	Identical	48	50	Online	Low	Under	On	Off	Yes	No	064LZ 0011						
12	6400 - Wastewater	064LZ-0511 HH	1	1oo1	064LZ-0511 HH	24	1oo1	Identical	48	90	Online	High	Under	On	Off	Yes	No	064LZ 0511						
13	6400 - Wastewater	064LZ-0511 LLL	1	1oo1	064LZ-0511 LLL	24	1oo1	Identical	48	90	Online	Low	Under	On	Off	Yes	No	064LZ 0511						
14	6400 - Wastewater	064LZ-0541 LL	1	1oo1	064LZ-0541	24	1oo1	Identical	48	90	Online	N/A	N/A	N/A	N/A	Yes	No	064LZ 0541						
15	6400 - Wastewater	064LZ-0712 LL	1	1oo1	064LZ-0712	24	1oo1	Identical	48	90	Online	Low	Under	On	Off	Yes	Yes	064LZ 0712						
16	6400 - Wastewater	064PDZ-0733 +HH	1	1oo1	064PDZ-0733 +HH	24	1oo1	Identical	48	90	Online	High	Under	On	Off	Yes	No	064PDZ 0733						
17	6400 - Wastewater	064PDZ-0733 -HH	1	1oo1	064PDZ-0733 -HH	24	1oo1	Identical	48	90	Online	Low	Under	On	Off	Yes	No	064PDZ 0733						
18	6400 - Wastewater	064PDZ-0830 HH	1	1oo1	064PDZ-0830	24	1oo1	Identical	48	90	Online	High	Over	On	Off	Yes	No	064PDZ 0830						
20	6400 - Wastewater	064XS-0020	1	1oo1	064XS-0020	24	1oo1	Identical	48	50	Offline	N/A	N/A	N/A	N/A	No	No	064XS 0020						

Fig. B.1. exSILentia SILVer Report



	F	H	BD	BE	BF	BG	BH	BI	BJ	BK	BL	BM	BN	BO	BP	BQ	CZ	DA	DB	DC	DD	DE	DF
1			Sensor Group 2															Logic Solver				Final Element Part	
2	Unit Name	SIF Tag	Voting Type	PTI	PTC	On/Offline	Trip	Alarm	Over/Under Range	Alarm Filter	Alarm voted as Trip	External Coparison	Tag 1	Tag 2	Tag 3	Tag 4	Name	Logic Solver	MTTR	PTI	PTC	Number of Groups	Voting
4	6400 - Wastewater	064FZ-0567 LL	Identical	24	90	Offline	N/A	N/A	N/A	N/A	No	No	064GBZ 6601				Yokogawa SIS	Yokogawa ProSafe-RS Redundant	24	120	95	1	1oo1
5	6400 - Wastewater	064FZ-0568 LL	Identical	24	90	Offline	N/A	N/A	N/A	N/A	No	No	064GBZ 6701				Yokogawa SIS	Yokogawa ProSafe-RS Redundant	24	120	95	1	1oo1
6	6400 - Wastewater	064FZ-0602 LL	Identical	24	90	Offline	N/A	N/A	N/A	N/A	No	No	064GBZ 6801				Yokogawa SIS	Yokogawa ProSafe-RS Redundant	24	120	95	1	1oo1
7	6400 - Wastewater	064FZ-0603 LL	Identical	24	90	Offline	N/A	N/A	N/A	N/A	No	No	064GBZ 6901				Yokogawa SIS	Yokogawa ProSafe-RS Redundant	24	120	95	1	1oo1
8	6400 - Wastewater	064FZ-0821 LL	Identical	24	90	Offline	N/A	N/A	N/A	N/A	No	No	064GBZ 0821	064GBZ 0822			Yokogawa SIS	Yokogawa ProSafe-RS Redundant	24	120	95	1	1oo1
9	6400 - Wastewater	064FZ-0831 LL	Identical	24	90	Offline	N/A	N/A	N/A	N/A	No	No	064GBZ 0831	064GBZ 0832			Yokogawa SIS	Yokogawa ProSafe-RS Redundant	24	120	95	1	1oo1
10	6400 - Wastewater	064FZ-0852 LL	Identical	24	90	Offline	N/A	N/A	N/A	N/A	No	No	064GBZ 0851	064GBZ 0852			Yokogawa SIS	Yokogawa ProSafe-RS Redundant	24	120	95	1	1oo1
11	6400 - Wastewater	064LZ-0011 LL															Yokogawa SIS	Yokogawa ProSafe-RS Redundant	24	120	95	2	1oo2
12	6400 - Wastewater	064LZ-0511 HH															Yokogawa SIS	Yokogawa ProSafe-RS Redundant	24	120	95	1	1oo1
13	6400 - Wastewater	064LZ-0511 LLL															Yokogawa SIS	Yokogawa ProSafe-RS Redundant	24	120	95	1	1oo1
14	6400 - Wastewater	064LZ-0541 LL															Yokogawa SIS	Yokogawa ProSafe-RS Redundant	24	120	95	1	1oo1
15	6400 - Wastewater	064LZ-0712 LL															Yokogawa SIS	Yokogawa ProSafe-RS Redundant	24	120	95	1	1oo1
16	6400 - Wastewater	064PDZ-0733 +HH															Yokogawa SIS	Yokogawa ProSafe-RS Redundant	24	120	95	1	1oo1
17	6400 - Wastewater	064PDZ-0733 -HH															Yokogawa SIS	Yokogawa ProSafe-RS Redundant	24	120	95	1	1oo1
18	6400 - Wastewater	064PDZ-0830 HH															Yokogawa SIS	Yokogawa ProSafe-RS Redundant	24	120	95	1	1oo1
20	6400 - Wastewater	064XS-0020															Yokogawa SIS	Yokogawa ProSafe-RS Redundant	24	120	95	1	1oo1

	F	H	DG	DH	DI	DJ	DK	DL	DM	DN	DO	DP	DQ	DR	DS	DT	DU	DV	DW	DX	DY	DZ	EA	EB	EC	ED	EE	EF
1			Final Element Group 1																									Final El
2	Unit Name	SIF Tag	Name	MTTR	Voting	Voting Type	PTI	PTC	On/Offline	Partial Stroke	PVST Int	Action	TSO	Severe Service	Tag 1	Tag 2	Tag 3	Tag 4	Tag 5	Tag 6	Name	MTTR	Voting	Voting Type	PTI	PTC	On/Offline	Partial Stroke
4	6400 - Wastewater	064FZ-0567 LL	064UZR-6601	24	1oo1	Identical	24	90	Offline	No	24	Close	No	No	064UZR 6601													
5	6400 - Wastewater	064FZ-0568 LL	064UZR-6701	24	1oo1	Identical	24	90	Offline	No	24	Close	No	No	064UZR 6701													
6	6400 - Wastewater	064FZ-0602 LL	064UZR-6801	24	1oo1	Identical	24	90	Offline	No	24	Close	No	No	064UZR 6801													
7	6400 - Wastewater	064FZ-0603 LL	064UZR-6901	24	1oo1	Identical	24	90	Offline	No	24	Close	No	No	064UZR 6901													
8	6400 - Wastewater	064FZ-0821 LL	064UZR-7901/2	24	2oo2	Identical	24	90	Offline	No	24	Close	No	No	064UZR 7901	064UZR 7902												
9	6400 - Wastewater	064FZ-0831 LL	064UZR-9201/2	24	2oo2	Identical	24	90	Offline	No	24	Close	No	No	064UZR 9201	064UZR 9202												
10	6400 - Wastewater	064FZ-0852 LL	064UZR-7801/2	24	2oo2	Identical	24	90	Offline	No	24	Close	No	No	064UZR 7801	064UZR 7802												
11	6400 - Wastewater	064LZ-0011 LL	064UZV-0202	24	1oo1	Identical	24	80	Offline	No	24	Close	No	Yes	064UZV 0202						064UZR-0201	24	1oo1	Identical	24	90	Offline	No
12	6400 - Wastewater	064LZ-0511 HH	064UZR-5001/2	24	2oo2	Identical	24	90	Offline	No	24	Close	No	No	064UZR 5001	064UZR 5002												
13	6400 - Wastewater	064LZ-0511 LLL	064UZR-5701/2	24	2oo2	Identical	24	90	Offline	No	24	Close	No	No	064UZR 5701	064UZR 5702												
14	6400 - Wastewater	064LZ-0541 LL	064UZR-5001/2	24	2oo2	Identical	24	90	Offline	No	24	Close	No	No	064UZR 5001	064UZR 5002												
15	6400 - Wastewater	064LZ-0712 LL	064UZR-9201/2	24	2oo2	Identical	24	90	Offline	No	24	Close	No	No	064UZR 9201	064UZR 9202												
16	6400 - Wastewater	064PDZ-0733 +HH	064UZR-7901/2	24	2oo2	Identical	24	90	Offline	No	24	Close	No	No	064UZR 7901	064UZR 7902												
17	6400 - Wastewater	064PDZ-0733 -HH	064UZR-7801/2	24	2oo2	Identical	24	90	Offline	No	24	Close	No	No	064UZR 7801	064UZR 7802												
18	6400 - Wastewater	064PDZ-0830 HH	064UZR-9201/2	24	2oo2	Identical	24	90	Offline	No	24	Close	No	No	064UZR 9201	064UZR 9202												
20	6400 - Wastewater	064XS-0020	064UZV-0202	24	1oo1	Identical	24	80	Offline	No	24	Close	No	Yes	064UZV 0202													

	F	H	EG	EH	EI	EJ	EK	EL	EM	EN	EO	EP
1		ement Group 2										
2	Unit Name	SIF Tag	PVST Int	Action	TSO	Severe Service	Tag 1	Tag 2	Tag 3	Tag 4	Tag 5	Tag 6
4	6400 - Wastewater	064FZ-0567 LL										
5	6400 - Wastewater	064FZ-0568 LL										
6	6400 - Wastewater	064FZ-0602 LL										
7	6400 - Wastewater	064FZ-0603 LL										
8	6400 - Wastewater	064FZ-0821 LL										
9	6400 - Wastewater	064FZ-0831 LL										
10	6400 - Wastewater	064FZ-0852 LL										
11	6400 - Wastewater	064LZ-0011 LL	24	Close	No	No	064UZR 0201					
12	6400 - Wastewater	064LZ-0511 HH										
13	6400 - Wastewater	064LZ-0511 LLL										
14	6400 - Wastewater	064LZ-0541 LL										
15	6400 - Wastewater	064LZ-0712 LL										
16	6400 - Wastewater	064PDZ-0733 +HH										
17	6400 - Wastewater	064PDZ-0733 -HH										
18	6400 - Wastewater	064PDZ-0830 HH										
20	6400 - Wastewater	064XS-0020										

Fig. B.2. exSILentia SILVer Report

Appendix C: SELECTED EXSILENTIA IEC61511

COMPLIANCE REPORT

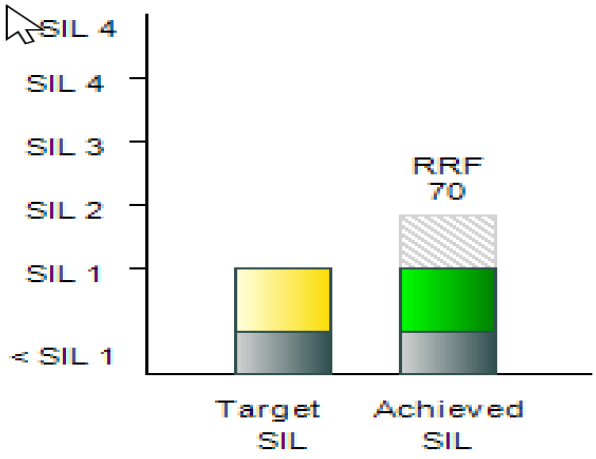


Fig. C.1. Target and Achieved SIL results for SIF 064FZ-0567 LL

Target SIL is SIL1 with RRF > 10.

SIL verification determined that the SIL achieved by the SIF is SIL1 with RRF = 70.

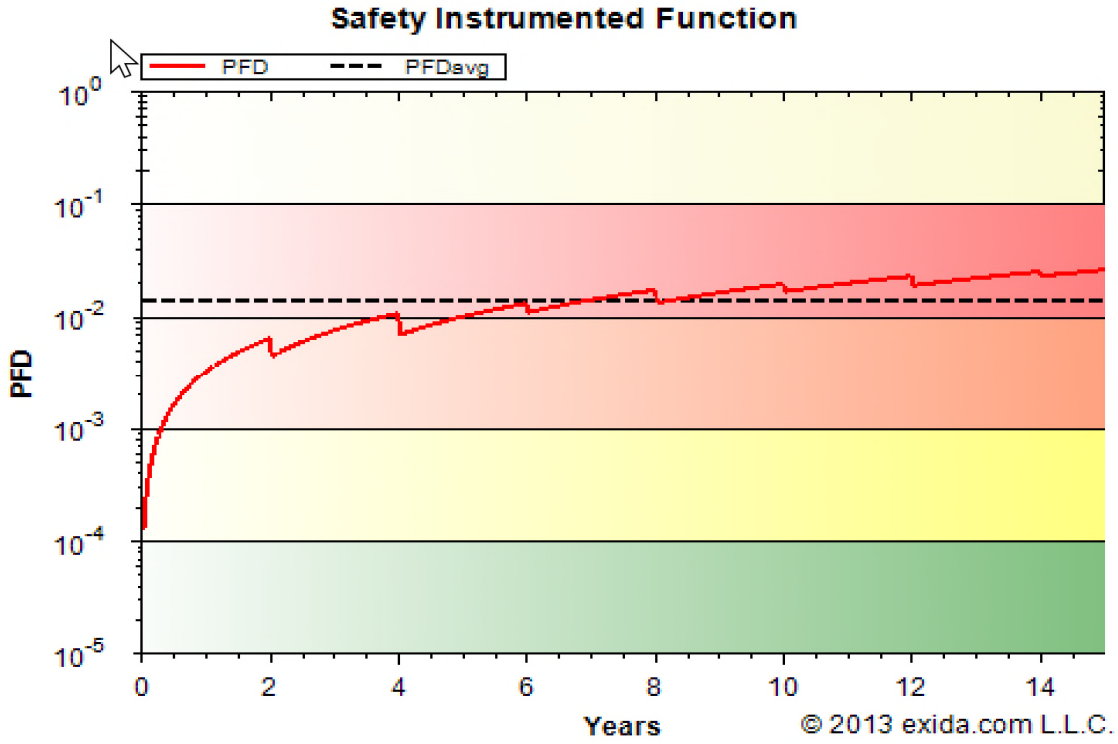


Fig. C.2. Analysis results for SIF 064FZ-0567 LL

Table C.1. Functional Safety Performance of SIF 064FZ-0567 LL

PFDavg	RRF	SIL (PFDavg)	SIL (Architectural Constraints IEC 61508:2000)	SIL (Systematic Capability)
1.42E-02	70	1	1	N/A

Table C.2. Functional Safety

MTTFS (years)
84.75

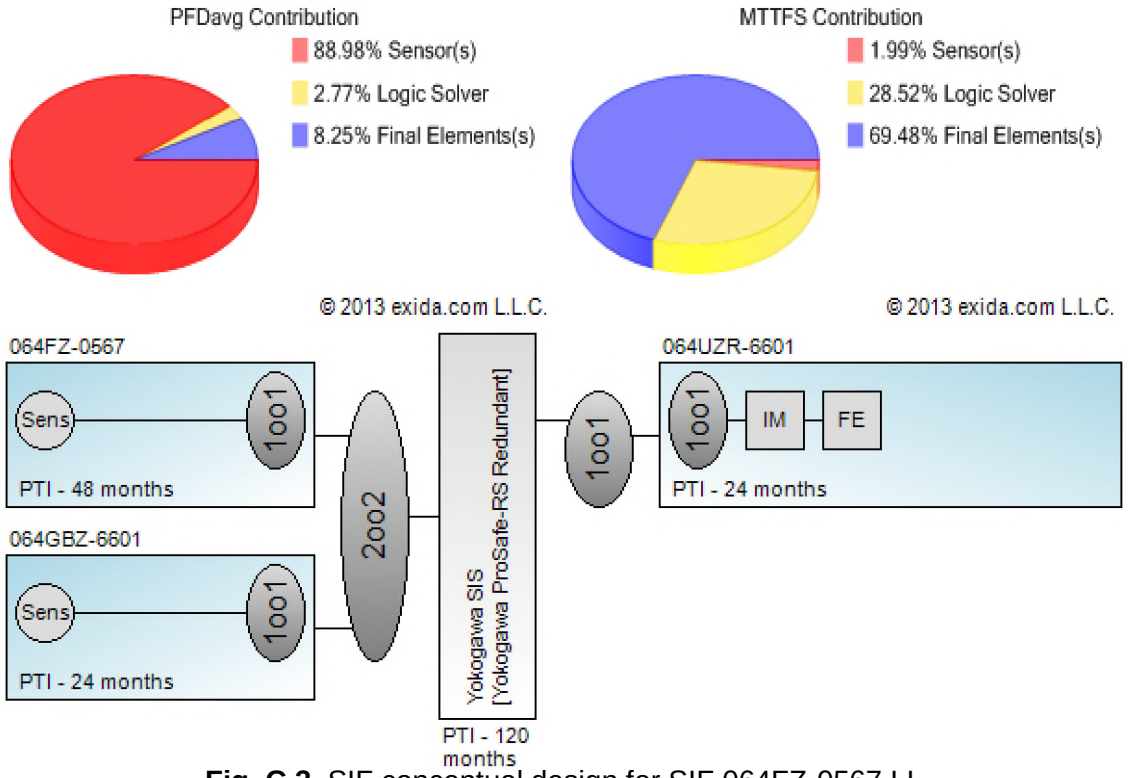


Fig. C.3. SIF conceptual design for SIF 064FZ-0567 LL

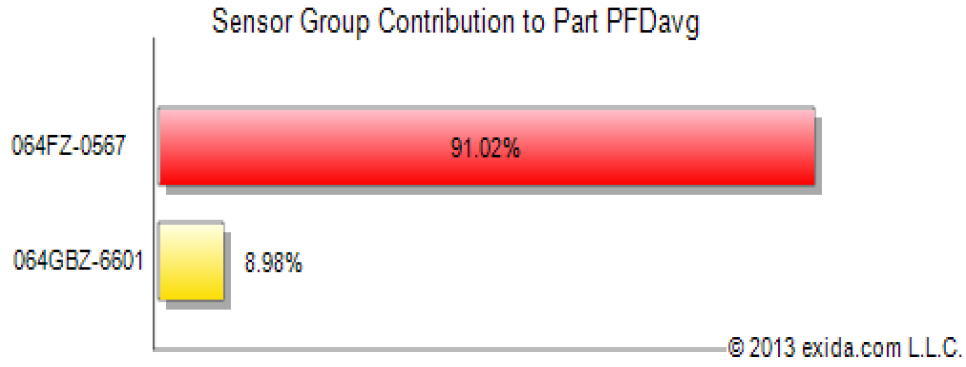


Fig. C.4. Sensor Part Configuration

Table C.3. Reliability Data Sensor Group 064FZ-0567

Component	Failure Rates [1/h]								Arch. Type	SFF [%]
	Fail Low	Fail High	Fail Det.	DD	DU	SD	SU	Res.		
Each Leg										79.2
Yokogawa EJX, A Series and J Series [2013.2.04]	6.10E-08	1.09E-07	1.61E-07	 *2.34E-08*	3.90E-08 *3.90E-08* *1.56E-08*	 *3.31E-07* *3.63E-07*	5.40E-08 *5.40E-08* *2.16E-08*	1.01E-07 *1.01E-07* *1.01E-07*	B	-
Impulse Line - plugging unlikey (x2)				 *3.00E-07*	5.00E-07 *5.00E-07* *2.00E-07*				A	-

Table C.4. Reliability Data Sensor Group 064GBZ-6601

Component	Failure Rates [1/h]								Arch. Type	SFF [%]
	Fail Low	Fail High	Fail Det.	DD	DU	SD	SU	Res.		
Each Leg										27.0
MCC Motor Contactor - Siemens (SIRIUS 3RT Series)					7.30E-08		2.70E-08		A	-

Table C.5. Reliability Data Logic Solver Yokogawa SIS

Component	Number used in analysis per leg	Failure Rates [1/h]					SFF [%]
		SD	SU	DD	DU	Res.	
Main Processor [SCP401, SEC401, and SSB401]	1	1.59E-06	2.06E-09	2.71E-06	2.06E-09		99.95
Power Supply [SPW482]	1	1.04E-06		1.04E-06			100.00
Analog In Module [SAI143 (16)]	1	6.27E-07	3.22E-09	1.60E-06	2.90E-09		99.85
Analog In Channel	1	3.92E-08	5.70E-10	6.19E-08	6.10E-10		-
Digital In Module [SDV144 (16)]	1	9.00E-07	1.09E-09	9.69E-07	1.09E-09		99.95
Digital In Channel	1	3.72E-08		8.15E-08			-
Digital Out Low Module [SDV531 (8)]	1	1.25E-06	1.09E-09	5.52E-07	1.09E-09		99.94
Digital Out Low Channel	1	9.55E-08		3.52E-08			-

Table C.6. Reliability Data Final Element Group 064UZR-6601

Component	Failure Rates [1/h]					Arch. Type	SFF [%]
	DD	DU	SD	SU	Residual		
Each Leg							92.6
Safety Relay, DTT (Phoenix PSR-SCP-24DC/FSP/1X1/1X2)		2.09E-09		9.10E-07		A	-
MCC Contactor, DTT (Siemens SIRIUS 3RT Series)		7.30E-08		2.70E-08		A	-

Appendix D: FRGM for SIFs per Table 4.1

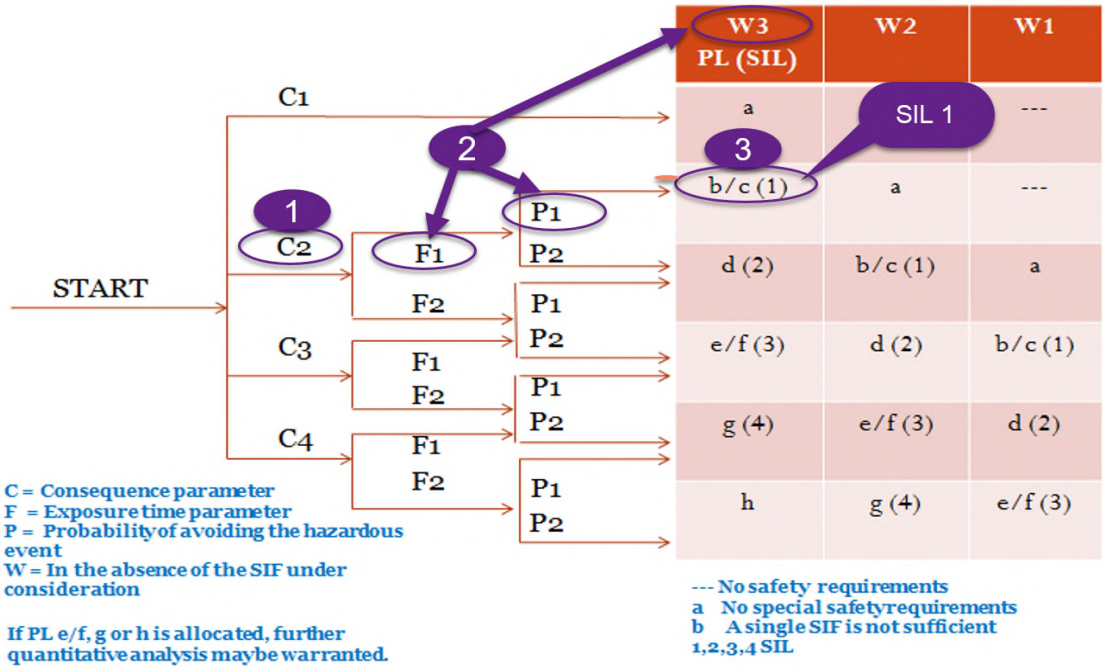


Fig. D.1. FRGM SIL Determination for 064FZ-0567 LL (SIL 1) per **Table 4.1**

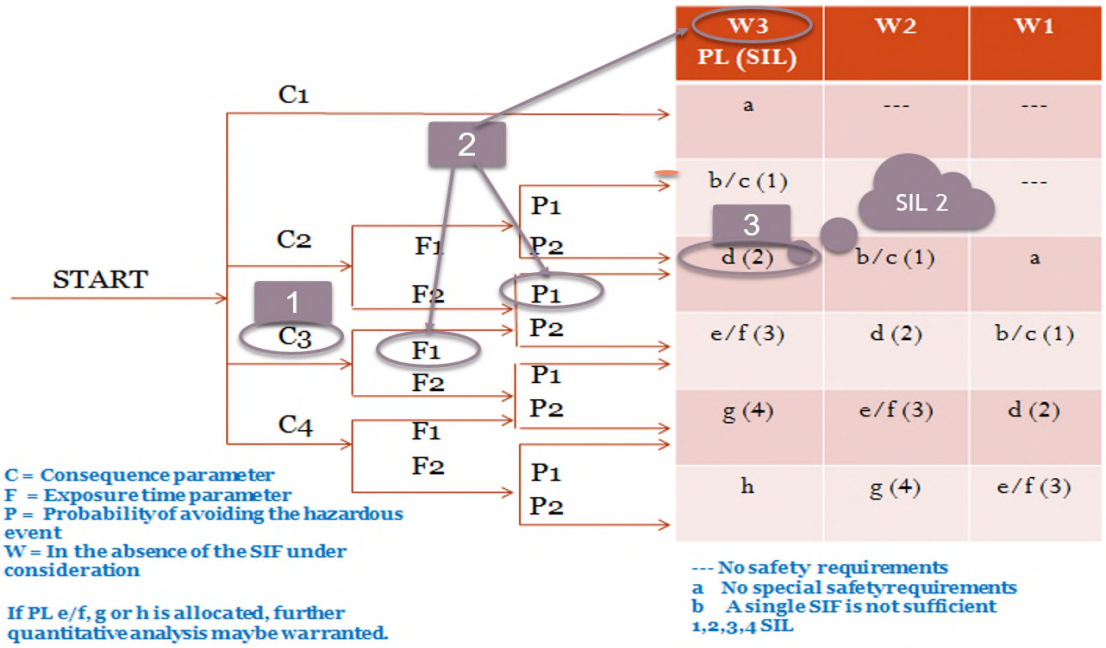


Fig. D.2. FRGM SIL Determination for SIF 064LZ-0712 LL (SIL 2) per **Table 4.1**

Attachment 1: SIEMENS 3RT CONTACTOR FAILURE RATE DATA

Siemens SIRUS 3RT Series Contactor - Failure Rate Calculation

(Failure rate per IEC 62061 Ed. 1.0 Par. 6.7.8.2.1 Note 2) [1].

B10 Failure Rate Value. (Number of Cycles in a Lifetime)

The number of operating cycles during the duration of a lifetime test after which 10% of the test objects fail.
The B10, referred to the standard load characteristics values and under standard operating and environmental conditions, can be read-off the catalogue as electrical and mechanical life

B10 1,000,000 Cycles in usable life (see Siemens IC 10 . 2014 Section 16 Data - 3RT Series Contactor. Copy attached.)

C The "duty cycle"; required number of operation per hour (*operating Cycles per hour*), (*or can be calculated from total expected number of the operations in a lifetime of the apparatus*).

C	24	operations per day
if	24	hour/day
then	1.000	operations per hour

Note: ***The "duty cycle" (C) has been estimated and must be reviewed between proof tests and where necessary these calculation shall be updated to reflect the actual operating data.***

T_L Lifetime (hours), the total number of hour the apparatus is expected to be available for operation.

T_L	15	years
if	8,760	hour/year
then	131,400	hours

Failure Rate Calculation:

Simplified calculation method for λ in operation (par.6.7.8.2.1 note 2 of the IEC 62061 ed.1.0)
The λ (PFH)-value is calculated on the below table according to the following formula:

λ = 0.1 x C / B10 [probability of failures / h]

For an approximate value of MTTF, the following simplified equation can be used:
MTTF = 1 / λ

Mode of Operation: High

λ = 0.1 x C / B10
1.000E-07

λ_D = λ * (A of λ_D)
7.300E-08 Failures/hour

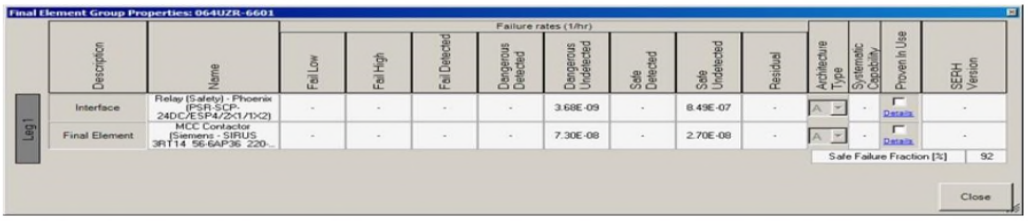
λ_S = λ * (A of λ_S)
2.700E-08 Failures/hour

MTTF = 1 / λ hours
1.000E+07 hours
1.142E+03 years

B10 : 1,000,000 Cycles in unusable life
λ_D : 73% of Total Failures
C : 1.0000 per hour

Notes:
1) Only applies under the conditions specified in the technical specifications.

2) Calculation of the B10 values was based on 66 % of the rated current value (Ie).



Mode of Operation: Low

λ = 1.00E-07 (100 FIT) failures/hour

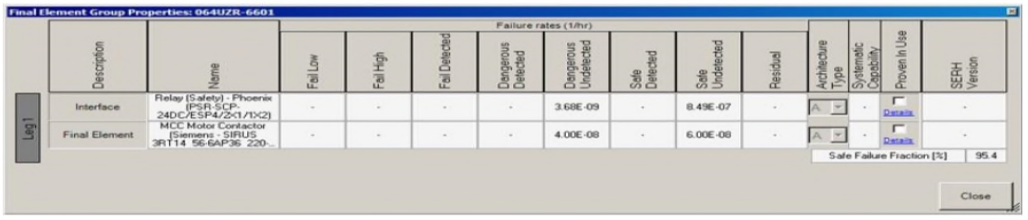
λ_D = λ * (A of λ_D)
4.00E-08 Failures/hour

λ_S = λ * (A of λ_S)
6.00E-08 Failures/hour

λ_D : 40% of Total Failures

λ_S : 100A - λ_D
60% of Total Failures

Notes:
1) Valid only under the previously mentioned conditions (Siemens IC 10 · 2014 Sect. 17 Page 16/17).



SIRUS 3RT Series Contactor - Failure Rate Calculation_rev. A SIRUS 3RT14 LNG PLANT A

Fig. E.1. Failure Rate Calculation: Siemens Sirus 3RT Series Contactor

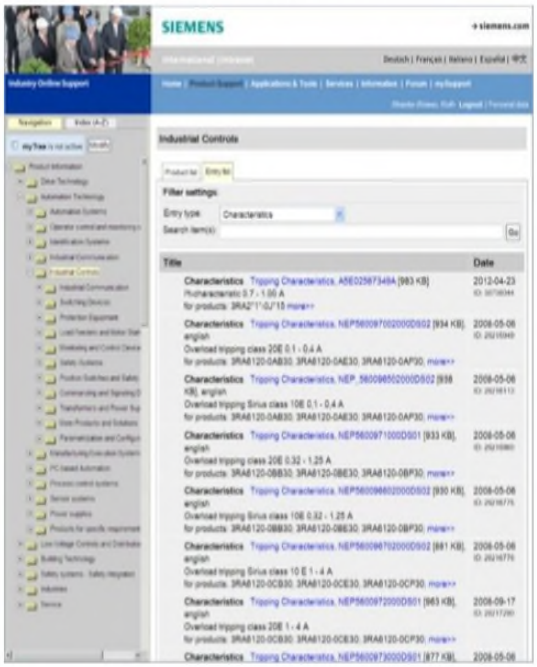
Standards and approvals

Approvals, test certificates, characteristic curves

An overview of the certificates available for Industrial Control products along with more technical documentation can be consulted daily on the Internet at:

www.siemens.com/sirius/approvals

Product support: Approvals/certificates



Safety characteristics

In the following standards, the so-called B10 values for calculating the safety integrity or safety integrity level (SIL) in functional safety at a high or continuous demand rate are required also for electromechanical switchgear:

- IEC 62061 "Safety of machines – Functional safety of safety-related electrical, electronic and programmable electronic control systems",
- ISO 13849-1 "Safety of machines – Safety-related components of controls – Part 1: General principles".

Failure rates of electromechanical components are required for calculating the safety integrity or safety integrity level (SIL) in functional safety:

- in the manufacturing industry at a high demand rate
- in the process industry at a low demand rate

Further requirements are laid down in IEC 61511-1 "Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements".

The German versions of the above standards are:

- EN 62061 (VDE 0113-50), October 2005, which since 31.12.2005 has been harmonized as EN 62061 under the Machinery Directive,
- EN ISO 13849-1:2008,
- EN 61511-1 (VDE B10-1).

The TOV-tested Safety Evaluation Tool assists in calculating the safety function as verification for the machine documentation. It is available on the Internet at www.siemens.com/safety-evaluation-tool.

At www.siemens.com/safety-integrated you will also find examples of functions with calculations according to the current standards.

Definitions

$\lambda(t)\,dt$ is the probability that a unit which has not failed by a certain time t will fail in the following interval $(t; t+dt)$.
Failure rates have the dimension 1/time unit, e.g. 1/h.
Failure rates for components are often specified in FIT (failures in time unit): 1 FIT equals 10^{-9}/h.
From the failure rate it is possible to derive a (mathematical) distribution function of the failure probability:

$F(t) = 1 - \exp(-\lambda t)$, with λ as constant failure rate

- The mean value of this exponential distribution is also referred to as:
  - Mean Time To Failure (MTTF) in the case of irreparable components; 63.2 % of components fail by the MTTF.
  - Mean Operating Time Between Failures (MTBF) in the case of reparable components.
- $MTTF = 1/\lambda$
  (MTTF is a statistical mean value but no guarantee for endurance)

Electromechanical components are often irreparable components. In general, the failure rate of monitored units changes with age.

Fig. E.2. Failure Rate Calculation: Approvals, Test Certificates, Characteristic Curves

The B10 value for devices subject to wear is expressed in number of operating cycles:

- it is the number of operating cycles after which 10 % of the test specimens fail in the course of an endurance test (or: the number of operating cycles after which 10 % of the devices have failed).

For low demand rates (mainly in the process industry), the failure rate and not the B10 value is used to determine the failure probability.

Standard B10 values at a high demand rate

With the help of the B10 value and a simplified formula (see section 6.7.8.2.1 of EN 62061), the user can then calculate the total failure rate of an electromechanical component:

$A = 0.1 \times C/B10$

with C = operating cycles per hour. C is specified by the user.

The failure rate is made up of safe (A_S) and dangerous (A_D) failures:

$A = A_S + A_D$

or

A_D = [share of dangerous failures in %] x A

A_S = [share of safe failures in %] x A

The failure rate of the dangerous failures A_D of the components used is needed for further calculations.

Listed in the following table are the standard B10 values and the share of dangerous failures for SIRIUS product groups at a high demand rate.

Standard B10 values (at a high demand rate)

SIRIUS product group (electromechanical components)	Standard B10 value[1] (operating cycles)	Share of dangerous failures
EMERGENCY-STOP control devices (with positive-opening contacts)		
- pulled to unlatch	30 000	20 %
- rotated to unlatch (also with lock)	100 000	20 %
Cable-operated switches for EMERGENCY-STOP function (with positive-opening contacts)	100 000	50 %
Standard position switches/basic switches (with positive-opening contacts)	10 000 000	20 %
Position switches with separate actuator (with positive-opening contacts)	1 000 000	20 %
Position switches with tumbler (with positive-opening contacts)	1 000 000	20 %
Hinge switches (with positive-opening contacts)	1 000 000	20 %
Pushbuttons (non-latching), with positive-opening contacts)	10 000 000	20 %
Contactors/motor starters for switching motors:		
- 3RT/3TF6/3TB	1 000 000[2]	73 %
- 3TC	1 000 000[2]	73 %
Contactor relays and auxiliary switches (with positively driven contacts, and at $I < 0.3 \cdot I_e$)	1 000 000	73 %

[1] Only applies under the conditions specified in the technical specifications.

[2] Calculation of the B10 values was based on 66 % of the rated current value I_e.

The $B10_d$ value used in EN ISO 13849-1:2008 is determined as follows:

$$B10_d = \frac{B10}{\text{Share of dangerous failures}}$$

Calculation example

A protective door is monitored by a position switch with a separate actuator.

The protective door is opened 4 times an hour.

The overall failure rate of the position switch is:

$A = 0.1 \cdot C/B10$ [failures/h]
$A = 0.1 \cdot 4/1000000 = 4 \cdot 10^{-7}$ [failures/h]

The dangerous failure rate is calculated with:

A_D = 20 % of $A = 0.2 \cdot 4 \cdot 10^{-7}$ [failures/h]
$A_D = 8 \cdot 10^{-8}$ [failures/h]

Standard failure rates (at a low demand rate)

On the basis of the failure rates, it is possible to calculate the average probability of failure on demand (PFD_{avg}) of a PLT protective device.

A so-called low demand rate is assumed, meaning the rate of demand on the safety-related system amounts to no more than once a year and is not greater than double the frequency of the repeat test.

A repeat test once a year is recommended for electromechanical components in order to reveal passive faults.

For special applications it is possible, in agreement with the inspecting institution (e.g. a technical inspectorate, government agency or the like) to extend the test intervals by using suitable solutions (e.g. a multi-channel version etc.).

Listed in the following table are the standard failure rates and the share of dangerous failures for SIRIUS product groups at a low demand rate.

Standard failure rates at a low demand rate

SIRIUS product group (electromechanical components)	Standard failure rates (in FIT)[1]	Share of dangerous failures[2]
EMERGENCY-STOP control devices (with positive-opening contacts)	100	20 %
Cable-operated switches for EMERGENCY-STOP function (with positive-opening contacts)	100	20 %
Standard position switches/basic switches (with positive-opening contacts)	100	20 %
Position switches with separate actuator (with positive-opening contacts)	100	20 %
Position switches with tumbler (with positive-opening contacts)	100	20 %
Hinge switches (with positive-opening contacts)	100	20 %
Pushbuttons (non-latching) (with positive-opening contacts)	100	20 %
Contactors/motor starters (with positively-driven contacts or mirror contacts)	100	< 40 %

[1] The failure rates specified in the table were limited to 100 FIT.

[2] Valid only under the previously mentioned conditions.

Fig. E.3. Failure Rate Calculation: Standards and Approvals

Attachment 2: ABB Axx-30 CONTACTOR FAILURE

RATE DATA

ABB Axx 30 Series Contactor (where 'xx' are series number) Failure Rate Calculation

(Failure rate per IEC 62061 Ed. 1.0 Par. 6.7.8.2.1 Note 2) [1].

B_{10} Failure Rate Value. (Number of Cycles in a Lifetime)

The number of operating cycles during the duration of a lifetime test after which 10% of the test objects fail.
The B10, referred to the standard load characteristics values and under standard operating and environmental conditions, can be read off the catalogue as electrical and mechanical life

B_{10}	1,000,000	Cycles in usable life (Refer to '*Comeca*' supplied data. Copy attached.)

Data for ABB contactors:
Useful life, B_{10} (operation cycle): 1,000,000
% of dangerous failures, (1 SFF): 75% (73% in annex K of IEC 60947 4 1) [2],

These data are valid for ABB contactors < 1000A.
(Refer to 'Comeca' supplied data. Copy attached.)

C The "duty cycle"; required number of operation per hour (*operating Cycles per hour*), (*or can be calculated from total expected number of the operations in a lifetime of the apparatus*).

C	24	Operations per day
if	24	hour/day
then	1.000	operations per hour

Note: *The "duty cycle" (C) has been estimated and must be reviewed between proof tests and where necessary these calculations shall be updated to reflect the actual operating data.*

T_L Lifetime (hours), the total number of hour the apparatus is expected to be available for operation.

T_L	20	years
if	8,760	hour/year
then	175,200	hours

Failure Rate Calculation:

Simplified calculation method for λ in operation (par.6.7.8.2.1 note 2 of the /EC 62061 ed.1.0) [1].
The λ (PFH) value is calculated on the below table according to the following formula:

λ = 0.1 x C / B10 [probability of failures / h]

For an approximate value of MTTF, the following simplified equation can be used:
MTTF = 1 / λ

Mode of Operation: High

λ = 0.1 x C / B_{10}
1.000E 07

B_{10} : 1,000,000 Cycles in unusable life
λ_D : 75% of Total Failures
C : 1.0000 per hour

λ_D = λ * (% of λ_D)
7.500E 08 Failures/hour (0.000000075 Failures/hour)

λ_S = λ * (% of λ_S)
2.500E 08 Failures/hour (0.000000025 Failures/hour

MTTF = 1 / λ
1.000E+07 hours
1.142E+03 years

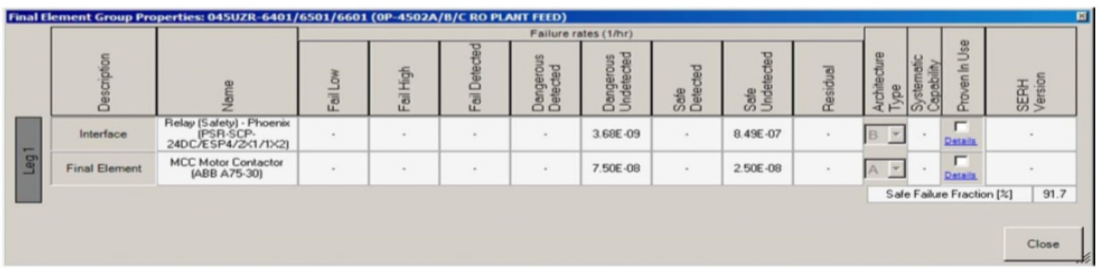


Fig. F.1. Failure Rate Calculation: ABB Axx-30 Contactor

Attachment 3: SIL SAFETY CONSIDERATIONS FOR FAIL SAFE RELAY PSR-SCP-24DC/ESP4/2X1/1X2

Table D.1: Results for DTS high demand mode of the ESP4 according to 1oo1 structure

Parameters acc. to IEC 61508	Results
Type of the Device	A
Mode of operation	high demand
Intended use	De-energized to safe application
HFT	0
SIL	3
A_{SD}	949 FIT
A_{SU}	58.3 FIT
A_{DD}	44.5 FIT
A_{DU}	0.093 FIT
A_{Total}	1052 FIT
SFF	99.99 %
MTBF [1)]	106.9 Years
PFH	$9.93 * 10^{-11}$
T_{1max}	20 years
Useful Lifetime	20 years
[1)] This includes failures which are not part of the safety function. MTTR has been set to 8 hours	

Table D.2: Results for DTS low demand mode of the ESP4 according to 1oo1 structure

Parameters acc. to IEC 61508	Results
Type of the Device	A
Mode of operation	Low demand
Intended use	De-energized to safe application
HFT	0
SIL	3
A_{SD}	0 FIT
A_{SU}	849 FIT
A_{DD}	0 FIT
A_{DU}	3.68 FIT
A_{Total}	853 FIT
SFF	99.56 %
MTBF [1)]	132,3 Years
PFD_{avg} for T_1 = 1 year	$1.61 * 10^{-5}$
T_{1max}	9 years
[1)] This includes failures which are not part of the safety function. MTTR has been set to 8 hours	

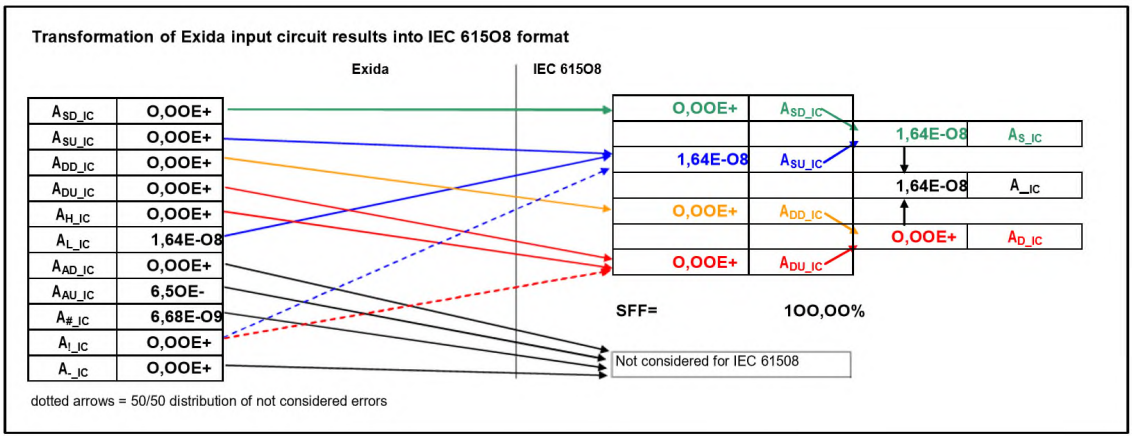


Fig. G.1. Raw results of the FMEDA - High demand – Input Circuit

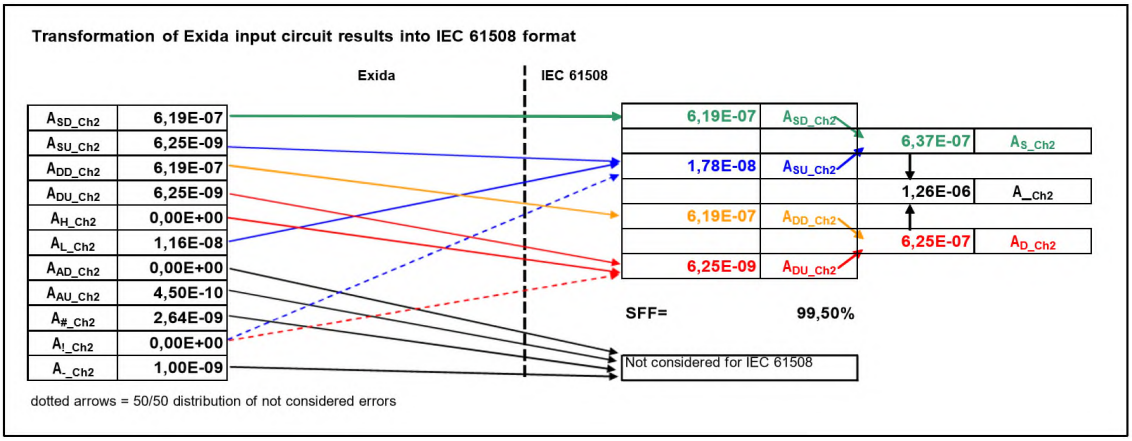


Fig. G.2. Raw results of the FMEDA – High demand – Relay Channel 1

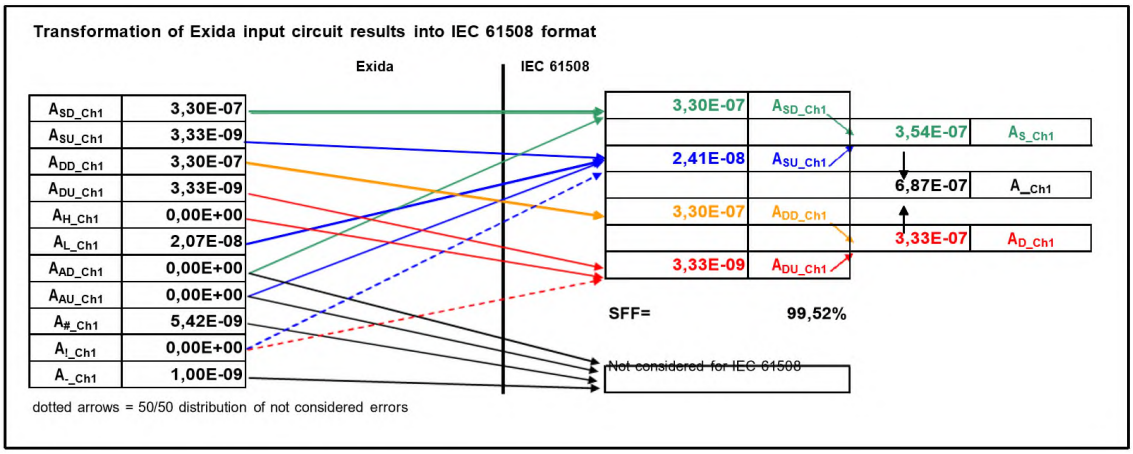
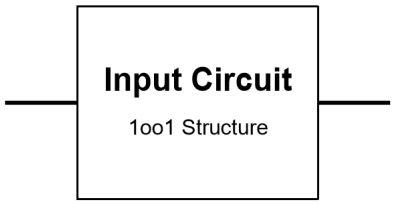


Fig. G.3. Raw results of the FMEDA – High demand – Relay Channel 2



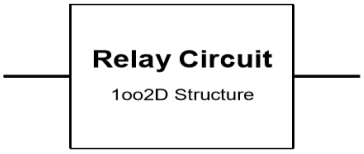
A_{SD_IC} = 0

A_{SU_IC} = 1.64 * 10^{-8}

A_{DD_IC} = 0

A_{DU_IC} = 0

Fig. G.4. Calculation for the input circuit



HFT=1

B = B_D = 2% (common cause factor)

T_1 = 240m = 20a (proof test interval = usefull lifetime)

T_D = 1h (Diagnose time = cycle time)

$$\lambda_{DU\_RC} = (1-\beta)^2 \cdot (\lambda_{DU\_Ch})^2 \cdot T_1 + (1-\beta_D)^2 \cdot (\lambda_{DD\_Ch})^2 \cdot \frac{T_D}{2} + \beta \cdot \lambda_{DU\_Ch} + \beta_D \cdot \lambda_{DD\_Ch} \cdot \frac{T_D}{T_1}$$

Because T_D << T_1 the above formula can be simplified:

A_{DU_RC} = (1-B)2 * (A_{DU_Ch1} * A_{DU_Ch2}) * T_1 + B * ((A_{DU_Ch1} + A_{DU_Ch2}) / 2)

A_{DU_RC} = (1-0.02)2 *(3.33 * 10^{-9} *6.25 * 10^{-9}) * 20a * 8760h/a + 0.02 *(3.33 *10^{-9} +6.25 *10^{-9})/2

A_{DU_RC} = 3.50 * 10^{-12} + 9.58 * 10^{-11}

A_{DU_RC} = 9.93 * 10^{-11}

Because T_D << T_1 the above formula is simplified.

$$\lambda_{D\_RC} = (1-\beta)^2 \cdot (\lambda_{D\_Ch})^2 \cdot T_1 + \beta \cdot \lambda_{D\_Ch}$$

A_{D_RC} = (1-0.02)2 * 3.33 * 10^{-7} * 6.25 * 10^{-7} * T_1 + B * (3.33 * 10^{-7} + 6.25 * 10^{-7})/2

A_{D_RC} = 3.50 * 10^{-8} + 9.58 * 10^{-9}

A_{D_RC} = 4.46 * 10^{-8}

$A_{DD-RC} = A_{D-RC} - A_{DU-RC}$
$A_{DD-RC} = 4.46 * 10^{-8} - 9.93 * 10^{-11}$
$A_{DD-RC} = 4.45 * 10^{-8}$

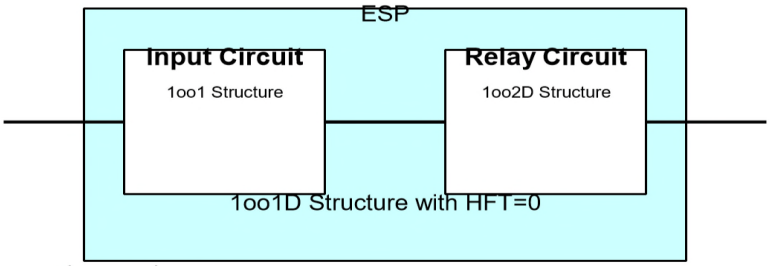
$A_{SD-RC} = A_{SD-Ch1} + A_{SD-Ch2}$
$A_{SD-RC} = 3.30 * 10^{-7} + 6.19 * 10^{-7}$
$A_{SD-RC} = 9.49 * 10^{-7}$

$A_{SU-RC} = A_{SU-Ch1} + A_{SU-Ch2}$
$A_{SU-RC} = 2.41 * 10^{-8} + 1.78 * 10^{-8}$
$A_{SU-RC} = 4.19 * 10^{-8}$

$A_{S-RC} = A_{SD-RC} + A_{SU-RC}$
$A_{S-RC} = 9.49 * 10^{-7} + 4.19 * 10^{-8}$
$A_{S-RC} = 9.91 * 10^{-7}$

$A_{-RC} = A_{S-RC} + A_{D-RC}$
$A_{-RC} = 9.91 * 10^{-7} + 4.46 * 10^{-9}$
$A_{-RC} = 9.536 * 10^{-7}$

Fig. G.5. Calculation for the redundant structure



$A_{DU} = A_{DU-IC} + A_{DU-RC}$
$A_{DU} = 0 + 9.93 * 10^{-11}$
$A_{DU} = 9.93 * 10^{-11}$

$A_{DD} = A_{DD-IC} + A_{DD-RC}$
$A_{DD} = 0 + 4.45 * 10^{-8}$
$A_{DD} = 4.45 * 10^{-8}$

$A_{SU} = A_{SU-IC} + A_{SU-RC}$
$A_{SU} = 1.64 * 10^{-8} + 4.19 * 10^{-8}$
$A_{SU} = 5.83 * 10^{-8}$

$A_{SD} = A_{SD-IC} + A_{SD-RC}$
$A_{SD} = 0.00 + 9.49 * 10^{-7}$
$A_{SD} = 9.49 * 10^{-7}$

$A_{Total} = A_{-DU} + A_{-DD} + A_{-SD} + A_{-SU}$
$A_{Total} = 9.93 * 10^{-11} + 4.45 * 10^{-8} + 9.49 * 10^{-7} + 5.83 * 10^{-8}$
$A_{Total} = 1.05 * 10^{-6}$

$$SFF = 1 - \frac{\lambda_{DU\_total}}{\lambda_{total}} = 1 - \frac{9.93,10^{-11}}{1.05,10^{-6}} = 99{,}99\%$$

$A_{\#-total} = A_{-IC} + A_{AD-IC} + A_{AU-IC} + A_{-CH1} + A_{-CH2} + A_{\#-IC} + A_{\#-CH1} + A_{\#-CH2} + A_{AD-CH1} + A_{AD-CH2} + A_{AU-CH1} + A_{AU-CH2}$

$A_{\#-total} = 0 + 0 + 6.50 * 10^{-10} + 1.00 * 10^{-9} + 1.00 * 10^{-9} + 6.68 * 10^{-9} + 5.42 * 10^{-9} + 2.64 * 10^{-9} + 0 + 0 + 0 + 4.50 * 10^{-10}$

$A_{\#-total} = 1.78 * 10^{-8}$

$$MTBF = MTTF + MTTR = \frac{1}{\lambda_{total} + \lambda_{\#total}} + 8h = 106.9\,years$$

Fig. G.6. Combined values according to 1oo1 structure

Table D.3: Results for DTS high demand mode of the ESP4 according to 1oo1 structure

Parameters acc. to IEC 61508	Results
Type of the Device	A
Mode of operation	high demand
Intended use	De-energized to safe application
HFT	0
SIL	3
A_{SD}	949 FIT
A_{SU}	58.3 FIT
A_{DD}	44.5 FIT
A_{DU}	0.093 FIT
A_{Total}	1052 FIT
SFF	99.99 %
MTBF [1)]	106.9 Years
PFH	$9.93 * 10^{-11}$
T_{1max}	20 years
Useful Lifetime	20 years
[1)] This includes failures which are not part of the safety function. MTTR has been set to 8 hours	

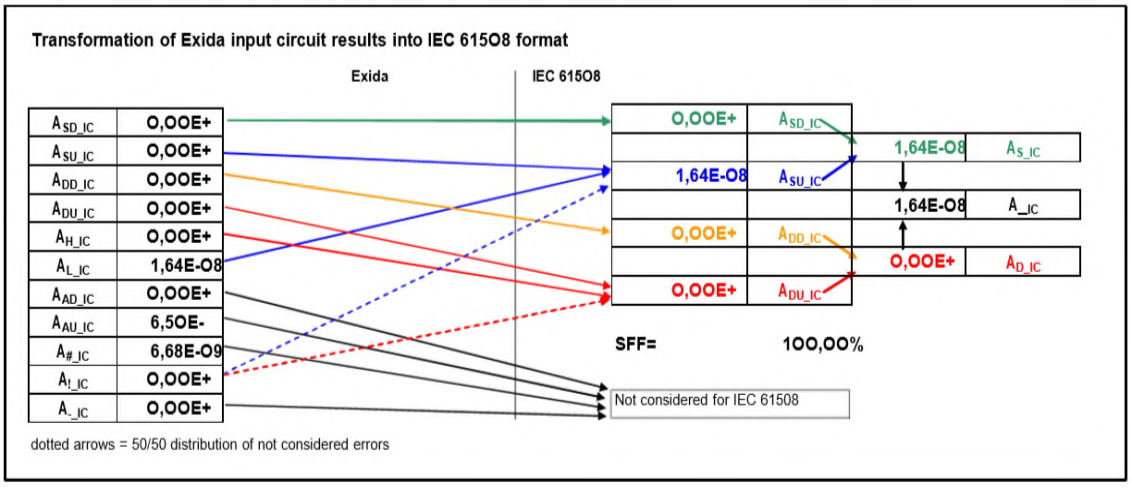


Fig. G.7. Raw results of the FMEDA - Low demand – Input Circuit

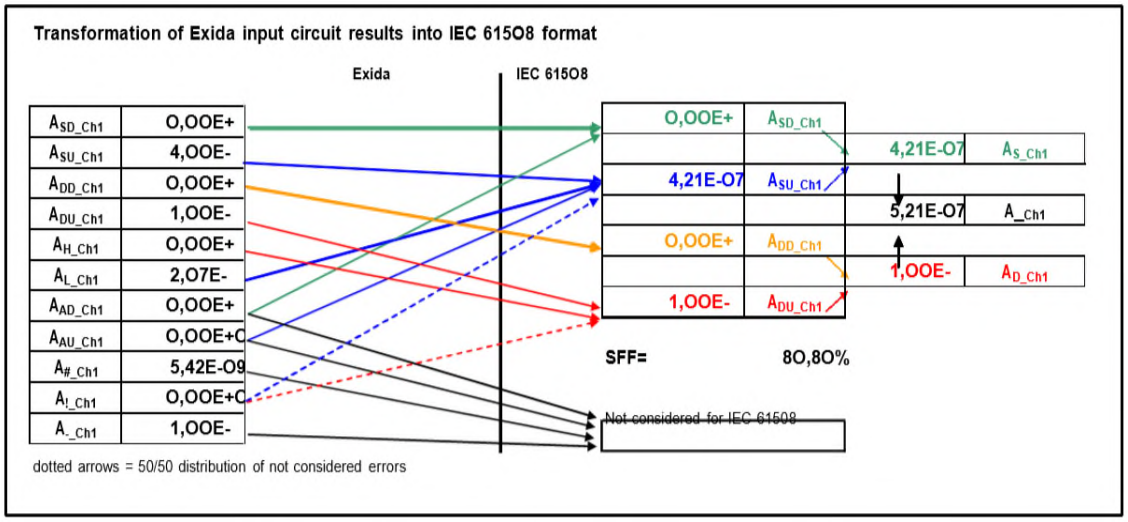


Fig. G.8. Raw results of the FMEDA - Low demand – Relay Channel 1

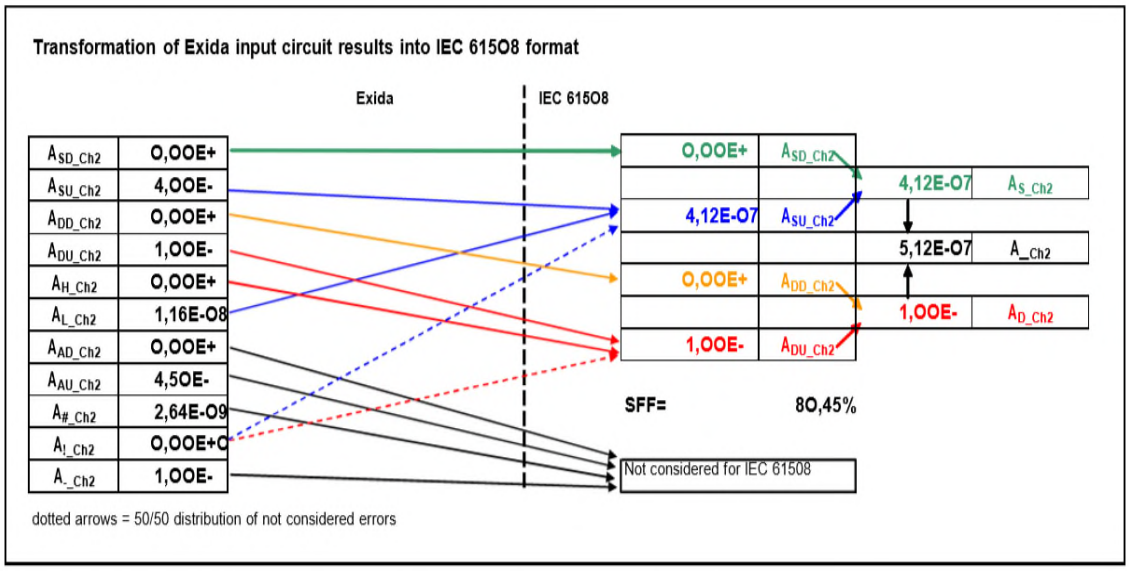
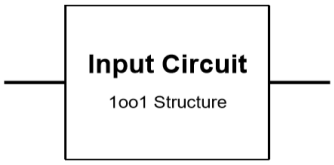


Fig. G.9. Raw results of the FMEDA - Low demand – Relay Channel 2



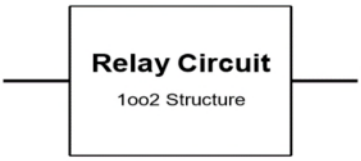
$A_{SD\_IC} = 0$

$A_{SU\_IC} = 1.64 * 10^{-8}$

$A_{DD\_IC} = 0$

$A_{DU\_IC} = 0$

Fig. G.10. Calculation for the input structure



HFT=1

B = 2% (common cause factor)

T_1 = 144m = 12a (proof test interval)

$A_{DU\_RC} = (1\text{-}B)^2 * (A_{DU\_Ch1} * A_{DU\_Ch2}) * T_1 + B * ((A_{DU\_Ch1} + A_{DU\_Ch2}) / 2)$ (DC=0% simpfified formula)

$A_{DU\_RC} = (1\text{-}0.02)^2 *(1.00 * 10^{-7} * 1.00 * 10^{-7}) * 20a * 8760h/a + 0.02 *(1.00 *10^{-7} + 1.00*10^{-7})/2$

$A_{DU\_RC} = 1.68 * 10^{-9} + 2.00 * 10^{-9}$

$A_{DU\_RC} = 3.68 * 10^{-9}$

$A_{DD\_RC} = 0$

$A_{SD\_RC} = 0$

$A_{SU\_RC} = A_{SU\_Ch1} + A_{SU\_Ch2}$

$A_{SU\_RC} = 4.21 * 10^{-7} + 4.12 * 10^{-7}$

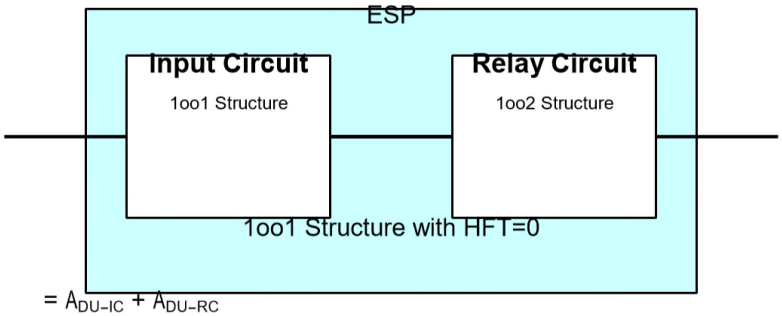
$A_{SU\_RC} = 8.33 * 10^{-7}$

$A_{\_RC} = A_{SU\_RC} + A_{DU\_RC}$

$A_{\_RC} = 8.33 * 10^{-7} + 3.68 * 10^{-9}$

$A_{\_RC} = 8.37 * 10^{-7}$

Fig. G.11. Calculation for the redundant structure



$A_{DU} = A_{DU\text{-}IC} + A_{DU\text{-}RC}$

$A_{DU} = 0.00 + 3.68 * 10^{-9}$

$A_{DU} = 3.68 * 10^{-9}$

$A_{DD} = A_{DD\text{-}IC} + A_{DD\text{-}RC}$

$A_{DD} = 0.00$

$A_{SU} = A_{SU\text{-}IC} + A_{SU\text{-}RC}$

$A_{SU} = 1.64 *10^{-8} + 8.33 * 10^{-7}$

$A_{SU} = 8.49 *10^{-7}$

$A_{SU} = A_{SU-IC} + A_{SU-RC}$

$A_{SU} = 1.64 * 10^{-8} + 8.33 * 10^{-7}$

$A_{SU} = 8.49 * 10^{-7}$

$A_{SD} = A_{SD-IC} + A_{SD-RC}$

$A_{SD} = 0.00$

$A_{total} = A_{-DD} + A_{-DU} + A_{-SD} + A_{-SU}$

$A_{total} = 0 + 3.68 * 10^{-9} + 0 + 8.49 * 10^{-7}$

$A_{total} = 8.53 * 10^{-7}$

$$SFF = 1 - \frac{\lambda_{DU\_total}}{\lambda_{total}} = 1 - \frac{3.68,10^{-9}}{8.53,10^{-7}} = 99{,}56\%$$

$$PFDav(T_1 = 1a) = \frac{1}{2} . \lambda_{DU\_total} . T_1 = \frac{1}{2} . 3.68 . 10^{-9} . 8760$$

$$PFDav(T_1 = 1a) = 1.61 . 10^{-5}$$

$$PFDav(T_1 = 9a) = 1.45 . 10^{-4} < (15\% SIL3)$$

$$PFDav(T_1 = 9a) = 1.45 . 10^{-4} < 1.5 . 10^{-4}$$

T_{1max}(SIL3) = 9 years

$A_{-\#-total} = A_{-IC} + A_{AD-IC} + A_{AU-IC} + A_{-CH1} + A_{-CH2} + A_{\#-IC} + A_{\#-CH1} + A_{\#-CH2} + A_{AD-CH1} + A_{AD-CH2} + A_{AU-CH1} + A_{AU-CH2}$

$A_{-\#-total} = 0 + 0 + 6.50 * 10^{-10} + 1.00 * 10^{-9} + 1.00 * 10^{-9} + 6.68 * 10^{-9} + 5.42 * 10^{-9} + 2.64 * 10^{-9} + 0 + 0 + 0 + 4.50 * 10^{-10}$

$A_{-\#-total} = 1.78 * 10^{-8}$

$$MTBF = MTTF + MTTR = \frac{1}{\lambda_{total} + \lambda_{-\#_{total}}} + 8h = 132.3 years$$

Fig. G.12. Combined values according to 1oo1 structure

Table D.4: Results for DTS low demand mode of the ESP4 according to 1oo1 structure

Parameters acc. to IEC 61508	**Results**
Type of the Device	A
Mode of operation	Low demand
Intended use	De-energized to safe application
HFT	0
SIL	3
A_{SD}	0 FIT
A_{SU}	849 FIT
A_{DD}	0 FIT
A_{DU}	3.68 FIT
A_{Total}	853 FIT
SFF	99.56 %
MTBF [1)]	132,3 Years
PFD_{avg} for T_1 = 1 year	$1.61 * 10^{-5}$
T_{1max}	9 years
[1)] This includes failures which are not part of the safety function. MTTR has been set to 8 hours	

Chapter 5 - NIST + FRGM: Consideration on Cybersecurity

5.1 Introduction

The safe and secure operation of critical infrastructure is dependent on appropriate responses to safety, security and operational priorities into Integrated Control and Safety Systems (ICSS), at design stage and throughout the life of the system. Digitisation as well as networked automation and control infrastructures have increased in the past years and are leading to remarkable potential security risks.

Recent news about serious security incidents such as Triton [127, 128] and WannaCry [129] ransomware affecting the whole world are heard more often. At the time of this writing, Triton (Trojan.Trisis) is the first to attack SIS devices. A new Trojan which was designed to target SIS, has the capability to deploy alternative logic changes that has the potential to cause disruption. Triton has reportedly been used against at least one organization in the Middle East. Attacks on SIS at worst can lead to facilitate sabotage or cause major plant shutdown. Stuxnet [130, 131] is the first and most notable example of Industrial Control System (ICS) malware which was designed to attack programmable logic controllers (PLCs) being used in the Iranian uranium enrichment program. The Dragonfly [132] cyber espionage group has also been known to target ICS and compromised a number of ICS equipment providers, infecting their software with the Oldrea Trojan [132] (aka Havex). The Disakil [133] disk-wiping malware

(Trojan.Disakil), which was used in attacks against the Ukrainian energy sector in late 2016, contained a component designed to target SCADA (supervisory control and data acquisition) ICS systems. The malware attempted to stop and delete a service used by software designed to communicate with legacy SCADA systems.

Cybersecurity threats exploit the organisation's security, economy, safety and health orchestrated by an augmented complexity and connectivity of critical infrastructure systems. The oil and gas industry has a huge demand to protect multi-billion mega project globally and is projected to spend up to $1.87 billion on cybersecurity by 2018 [129, 134]. Cybersecurity risk affects a company's bottom line similar to financial and reputational risk. It can drive up costs and impact revenue. It can damage an organisation's ability to innovate and to gain and maintain customers. In the past years, separate research communities have dealt with threats to safety versus security [135]. Two international standards have been proposed by the International Society of Automation (ISA) to address ICSS safety and security needs: ISA 84 standard (also called IEC 61511) on safety instrumented systems [136] and ISA 99 standard (also called IEC 62443) on control system security [137]. As ICSS are becoming more complex and more integration of systems and subsystems required, the contrast between safety and security is beginning to deteriorate. Collaboration between safety and security [34] are starting to be of interest among researchers [18, 135]. ISA has also identified a need of alignment between safety and security, and formed a working group, Work Group 7 - Safety and Security, to investigate alignment and common issues between security and safety [22].

Due to these real threats and alarming trends in ICSS cybersecurity, this complementary chapter of the thesis is dedicated to come up with an integrated and optimised evaluation framework for ICSS and related subsystems considering cybersecurity and safety. This can be achieved by the alignment of the cybersecurity framework formulated by the National Institute of Standards and Technology (NIST) with safety and security standards ISA84 (IEC 61511) and ISA99 (IEC 62443), and the novel Funnel Risk Graph Method (FRGM). The need of such alignment between safety and security has been recognised by the research community [13-21], the industry, as well as the International Society of Automation (ISA) [22].

Section 5.2 discusses the NIST concepts. Sections 5.3 to 5.5 explores the NIST Framework, Implementation Tiers and Framework Profile. Section 5.6 and Section 5.7 elaborate examples of alignment between safety and security. Section 5.8 discusses the overview of the proposal. Section 5.9 details the proposal on the alignment of NIST and FRGM called NIST + FRGM framework. Section 5.10 explores a case study using SIF 064FZ-0567 LL as it applies to the NIST + FRGM framework. Finally, Section 5.11 concludes the Chapter.

5.2 NIST

In February 2014, as directed by a presidential executive order, the cybersecurity framework [138] was published following a collaborative process involving government agencies, industry, and academia. The NIST framework is a risk-based approach to managing cybersecurity risk, and is composed of three parts: the Framework Core, the Framework Implementation Tiers, and the

Framework Profiles. Each Framework component supports the connection between business drivers and cybersecurity activities. These Framework components are explored as follows:

5.3 NIST Framework Core [138]

As depicted in **Figures 5.1** and **5.2**, NIST framework is a group of cybersecurity actions, preferred results, and appropriate references that are collective across critical infrastructure sectors. The Core is not a checklist of things to do. Basically, it contains vital cybersecurity outcomes identified by industry to help in cybersecurity risk management. There are four elements in the Core NIST Framework, namely: Functions (Identify, Protect, Detect, Respond and Recover), Categories, Subcategories and Informative References as shown in **Figure 5.1.**

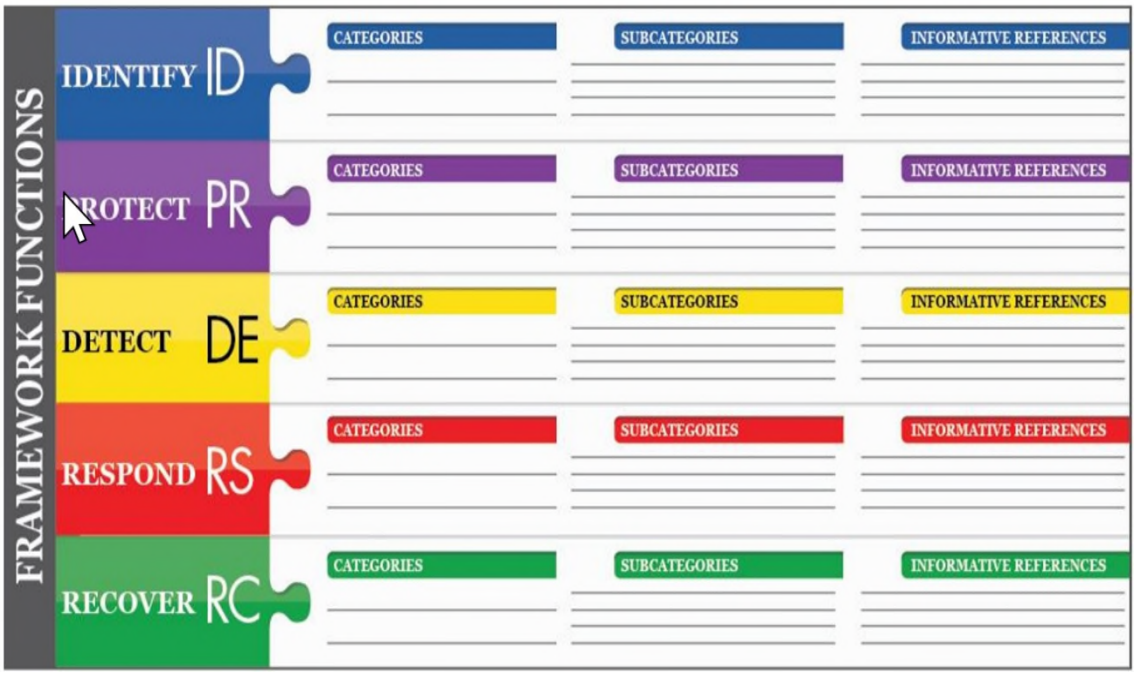


Fig. 5.1. NIST Framework Core

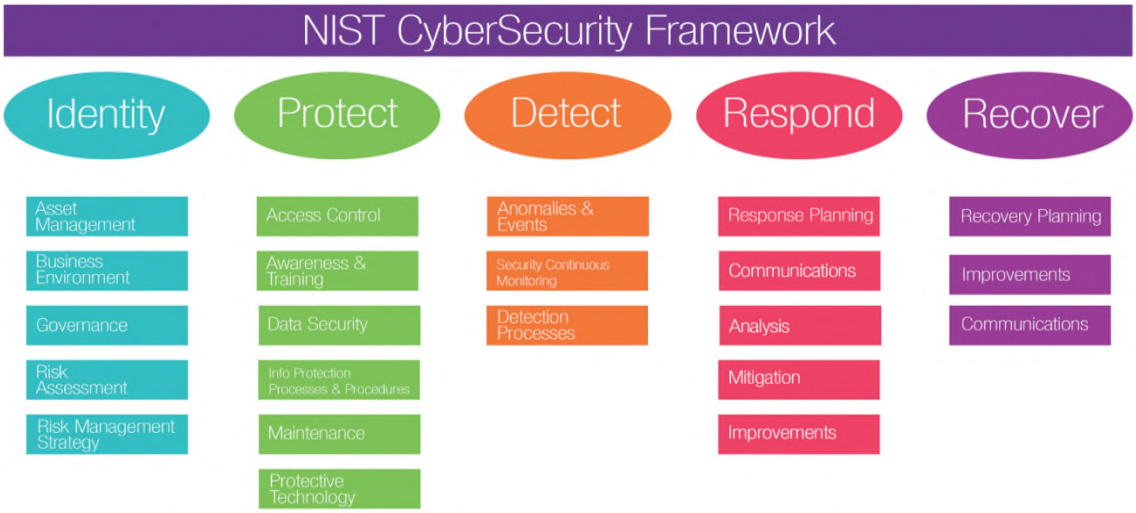


Fig. 5.2. NIST Cybersecurity Framework

This can be considered a high-level approach of an organization's cybersecurity risk management.

The Framework Core elements can be described as follows:

- Functions – cybersecurity activities are organised at a macro level. The Functions are Identify, Protect, Detect, Respond and Recover. Functions help the organisation in communicating its cybersecurity risk management through organising information, enabling risk management decisions, addressing threats and learning by previous experience. It also aligns with the current methodologies for incident management that can be an aid in cybersecurity investment management.
- Categories are the sectors of a Function subdivided into groups of cybersecurity outcomes like 'Asset Management', 'Access Control' and 'Detection Processes.'

- Subcategories are divisions of Categories into specific outcomes of management or technical tasks. They help in the achievement of the outcome of each Category. Examples are ‘Data-at-rest is protected’, ‘External information systems are catalogued’ and ‘Notifications from detection system are investigated.’
- Informative References refer to the specific sections of standards, guidelines and practices that are normally used in the industry.

5.4 NIST Framework Implementation Tiers

(“Tiers”) defines the extent to which an organization’s cybersecurity risk management practices demonstrate the characteristics defined in the NIST Framework. There are four tiers (Partial, Risk Informed, Repeatable and Adaptive) that provide perspective on how an organization assess cybersecurity risk and the activities in place to manage that risk. When selecting the Tier, an organisation should consider the current risk management practices, threat environment, legal and regulatory requirements, information sharing practices, business/mission objectives, cyber supply chain risk management needs, and organizational constraints. Organisations should identify the desired Tier, ensuring that the selected level meets the organisational goals, is feasible to implement, and reduces cybersecurity risk to critical assets and resources to levels acceptable to the organisation. Definitions of Tiers are described below:

5.4.1 Tier 1: Partial

When an organisation is assessed as Tier 1 (Partial), it is highly encouraged to improve moving towards higher Tiers like Tier 2 or greater. This means that the organisation is not mature enough to handle cybersecurity and thus, encouraged to change for the better to reduce cybersecurity risk.

- *Risk Management Process* – the approach to cybersecurity risk management practices are unplanned, informal, and mitigative. Priority for cybersecurity activities may be low.
- *Integrated Risk Management Program* – the approach to managing awareness of cybersecurity risk is limited or has not been established. The organisation may not have processes that enable cybersecurity information to be shared within the organisation.
- *External Participation* – An organisation may not have the practices and processes in place to collaborate with other organisations.
- *Cyber Supply Chain Risk Management* - An organisation may not understand the risk involved in cyber supply chain risks or have the systems in place to identify, assess and mitigate its cyber supply chain risks.

5.4.2 Tier 2: Risk Informed

The organisation in the Tier 2 is better than Tier 1, it has awareness campaign, risk management practices are approved and cascaded down the line. The organisation if aware of its role in the larger ecosystem and understand the cyber supply chain risks.

- *Risk Management Process* – the approach to cybersecurity risk management practices are approved by management but may not be strategically throughout the organization.
- *Integrated Risk Management Program* – the approach to managing awareness of cybersecurity risk is at the organizational level but an organization-wide methodology to managing cybersecurity risk has not been established.
- *External Participation* – The organization understand its responsibility in the larger environment but does not have a formalized approach to impart to external parties.
- *Cyber Supply Chain Risk Management* - An organisation understand the risk involved in cyber supply chain risks or have the systems in place to identify, assess and mitigate its cyber supply chain risks but they haven't formalised the process to manage with suppliers and partners.

5.4.3 Tier 3: Repeatable

The organisation in the Tier 3 is better than Tier 2, its cybersecurity practices are regularly updated, consistent methods are applied to respond effectively to changes, there are collaborations within the organisation in response to events and the organisation has formal agreements with its suppliers and partners in terms of cyber supply management.

- *Risk Management Process* – The organization's risk management practices are officially approved and communicated as policy.
- *Integrated Risk Management Program* – Management of cybersecurity risk is an organization-wide approach.
- *External Participation* – There is collaboration among partners and risk-based management decisions within the organization in response to incidents.
- *Cyber Supply Chain Risk Management* – Management is via enterprise risk management policies, processes and procedures. Organisations' personnel has knowledge and skills to perform cyber supply chain risk management and mitigate its cyber supply chain risks tasks and have formalised the process to manage with suppliers and partners.

5.4.4 Tier 4: Adaptive

The organisation in the Tier 4 is considered the ideal scenario. Its cybersecurity practices are regularly updated, lessons incorporated, there is a trust amongst personnel as the culture is embedded in the system, proactive and open data sharing is evident.

- *Risk Management Process* - There is a process of continuous improvement wherein the organisation adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities.
- *Integrated Risk Management Program* – Cybersecurity risk management is embedded in the organisational culture. Methodology in managing cybersecurity risk is through organisational-wide risk-informed policies, processes, and procedures to address potential cybersecurity incidents.
- *External Participation* – A proactive, accurate and up-to-date information is being distributed and prior to cybersecurity incidents. There is an open sharing of data among partners.
- *Cyber Supply Chain Risk Management* – Organisation can quickly and in an efficiently manner for emerging cyber supply chain risks using real-time or near real-time information and leveraging an institutionalised knowledge of cyber supply chain risk management with its external suppliers. There is an open communication and

uses formal (e.g. agreements) and informal mechanisms to develop and maintain strong relationships with its stakeholders.

5.5 NIST Framework Profile (“Profile”)

The Profile can be considered as the alignment of standards, guidelines, and practices to the Framework Core. Profiles can be characterized as “gap analysis” to identify opportunities for improving cybersecurity posture by comparing a “Current” Profile (the “as found” state) with a “Target” Profile (the “desired” state). The result of the “gap analysis” between the Current Profile and Target Profile can be used to aid prioritization and extent of development.

To enable critical infrastructure suppliers to achieve flexibility, the NIST framework depend on a range of existing standards, guidelines, and practices. Based from these standards, guidelines, and practices, the NIST provides a structure to conduct gap analysis from the current and target state, prioritize improvement action plans, evaluate development to attain the desired target state and communicate among relevant stakeholders about cybersecurity risk.

5.6 ISA 99 (IEC 62443) – Industrial Automation and Control Systems Security

ISA 99 (IEC 62443) [139] aims to establish an industrial automation and control system security program, and is inherently referenced with the NIST framework. **Figure 5.3** [137] represents the elements of the cyber security management system, which has three main categories:

- Risk analysis,
- Addressing risk with the Cybersecurity Management (CSMS), and;
- Monitoring and improving the CSMS

While safety is aimed at protecting the systems from accidental failures to eliminate or minimize hazards, security is focused on protecting the systems from deliberate malicious attacks [34]. Technology in the past did not demand automation systems to be integrated and connected to the Internet. However, due to the proliferation of Internet-connected systems, security has become increasingly important. Even though SIS is typically not connected to the outside world, malicious hacking is still not impossible. With this vulnerability, it is proposed that SIS cybersecurity risk assessment should be included in its design and evaluation. The standard [139] elaborates the elements and provides guidance on what should be included for the establishment of an organization's cybersecurity management system (CSMS) for ICSS as a whole, in which SIS is part of. The CSMS elements pertain in this standard are majority discussed about policy, procedure, practice and personnel management suggesting what should be part of the organization's CSMS.

5.7 Related Works

There have been a few studies relating to the alignment of safety and security. Selected relevant studies are discussed here. The merging of ISA 84 (IEC 61511) and ISA 99 (IEC 62443) lifecycles [13] as depicted in **Figure 5.4** is

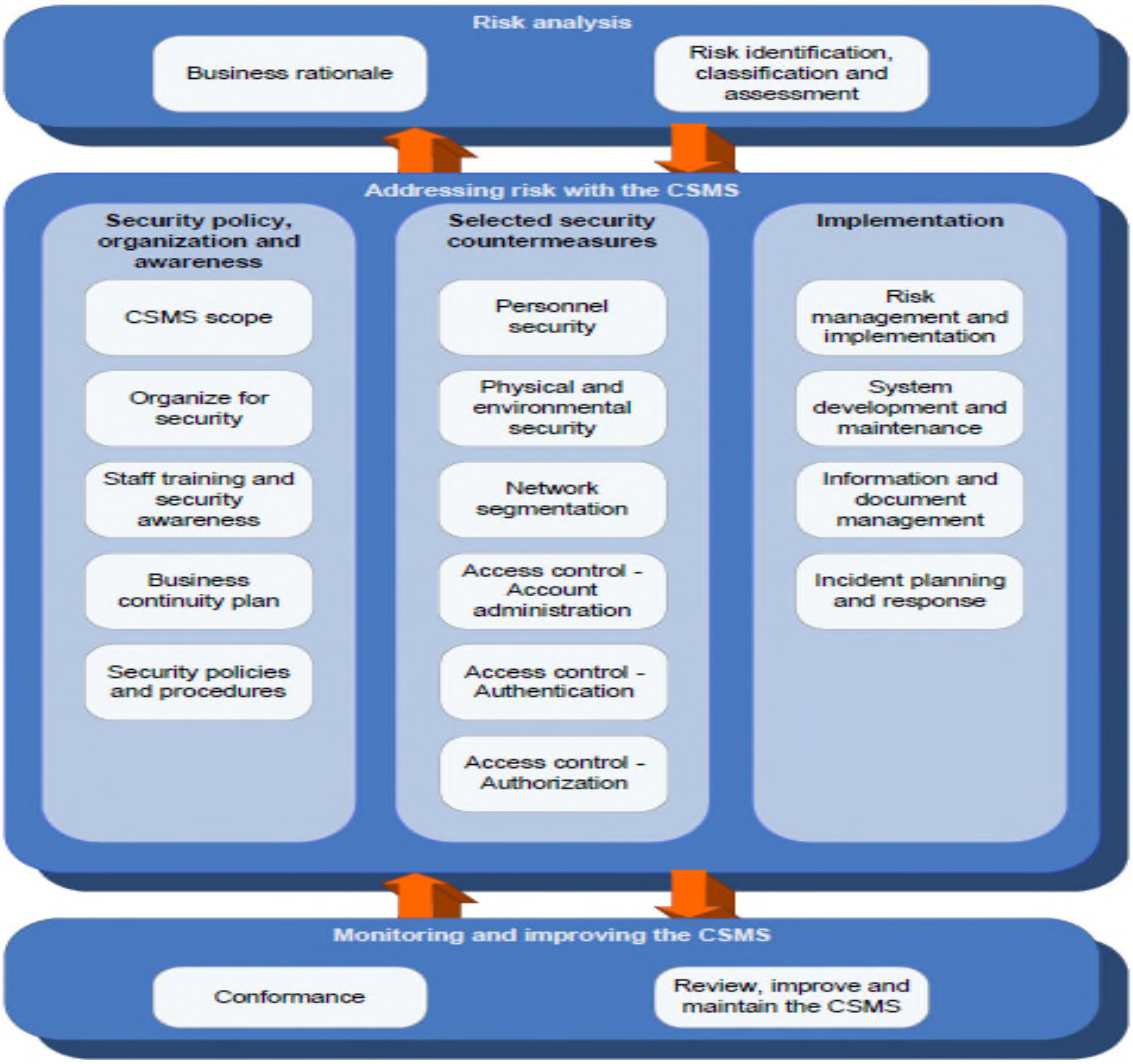


Fig. 5.3. ISA 99 (IEC 62443) [137]

derived by merging safety and security lifecycle phases and is called the Failure-Attack-CounTermeasure (FACT) [13] . **Figure 5.5** shows the interconnection among activities involved in defining safety, security and operational functions. **Figure 5.7** shows the structure of the framework presented in a manner that aligns safety and security within the design stage in a modular concept. These concepts are discussed in the following sections:

5.7.1 Alignment between safety and security standards ISA 84 (IEC 61511) and ISA 99 (IEC 62443)

The alignment is derived by merging safety and security lifecycle phases and is called the Failure-Attack-CounTermeasure (FACT) as the graph shown in **Figure 5.4**. It incorporates safety artefacts (fault trees and safety countermeasures) and security artefacts (attack trees and security analysis) [13]. This proposed alignment between safety and security aims to ensure consistent implementation and help the organization to scrutinize latest system weaknesses, to ultimately provide necessary level of safety and security countermeasures.

The merged safety and security lifecycle model is shown in **Figure 5.4**, which composed of 14 phases. The process begins with safety risk assessment and design phases (phases 1 – 4), borrowed from ISA 84 (IEC 61511), followed by security risk assessment and design phases (phases 5 – 9), from ISA 99 (IEC 62443). The alignment between safety and security is conducted in phase 10. The final phase of the lifecycle, phases 11-14 are the merged phases of ISA 84 and ISA 99 lifecycles and include validation, development, and verification, operation and maintenance, safety and

security monitoring and periodic assessment, and modification and decommissioning related activities.

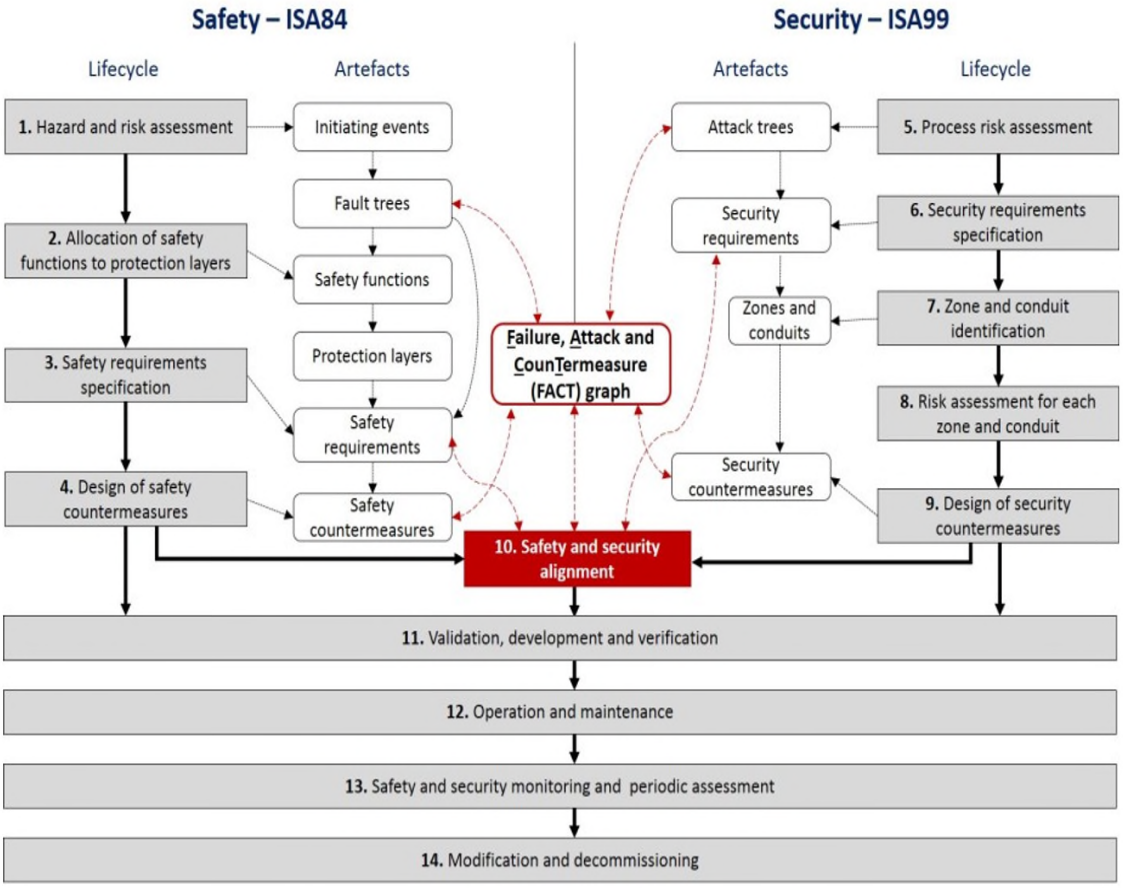


Fig. 5.4. FACT: Merged ISA 84 (IEC 61511) and ISA 99 (IEC 62443) lifecycles [13]

5.7.2 Integrating Industrial Control System (ICS) Safety and Security

The integration of ICS, Safety and Security study [14] proposes some techniques that can be used, and potentially development of ICS security. This provides a logical and structured approach through continual consideration of the effect of decisions on pre-determined and prioritized safety, security and operational functions throughout the design and implementation lifecycle. It proposes some techniques that can be

employed in whole or part, are scalable and are suitable for further investigation, and potentially development by one of the groups currently looking at ICS security.

Figure 5.5 shows the interconnection among activities involved in defining safety, security and operational functions. It is important that each activity stream (Safety, Security and Operational output) must be performed by specialists on their field and then collaboration among them is crucial to the success of the activities.

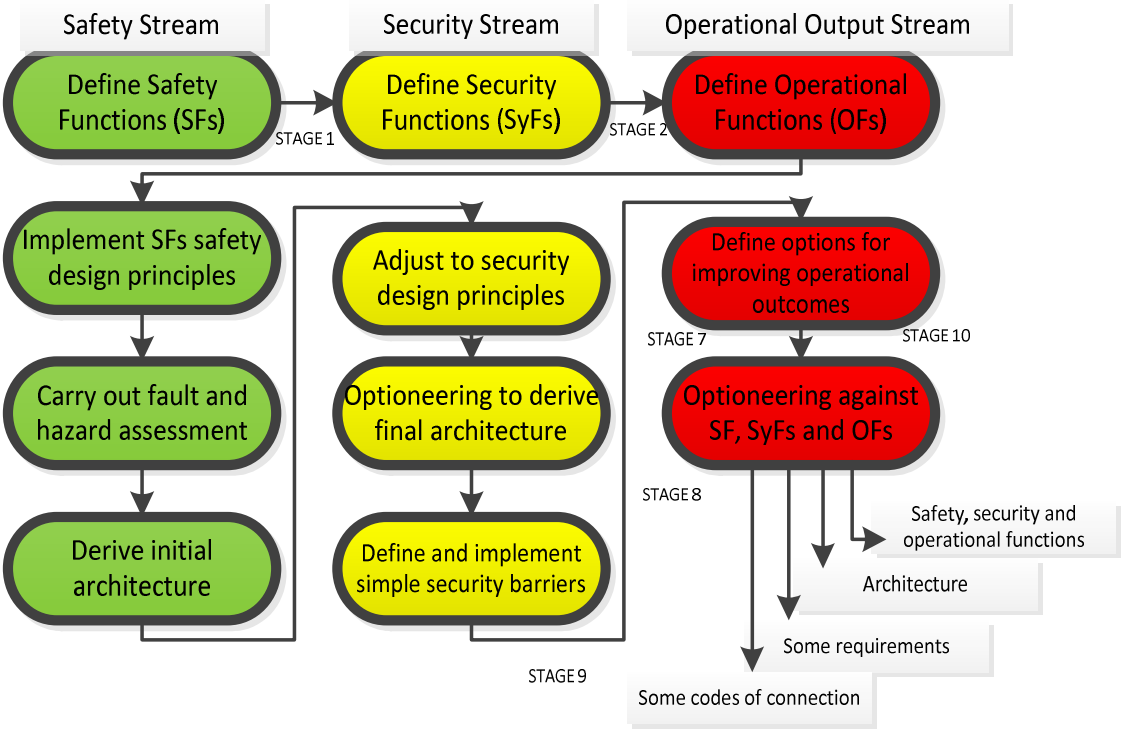


Fig. 5.5. Safety, Security and Operational Output Stream [14]

Several stages need to be conducted to define safety, security and operational functions, define ICS architecture, and once an architecture has been decided, this can be inputted into a design lifecycle. The design lifecycle is based on a V-model as shown in **Figure 5.6.**

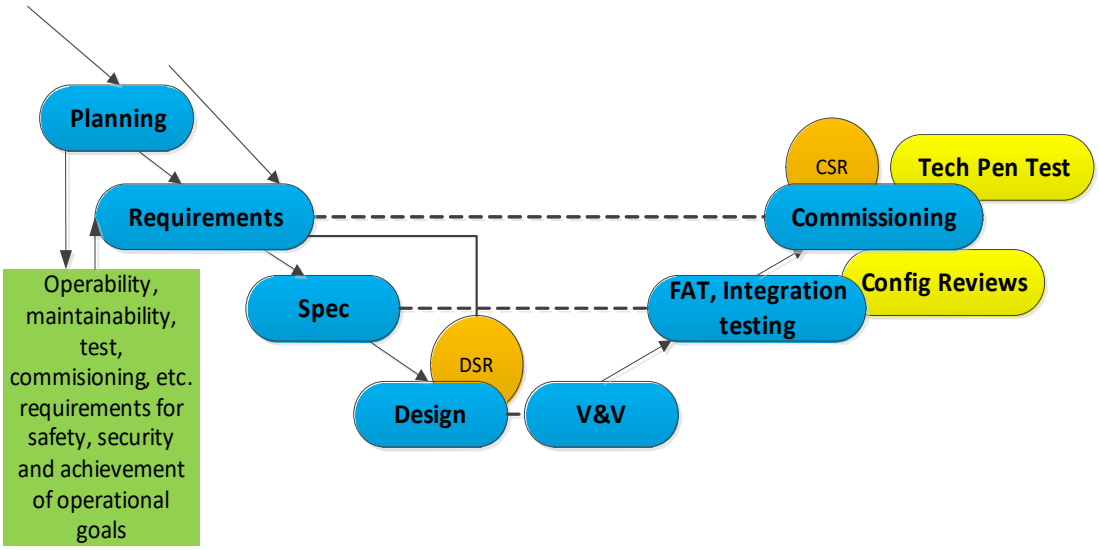


Fig. 5.6. V-model Lifecycle [10]

5.7.3 Safety and security aware framework for the development of feedback control systems

The safety and security aware framework study [15] is for the military drive-by-wire land systems and civilian vehicles. The fundamental part of the study is to propose a framework consists of a Simulink model for the development of feedback control system as shown in **Figure 5.7.** The structure of the framework was presented in a manner that aligns safety and security within the design stage in a modular concept. These systems often include network enabled capability (NEC) allowing the use of electronics architectures to integrate different sub-systems. However, like ICSS, this increased complexity of integration capability is accompanied with augmented safety and cybersecurity risks. The study analyses how the

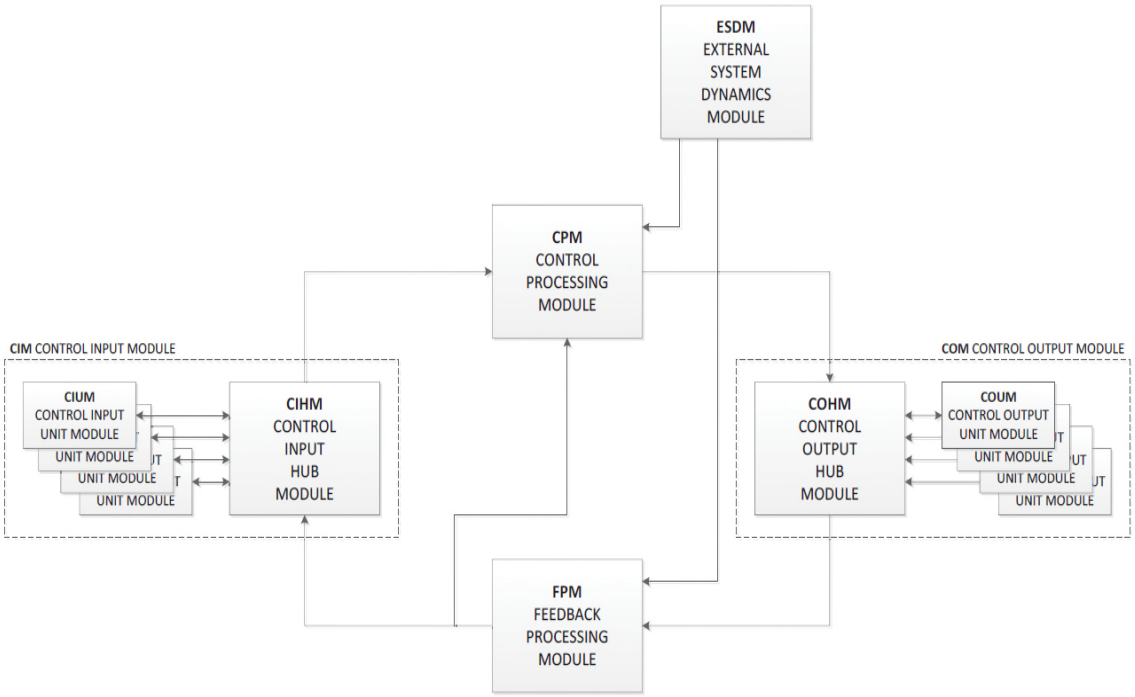


Fig. 5.7. Top level architecture of the Simulink model of the framework [15]

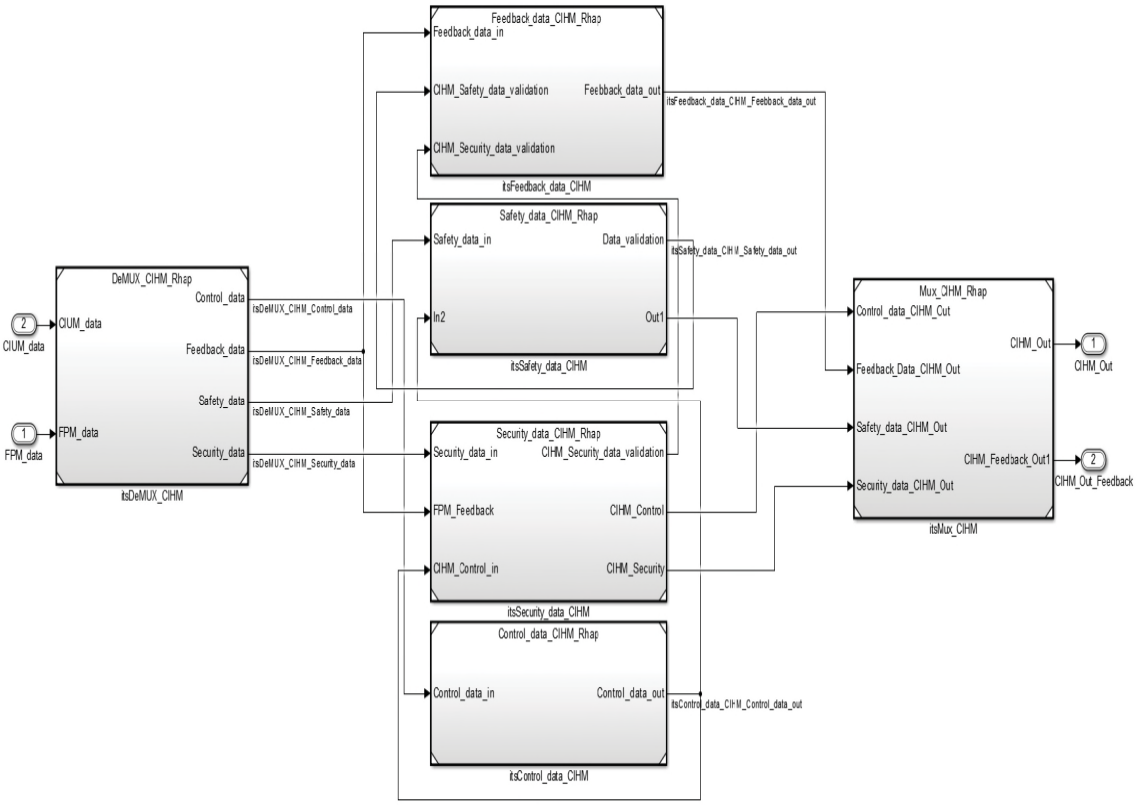


Fig. 5.8. Processing segmentation inside the main modules of the framework [15]

process of developing feedback control system for military land systems could benefit from the use of a framework that addresses safety and security issues at the system modelling level. **Figure 5.8** shows each of the modules except the Control Input Unit Modules (CIUMs) and the Control Output Unit Modules (COUMs) which is made of the sub-modules.

5.8 Overview of the proposal

The core proposal is a seamless integration of cybersecurity framework by the National Institute of Standards and Technology (NIST) [140] with safety and security standards ISA 84 (IEC 61511) [3] and ISA 99 (IEC 62443) [139], and the novel Funnel Risk Graph Method (FRGM) as shown in **Figure 5.9**. Economic benefits and practicality are presented. The Functions [140] can be conducted in parallel and constantly to address the changing cybersecurity and safety risk. Except Risk Assessment and FRGM, functions below are not envisioned to form a sequential path or come to a final complete state, rather it is dynamic.

- Identify – The activities in this function are the building block for operative use of the NIST and FRGM framework. This includes development of the organizational understanding to manage cybersecurity and safety risk to systems, assets, data, and capabilities. Expected outcome categories within this function include: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy as shown in **Figure 5.9.**

- Risk Assessment – This can serve as risk assessment for cybersecurity and for safety. The organization's risk management process can be utilized to analyse the operational environment to distinguish the likelihood and impact of a cybersecurity event. For safety, the organization can utilize FRGM [34]:
- FRGM [6] – Use FRGM instead of using traditional standard methods such as Fault Tree Analysis (FTA), Event Tree Analysis (ETA) and semi-quantitative method Layers of Protection Analysis (LOPA).

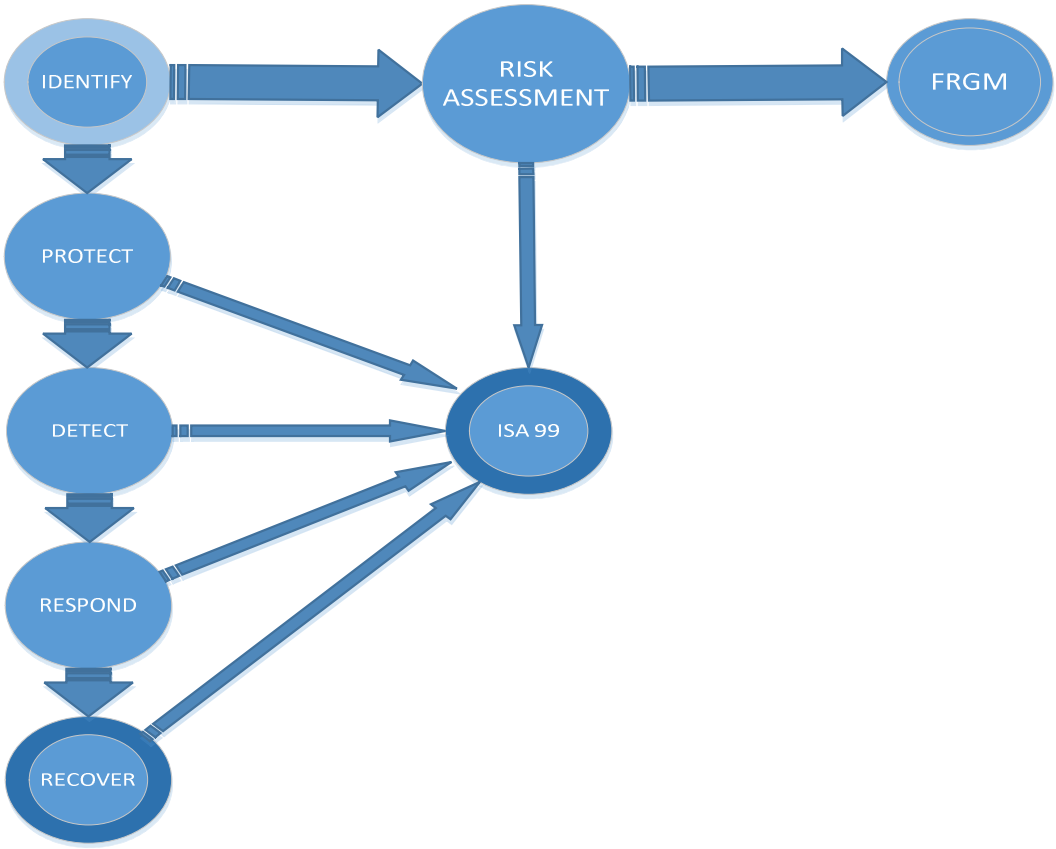


Fig. 5.9. Overview of the alignment framework

- Protect – The Protect function supports the ability to constraint or exclude the impact of a potential cybersecurity incident by development of appropriate measures. Expected outcome categories within this Function include: Access

Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology.

- Detect – The Detect function facilitates suitable detection of cybersecurity incidents through development of appropriate activities. Expected outcome categories within this function includes: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.
- Respond – Mitigative action regarding an identified cybersecurity incident.
- ISA 99 (IEC 62443) – NIST framework is inherently referenced with ISA 99.
- Recover - The Recover function supports timely recovery to normal operations to reduce the impact from a cybersecurity event.

5.9 Detailed Proposal: Alignment of the NIST Framework with the FRGM

Figure 5.10 shows the detailed proposed framework for the alignment of NIST with FRGM. The unified NIST + FRGM framework can be used to evaluate a new cybersecurity and SIS or improve an existing system. These steps are iterative process until appropriate stage has been reached. To better illustrate the process and benefits of this novel approach, a case study is presented in Section 5.10. The steps for the NIST + FRGM framework can be achieved using the following steps:

Step 1: NIST – Identify, Scope and Prioritize.

At a high-level, the organization identifies its business/mission objectives. With this information, the organization makes strategic decisions regarding

cybersecurity and safety implementations and determines the scope of systems and assets that support the selected business line or process. Scoping includes identification and inventory of all assets involved. Using the NIST framework as shown in **Figure 5.10**, the *Identify* step is performed. The activities in the Identify Function provides groundwork for are foundational for valuable use of NIST.

Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritise its efforts, consistent with its risk management strategy and business needs. The activities in the Identify stage are shown in **Figure 5.10** that includes, Asset Management, Business Environment, Governance, Risk Assessment and Risk Management Strategy.

Step 1.1: NIST + FRGM - Perform a Risk Assessment (ID.RA).

The organization's risk management process can be utilised to analyse the operational environment to distinguish the likelihood and impact of a cybersecurity (using ISA 99) event and safety (using ISA 84). This is where the proposed integration of NIST and FRGM takes place. Highlighted boxes in **Figure 5.10** are the path towards FRGM. The combined safety lifecycle process on *Phase 5: Safety Requirements Allocation* using the FRGM was based on [3] in reference to the general scheme described in [2] but characterized as a "*funnel*" approach. The three (3) steps to the FRGM approach are as follows:

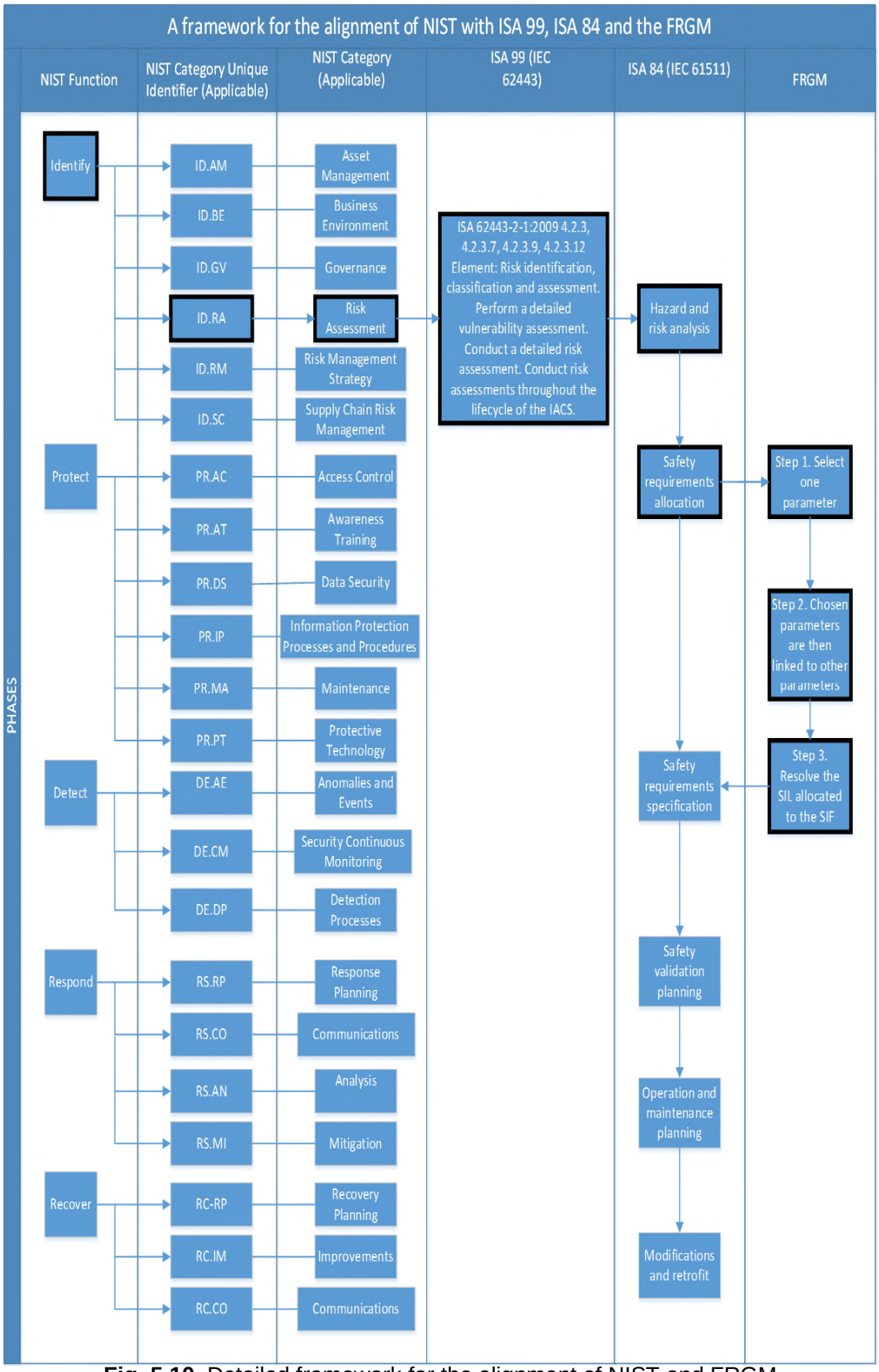


Fig. 5.10. Detailed framework for the alignment of NIST and FRGM

Step 1. Select one parameter (say Consequence C2 parameter) from Figure 4;

Step 2. Chosen parameters are then linked to other parameters (Exposure, Probability, Demand W);

Step 3. Resolve the SIL allocated to the SIF.

For example, Consequence C2, Frequency F1, Probability P1 with demand W3 would yield a SIL1. But if the Probability changes to P2 with the same condition, then SIL2 is allocated. The FRGM approach can also be utilized to enable assessment of SIS where the potential consequences include severe environmental impact or property loss.

Step 2: NIST - Protect – This step involves development and implementation of the required appropriate defenses deployed to critical infrastructure services. The expected result of this step includes Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance and Protective Technology as shown in **Figure 5.10**. This is part of the preventative measures of the Framework.

Step 3: NIST - Detect – This step involves development and implementation of applicable activities to identify the occurrence of a cybersecurity event. This function enables timely discovery of cybersecurity events. Some of the examples of result include Anomalies and Events, Security Continuous Monitoring and Detection Processes. This function is critical such that detection process must be effective to determine real threats and vulnerabilities.

Step 4: NIST - Respond – This step involves development and implementation of applicable activities to take action regarding a detected

cybersecurity event. The Respond function supports the ability to contain the impact of a potential cybersecurity event. Examples of outcome categories within this function include Response Planning, Communications, Analysis, Mitigation and Improvements.

Step 5: NIST - Recover – This step involves development and implementation of applicable activities to maintain plans for resilience and to restore any capabilities or services that were affected due to a cybersecurity event. The Recover function supports timely recovery to normal operations to reduce the impact from a cybersecurity event. Examples of outcome categories within this function include Recovery Planning, Improvements and Communications. Restoration test activities are important to this step.

5.10 Application of the Proposed Framework to a Case Study

This section discusses a case study example **SIF 064FZ-0567 LL** and presents the application of the proposed framework to this real case-study. This SIF is part of LNG Plant A PU6400 discussed in Chapter 4. The **SIF 064FZ-0567 LL** case study from Chapter 4 is re-analysed in this section to illustrate the application of the integrated NIST + FRGM. The objective is to demonstrate how SIL assessment would be impacted in the consideration of cyber security threats.

The focus is on demonstrating how the alignment between safety and security takes place for Case Study **SIF 064FZ-0567 LL** as modelled in **Fig. 5.11.**

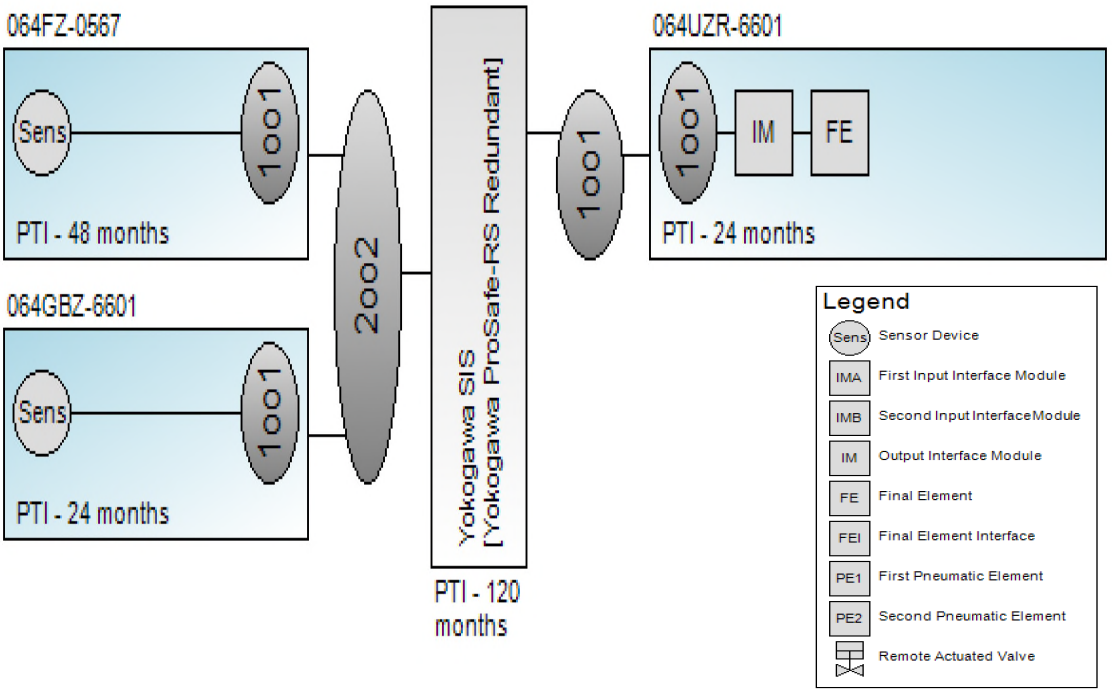


Fig. 5.11. Modelling of the SIF 064FZ-0567 LL Conceptual Design

5.10.1 SIF 064FZ-0567 LL NIST Risk Assessment

The purpose of the cybersecurity risk assessment component under *Identify* NIST Function (ID.RA) per **Figure 5.10.** is to identify threat to organisations or threats directed through organisations against other organisations or the Nation, internal and external vulnerabilities, the adverse impacts (harm) that may occur; the likelihood that harm will occur. The end result of a risk assessment is a determination of risk.

The sensor of SIF 064FZ-0567 LL is a Yokogawa EJX, A and J Series differential pressure transmitter as shown in the photo of **Fig. 5.12.** There is no

cybersecurity risk identified or any known issue for the Yokogawa sensor part of SIF 064FZ-0567 LL.

Fig. 5.12. Sensor of SIF 064FZ-0567 LL

Vulnerability of malware attacks during transmitter configuration/calibration using handheld terminals or through the Plant Resource Manager (PRM) [141] is possible but no known case yet for Yokogawa transmitters. However, Emerson has recorded a vulnerability cybersecurity notification affecting any HART Device Type Manager (DTM) build using CodeWrights DTM Studio [142]. DTMs are used by device configuration software for field device configuration purposes only. This vulnerability can be used to crash an FDT (Field Device Tool) frame application under specific circumstances, requiring a restart of the FDT frame application (not the computer) to resolve. Note that an attacker would require physical access to the HART loop in order to execute this attack. Field devices and Wireless HART installations are unaffected. The impact of SIF 064FZ-0567 LL being out of service is that the control system will speed up running pump.

Level in the tank will decrease; if level is lost, resulting to damage to running downstream pumps. The impact to operations is that the inability to dispose of LNG plant produced water. There is also a potential shutdown of LNG plant A.

For the Logic Solver part, Yokogawa ProSafe-RS Redundant [143] is utilised as shown in **Figure 5.13.**

Fig. 5.13. Logic Solver Yokogawa ProSafe-RS and Workbench

Yokogawa's ProSafe-RS SIS can be integrated with the CENTUM VP integrated production control system and is widely used mainly in ESD applications all over the world. Integration of SIS and ICS has pros and cons. Although flexibility and scalability are a good advantage, however, due to this integration and the use of Windows-based applications, they are vulnerable to cyber-attacks. Yokogawa has claimed that cybersecurity has been strengthened in the release of enhanced version of ProSafe-RS SIS 2017 [144]. From a stand-

alone process network, ICSS has developed into a geographically distributed system as shown in **Figure 5.14**.

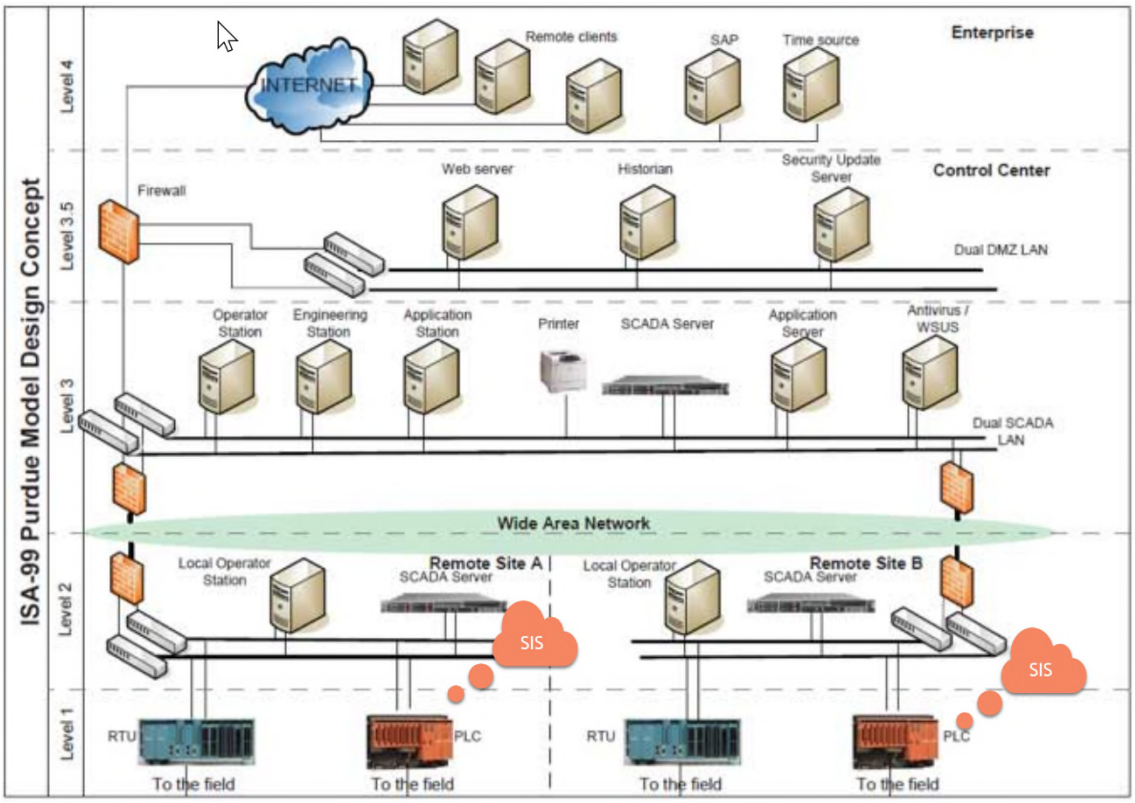


Fig. 5.14. ICSS/SCADA Network, in accordance with ISA-99 [145]

With that, the effects of internet and public networking are inevitable and thus, this vulnerability must be addressed. This requires a different IT security strategy and network orchestration, in which detailed implementation is outside of the scope of this thesis. However, for the purpose of risk assessment of the logic solver, consequence of logic solver failure due to cyber-attacks may lead to plant shutdown causing financial and/or environmental impact, injury or fatality. Normally, the behaviour of the SIS is to bring the process into its fail-safe condition with minimal impact. A similar incident of malicious software attacked on SIS in August 2017 at Saudi Aramco, the world's largest oil company, in what

is considered the first-ever example of malware targeting the computer systems designed to prevent catastrophes [128]. Initially, the internet and office domain were not in direct connection with the process control network. This philosophy has changed significantly since the introduction of SCADA and Manufacturing Execution Systems (MES). There are few strategies on the Physical Protection. The first layer of defense is by Physical Protection. Attacks can be carried out by malicious individuals who have unsecured physical access to the system. Malicious incidents, unexpected infections are becoming more common, for instance by using an infected USB stick. These attacks can range from disconnecting a cable to deliberately pushing a virus by USB or installing a key logger for espionage purposes. By implementing proven methods of system hardening and company security regulations these risks are mitigated. Other methods are network protection, through applying a firewall in an ICSS network, network communications, end-point protection, anti-virus solution, system update, contingency plan, application protection among others [146]. These strategies are more often implemented in plant operations. The consequence of Logic Solver failure is high, however, after implementing the above-mentioned strategies, the risk would bring down to low.

The Final Element part of the SIF 064FZ-0567 LL is 064UZR 6601 with Safety Relay, DTT (Phoenix PSR-SCP-24DC/FSP/1X1/1X2) and MCC Contactor, DTT (Siemens SIRIUS 3RT Series). These relay devices don’t have cybersecurity issues. Considering all factors above, the risk assessment for SIF 064FZ-0567 LL is low.

5.10.2 SIF 064FZ-0567 LL FRGM Risk Assessment

Applying the FRGM approach for SIF 064FZ-0567, the result is SIL 1 as shown in **Figure 5.15.**

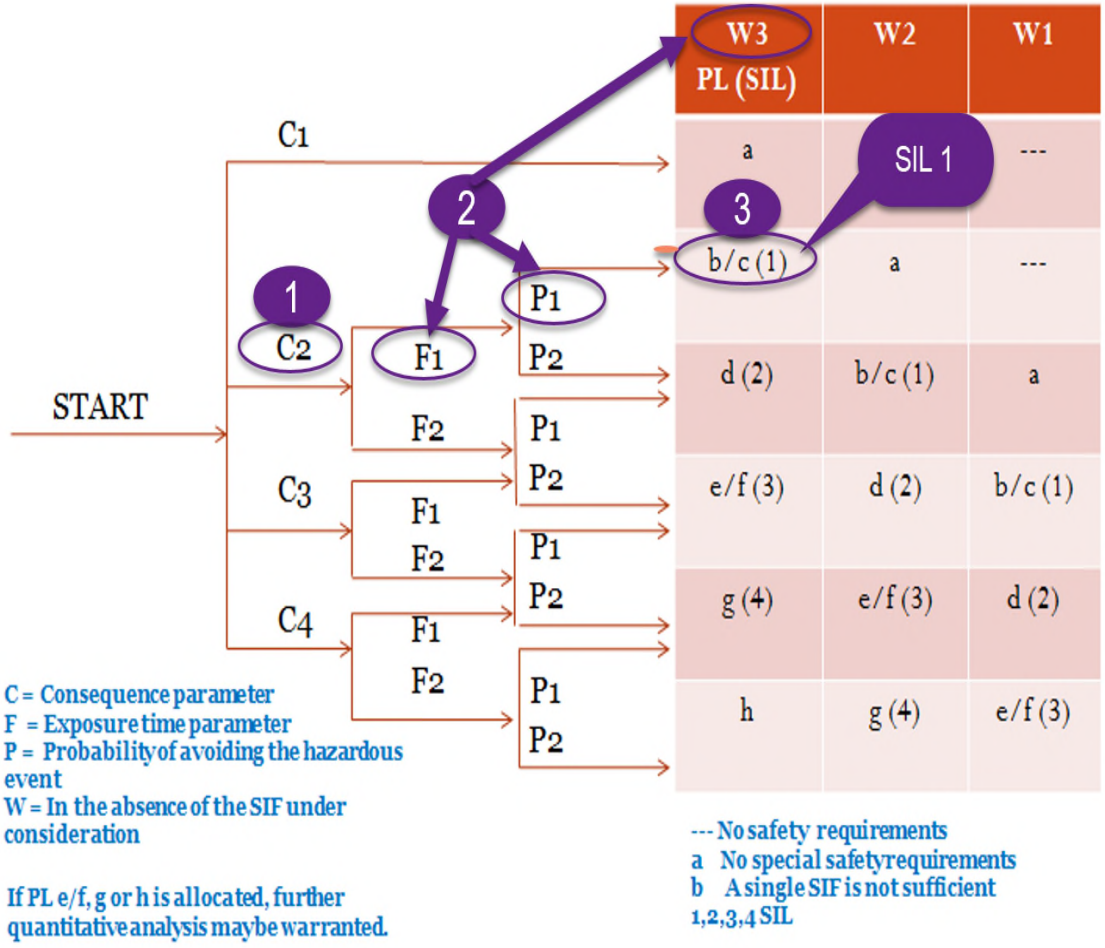


Fig. 5.15. FRGM SIL Determination for SIF 064FZ-0567 – SIL 1

To further verify and calculate the SIL, the functional safety and spurious trip behaviour of the sensor part (Yokogawa EJX, A Series and J Series) of the SIF 064FZ-0567 LL is quantified as follows:

- Sensor part PFDavg: 1.27E-02
- Sensor part HFT: 0
- Sensor part MTTFS: 4251.57 years

Sensor part Architectural Constraints IEC 61508 [2] allow use up to SIL 1. The Sensor part of the 064FZ-0567 LL Safety Instrumented Function has a Maintenance Capability of MCI 2 (Good – 90%). It consists of 2 Sensor Group(s). The voting between these Sensor Groups is 2oo2. A common cause factor of 2% was considered between the groups in this Sensor part as shown in **Fig. 5.16.**

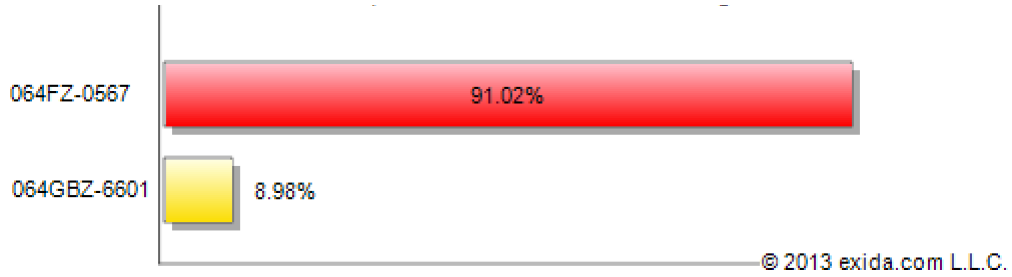


Fig. 5.16. Sensor Group Contribution to Part PFDavg

In order to perform the reliability calculation part of the SIL verification, the following assumptions have been made:

- Mission Time: 15 years
- Startup time: 24 hours
- The SIF operates in Low demand mode.

The systematic capability of the various components in the 064FZ-0567 LL Safety Instrumented Function was not considered. Consequently, the SIL verification performed only addresses the quantitative requirements of IEC 61511 [1].

Considering the reliability data and calculation details described in Chapter 4, the SIF 064FZ-0567 LL achieves the functional safety performance as displayed in **Table 5.1.**

Table 5.1. SIF 064FZ-0567 LL Functional Safety Performance

PFDavg	RRF	SIL (PFDavg)	SIL (Architectural Constraints IEC 61508:2000)	SIL (Systematic Capability)
1.42E-02	70	1	1	N/A

Moreover, **Figure 5.17** shows the SIL Certificate for 064FZ-0567 LL EJX differential pressure transmitter. Therefore, it is verified that this transmitter is SIL3 capable in terms of systematic capability, SIL 2 at HFT = 0; SIL 3 at HFT = 1; Route 1_H. For models where SFF ≥ 90%, SIL 2 at HFT = 0, SIL 3 at HFT = 1; Route 2_H. This has been assessed per the relevant requirements of IEC 61508 [2].

Summing it up, we have evaluated SIF 064FZ-0567 LL against cybersecurity and safety using the proposed Framework of NIST + FRGM. The result showed that the SIF has low cybersecurity risk (after implementing the mentioned strategies) and SIL rating of SIL 1. The primary advantage of this approach is that it ensures all risks (cybersecurity and safety) are considered. Secondarily, optimising the evaluation process into a unified approach would mean significant cost benefit as described in previous chapters.

Fig. 5.17. SIL Certificate for 064FZ-0567 LL EJX Differential Pressure Transmitter

5.11 Conclusion

Recent news about serious security incidents such as *Triton* [127, 147, 148] malware and *WannaCry* [129] ransomware affecting the whole world are heard more often. This complementary chapter of the thesis is dedicated to come up with an integrated and optimised evaluation framework for ICSS and related subsystems considering cybersecurity and safety. This can be achieved by the alignment of the cybersecurity framework formulated by the National Institute of Standards and Technology (NIST) with safety and security standards ISA84 (IEC 61511) and ISA99 (IEC 62443), and the novel Funnel Risk Graph Method (FRGM).

The need of such alignment between safety and security has been recognised by the research community [13-21], the industry, as well as the International Society of Automation (ISA) [22]. Alignment of safety and security has many advantages. Both can utilise the same systems and assets that support the selected business line or process. Evaluating them against cybersecurity threats and safety risks using the integrated NIST and FRGM framework in one approach could eliminate or minimise loss to an organization thus entail economic advantage. For safety risk assessment, given the complexity of process industries, SIL and PL allocation should be performed via a quantitative or semi-quantitative methodology. However, it may be impracticable to apply a semi-quantitative or quantitative approach due to the substantial amount of time and resources involved, thus FRGM [34] approach is proposed as part of Step 4 above. The main difference with this proposed technique is that, instead of jumping into costly and time-consuming methods (semi-quantitative or

quantitative), all SIF will first undergo FRGM (qualitative), which usually takes only a few minutes for each SIF to collaborate with a multi-disciplinary team assuming that calibration process has been completed. Only those SIF which falls under the following category, which typically around 5% of the total SIF, will undergo a quantitative or semi-quantitative method:

- SIF with SIL allocation of more than SIL2 during the FRGM "*initial pass*".
- Did not achieve a satisfactory level of consensus within the multi-disciplinary team during the "*initial pass*".
- Pose a high EUC risk.

Chapter 6 – Summary & Future Works

6.1 Summary

The main focus of this thesis is to explore a more cost-effective, simplified and enhanced approach for the design and evaluation of SIS through the novel FRGM approach. Safety Integrity Level (SIL) and Performance Level (PL) allocation for process, mining and other related industries require deeper level of analysis. For each of the Equipment Under Control (EUC), risks were identified, the level of risk was calculated or estimated and then one or more risk reduction measures were designated. The objective of this risk management approach is to apply sufficient risk reduction measures against the EUC risk such that the "actual risk reduction" exceeds the "necessary risk reduction" to achieve an acceptable "tolerable risk".

Based on this concept, this research project's main aim is to develop and apply an optimised approach for the design and evaluation of ICSS using the FRGM.

Real-life industrial scenarios were analysed to prove the advantage of FRGM over the traditional approach. The specific objectives of this study were to:

1. Develop the framework of the FRGM approach by aligning to the phases of the safety lifecycle as a 'funnel';

2 Present case study analyses to prove the advantages of FRGM over the traditional approach;

3 Carry out an evaluation of different kinds of SIF using FRGM and comparing it to the traditional method. Used verification tools to verify the outcome of the FRGM to show that;

- FRGM will result in equal functional safety;
- FRGM requires few number of steps required and time taken, thus achieving economic benefit.

4 Propose a framework for the alignment of cybersecurity and SIS by integrating FRGM with NIST. Presented a case study to show how the alignment takes place.

As a summary of concepts; all safety standards exist to reduce risk, which is inherent in any industry. It is impossible to eliminate risk and bring about a state of absolute safety. However, more realistically, risk can be categorized as being either negligible, tolerable or unacceptable. The foundation for any modern safety system is to reduce risk to an acceptable or tolerable level. In this context, safety can be defined as ‘freedom from unacceptable risk’.

In *Chapter 2*, various target SIL determination and calculation methodologies have been reviewed and summarised. Comparison of different methods using well-defined criteria, based on collaborative assessments is presented. Furthermore, the advantages and disadvantages of the reviewed methods from complexity, accuracy and cost-effectiveness perspectives are explored.

The risk graph method has gained wide attention due to its simplicity and easy-to-use features [33-35, 65]. The simulations presented in this thesis using the risk graph-based FRGM and comparing to other traditional methods such as LOPA, the FRGM yields more advantages in terms of cost-reduction and ease of use. It can further deduced that the FRGM can be used as a filter to determine lower SIL ratings and practice more rigor at higher SIL. These inherent characteristics of the risk graph method of being coarser and less accurate are not much of a concern as it is proposed to be used as a filter only from a broad range of lower SILs. A lot of resources can be saved utilising this approach [34, 35] as discussed in this work. For higher SILs, which require greater degree of functional safety, extra care must be exercised, and more accurate method must be employed. Careful calibration against the company's risk matrix must be conducted to ensure the accuracy of the FRGM.

In *Chapter 3*, the development of FRGM was explained and explored. FRGM approach is based on qualitative [2, 3] knowledge of the likelihood and consequences of hazardous events, as well as the number of layers of protection available. It is based on the assumption that each added protection layer provides a risk reduction of one order of magnitude. The factors used in the FRGM matrix are:

- Severity rating;
- Likelihood of the hazardous event;
- Number of independent protection layers for the specific hazardous event.

The FRGM is simple and more useful in funnelling a large number of SIFs and then determine which SIFs need further evaluation. Specifically, the FRGM is best useful as a first screening pass prior to using quantitative or semi-quantitative methods such as the LOPA. The development of FRGM was extensively explained and has been applied in a real-world case examples with different SIL ratings. Comparison between different methodologies using different kinds of SIFs were also discussed, highlighting the advantage derived from utilising the FRGM. Further analyses of novel SIL determination methods were discussed with its notable complexity. The benefit calculation and sensitivity analysis were presented after calibration of the FRGM using an example risk matrix.

In *Chapter 4*, SIL calculations were performed for each Safety Instrumented Function (SIF) loop that has been assigned a SIL target of SIL 1 or greater. SIL1 or greater was chosen on the assumption that the company risk matrix calibration called to do so. SIL targets for Safety Instrumented Function (SIF) loops were assigned during PHA/SOA studies. Detailed SIL calculations were presented for process unit 6400 with target and achieved SILs using exSILentia, coupled with the latest reliability database SERH. Calculations were based on the actual hardware selected for the Sensor, the Logic Solver and the Final Element. Results from FRGM approach were compared to the same SIFs. Cost reduction were realised initially for Process Unit 6400. Considering the entire LNG Plant A, which has around 3,000 SIFs and cost reduction was realised amounting to around $3,906,000.

Finally, in *Chapter 5*, the consideration of cybersecurity for SIS was proposed. Alignment of safety and security has many advantages. Both can utilise the same systems and assets that support the selected business line or process. The safe and secure operation of critical infrastructure is dependent on appropriate responses to safety, security and operational priorities into Integrated Control and Safety Systems (ICSS), at design stage and throughout the life of the system. Digitisation as well as networked automation and control infrastructures have increased in the past years and are leading to remarkable potential security risks. Recent news about serious security incidents such as *Triton* malware and *WannaCry* ransomware affecting the whole world are heard more often. This complementary chapter of the thesis is dedicated to come up with an integrated and optimised evaluation framework for ICSS and related subsystems considering cybersecurity and safety. This can be achieved by the alignment of the cybersecurity framework formulated by the National Institute of Standards and Technology (NIST) with safety and security standards ISA84 (IEC 61511) and ISA99 (IEC 62443), and the novel Funnel Risk Graph Method (FRGM). The need of such alignment between safety and security has been recognised by the research community, the industry, as well as the International Society of Automation (ISA).

Evaluating them against cybersecurity threats and safety risks using the integrated NIST and FRGM framework in one approach could eliminate or minimise loss to an organization; thus, entail economic advantage. For safety risk assessment, given the complexity of process industries, SIL and PL allocation should be performed via a quantitative or semi-quantitative methodology.

However, it may be impracticable to apply a semi-quantitative or quantitative approach due to the substantial amount of time and resources involved, thus FRGM [34] approach is proposed as part of the steps. The main difference with this proposed technique is that, instead of jumping into costly and time-consuming methods (semi-quantitative or quantitative), all SIF will first undergo FRGM (qualitative), which usually takes only a few minutes for each SIF to collaborate with a multi-disciplinary team assuming that calibration process has been completed. Only those SIF which falls under the following category, which typically around 5% of the total SIF, will undergo a quantitative or semi-quantitative method:

- SIF with SIL allocation of more than SIL2 during the FRGM "*initial pass*".
- Did not achieve a satisfactory level of consensus within the multi-disciplinary team during the "*initial pass*".
- Pose a high EUC risk.

6.2 Future Works

The scope of this work is limited to the development of FGRM and proposal for integrating ICSS cybersecurity. Future work needs to be developed on the aspect of cybersecurity of ICSS and integrating with FRGM. Over the last several decades we have seen a range of cyber-attacks on ICSS and critical infrastructure. The first recorded cyber-attack on critical infrastructure happened at the Trans-Siberian pipeline [149] in 1982. This incident has resulted into an explosion visible from space. In 2003, a slammer worm penetrated a network at

the Davies-Besse nuclear plant in Ohio [150]. A computer virus named Sobig shut down Florida's train signalling systems [149]. A hacker penetrated the operation system of a water treatment facility in Harrisburg, USA [150]. The Stuxnet malware which was used against Iran in 2010 and Industroyer, believed was deployed to attack Ukraine in 2016. In December 2017, a malware called Triton [147] attacked Triconex Safety Instrumented Systems. Triton is one of a limited malware kind that targeted the ICS.

Evaluating ICSS and related subsystems against cybersecurity threats and safety risks using the integrated NIST and FRGM framework in one approach as presented in this thesis could eliminate or minimise loss to an organization; thus, entail economic advantage.

With the current trend of integrating BPCS and SIS in a single network, an integrated safety and security evaluation framework for ICSS and related subsystems such as FRGM + NIST can still be further explored. The need of such alignment between safety and security has been recognised by the research community, the industry, as well as the International Society of Automation (ISA).

References

[1] W. E. Anderson, "Risk analysis methodology applied to industrial machine development," *IEEE Transactions on Industry Applications,* vol. 41, no. 1, pp. 180-187, 2005.

[2] IEC, "IEC 61508 1-7. Functional safety of electrical / electronic /programmable electronic safety-related systems, parts 1-7," 2010.

[3] IEC, "IEC 61511 1-3. Functional safety—safety instrumented systems for the process industry sector. Parts 1–3," 2003.

[4] M. Catelani, L. Ciani, and V. Luongo, "A simplified procedure for the analysis of Safety Instrumented Systems in the process industry application," *Microelectronics Reliability,* vol. 51, no. 9, pp. 1503-1507, 2011/09/01/ 2011.

[5] H. Gall, "Functional safety IEC 61508 / IEC 61511 the impact to certification and the user," in *2008 IEEE/ACS International Conference on Computer Systems and Applications*, 2008, pp. 1027-1031.

[6] D. Kirkwood and B. Tibbs, "Developments in SIL determination," *Computing & Control Engineering Journal,* vol. 16, no. 3, pp. 21-27, 2005.

[7] K. B. a. P. S. L. Moore, "Performance Based Safety Standards: An Integrated Risk Assessment Program," *Instrumentation Society of America,* vol. Tech. Rep, 1997.

[8] C. S. a. J. A. M. Sallak, "A Fuzzy Probabilistic Approach for Determining Safety Integrity Level," *IEEE Transactions on Fuzzy Systems,* vol. vol.16, no. no.1, pp. pp.239-248, 2008.

[9] B. Schrörs, "Functional Safety: IEC 61511 and the industrial implementation," vol. vol. 1, no. no.1, pp. pp.45-48, 15-18 2010.

[10] M. Punch, "Functional Safety for the Mining and Machinery-based Industries," vol. 2nd Ed, 2010, 2013.

[11] M. L. a. D. Harp, "Breaches on the Rise in Control Systems: A SANS Survey," 2014.

[12] M. Generowicz, "Functional Safety: the Next Edition of IEC 61511," 2015.

[13] G. Sabaliauskaite and A. P. Mathur, "Aligning cyber-physical system safety and security," in *Complex Systems Design & Management Asia*: Springer, Cham, 2015, pp. 41-53.

[14] A. Ellis, "Integrating Industrial Control System (ICS) safety and security — A potential approach," *10th IET System Safety and Cyber-Security Conference 2015, Bristol,* pp. pp. 1-7. doi: 10.1049/cp.2015.0294., 2015.

[15] P. C. a. E. S. J. P. Lobo, "Safety and security aware framework for the development of feedback control systems," *10th IET System Safety and Cyber-Security Conference 2015, Bristol,* pp. pp. 1-5. doi: 10.1049/cp.2015.0280., 2015.

[16] Z. Li and M. Shahidehpour, "Deployment of cybersecurity for managing traffic efficiency and safety in smart cities," *The Electricity Journal,* vol. 30, no. 4, pp. 52-61, 2017/05/01/ 2017.

[17] J. Ross, "Cybersecurity: A Real Threat to Patient Safety," *Journal of PeriAnesthesia Nursing,* vol.

32, no. 4, pp. 370-372, 2017/08/01/ 2017.

[18] G. Stoneburner, "Toward a Unified Security-Safety Model," *Computer*, vol. 39, no. 8, pp. 96-97, 2006.

[19] L. Pietre-Cambacedes and M. Bouissou, *Modeling safety and security interdependencies with BDMP (Boolean logic Driven Markov Processes)*. 2010, pp. 2852-2861.

[20] A. Banerjee, K. K. Venkatasubramanian, T. Mukherjee, and S. K. S. Gupta, "Ensuring Safety, Security, and Sustainability of Mission-Critical Cyber–Physical Systems," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 283-299, 2012.

[21] L. Piètre-Cambacédès and M. Bouissou, "Cross-fertilization between safety and security engineering," *Reliability Engineering & System Safety*, vol. 110, pp. 110-126, 2013/02/01/ 2013.

[22] I. W. G. 7, "Safety and Security (Joint with ISA 84 committee). http://isa99.isa.org/ISA99%20Wiki/WG7.aspx (accessed on 11 April 2014)." *ISA*, 2014.

[23] IEC, "IEC 62061. Safety of machinery – functional safety of safety-related electrical, electronic and programmable electronic control systems. ," 2005.

[24] ISO, "ISO13849-1. Safety of machinery -Safety-related parts of control systems.," 2006.

[25] AS, "Australian Standards. AS4024.1, Safeguarding of machinery. Australian Standards. AS4024.3610, Safety of machinery-conveyors- General requirements. Australian Standards. AS4024.3611, Safety of machinery-Part3611: Conveyors-Belt conveyors for bulk materials handling.," 2006.

[26] M. A. Lundteigen and M. Rausand, "Common cause failures in safety instrumented systems on oil and gas installations: Implementing defense measures through function testing," *Journal of Loss Prevention in the Process Industries*, vol. 20, no. 3, pp. 218-229, 2007/05/01/ 2007.

[27] IEC, "IEC 61508-6. Functional safety of electrical / electronic /programmable electronic safety-related systems – Part 6: guidelines on the application of IEC 61508- 2 and IEC 61508-3," 2010.

[28] P. Baybutt, "Using risk tolerance criteria to determine safety integrity levels for safety instrumented functions," *Journal of Loss Prevention in the Process Industries*, vol. 25, no. 6, pp. 1000-1009, 2012/11/01/ 2012.

[29] F. Wang, O. Yang, R. Zhang, and L. Shi, "Method for assigning safety integrity level (SIL) during design of safety instrumented systems (SIS) from database," *Journal of Loss Prevention in the Process Industries*, vol. 44, no. Supplement C, pp. 212-222, 2016/11/01/ 2016.

[30] A. E. Summers, "Viewpoint on ISA TR84.0.02 — simplified methods and fault tree analysis," *ISA Transactions*, vol. 39, no. 2, pp. 125-131, 2000/04/01/ 2000.

[31] S. K. Kim and Y. S. Kim, "An evaluation approach using a HARA and FMEDA for the hardware SIL," *Journal of Loss Prevention in the Process Industries*, vol. 26, no. 6, pp. 1212-1220, 2013/11/01/ 2013.

[32] K. Chang, S. Kim, D. Chang, J. Ahn, and E. Zio, "Uncertainty analysis for target SIL determination in the offshore industry," *Journal of Loss Prevention in the Process Industries*, vol. 34, pp. 151-162, 2015/03/01/ 2015.

[33] A. C. Torres-Echeverria, "On the use of LOPA and risk graphs for SIL determination," *Journal of*

Loss Prevention in the Process Industries, vol. 41, no. Supplement C, pp. 333-343, 2016/05/01/ 2016.

[34] A. Gabriel, "Design and Evaluation of Safety Instrumented Systems: A Simplified and Enhanced Approach," *IEEE Access,* vol. 5, pp. 3813-3823, 2017.

[35] A. Gabriel, J. Shi, and C. Ozansoy, "A Proposed Alignment of the National Institute of Standards and Technology Framework with the Funnel Risk Graph Method," *IEEE Access,* vol. 5, pp. 12103-12113, 2017.

[36] T. Aven and E. Zio, "Some considerations on the treatment of uncertainties in risk assessment for practical decision making," *Reliability Engineering & System Safety,* vol. 96, no. 1, pp. 64-74, 2011/01/01/ 2011.

[37] M. Khalil, M. A. Abdou, M. S. Mansour, H. A. Farag, and M. E. Ossman, "A cascaded fuzzy-LOPA risk assessment model applied in natural gas industry," *Journal of Loss Prevention in the Process Industries,* vol. 25, no. 6, pp. 877-882, 2012/11/01/ 2012.

[38] E. H. Mamdani, "Application of fuzzy algorithms for control of simple dynamic plant," *Electrical Engineers, Proceedings of the Institution of,* vol. 121, no. 12, pp. 1585-1588, 1974.

[39] L. Ding, H. Wang, K. Kang, and K. Wang, "A novel method for SIL verification based on system degradation using reliability block diagram," *Reliability Engineering & System Safety,* vol. 132, pp. 36-45, 2014/12/01/ 2014.

[40] Y. Dutuit, F. Innal, A. Rauzy, and J. P. Signoret, "Probabilistic assessments in relationship with safety integrity levels by using Fault Trees," *Reliability Engineering & System Safety,* vol. 93, no. 12, pp. 1867-1876, 2008/12/01/ 2008.

[41] R. Nait-Said, F. Zidani, and N. Ouzraoui, "Modified risk graph method using fuzzy rule-based approach," *Journal of Hazardous Materials,* vol. 164, no. 2, pp. 651-658, 2009/05/30/ 2009.

[42] Y. D. Shu and J. S. Zhao, "A simplified Markov-based approach for safety integrity level verification," (in English), *Journal of Loss Prevention in The Process Industries,* vol. 29, pp. 262-266, 2014.

[43] B. Knegtering and A. C. Brombacher, "Application of micro Markov models for quantitative safety assessment to determine safety integrity levels as defined by the IEC 61508 standard for functional safety," *Reliability Engineering & System Safety,* vol. 66, no. 2, pp. 171-175, 1999/11/01/ 1999.

[44] R. Pilch, "Extending the Possibilities of Quantitative Determination of SIL – a Procedure Based on IEC 61508 and the Markov Model with Common Cause Failures," *Quality and Reliability Engineering International,* vol. 33, no. 2, pp. 337-346, 2017.

[45] M. Sallak, C. Simon, and J. F. Aubry, "A Fuzzy Probabilistic Approach for Determining Safety Integrity Level," *IEEE Transactions on Fuzzy Systems,* vol. 16, no. 1, pp. 239-248, 2008.

[46] L. Beckman, "Expanding the applicability of ISA TR84.02 in the field," *ISA Transactions,* vol. 39, no. 3, pp. 357-361, 2000/07/01/ 2000.

[47] P. Stavrianidis and K. Bhimavarapu, "Safety instrumented functions and safety integrity levels (SIL)," *ISA Transactions,* vol. 37, no. 4, pp. 337-351, 1998/09/01/ 1998.

[48] ISA, "ISA-TR84.00.02-2002, Safety Instrumented Functions (SIF), Safety Integrity Level (SIL),

Evaluation techniques.," 2002.

[49] H. Jahanian, "Generalizing PFD formulas of IEC 61508 for KooN configurations," *ISA Transactions*, vol. 55, pp. 168-174, 2015/03/01/ 2015.

[50] T. Zhang, W. Long, and Y. Sato, "Availability of systems with self-diagnostic components—applying Markov model to IEC 61508-6," *Reliability Engineering & System Safety*, vol. 80, no. 2, pp. 133-141, 2003/05/01/ 2003.

[51] L. Lu and G. Lewis, "Configuration determination for k-out-of-n partially redundant systems," *Reliability Engineering & System Safety*, vol. 93, no. 11, pp. 1594-1604, 2008/11/01/ 2008.

[52] L. F. Oliveria, "Evaluating the PFD of instrumented safety systems with partial stroke testing. ," in *Proceedings of the Annual Reliability and Maintainability Symposium*, Hong Kong, China, 2008.

[53] R. N. A. Luiz Fernando Oliveira, "Extension of ISA TR84.00.02 PFD equations to KooN architectures," *Reliability Engineering & System Safety*, vol. 95, pp. 707-715, 2010.

[54] Z. T. Long W, Oshima M., "Quantitative Evaluation on Safety - related Systems 2002.," 2002.

[55] A. C. Torres-Echeverría, S. Martorell, and H. A. Thompson, "Modeling safety instrumented systems with MooN voting architectures addressing system reconfiguration for testing," *Reliability Engineering & System Safety*, vol. 96, no. 5, pp. 545-563, 2011/05/01/ 2011.

[56] M. Rausand, "Reliability of Safety-Critical Systems: Theory and Applications," in *Reliability of Safety-Critical Systems*: John Wiley & Sons, Inc., 2014, pp. i-xviii.

[57] H. Jin and M. Rausand, "Reliability of safety-instrumented systems subject to partial testing and common-cause failures," *Reliability Engineering & System Safety*, vol. 121, no. Supplement C, pp. 146-151, 2014/01/01/ 2014.

[58] H. Guo and X. Yang, "A simple reliability block diagram method for safety integrity verification," *Reliability Engineering & System Safety*, vol. 92, no. 9, pp. 1267-1273, 2007/09/01/ 2007.

[59] J. K. Vaurio, "Unavailability equations for k-out-of-n systems," *Reliability Engineering & System Safety*, vol. 96, no. 2, pp. 350-352, 2011/02/01/ 2011.

[60] M. Chebila and F. Innal, "Generalized analytical expressions for safety instrumented systems' performance measures: PFDavg and PFH," *Journal of Loss Prevention in the Process Industries*, vol. 34, no. Supplement C, pp. 167-176, 2015/03/01/ 2015.

[61] R. Ouache, M. N. Kabir, and A. A. J. Adham, "A reliability model for safety instrumented system," *Safety Science*, vol. 80, pp. 264-273, 2015/12/01/ 2015.

[62] W. Mechri, C. Simon, and K. BenOthman, "Switching Markov chains for a holistic modeling of SIS unavailability," *Reliability Engineering & System Safety*, vol. 133, pp. 212-222, 2015.

[63] Y. Langeron, A. Barros, A. Grall, and C. Bérenguer, "Combination of safety integrity levels (SILs): A study of IEC61508 merging rules," *Journal of Loss Prevention in the Process Industries*, vol. 21, no. 4, pp. 437-449, 2008/07/01/ 2008.

[64] Y. Liu and M. Rausand, "Reliability assessment of safety instrumented systems subject to different demand modes," *Journal of Loss Prevention in the Process Industries*, vol. 24, no. 1, pp. 49-56, 2011/01/01/ 2011.

[65] A. Baghaei, "3-Parameters SPW technique: A new method for evaluation of target safety integrity level," *Journal of Loss Prevention in the Process Industries*, vol. 26, no. 6, pp. 1257-1261, 2013/11/01/ 2013.

[66] B. Cai, Y. Liu, and Q. Fan, "A multiphase dynamic Bayesian networks methodology for the determination of safety integrity levels," *Reliability Engineering & System Safety*, vol. 150, pp. 105-115, 2016/06/01/ 2016.

[67] K. Tsilipanos, I. Neokosmidis, and D. Varoutas, "A System of Systems Framework for the Reliability Assessment of Telecommunications Networks," *IEEE Systems Journal*, vol. 7, no. 1, pp. 114-124, 2013.

[68] O. Doguc and J. Emmanuel Ramirez-Marquez, "An automated method for estimating reliability of grid systems using Bayesian networks," *Reliability Engineering & System Safety*, vol. 104, pp. 96-105, 2012/08/01/ 2012.

[69] Y. Jiang *et al.*, "Bayesian-Network-Based Reliability Analysis of PLC Systems," *IEEE Transactions on Industrial Electronics*, vol. 60, no. 11, pp. 5325-5336, 2013.

[70] L. Zhang, X. Wu, M. J. Skibniewski, J. Zhong, and Y. Lu, "Bayesian-network-based safety risk analysis in construction projects," *Reliability Engineering & System Safety*, vol. 131, pp. 29-39, 2014/11/01/ 2014.

[71] T. Daemi and A. Ebrahimi, "Detailed reliability assessment of composite power systems considering load variation and weather conditions using the Bayesian network," *International Transactions on Electrical Energy Systems*, vol. 24, no. 3, pp. 305-317, 2014.

[72] F. Innal, Y. Dutuit, and M. Chebila, "Safety and operational integrity evaluation and design optimization of safety instrumented systems," *Reliability Engineering & System Safety*, vol. 134, pp. 32-50, 2015/02/01/ 2015.

[73] P. Baraldi, L. Podofillini, L. Mkrtchyan, E. Zio, and V. N. Dang, "Comparing the treatment of uncertainty in Bayesian networks and fuzzy expert systems used for a human reliability analysis application," *Reliability Engineering & System Safety*, vol. 138, pp. 176-193, 2015/06/01/ 2015.

[74] A. O'Connor and A. Mosleh, "A general cause based methodology for analysis of common cause and dependent failures in system risk and reliability assessments," *Reliability Engineering & System Safety*, vol. 145, pp. 341-350, 2016/01/01/ 2016.

[75] B. Cai, Y. Liu, Z. Liu, X. Tian, X. Dong, and S. Yu, "Using Bayesian networks in reliability evaluation for subsea blowout preventer control system," *Reliability Engineering & System Safety*, vol. 108, pp. 32-41, 2012/12/01/ 2012.

[76] B. Cai, Y. Liu, Z. Liu, F. Wang, X. Tian, and Y. Zhang, "Development of an automatic subsea blowout preventer stack control system using PLC based SCADA," *ISA Transactions*, vol. 51, no. 1, pp. 198-207, 2012/01/01/ 2012.

[77] B. Cai, Y. Liu, Y. Ma, L. Huang, and Z. Liu, "A framework for the reliability evaluation of grid-connected photovoltaic systems in the presence of intermittent faults," *Energy*, vol. 93, pp. 1308-1320, 2015/12/15/ 2015.

[78] P. A. P. Ramírez and I. B. Utne, "Use of dynamic Bayesian networks for life extension assessment of ageing systems," *Reliability Engineering & System Safety*, vol. 133, pp. 119-136, 2015/01/01/ 2015.

[79] F. Flammini, S. Marrone, N. Mazzocca, and V. Vittorini, "A new modeling approach to the safety evaluation of N-modular redundant computer systems in presence of imperfect maintenance," *Reliability Engineering & System Safety*, vol. 94, no. 9, pp. 1422-1432, 2009/09/01/ 2009.

[80] F. Flammini, S. Marrone, N. Mazzocca, R. Nardone, and V. Vittorini, "Using Bayesian Networks to evaluate the trustworthiness of '2 out of 3' decision fusion mechanisms in multi-sensor applications," *IFAC-PapersOnLine*, vol. 48, no. 21, pp. 682-687, 2015/01/01/ 2015.

[81] ISA, "ISA-TR84.00.02. Safety instrumented functions (SIF) – safety integrity level (SIL) evaluation techniques, Part1–5," *ISA*, 2002.

[82] P. Stavrianidis and K. Bhimavarapu, "Performance-based standards: safety instrumented functions and safety integrity levels," *Journal of Hazardous Materials*, vol. 71, no. 1, pp. 449-465, 2000/01/07/ 2000.

[83] IEC, "International Electrotechnical Commission (IEC 61078). Analysis techniques for dependability – reliability block diagram and Boolean methods," 2006.

[84] G. Kaczor, S. Młynarski, and M. Szkoda, "Verification of safety integrity level with the application of Monte Carlo simulation and reliability block diagrams," *Journal of Loss Prevention in the Process Industries*, vol. 41, no. Supplement C, pp. 31-39, 2016/05/01/ 2016.

[85] IEC, "International Electrotechnical Commission (IEC 61165). Application of Markov techniques," 2006.

[86] G. W. M. Bukowski J V, "Using Markov models for safety analysis of programmable electronic systems," *ISA Trans 1995; 34: 193–8.* , 1995.

[87] IEC, "International Electrotechnical Commission (IEC 61025): Fault tree analysis (FTA)," 2006.

[88] IEC, "International Electrotechnical Commission (IEC 60812). Analysis techniques for system reliability – procedure for failure mode and effects analysis (FMEA)," 2006.

[89] S. Verlinden, G. Deconinck, and B. Coupé, "Hybrid reliability model for nuclear reactor safety system," *Reliability Engineering & System Safety*, vol. 101, pp. 35-47, 2012/05/01/ 2012.

[90] G. Kaczor, S. Młynarski, and M. Szkoda, "Verification of safety integrity level with the application of Monte Carlo simulation and reliability block diagrams," *Journal of Loss Prevention in the Process Industries*, vol. 41, pp. 31-39, 2016/05/01/ 2016.

[91] H. Guo and X. Yang, "Automatic creation of Markov models for reliability assessment of safety instrumented systems," *Reliability Engineering & System Safety*, vol. 93, no. 6, pp. 829-837, 2008/06/01/ 2008.

[92] F. Innal, "Contribution to modelling safety instrumented systems and to assessing their performance / critical analysis of IEC 61508 standard.," (Ph.D. thesis) France: University of Bordeaux 2008.

[93] H. Jin, M. A. Lundteigen, and M. Rausand, "Reliability performance of safety instrumented systems: A common approach for both low- and high-demand mode of operation," *Reliability Engineering & System Safety*, vol. 96, no. 3, pp. 365-373, 2011/03/01/ 2011.

[94] A. G. King, "SIL determination: Recognising and handling high demand mode scenarios," *Process Safety and Environmental Protection*, vol. 92, no. 4, pp. 324-328, 2014/07/01/ 2014.

[95] IEC62443-2-1, "Industrial Communications Networks—Network and System Security— 790 Part 2–1: Establishing An Industrial Automation and Control System 791 Security Program, Edition 1.0, document IEC62443-2-1, International 792 Electrotechnical Commission, Geneva, Switzerland, 2011," 2011.

[96] W. M. Goble and A. C. Brombacher, "Using a failure modes, effects and diagnostic analysis (FMEDA) to measure diagnostic coverage in programmable electronic systems," *Reliability Engineering & System Safety,* vol. 66, no. 2, pp. 145-148, 1999/11/01/ 1999.

[97] W. M. Goble, J. V. Bukowski, and A. C. Brombacher, "Systematic Development of Markov Models for the 1oo2D Programmable Electronic System Architecture - Analysis of Safety and Availability," in *Safe Comp 96: The 15th International Conference on Computer Safety, Reliability and Security, Vienna, Austria October 23–25 1996*, E. Schoitsch, Ed. London: Springer London, 1997, pp. 173-182.

[98] E. M. H. Amer, "Weighted coverage in fault tolerant systems," in *Proceedings of the Annual Reliability and Maintainability Symposium*, New York, 1987: IEEE.

[99] P. Luthra, "FMECA: an integrated approach," in *1991 Proceedings of the Annual Reliability and Maintainability Symposium*, 1991: IEEE.

[100] R. Lasher, "Integrity testing of control systems," *Control Engineering,* 1990 1990.

[101] D. Johnson, "Automatic fault insertion," *INTECH, Raleigh, NC: ISA*, 1994.

[102] R. A. L. Oliveira, "Extension of ISA TR 84.00.02 PFD equations to KooN architectures," *Reliab Eng Syst Saf* vol. 95:707–15, 2010.

[103] A. Lisnianski, "Extended block diagram method for a multi-state system reliability assessment," *Reliability Engineering & System Safety*, vol. 92, no. 12, pp. 1601-1607, 2007/12/01/ 2007.

[104] A. C. Torres-Echeverría, S. Martorell, and H. A. Thompson, "Modelling and optimization of proof testing policies for safety instrumented systems," *Reliability Engineering & System Safety*, vol. 94, no. 4, pp. 838-854, 2009/04/01/ 2009.

[105] J. K. Vaurio, "Availability and cost functions for periodically inspected preventively maintained units," *Reliability Engineering & System Safety,* vol. 63, no. 2, pp. 133-140, 1999/02/01/ 1999.

[106] D. Kančev and M. Čepin, "Evaluation of risk and cost using an age-dependent unavailability modelling of test and maintenance for standby components," *Journal of Loss Prevention in the Process Industries,* vol. 24, no. 2, pp. 146-155, 2011/03/01/ 2011.

[107] S. Martorell *et al.*, "RAMS+C informed decision-making with application to multi-objective optimization of technical specifications and maintenance using genetic algorithms," *Reliability Engineering & System Safety,* vol. 87, no. 1, pp. 65-75, 2005/01/01/ 2005.

[108] J. L. Rouvroye and A. C. Brombacher, "New quantitative safety standards: different techniques, different results?," *Reliability Engineering & System Safety*, vol. 66, no. 2, pp. 121-125, 1999/11/01/ 1999.

[109] J. L. Rouvroye and E. G. van den Bliek, "Comparing safety analysis techniques," *Reliability Engineering & System Safety,* vol. 75, no. 3, pp. 289-294, 2002/03/01/ 2002.

[110] J. V. Bukowski, "A comparison of techniques for computing PFD average," in *Annual Reliability and Maintainability Symposium, 2005. Proceedings.*, 2005, pp. 590-595.

[111] IEC, "IEC61078, Analysis techniques for dependability – reliability block diagram and Boolean methods, 2006.," 2006.

[112] ISA, "ISA-TR84.00.01-2004, Functional Safety: Safety Instrumented Systems for the process Industry Sector - Part 1: Framework, Definitions, System, Hardware and Software Requirements.," *The International Society of Automation, North Carolina, USA.*, 2004.

[113] M. S. a. E. W. Marszal Edward, "Safety Integrity Level Selection," *ISA-The Instrumentation, System, and Automation society, 2002,USA.*, 2002.

[114] H. Jahanian and Q. Mahboob, "SIL determination as a utility-based decision process," *Process Safety and Environmental Protection*, vol. 102, no. Supplement C, pp. 757-767, 2016/07/01/ 2016.

[115] AS, "Australian Standards. AS4024.1501, Safety of machinery Design of safety related parts of control systems - General principles for design," 2006.

[116] AS, "Australian Standards. AS4024.1502, Safety of machinery Design of safety related parts of control systems - Validation," 2006.

[117] D. Baigent and E. Lebenhaft, "Microprocessor-based protection relays: design and application examples," *IEEE Transactions on Industry Applications*, vol. 29, no. 1, pp. 66-71, 1993.

[118] T. Innovations, "Target Innovations, conveyor metal detector for coal. [Online] Available:http://news.targetinnovations.com/conveyor-metal-detector-for-coal-handling-plant-chp-cement-industry/ [Accessed: 18-January-2018]." 2015.

[119] M. M. O. Training, "The University of Alaska Fairbanks. [Online] Available:https://millops.community.uaf.edu/amit-129/amit-129-lesson-6/ [Accessed: 18-January-2018]." 2018.

[120] P. Baybutt, "Overcoming challenges in using layers of protection analysis (LOPA) to determine safety integrity levels (SILs)," *Journal of Loss Prevention in the Process Industries*, vol. 48, no. Supplement C, pp. 32-40, 2017/07/01/ 2017.

[121] S. S. Grossel, *Layers of protection analysis—simplified process risk assessment (2001): Center for Chemical Process Safety, American Institute of Chemical Engineers, New York, 270 pp, US$139.00*. 2002, pp. 319–320.

[122] M. C. a. B. M. Andrija Volkanovski, "Application of the fault tree analysis for assessment of power system reliability," *Reliability Engineering & System Safety*, vol. 94, pp. 1116-1127, 2009.

[123] Exida, "Exida exSILentia. [Online] Available: http://www.exida.com/exSILentia [Accessed: 23-January- 2018]." 2018.

[124] Wikipedia, "Process hazard analysis," *[Online] Available: https://en.wikipedia.org/wiki/Process_hazard_analysis. [Accessed: 18- December-2017]*. 2017.

[125] Yokogawa, "Yokogawa Electric Corporation, ProSafe-RS, Safety Manual, User's Manual, IM 32Q01S10-31E, 4th Ed., Jan. 2015.," 2015.

[126] Yokogawa, "Yokogawa Centum VP General Specifications, Integrated Production Control System, 10th Edition, Oct.5, 2010. [Online] Available: http://www.yokogawa.com/dcs/pdf/GS33L01A10-40E.pdf. [Accessed: 11- December- 2015]." 2010.

[127] Symantec, "Triton: New Malware Threatens Industrial Safety Systems.," *[Online] Available: https://www.symantec.com/blogs/threat-intelligence/triton-malware-ics [Accessed: 23-January-2018]*. 2017.

[128] F. Policy, "Cyberattack Targets Safety System at Saudi Aramco," *[Online] Available: https://foreignpolicy-com.cdn.ampproject.org/c/foreignpolicy.com/2017/12/21/cyber-attack-targets-safety-system-at-saudi-aramco/amp/ [Accessed: 23-January-2018]*. 2017.

[129] B. News, "WannaCry ransomware cyber-attacks slow but fears remain," *[Online] Available: http://www.bbc.com /news/technology-39920141#_=_. [Accessed: 18-May-2017]*. 2017.

[130] K. Zetter, "An unprecedented look at Stuxnet, the world's first digital weapon," *[Online] Available: http://www.wired.com /2014/11/ countdown-to-zero-day-stuxnet/. [Accessed: 11-December- 2015]*. *Wikipedia, [Online] Available: https://en.wikipedia.org/wiki/ Stuxnet. [Accessed: 11- December- 2015]*. 2014.

[131] Symantec, "W32.Stuxnet," *[Online] Available: https://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99 [Accessed: 23-January-2018]*. 2017.

[132] Symantec, "Backdoor.Oldrea," *[Online] Available: https://www.symantec.com/security_response/writeup.jsp?docid=2013-052817-2105-99 [Accessed: 23-January-2018]*. 2017.

[133] Symantec, "Destructive Disakil malware linked to Ukraine power outages also used against media organizations," *[Online] Available: https://www.symantec.com/connect/blogs/destructive-disakil-malware-linked-ukraine-power-outages-also-used-against-media-organizations [Accessed: 23-January-2018]*. 2016.

[134] O. a. G. C. S. Conference, "Oil and Gas Cyber Security Conference, 3-4 June 2014, Oslo, Norway, [Online] Available: http://www. Smi -online.co.uk/energy/ europe /conference /Oil-and-Gas-Cyber- Security- Nordics? utm_source = E-046&utm_medium=oilandgas-cybersecurity7. asp&utm_campaign= GOTO&o=login&dl=br&p1=4515#tab_ overview. [Accessed: 6-July-2017]." 2017.

[135] L. Piètre-Cambacédès and M. Bouissou, *Cross-fertilization between safety and security engineering*. 2013, pp. 110–126.

[136] A. I. 84.00.01, "Application of Safety Instrumented Systems for the Process Industries.," *The Instrumentation, Systems, and Automation Society, Research Triangle Park, NC, 2004.*, 2004.

[137] ANSI/ISA-99-00-01, "Security for Industrial Automation and Control Systems. Part 1: Terminology, Concepts, and Models. ," *The Instrumentation, Systems, and Automation Society, Research Triangle Park, NC, 2007.*, 2007.

[138] NIST, "NIST Releases Cybersecurity Framework Version 1.0 " *[Online] Available: https://www.nist.gov/news-events/news/2014/02/nist-releases-cybersecurity-framework-version-10 [Accessed: 23-January-2018]*. 2014.

[139] IEC, "IEC62443-2-1, Industrial communications networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program, Edition 1.0, Geneva, Switzerland, 2010-2011. ," 2011.

[140] N. I. S. Technology, "Framework for Improving Critical Infrastructure Cybersecurity," 2014.

[141] Yokogawa, "Yokogawa Electric Corporation, Technical Information, Plant Resource Management. [Online] Available:https://www.yokogawa.com/au/solutions/products-platforms/solution-based-software/asset-management-software/field-device-management-prm/. [Accessed: 18- December- 2017]." 2017.

[142] Emerson, "EMERSON CYBER SECURITY NOTIFICATION - HART DTM," *[Online] Available: http://www2.emersonprocess.com/siteadmincenter/PM%20Central%20Web%20Documents/EMR%20EPM14001-1.pdf [Accessed: 23-January-2018]*. 2015.

[143] Yokogawa, "Yokogawa Electric Corporation, ProSafe-RS, Engineering Guide, IM 32Q01C10-31E, 4th Ed. Jan. 2015.," 2015.

[144] Yokogawa, "Yokogawa Releases Enhanced Version of ProSafe®-RS Safety Instrumented System 2017," *[Online] Available: https://www.yokogawa.com/au/news/press-releases/2017/yokogawa-releases-enhanced-version-of-prosafer-rs-safety-instrumented-system-2017/ [Accessed: 23-January-2018]*. 2017.

[145] ISA, "ISA99, Industrial Automation and Control Systems Security," *ISA*, 2018.

[146] Yokogawa, "SCADA Cyber Security," *[Online] Available: https://www.yokogawa.com/au/library/resources/application-notes/scada-cyber-security/ [Accessed: 23-January-2018]*. 2017.

[147] FireEye, "Attackers Deploy New ICS Attack Framework “TRITON” and Cause Operational Disruption to Critical Infrastructure," *[Online] Available: https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html [Accessed: 7-January-2018]*. 2017.

[148] T. Post, "Triton Malware Targets Industrial Control Systems in Middle East," *[Online] Available: https://threatpost.com/triton-malware-targets-industrial-control-systems-in-middle-east/129182/ [Accessed: 25-December-2017]*. 2017.

[149] B. Miller and D. Rowe, "A survey of SCADA and critical infrastructure incidents. In: Proceedings of the 1st annual conference on research in information technology. ACM.," 2012.

[150] J. Guan, J. Graham, and J. Hieb, "A diagraph model for risk identification and management in SCADA systems. 2011 IEEE international conference on intelligence and security informatics (ISI), IEEE CP.,," 2011, pp. p. 150-155.