People's Democratic Republic of Algeria

Ministry of Higher Education and Scientific Research

وزارة التعليم العالي والبحث العلمي

Badji Mokhtar Annaba University

جامعة باجي مختار – عنابـــة

Faculty of Technology

كـلـيـة التكنـولـوجـيـا

Mechanical Engineering Department

قســم الهندسة الميكانيكية

Thesis

Presented to obtain the degree of:

Doctorate

Field : Mechanical Engineering

by :

Rabah Bilal

Title:

Contribution of analysis tools in preventive maintenance for the detection of defects related to safety instrumented systems to reduce industrial risks in a gas complex

Thesis defended on January 8, 2026 in front of the jury:

01	Bouchelaghem Abdelaziz Mahmoud	Prof.	Badji Mokhtar University/Annaba	President
02	Younes Ramdane	Prof.	Echahid Cheikh Larbi Tebessi University/ Tebessa	Supervisor
03	Laouar Lakhdar	Prof.	Badji Mokhtar University/Annaba	Co-supervisor
04	Deghboudj Samir	Prof.	Echahid Cheikh Larbi Tebessi University/ Tebessa	Examiner
05	Meddour Ikhlas	Prof.	ENSTA,Dergana-Bordj El Kiffan/ Alger	Examiner
06	Babouri Mohamed Khemissi	Prof.	USTHB/ Alger	Examiner
07	Khelif Rabia	Prof.	Badji Mokhtar University/Annaba	Guest

Dedication

I dedicate this thesis to:

My beloved parents, for their encouragement and for enabling me to pursue my studies under the best conditions,

To my dear wife,

To my brothers and sisters,

To all my family,

To all my friends,

To those who supported me throughout my studies,

To those who love me,

To those whom I love.

Acknowledgments

This work marks the culmination of a lengthy journey during which I was fortunate to receive guidance, encouragement, and support from numerous individuals, to whom I extend my heartfelt gratitude.

I am particularly grateful to my thesis supervisor, **Pr.Younes Ramdane**, for his exceptional mentorship both on a personal and academic level, as well as for his unwavering patience throughout the completion of this work. I also extend my thanks to my co-supervisor**, Pr. Laouar Lakhadar**, , for his collaborative supervision over the course of this doctorate study.

Additionally, I wish to express my gratitude to **Dr.Djeddi Choayb**,/ Sonatrach Process Safety Engineer for his huge support especially with practical aspect related to this thesis.

Finally, I extend my heartfelt tribute to all those who, in various capacities and at different times, directly or indirectly, contributed to the successful completion of this thesis.

ملخص

في صناعة الغاز ، تعتبر أنظمة السلامة الآلية (SIS) أكثر حاجز فعالية للسلامة .تم تصميم هذه الأنظمة الآلية لمنع وقوع حوادث كبيرة ، وإذا وقع حادث غير مرغوب فيه ، فإنها تقلل من الضرر الذي يلحق بالأشخاص والبيئة والأصول .ومع ذلك ، فإن أداءها يعتمد على عدة عوامل بما في ذلك نهج الصيانة المختار .تساهم هذه الدراسة في مجال العمليات من خلال التركيز على كيفية قدرة استراتيجيات الصيانة المختلفة على تحسين أداء أنظمة السلامة .(SISs) .تقترح هذه الأطروحة نموذجًا باستخدام شبكة بيتري العشوائية (SPN) لتقييم أداء نظام إيقاف التشغيل الطارئ (ESD) الموجود في محطة استرجاع الغازات المحترقة في حقل اجلي في جنوب الجزائر .هذا البحث أيضًا يدرس التأثير المالي لاختبارات البرهان الدورية ، والتي يمكن أن تكون كبيرة ، بما في ذلك التكاليف المباشرة (مثل الأفراد والمعدات والخدمات اللوجستية) والتكاليف غير المباشرة (مثل خسائر الإنتاج وعقوبات حرق الغاز) .يمكن لاستراتيجية شاملة تعمل على تحسين وتيرة اختبارات البرهان الدورية وإجرائها أثناء عمليات التوقف المخطط لها لصيانة المنشأة أن تدير وتقلل هذه التكاليف بشكل فعال .تؤكد نتائج الدراسة أن نموذج شبكة بيتري العشوائية (SPN) المقترح يقيم بشكل فعال كيف تؤثر اختبارات البرهان الدورية الكاملة والجزئية غير المثالية على قيم متوسط احتمالية الفشل عند الطلب (PFDavg) لوظائف السلامة الآلية (SIFs) . بالإضافة إلى ذلك ، يؤكد التطبيق في العالم الواقع في وحدة غاز تشغيلية على قدرة النموذج المقترح على تحسين نفقات قطع الغيار من خلال تحليل الموثوقية .يُترجم هذا إلى وفورات كبيرة في التكاليف دون المساس بمستويات سلامة السلامة المطلوبة (SILs) ، في غضون عامين ، تم تحقيق فائدة بنسبة 60٪ تقريبًا بالمقارنة بعملية المشتريات الحالية لنفس الإطار الزمني .يقدم هذا البحث رؤى قيمة لكل من مرحلة تصميم مشاريع هندسة وتوريد وبناء (EPC)الجديدة ومرحلة تشغيل المنشآت القائمة.

كلمات مفتاحية:أنظمة السلامة الآلية،استراتيجيات الصيانة، اختبارات البرهان الدورية،شبكة بيتري العشوائية،صناعة الغاز

Résumé

Dans l'industrie de traitement du gaz, les Systèmes Instrumentés de Sécurité (SIS) représentent la couche de sécurité la plus efficace, conçue pour prévenir les accidents majeurs et minimiser les dommages aux personnes, à l'environnement et aux biens en cas d'événement indésirable. La performance de ces systèmes dépend de plusieurs facteurs, notamment la stratégie de maintenance adoptée. Cette étude explore comment différentes stratégies de maintenance peuvent optimiser la performance des SIS en utilisant un modèle de Réseau de Petri Stochastique (RPS) pour évaluer un système d'arrêt d'urgence (ESD) dans l'unité de récupération des gaz torchés au champ d'Edjeleh, en Algérie. Elle analyse aussi l'impact financier des tests périodiques, incluant les coûts directs (personnel, équipement, logistique) et indirects (perte de production, pénalités de torchage). Une stratégie globale, optimisant la fréquence des tests périodiques et les effectuant lors des arrêts planifiés, peut réduire efficacement ces coûts. Les résultats montrent que le modèle RPS évalue efficacement l'impact des tests périodiques imparfaits sur la probabilité moyenne de défaillance à la demande (PFDavg) des Fonctions Instrumentées de Sécurité (SIF). De plus, une application pratique dans une unité de gaz opérationnelle confirme que ce modèle optimise les dépenses de pièces de rechange grâce à une analyse de fiabilité, permettant des économies significatives sans compromettre les niveaux d'intégrité de sécurité (SIL), avec environ 60% de bénéfices atteints en deux ans par rapport au processus d'approvisionnement existant. Cette recherche offre des données précieuses pour la conception de nouveaux projets EPC (Ingénierie, Approvisionnement et Construction) et pour l'exploitation des installations existantes.

Mots clés : Systèmes Instrumentés de Sécurité, stratégies de maintenance, Tests périodiques, Réseaux de Petri stochastiques, Industrie du traitement du gaz

Abstract

In the gas processing industry, Safety Instrumented Systems (SISs) are deemed as the most effective safety layer. These automated systems are designed to prevent major accidents from happening and if undesired event occurs, they minimizethe harm on people, environment and assets. However, their performance hinges on several factors including the chosen maintenance approach. This study contributes to the field of process safetyby focusing on how different maintenance strategies can optimize the performance of Safety Instrumented Systems (SISs). This thesis proposes a model using Stochastic Petri Net (SPN) to assess the performance of an existing Emergency Shutdown System (ESD) in a Flared Gases Recovery Unitat the Edjeleh field in southern Algeria. This research also analyzes the financial effect of proof tests, which can be significant, including direct costs (such as personnel, equipment, and logistics) and indirect costs (such as loss of production and gas flaring penalties). A comprehensive strategy that optimizes proof test frequency and performs them during planned facility shutdowns can effectively manage and reduce these costs. The study's findings confirm that the proposed Stochastic Petri Net (SPN) model effectively evaluates how imperfect full and partial proof tests affect the average Probability of Failure on Demand (PFDavg) of Safety Instrumented Functions (SIFs). In addition, real-world application in an operational gas unit validates the proposed model's ability to optimize spare parts expenses through reliability analysis. This translates to significant cost savings without compromising the desired safety integrity levels (SILs), within two years, about 60% benefit has been achieved comparing to the existing procurement process for the same timeframe. This research offers valuable insights for both the design phase of new EPC (Engineering, Procurement, and Construction) projects and the operation phase of existing facilities.

Keywords: Safety instrumented system, Maintenance strategies, Proof tests, Stochastic Petri Net, Gas processing industry

Table of Contents

List of Figures

List of Tables

Nomenclature

AEGR	Flared Gases Recovery Unit
Av	Availability
CCF	Common Cause Failure
CI	Confidence Interval
DD	Dangerous Detected
DC	Diagnostic Coverage
DU	Dangerous Undetected
ESDs	Emergency Shutdown System
ESDV	Emergency Shutdown Valve
EUC	Equipment Under Control
FT	Full Test
FTA-BN	Fault Tree Analysis - Bayesian Network
GRIF	Graphical Interface for Reliability Forecasting
IEC	International Electrotechnical Commission
LSHH	Level Switch Low Low
MTBF	Mean Time Between Failures
MTTR	Mean Time To Repair
PFD	Probability of Failure on Demand
PAHH	Pressure Alarm High High
PHA	Process Hazard Analysis
PMI	Proactive Maintenance Interval
PN	Petri Nets
PT	Partial Test
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SP	Spare Parts
SPN	Stochastic Petri Nets
SPNPA	Stochastic Petri Nets with Predicates and Assertions
SRS	Safety Requirements Specification
TAHH	Temperature Alarm High High
TMR	Triple Modular Redundancy
U	Unavailability
IM	Input Module
MP	Main Processor
OM	Output Module
λ	Total Failure Rate
λ_{DD}	Dangerous Detected Failure Rate
λ_{DU}	Dangerous Undetected Failure Rate
τ	Length of a Proof Test
$\tilde{\tau}$	Length between two consecutive periodic partial tests
KooN	K-out-of-N
PFD(t)	Time dependent PFD of the system
PFDavg	Average Probability of Failure on Demand
β	Beta factor
γ_1	Partial Proof Test Coverage
γ_2	imperfect partial proof test coverage

List of Works

Publication

[1]. **B. Rabah**, R. Younes, C. Djeddi, and L. Laouar, "Optimization of safety instrumented system performance and maintenance costs in Algerian oil and gas facilities," Process Safety and Environmental Protection, vol. 182, pp. 371-386, 2024/02/01/ 2024, doi: https://doi.org/10.1016/j.psep.2023.11.081.

General introduction

The hydrocarbon sector is the backbone of Algeria's economy, significantly contributing to the country's GDP and global energy markets. However, this sector is fraught with inherent industrial risks due to the hazardous nature of hydrocarbon production, processing, and distribution. Ensuring the technical integrity of facilities and controlling associated risks is fundamental to prevent catastrophic accidents, which can result in multiple casualties, serious injuries, environmental damage, and negative economic impact.

Since 2014, the Algerian authoritiespromoted the high importance of strengthening the regulatory framework related to safety management of oil & gas industry. Initially, Executive Decree 14-349 was issued in order to reinforcethe safety systems against industrial risks, particularly through the development of an Integrity Management System. However, as the industry evolved and new challenges arose, this decree has been replaced in 2021 by Executive Decree 21-331. This new decree provides a comprehensive framework that integrates principles of sustainable development, health preservation, and continuous improvement while defining the technical integrity requirements of hydrocarbon facilities and equipment.

Executive Decree 21-331 requires operators to formalize diagnostics and recording practices, demanding initial conformity assessments for all facilities involved in hydrocarbon activities. The Safety Instrumented Systems (SIS) are considered as important safety barriers in oil and gas sector which should comply with international standards IEC 61508 and IEC 61511 standards. These systems are designed to detect process abnormalities and deviationsthen initiate corrective actions to bring operations to a safe state.

Considering the severe human and financial costs associated with SIS failures, operators must implement rigorous measures to ensure these systems' reliability and effectiveness. Failures can arise from both hardware degradation and software errors, emphasizing the need for a comprehensive Integrity Management System that proactively monitors, diagnoses, and maintains these crucial systems.

The overarching goal of this research is to establish a comprehensive and integrated approach for diagnosing, assessing performance, and optimizing preventive maintenance of Safety Instrumented Systems (SIS). The key objectives are:

1. **Evaluate the Effectiveness ofMaintenance approach:**Analyze the effectiveness of different maintenance approaches on the performance of Safety Instrumented Systems (SIS), specifically in preventing and mitigating hazardous situations in the oil and gas sector.
2. **Develop and Apply a Stochastic Petri Net (SPN) Model:**Propose a Stochastic Petri Net (SPN) model to analyze the performance of an Emergency Shutdown Systems (ESDs) in a Flared Gases Recovery Unit located at south Algerian field.
3. **Analyze Financial Impacts of Proof Tests:** Investigate and quantify the direct and indirect financial impacts of proof tests on SISs, including costs related to manpower, equipment, transportation, production losses, and gas flaring tax.
4. **Optimize Proof Test Intervals:** Develop a systematic approach to optimize proof test intervals, scheduling tests during planned plant shutdowns to minimize costs while ensuring safety compliance.
5. **Optimize Spare Parts Management:** Implement the SPN model to control the procurement strategy based on reliability analysis, minimizing spare parts expenses while maintaining the desired Safety Integrity Levels (SILs).

The thesis is basically organized infour interconnected chapters in order to offer a holistic understanding of SIS implementation and performance evaluation.

Chapter 1: This chapter provides a comprehensive overview and performance analysis of Safety Instrumented Systems (SIS). It begins by defining key terms and concepts related to SIS, including safety instrumented functions, safety integrity levels, and classifications of failures. Diagnostic tests such as full and partial valve stroke tests are also discussed. The chapter then explores relevant standards like IEC 61508 and IEC 61511, emphasizing the safety lifecycle, risk analysis, and risk reduction strategies. SIL allocation and safety requirements are addressed, along with the quantitative and architectural requirements necessary to achieve specific SILs. Methods to prevent systematic failures and concepts like proven and prior use are also examined. The chapter concludes with a performance analysis using various analytical approaches to assess SIS effectiveness.

Chapter 2: This chapter examines the importance of maintenance strategies in ensuring the performance of Safety Instrumented Systems (SIS) during the operational phase of the safety

lifecycle. It covers key factors influencing SIS performance, such as redundancy, failure rates, diagnostic coverage, common failure modes, proof testing intervals, and repair times. The importance of conducting tests for SIS during their operational phase is highlighted taking in consideration different categories of tests such diagnostic, proof, and partial tests. The chapter particularly emphasizes the necessity of proof testing for detecting faults and preventing failures that could increase the probability of failure on demand (PFDavg). Various testing methods are presented, ranging from automatic and semi-automatic to manual. This chapter also contributes to the mathematical modeling of imperfect partial proof tests, enhancing the understanding of their impact on SIS performance.

Chapter 3: This chapter presents a sophisticated model using Stochastic Petri Nets (SPN) to assess and optimize the performance and cost-efficiency of Safety Instrumented Systems (SIS) during their operational phase. It integrates Stochastic Petri Nets with Monte Carlo simulations to analyze the dynamic and probabilistic behaviors of these systems, thereby enhancing their reliability and effectiveness in practical scenarios. The chapter features several innovative models, including SPN models for single component with partial, imperfect, and perfect proof testing, simulating real-time dynamics of component failures and the effectiveness of testing protocols. Additionally, the chapter shows an SPN model for redundant components, addressing challenges like common-cause failures in systems with backup components. A novel approach to Reliability-Based Spare Parts Optimization is also introduced, which aims to optimize inventory management to improve system uptime and efficiency. The chapter details the integration of sensors, logic solvers, and actuators into SPN models to calculate the Probability of Failure on Demand (PFDavg) for system components. Specific SPN applications for calculating the PFD of Safety Instrumented Functions (SIFs) are elaborated, illustrating how SPNs can enhance the reliability of critical safety functions. These models together advance the understanding of SIS behavior under various conditions, providing a solid framework for enhancing safety and reliability through targeted interventions.

Chapter 4: This chapter explores the pivotal role of Emergency Shutdown Systems (ESDs) in safeguarding gas compression processes and controlling risks. It begins with an overview of the emergency shutdown and depressurization philosophy across various safety levels and provides

a comprehensive description of the ESD system. The architecture and components of the ESD for the compression section are explored in detail, including the sensor, logic solver (LS), and final element (FE) subsystems. The chapter then describes the activation scenarios for the ESD system, emphasizing its importance in protecting personnel and equipment. The performance of the ESD system in the compression section is assessed using Petri Nets (PN) coupled with Monte Carlo (MC) simulations. The chapter presents subsystem models for sensors, logic solvers, and final elements, using these models to evaluate the impact of full and partial proof tests on system integrity. It analyzes how imperfections in proof tests affect ESD reliability and discusses the financial implications of full proof testing. The chapter concludes with a reliability-based approach in order to optimize spare parts expenses, aiming to enhance system reliability while minimizing maintenance costs.

A conclusion is presented at the end of thesis to summarize the key findings and to offer insights into potential future research perspectives. By providing a framework for diagnostics, performance assessment, and preventive maintenance optimization, this study aims to improve SIS reliability and align Algeria's Oil & Gas safety management practices with international standards.

CHAPTER I

SIS OVERVIEW & PERFORMANCE ANALYSIS

This chapter provides a comprehensive overview and performance analysis of Safety Instrumented Systems (SISs). It begins with basic definitions and terminology related to SIS, including safety instrumented functions, safety integrity levels, and classifications of failures. Diagnostic tests such as full and partial valve stroke tests are discussed. The chapter then explores relevant standards like IEC 61508 and IEC 61511, emphasizing the safety lifecycle, risk analysis, and risk reduction strategies. SIL allocation and safety requirements specification are defined, alongside quantitative and architectural requirements for achieving desired SILs. Methods to prevent systematic failures and concepts of proven and prior use are examined. The chapter concludes with a performance analysis using various analytical approaches to assess SIS effectiveness.

Safety Instrumented Systems (SIS) play a pivotal role in managing operational risks of process industries, where they act as a defense barrier against process anomalies that could lead to industrial incidents, environmental harm, or business losses. This thesis chapter provides a thorough exploration of SIS, emphasizing their design, functionality, performance analysis, and compliance with international standards like IEC 61508 and IEC 61511. The chapter offers a structured overview of SIS components, including detailed explanations of safety instrumented functions (SIFs), safety integrity levels (SILs), and failure classifications, alongside a discussion on the diagnostic tests that validate the operational readiness of these systems.

A Safety Instrumented Systems (SIS) are defined as a structured assembly of hardware and software controls which are designed and installed to take a process to a safe state when predetermined conditions are violated. Understanding the components of an SIS—sensors, logic solvers, and final elements—is essential for comprehending how these systems mitigate risks. Each component plays a vital role: sensors detect deviations from normal operational parameters; logic solvers make decisions based on inputs from sensors; and final elements execute the physical actions required to bring the process to a safe state. This chapter details each component's function, highlighting their interdependencies and importance in maintaining operational integrity.

The chapter discusses the impact and necessity of adhering to international safety standards, particularly IEC 61508 and IEC 61511, which provide the frameworks for ensuring the reliability and effectiveness of SIS. IEC 61508 is described as the umbrella standard for electronic safety-related systems, detailing generic requirements across various industries. IEC 61511, on the other hand, tailors these guidelines specifically for the process industry, emphasizing the importance of integrating proven-in-use or compliant hardware and software to manage process industry hazards effectively. These standards not only prescribe methodologies for the design and implementation of safety systems but also outline the safety lifecycle—a critical concept for managing SIS from conception till commissioning.

Successful deployment of Safety Instrumented Systems (SIS) hinges on conducting thorough risk analysis, which identify potential hazards and evaluate the risks associated with industrial processes. Techniques such as Hazard and Operability Studies (HAZOP) and Layer of Protection Analysis (LOPA) are examined, detailing how they contribute to a deeper understanding of operational risks and facilitate the effective implementation of SIS. This section underscores the necessity of a systematic approach to risk assessment and the critical role of SIS in mitigating identified risks to tolerable levels.

Determining the appropriate Safety Integrity Level (SIL) is crucial for matching the risk reduction needs with the capability of an SIS. This chapter explores the methodologies for SIL allocation, including risk graphs and matrices that help quantify and manage the risks associated with specific process scenarios. The requirements for achieving and maintaining designated SILs—through both quantitative measures like Probability of Failure on Demand (PFD) and qualitative assessments of system architecture—are discussed in detail. These discussions highlight the rigorous standards that SIS must meet to ensure that they perform reliably and effectively under demanding conditions.

Systematic failures represent a significant challenge in the operation of SIS. This chapter discusses strategies for managing these failures, emphasizing the importance of design, testing, and maintenance practices that can mitigate the likelihood of such failures impacting safety functions. The role of diagnostic coverage, including tests like the Valve Stroke Test, in identifying and managing failures is also highlighted, illustrating how regular diagnostics contribute to the overall reliability of SIS.

The concepts of 'proven in use' and 'prior use' are crucial for validating the reliability of components used within an SIS. This section elaborates on how these criteria are applied within the frameworks of IEC standards to ensure that components are suitable for safety-critical applications. It details the requirements that manufacturers and end-users must fulfill to demonstrate that their equipment can perform reliably in safety-instrumented functions.

Finally, the chapter delves into various analytical approaches used to assess the performance of SIS. It describes how different methods, including those outlined in IEC 61508 and alternative models like the PDS method prevalent in the Norwegian petroleum industry, are employed to calculate the Probability of Failure on Demand (PFD). This analysis is crucial for verifying that SIS are capable of achieving the required safety performance levels.

In conclusion, this chapter offers a comprehensive overview of the critical aspects of Safety Instrumented Systems, from their fundamental components and operational principles to the standards governing their implementation and the methods used for performance evaluation. By providing a detailed exploration of these topics, the chapter lays a solid foundation for understanding the operational and safety challenges addressed by SIS in the process industry.

I.1. Definitions and terminology

I.1.1. Safety instrumented systems (SIS):

A SIS is an instrumented system used to implement one or more Safety Instrumented Functions (SIFs) [1]. A typical SIS consists of three key parts [2]:

Input Elements: It consists of a set of input elements (sensors, detectors) that monitor the evolution of physico-chemical parameters that represent the process conditions (temperature, pressure, flow, level...). If at least one of these parameters deviates beyond a set value and maintains it, this deviation constitutes what has been called a demand or solicitation emanating from the process, from the EUC. It is detected by the concerned sensors which send a signal to the LS subsystem.

Logic Solvers: Once the input elements detect a potential hazard, the information will be sent to the logic solver. Logic solvers are often programmable logic controllers (PLC) or similar systems. They analyze the inputs based on pre-programmed safety logic and decide whether to take action.

Final Elements: These elements act directly (emergency shutdown valves) or indirectly (solenoid valves) on the process to implement the physical action necessary to achieve or maintain a safe state after a delay that must be specified for each safety function [1].

SISs may also include communication and ancillary equipment such as cables, tubing, power supply, air supply, impulse lines, and heat tracing,as well as software and human action [3].

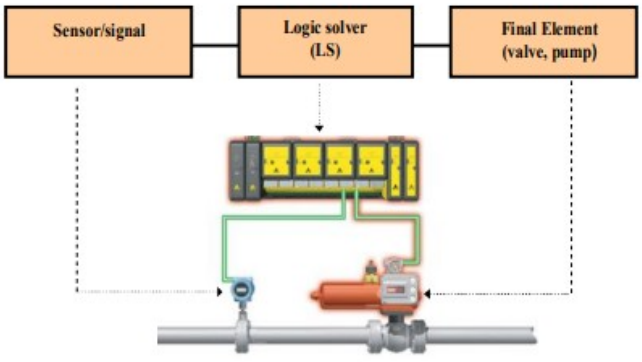


Figure I.1: SIS structure

I.1.2. Safety Instrumented function:

In IEC 61511 [1], a SIF is defined as a "safety function to be implemented by a safety instrumented system." IEC 61511 [1] also defines a safety function as a "function to be implemented by one or more protective layers, which is intended to achieve or maintain a safe state for the process, with respect to a specific hazardous event." [3].

I.1.3. Safety Integrity levels

IEC 61508 and 61511 [4] [1] outline requirements for safety functions, introducing a probabilistic approach to assess the unavailability of Safety Instrumented Systems (SIS). This approach hinges on two key metrics: the average probability of failure on demand (PFD) for low demand operations, and the probability of failure per hour (PFH) for high demand systems. PFD effectively measures the system's unavailability, reflecting its capacity to respond to hazards, also known as safety unavailability [5] [6]. The performance quantification in terms of safety is determined by Safety Integrity Levels (SIL). The IEC 61508 standard categorizes four SIL classifications based on PFD and/or PFH values as seen in Table 1.

Table I.1: Safety integrity levels for safety functions operating on demand or in a continuous / high demand mode

SafetyIntegrityLevel	**Demand Mode of Operation** (average probability of failure to perform its design function on demand - PFD)	**Continuous / High Demand Mode of Operation** (probability of a dangerous failure per hour - PFH)
4	$\geq 10^{-5}$ to $< 10^{-4}$	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-4}$ to $< 10^{-3}$	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-3}$ to $< 10^{-2}$	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-2}$ to $< 10^{-1}$	$\geq 10^{-6}$ to $< 10^{-5}$

I.1.4. Classification of failures:

The IEC 61058, which relates to Safety Instrumented Systems (SIS), makes a distinction between two types of failures that can occur in the components of such systems: random hardware failures and systematic failures [2].

I.1.4.1. Random Hardware Failures: These are unpredictable failures that occur due to the physical properties or wear and tear of hardware components. They are considered random because they do not follow a specific pattern and can happen at any time. Factors such as material fatigue, environmental conditions, or manufacturing defects can contribute to these failures. The likelihood of random

hardware failures is often quantified using statistical methods based on historical data and is usually expressed in terms of failure rates.

I.1.4.2. Systematic Failures: In contrast, systematic failures are not occurred due to the hardware's physical properties but are the result of errors in specification, design, implementation, operation, maintenance, or changes to the system. These failures are more predictable and can be traced back to a specific cause. They often stem from human error or flaws in the system's process and can be addressed by improving the system's design, development processes, or operational procedures. Systematic failures are generally not amenable to statistical prediction in the same way as random hardware failures.

The PDS method [7], elaborates on the classification of failures in Safety Instrumented Systems (SIS) similar to what is described in standards like IEC 61058. However, the PDS method provides a more detailed breakdown, especially concerning systematic failures. Systematic failures, as mentioned, are non-random and are typically due to human errors or deficiencies in processes during various lifecycle phases of the SIS.

Figure I.2 presents a comparative summary of how component-level failures are classified according to IEC 61508, the PDS method, and ISO TR 12489.

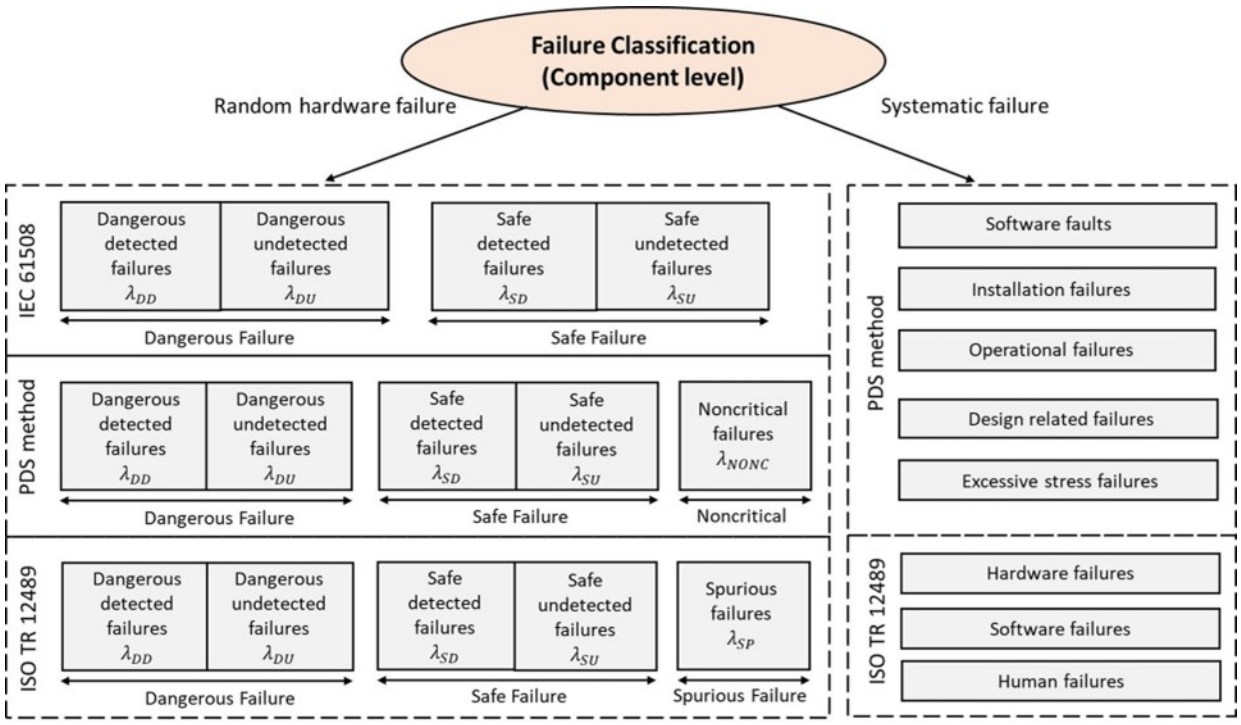


Figure I.2: Failure classification at the SIS component level [2].

I.1.5. Low demand vs high demand

In the context of Safety Instrumented Systems (SIS), as defined by IEC 61508 [4], there are two distinct modes of operation based on demand frequency: low demand and high demand. The classification into either mode depends on two key factors: (1) the frequency of SIS activation in response to demands, and (2) the length of time a failure might go undetected, influenced by the frequency of proof testing. A SIS operates in low demand mode when it is expected to respond to demands less than or equal to once per year [5]. Conversely, it operates in high demand mode when the frequency of demands exceeds this threshold. The demand rate for a SIS can range from continuous to very infrequent, and the duration of each demand can vary from instantaneous to extended periods, potentially lasting hours.

I.1.6. Failure modes

Failure modes in Safety Instrumented Systems (SIS) as outlined in IEC 61508 are crucial for understanding and managing the reliability and safety of these systems. These modes are broadly categorized into two types: safe failures and dangerous failures.

Safe failures are those where the system fails in a manner that does not compromise safety. For example, a component might continue to operate safely without demand [8]. These failures can be further classified into Safe Detected (SD) failures, which are identified immediately, and Safe Undetected (SU) failures, which remain undetectable. Crucially, these failure modes do not compromise the SIS's ability to fulfill its safety functions.

On the other hand, dangerous failures are those that prevent the SIS from executing its expected safety function, meaning the component fails to operate when required. These are split into Dangerous Detected (DD) failures, which are identified almost immediately, and Dangerous Undetected (DU) failures. DU failures are particularly insidious as they might not be discovered until a proof test or functional test is conducted, or worse, until an actual demand for the system occurs [8].

$$\lambda_D = \lambda_{DD} + \lambda_{DU} \quad (1)$$

The total dangerous failure rate of a component (λ_D) is obtained by adding the rates of Dangerous Detected (λ_{DD}) and Dangerous Undetected (λ_{DU}) failures. Although many failures can be detected through online diagnostic testing, regular proof tests are essential to identify and correct dangerous undetected failures before an actual demand situation arises.

I.1.7. Diagnostic coverage

Diagnostic testing, as per IEC 61508 [4], is a critical tool for ensuring system reliability and safety. This testing is designed to identify specific types of failures, such as runtime errors and signal transmission errors, without disrupting the main functions of the component under control.

These diagnostic tests are conducted at varying intervals, ranging from seconds to hours. In low-demand SIS environments, the frequency of these tests allows sufficient time for repair activities to be carried out and the component's function to be restored before the next process demand arises.

The effectiveness of diagnostic testing in detecting dangerous failures and thereby minimizing SIS unavailability is measured by the Diagnostic Coverage (DC) rate [9]. The IEC 61508 defines DC rate as the ratio of the failure rate of detected dangerous failures (λ_{DD}) to the total failure rate of dangerous failures (λ_D). This rate demonstrates how effectively the diagnostic testing can identify dangerous failures.

Diagnostic testing can detect dangerous failures almost immediately after they occur, but it's important to note that only a fraction of dangerous failures can typically be detected through this method. These detectable failures are referred to as DD (Dangerous Detected) failures. The remaining failures, which are only identified through proof testing, are categorized as DU (Dangerous Undetected) failures. Thus, the DC rate differentiates dangerous failures into these two categories:

$$\lambda_{DD} = DC \times \lambda_D \tag{2}$$

$$\lambda_{DU} = (1-DC) \times \lambda_D \tag{3}$$

The total dangerous failure rate (λ_D) is then calculated by considering the estimated DC rate:

$$\lambda_D = DC \times \lambda_D + (1-DC) \times \lambda_D \tag{4}$$

When designing an SIS, the impact of diagnostic testing must be carefully considered, taking into account various factors such as the frequency of process demands, the diagnostic coverage rate, the interval between diagnostic tests, and the time required to complete repair activities. This comprehensive evaluation ensures the SIS is both reliable and capable of responding effectively to safety demands.

I.1.8. Valve Stroke Test

I.1.8.1. Full Stroke Test (FST)

The Full Stroke Test (FST) is a crucial procedure in valve testing. It involves fully opening or closing a valve to assess its operational efficiency. During this test, the response time – the duration it takes for the

valve to either completely open or close – is meticulously recorded. This aspect of the test is critical in evaluating the valve's performance under operational conditions.

One of the unique benefits of FST is its ability to check for leaks in the system, particularly when the valve is in a fully closed position. This leakage check is a significant advantage over the Partial Stroke Test (PST), which doesn't offer this capability. Identifying leaks is essential for ensuring the system's integrity and preventing potential failures.

The FST is not just a mechanical check but also involves a thorough inspection of various components of the valve system. It verifies the functionality of several key parts, including the solenoid, the pilot valve, the actuator, and to some extent, the main valve itself. This comprehensive approach ensures all elements of the valve system are functioning correctly and in harmony.

For quality assurance and safety, the results of the FST are observed and recorded by a safety operator. This step is crucial for maintaining accurate records and ensuring that the valve meets all necessary safety standards.

I.1.8.2. Partial Stroke Test (PST)

The Partial Stroke Test (PST) is another method of assessing valve performance, albeit in a more limited capacity compared to FST. In PST, the valve is only partially closed – typically to about 20-25% of its full capacity [10]. This test is designed to deactivate the valve's open position briefly before returning it to the open state.

PST is particularly useful for verifying the functionality of several components, similar to FST. It checks the solenoid, pilot valve, actuator, and partially the main valve. However, unlike FST, PST cannot determine if the valve closes properly, necessitating the need for a full stroke test according to the testing program.

A critical requirement for valves undergoing PST is that they must have a total travel time of at least 8-10 seconds. This requirement is in place to prevent over-stroking the valve, which could lead to process disturbances. Over-stroking refers to the valve moving beyond its intended limits, potentially causing mechanical stress or operational issues.

The primary purpose of PST is to ensure that the valve responds accurately to a shutdown command. This means verifying that the valve can freely travel upon activation of each solenoid, without fully closing and causing process disruptions or spurious trips. By frequently performing PST, the intervals

between the more comprehensive full stroke tests can be extended, thereby optimizing maintenance schedules and reducing operational downtime.

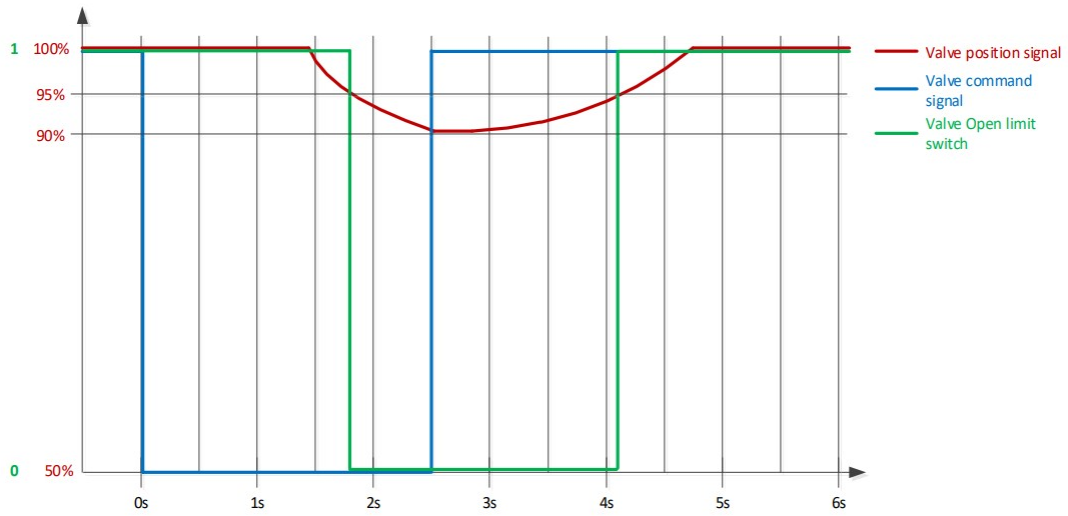


Figure I.3: Partial stroke test, Feedback signals [11].

The Figure I.3 illustrates a valve reopening to 90% during a stroke test, with its ZSH limit switch deactivating at 95% [11].

I.2. SIS Related Standards - IEC 61508 and IEC 61511

I.2.1. General

The international standards IEC 61508 and IEC 61511 have been widely recognized as the foundation for specification, design, and operation of SIS. IEC 61508 is a generic standard common to several industries, that establishes comprehensive requirements and constraints for design of new hardware and software for safety-critical applications. IEC 61511 has been establishedfor the process industry to address two key purposes [12]:

- Substitute generic terms and practices with specific ones that are commonly used in this industry sector.
- Extract those requirements and principles relevant to the integration of proven-in-use or IEC 61508 compliant hardware and software, as this is normally the main challenge when introducing or modifying a SIS/SIF at a process facility.

IEC 61508 is structured in seven parts, divided into normative and informative sections:

- Normative Parts (Mandatory)

- Part 1: General - Outlines the basic requirements and strategies for achieving functional safety.
- Part 2: Hardware Design and Hardware and Software Integration - Specifies the requirements for hardware design and the integration of hardware and software.
- Part 3: Software Development ("Application Program") - Deals with the software development processes and requirements for safety-related applications.
- Part 4: Definitions and Abreviations

– Informative Parts (Supportive)

- Part 5: Guidelines on Part 1 and Methods to Determine Safety Integrity Level (SIL) Requirements - Provides guidance on the application of Part 1 and methodologies for determining SIL, a key concept in quantifying safety performance levels.
- Part 6: Guidelines on the Application of Part 2 and 3 - Offers additional information on applying the standards in Parts 2 and 3, including quantification methods and formulas for calculating Probability of Failure on Demand (PFD) and Probability of Failure per Hour (PFH).
- Part 7: Overview of Various Measures and Techniques Referenced in Part 2 and 3 - Summarizes the different measures and techniques that are referenced in the hardware and software requirements.

Figure I.4-1 illustratesthe key differences and application between IEC 61508 and IEC 61511 .According to this figure, manufacturers involved with field sensors, logic solvers, and final elements must demonstrate compliance with IEC 61508, whereas system integrators (often referred to as "engineering companies") and end users should adhere to IEC 61511. For this reason, IEC 61508 is commonly referred to as the "manufacturers' standard," while IEC 61511 is known as the "system integrators and end users' standard."

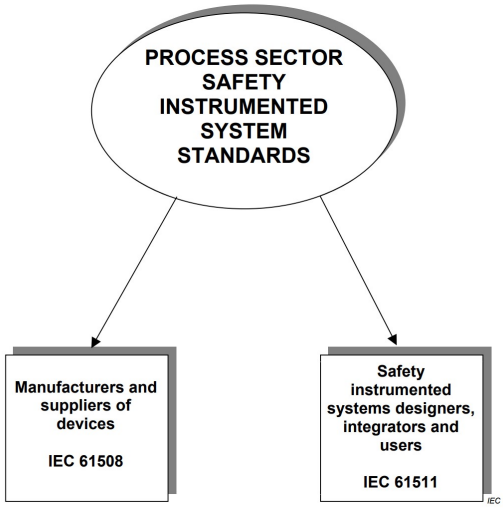


Figure I.4-1: Relationship between IEC 61511 and IEC 61508 (Figure 2 in IEC 61511-1)

Detailed relationship between IEC 61511 and IEC 61508is shown in Figure I.4-2;

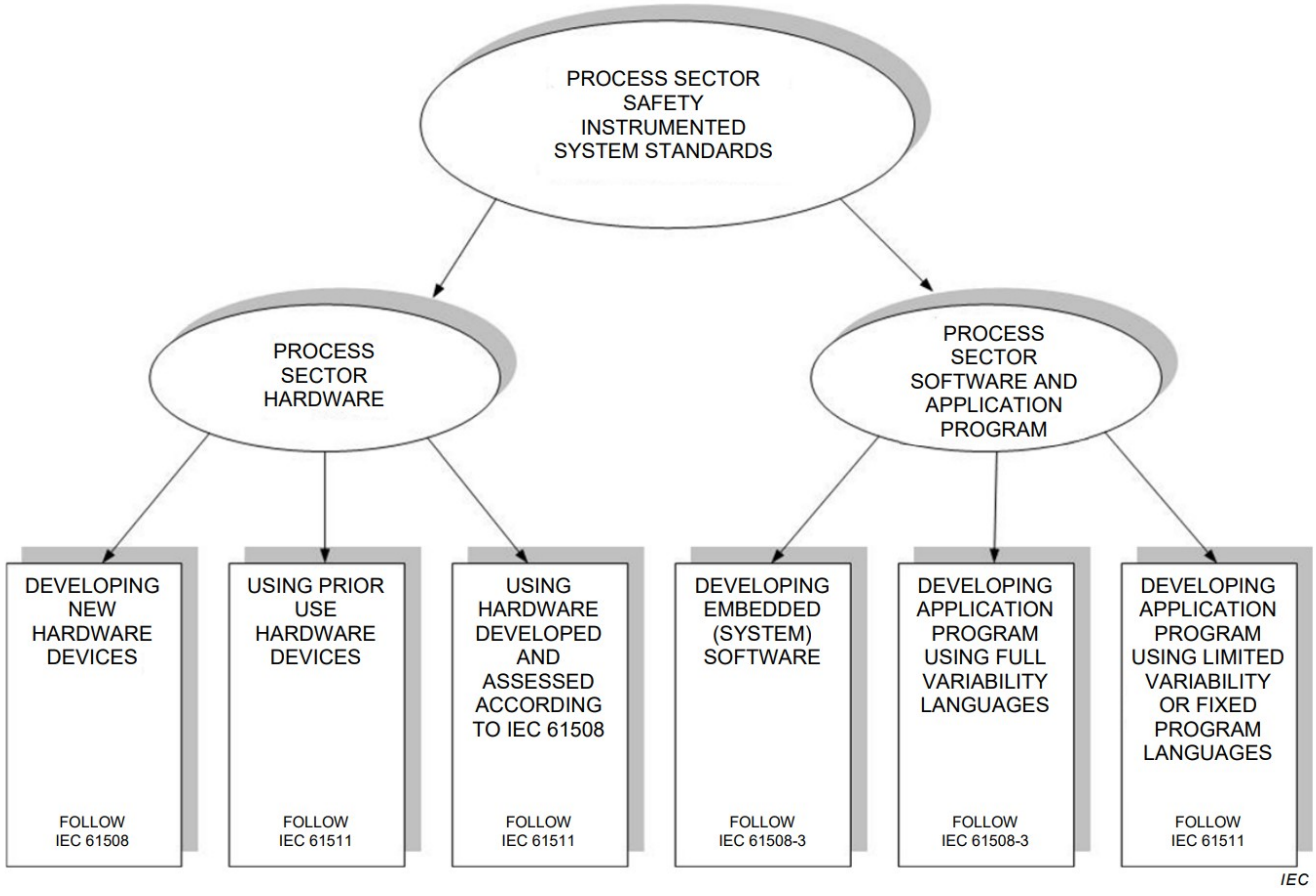


Figure I.4-2: Detailed relationship between IEC 61511 and IEC 61508 (Figure 3 in IEC 61511- 1)

Both IEC 61508 and IEC 61511 advocate a risk-based approach to determining the performance levels of Safety Instrumented Functions (SIFs) by assigning a Safety Integrity Level (SIL).

I.2.2. Safety lifecycle

Both IEC 61508 and IEC 61511 emphasize the "safety lifecycle" approach for managing SIS/SIF. This lifecycle approach uses a structured framework in order to define requirements for each stage including specification, design, integration, operation, maintenance, modification and decommissioning
Each phase has a set of defined inputs and outputs, and towards the end of each phase, a check (or verification) shall be performed to confirm that the required outputs are as planned [12].

Figure I.5-1 illustrates the safety lifecycle presented in IEC 61511. For a summary of requirements related to each lifecycle phase, reference is made to Table 2 in IEC 61511-1.

For the purpose of completeness, the lifecycle figure from IEC 61508 is also included, see Figure I.5-2. For further specification of requirements to each lifecycle phase, reference is made to Table 1 in IEC 61508-1.

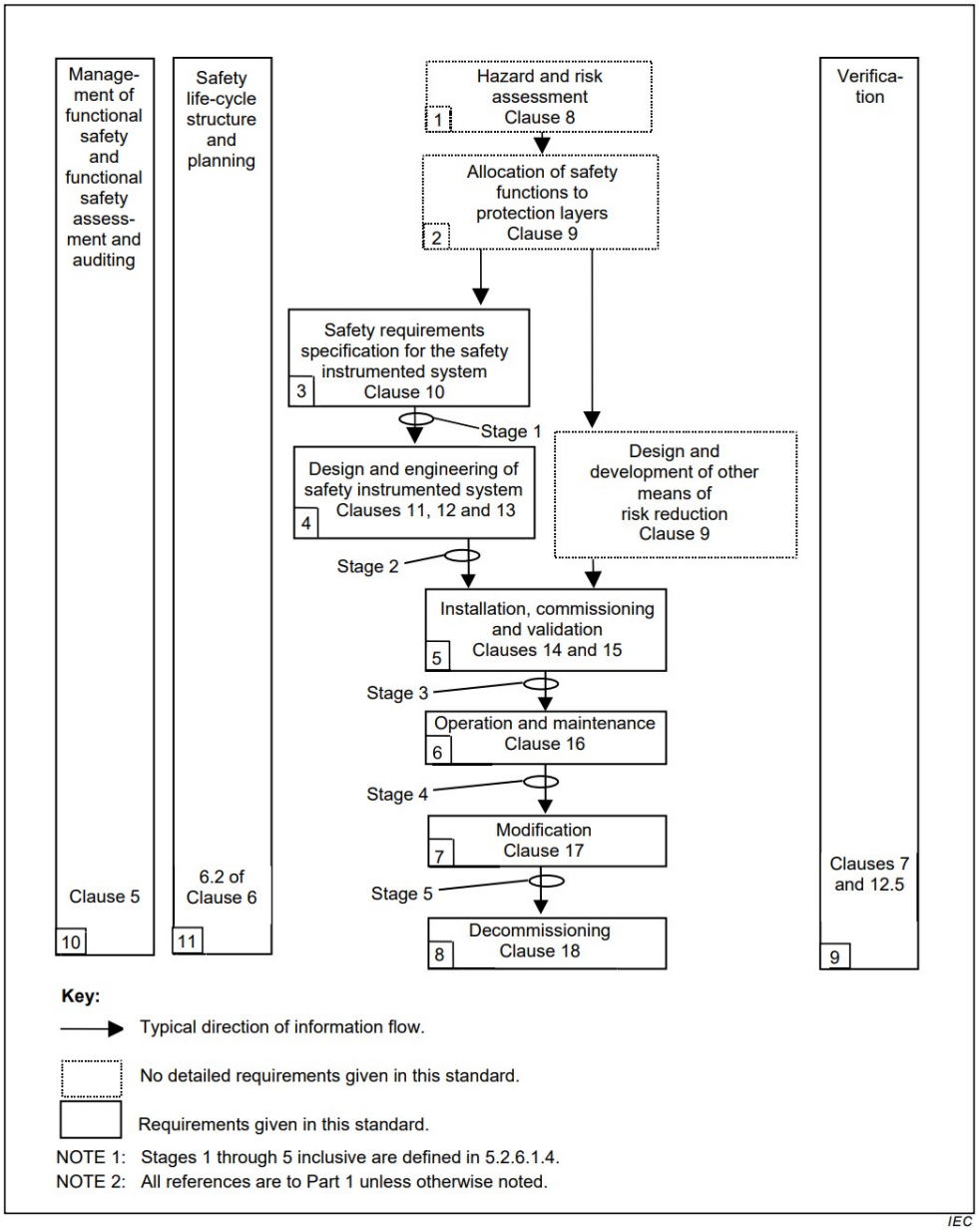


Figure I.5-1: Lifecycle from IEC 61511 (Figure 8 from IEC 61511-1)

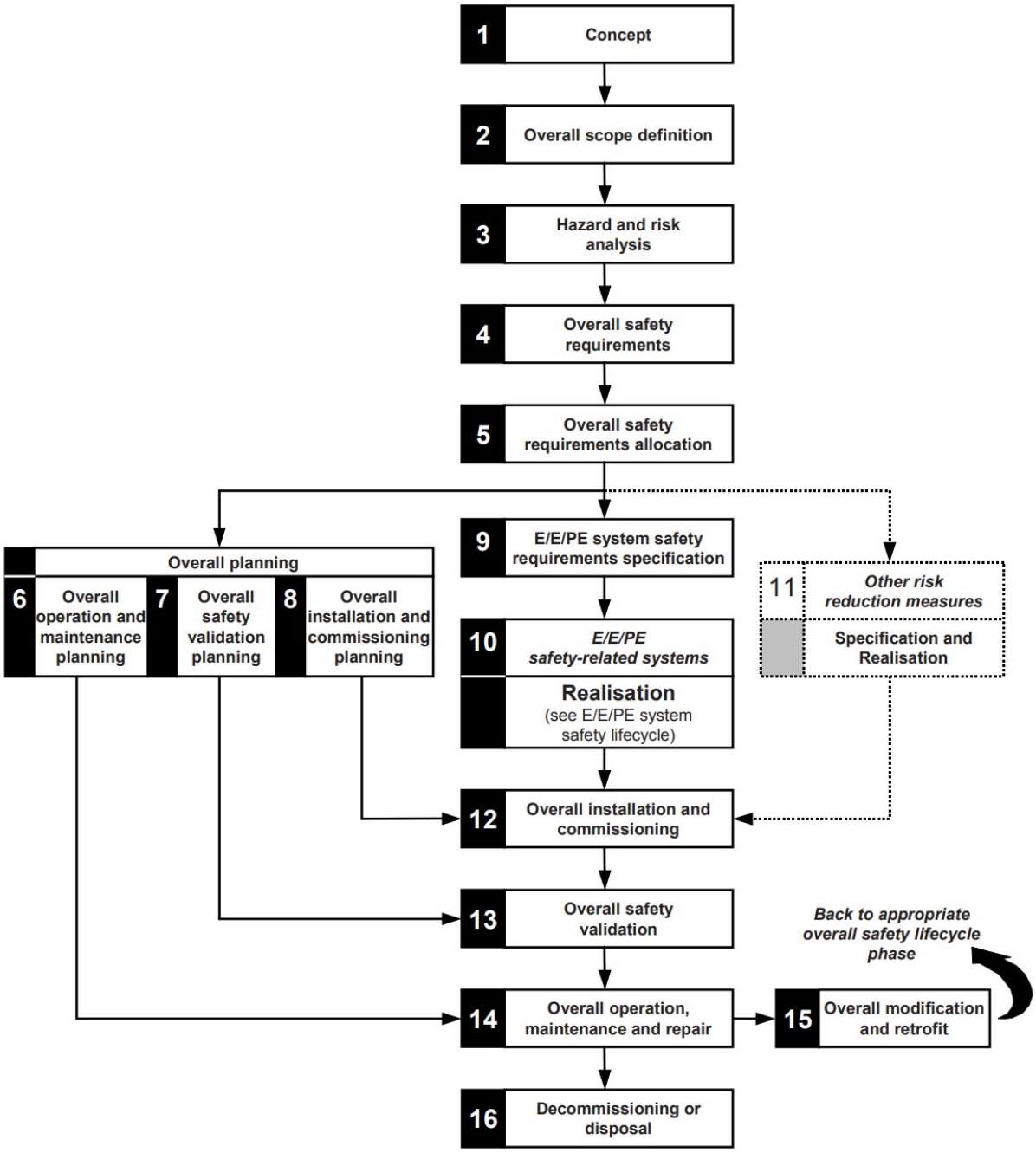


Figure I.5-2: Lifecycle from IEC 61508 (Figure 2 from IEC 61508-1)

I.3. Risk analysis &Risk reduction

I.3.1. Hazard and risk analysis

The approach of hazard and risk analysisis developed to thoroughly identify several key concerns: the hazards and hazardous situationsassociated with the process and control equipment, the sequence of events leading to these hazards, the risks associated with the identified hazards, and requiredcontrols for

risk reduction. This analysis is an essential tool for identifying and mitigating potential risks within the system's operations.

The objective of the Process Hazard Analysis (PHA), including hazard identification studies (HAZID) and hazard and operability studies (HAZOP), is to identify the potential hazards inherent to the process assumingno safety-related functions are in place. The PHA should be conducted with careful consideration of various factors, such as the properties of the fluids and gases being handled, operational and maintenance procedures, and different operational modes like startup, shutdown, maintenance, pigging, and well interventions. It also considers hazards arising from human interaction with the process and its systems, the novelty and complexity of the installation, and interfaces under consideration. This includes assessing if a failure of the Basic Process Control System (BPCS) could lead to separate hazards or a demand on the Safety Instrumented System (SIS) or Safety Instrumented Function (SIF). A multidisciplinary team with diverse engineering, operational, and maintenance expertise should perform hazard identification to minimize the risk of overlooking any hazards. The selection of hazard identification techniques is driven by several factors such as the lifecycle phase at which the identification is undertaken (design, construction, operation), the type and complexity of the installation. Generally, the more novel and complex installation requirea more structured approach.

I.3.2. Risk reduction

In most situations, safety is achieved through a combination of Safety Instrumented Systems (SIS) such as Emergency Shutdown (ESD), Fire & Gas (F&G), and Process Shutdown (PSD), along with other risk-reducing measures. These additional measures may include technical solutions based on technologies other than SIS, such as Pressure Safety Valves (PSV), passive fire protection, drainage systems, increased wall thickness, and separation or distancing. Operational and organizational measures also contribute to safety, including manual operator interventions, third-party verification, and the use of procedures and checklists [12]. This approachisillustrated in Figure I.6 below.

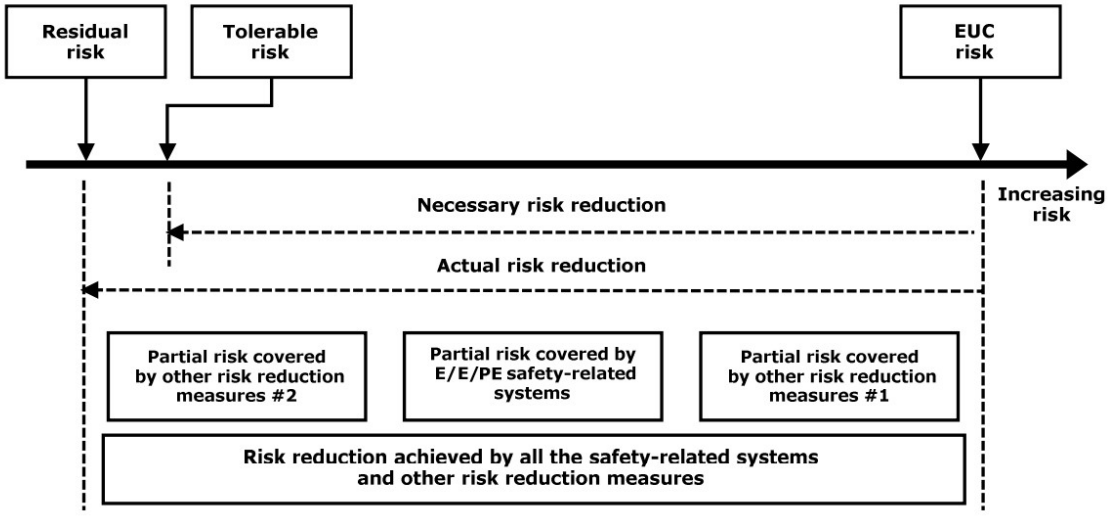


Figure I.6: Risk reduction – general concepts (figure A.1 in IEC 61508-5)

Two key factors are crucial in understanding the framework for risk reduction. First, the risk reduction achieved by each individual measure cannot be viewed in isolation. It is essential to record the cumulative effect of all risk reduction measures in order to demonstrate that tolerable risk levels have been achieved. Second, when evaluating the risk reduction provided by a Safety-Instrumented Function (SIF), all components of the barrier of which the SIF may be just a part should be considered. This includes understanding the reliability of the initiating elements (e.g., a push button), the final elements (e.g., a valve), and the SIF itself to accurately determine the overall reliability of the safety barrier [12].

I.4. SIL Allocation

The methods used to allocate Safety Integrity Levels (SIL) to a safety instrumented function are critical in ensuring the overall safety of an industrial process. Thesemethodsinclude:

1. **Risk Graphs**: This qualitative tool helps visualize the potential risks associated with different system scenarios. It simplifies decision-making by plotting the severity of potential harm against the likelihood of occurrence, helping to determine the necessary SIL for each safety function.
2. **Matrices of Hazardous Event Severity (Severity Matrix)**: Similar to risk graphs, this matrix categorizes and prioritizes hazards by assessing the potential severity and likelihood of hazardous events. It systematically evaluates the impact and probability to help set appropriate SIL levels.

3. **Layer of Protection Analysis (LOPA)**: LOPA is a more semi-quantitative method that identifies and analyzes the layers of protection surrounding a potential hazard. By examining existing safeguards and their failure probabilities, LOPA helps quantify the residual risk and determine if additional safety functions are needed to achieve the desired SIL.

I.5. Safety Requirements Specification

The Safety Requirements Specification (SRS) is essential for safety-instrumented systems (SIS) and is established based on the allocation of Safety Instrumented Functions (SIFs) and requirements identified during safety planning. The SRS serves as a foundational document for SIS design and is continuously refined and maintained throughout all lifecycle phases of the SIS. According to chapters IEC 61511 and IEC 61508, which focus on risk reduction for SIS [12].

The SRS documents define safety-related requirements and parameters for the SIS, including reliability/PFD targets, assumed demand rates, and spurious trip rates. It should articulate the most critical requirements succinctly and clearly, avoiding the replication of information and ensuring consistency by referencing other detailed documents when necessary. Furthermore, as part of the SRS development, specific safety requirements for the application programs of the SIS should be drafted and included in the SRS or in a separate document [12].

I.6. SIL requirements

To achieve a specified Safety Integrity Level (SIL) through Safety Instrumented System (SIS) technology, three main types of requirements must be satisfied:

- **Quantitative Requirements**: These are articulated as either a Probability of Failure on Demand (PFD) or as a Probability of a Dangerous Failure per Hour (PFH), detailed in Table I.1.
- **Qualitative Requirements**: These pertain to the hardware fault tolerance of the subsystems within the SIS that perform the safety function, as outlined in Tables I.2 to I.4.
- **Functional Safety Management**: This involves specific requirements concerning the techniques and measures that should be implemented to prevent and manage systematic faults effectively.

Below, we briefly explore these three types of requirements. For further details, please refer to IEC 61511-1, clauses 9.2 and 11.4.

I.6.1. Quantitative requirements

IEC 61511 is applicable to systems that operate both 'on demand' and 'continuously' to maintain a safe state. For instance, an Emergency Shutdown (ESD) system is an example of a demand mode system, while a process control system for an unstable process, such as an exothermic reactor, exemplifies a continuous mode system. Table I.1 illustrates the relationship between the Safety Integrity Level (SIL) and the required probability of failure, as detailed in IEC 61511-1, Tables 4 and 5 [1].

It is important to understand that the Probability of Failure on Demand (PFD) requirement applies to the entire safety function, encompassing the field sensor, the logic solver, and the final element, such as a valve. While a component may be certified for a specific Safety Integrity Level (SIL), this certification represents only a portion of the necessary verification effort. The required failure probability, as outlined in Table I.1, must be confirmed for the complete safety function.

I.6.2. Architectural constraints

The highest safety integrity level that a safety function can achieve is constrained by architectural limitations as outlined in IEC 61508-2, clause 7.4, and IEC 61511-1, clause 11.4. To meet these architectural constraints, one of two possible approaches can be implemented, as specified in IEC 61508-2, clause 7.4.4 [4][1]:

- **Route 1H**: This approach is based on the concepts of Hardware Fault Tolerance (HFT) and Safe Failure Fraction (SFF). It is typically used for the development of new technologies where no prior field experience is available.
- **Route 2H**: This method relies on reliability data obtained from field feedback on similar devices, enhanced confidence levels, and HFT for specified safety integrity levels. Route 2H is suitable for integrators and end users who have relevant field experience with the equipment being applied. This equipment must either be developed in compliance with IEC 61508, or documented as proven in use.

I.6.2.1. Architectural requirements according to IEC 61508 (Route 1H)

Architectural constraints on hardware safety integrity are defined by three key parameters:

- **Hardware Fault Tolerance (HFT):** Each Safety Instrumented Function (SIF) must have a specified minimum HFT. If the Safety Instrumented System (SIS) can be divided into separate subsystems (e.g., sensors, logic solvers, and final elements), the HFT should be assigned at the level of these

SIS subsystems. For example, a subsystem with an HFT of 1, such as in 1oo2 voting configurations, can withstand one failure and still maintain functionality.

- **Safe Failure Fraction (SFF):** This refers to the portion of failures that are considered "safe" because they are either detected through diagnostic tests or do not result in a loss of the safety function.
- **Subsystem Type (A or B):** Type A subsystems have all potential failure modes determinable for all constituent components (e.g., a solenoid), whereas Type B subsystems cannot fully determine behavior under fault conditions for at least one component (e.g., a logic solver).

Detailed information can be found in IEC 61508-2, clause 7.4.4.2. Architectural requirements for different safety integrity levels are outlined in Tables I.2 and I.3 below.

The 2010 version of IEC 61508 (IEC 61508-4, clauses 3.6.13-14) clarifies that failures not affecting safety functions should be excluded from Safe Failure Fraction (SFF) calculations. This approach can lead to lower SFF values when using the 2010 version of IEC 61508 compared to the 2002 version, since previously no-effect failures may have been counted as safe [12].

Table I.2: Hardware safety integrity: architectural constraints on type A safety-related subsystems (IEC 61508-2, Table 2)

Safe failure fraction (SFF)	**Hardware faulttolerance**		
	0	**1**	**2**
< 60 %	SIL1	SIL2	SIL3
60 % - 90 %	SIL2	SIL3	SIL4
90 % - 99 %	SIL3	SIL4	SIL4
> 99 %	SIL3	SIL4	SIL4

Table I.3: Hardware safety integrity: architectural constraints on type B safety-related subsystems (IEC 61508-2, Table 3)

Safe failure fraction (SFF)	**Hardware faulttolerance**		
	0	**1**	**2**
< 60 %	not allowed	SIL1	SIL2
60 % - 90 %	SIL1	SIL2	SIL3
90 % - 99 %	SIL2	SIL3	SIL4
> 99 %	SIL3	SIL4	SIL4

I.6.2.2. Hardware fault tolerance according to IEC 61511 (Route 2_H)

If the equipment is developed in compliance with IEC 61508 or is documented as having prior usage, Route 2H can be applied. In this case, the minimum Hardware Fault Tolerance (HFT) must align with the standards specified in Table I.4 below, as referenced in [1] (IEC 61511-1, Table 6)

Table I.4: Minimum HFT requirements according to SIL (ref. Table 6 in IEC 61511-1)

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

I.6.3. Capability to prevent Systematic Failures

Systematic failures, manifestingas faults in hardware and software which could be occurred during specification, design, operation, or maintenance/testing and may lead to the failure of the safety function under particular circumstances (e.g., for particular input signal states). According IEC 61508/61511, unlike random hardware failures, systematic failures are not quantified. Instead, IEC 61511 and IEC 61508 mandate the adoption of specific measures and techniques to prevent and control such failures. During the design phase,these preventive and control measures should be implemented and customizedbased on the Safety Integrity Level (SIL) requirements. Detailed guidelines for these methods can be obtained from IEC 61508-2 for hardware and IEC 61508-3 for software.

I.7. Proven in use and Prior use

The concepts of "proven in use" and "prior use" may look similar, but they exhibit significant differences. "Proven in use" is a concept explained in IEC 61508-2, providingmanufacturers withan alternative method to show compliancefor avoiding and controlling systematic failures. Conversely, "prior use" is a concept outlined in IEC 61511-1, which enables end users to certify devices that were not developed in accordance with IEC 61508. This distinction showcases different applications and requirements for manufacturers and end users within the safety standards framework.

I.7.1. Proven in use

The requirements for fulfilling the "proven in use" criteria are specified in IEC 61508-2, clause 7.4.10. This clause describes one of three approachesto demonstrate howavoid and controlthe systematic failures in a device. The demonstration entails two key tasks:

- Providing documented record that the operational dangerous failure rate does not exceed the rate claimed by the manufacturer.
- Providing evidence that the contribution of systematic faults is sufficiently low to ensure compliance with the Safety Integrity Level (SIL) requirements.

Both tasks require a thorough review of all reported failures and stipulate that the observation period must be extensive enough to provide the necessary confidence in the results.

I.7.2. Prior use

The main objective of the prior use evaluation is to collect data demonstrating that dangerous systematic are sufficiently mitigated to meet the required safety integrity level. Although IEC 61511 primarily focuses on system integration, it also imposes certain restrictions on device selection. "Prior use" is one of several such restrictions for devices not developed according to IEC 61508. Demonstrating prior use requires end users to collect evidence of suitability, which includes:

- Verification of the manufacturer’s quality, management, and configuration management systems;
- Precise identification of the devices with detailed specifications;
- Historical data on device performance under similar operating conditions, including failure rates and demand rates;
- An assessment of the extent of operating experience for statistical validation.

For field devices, the user’s list of approved equipment can support claims of operational experience or prior use. It's important to note that IEC 61511 does not specify a minimum volume of operating experience required. However, the standard does mention that obtaining credible statistical reliability data typically requires significantly more operational experience than that necessary to establish evidence of prior use. This can be confusing since demonstrating prior use also demands a high level of statistical confidence, which generally necessitates extensive operational data.

In the absence of explicit requirements regarding the volume of operating experience, reference is often made to the criteria for field experience as suggested in IEC 61508-7, clause B.5.4 [4]:

- Unchangedspecification;
- Use in 10 different applications;
- 100,000 operating hours and at least one year of service history.

Although 100,000 operating hours may not be sufficient alone to demonstrate the main intent of prior use, i.e., "to gather evidence that the dangerous systematic failures have been reduced to a sufficiently low level compared to the required safety integrity," additional analytical work (e.g., FMEDA) and other documentation will be necessary to establish evidence of suitability. As part of this documentation process, the end user or an integrator acting on the end user's behalf should make a qualitative assessment and provide documentary evidence that safety devices, including Programmable Electronic (PE) logic solvers, are suitable based on prior use. This assessmentmightinclude[12]:

- Evaluating information provided by the manufacturer, such as safety manuals;
- Establishing operating references and making judgments on available failure data;
- Verifying whether quantitative and architectural requirements are met.

For programmable field devices (sensors and final elements) and logic solvers (e.g., PSD nodes), judgements on prior use should be based on Failure Probability Level (FPL) and Logic Verification Level (LVL), respectively. Applications programmed using a Functional Verification Level (FVL) must ensure that the PE device complies with IEC 61508-2:2010 and IEC 61508-3:2010.

Lastly, it is crucial to acknowledge that the recommended observation period for systems operating in low demand mode assumes regular activations (i.e., tests and/or actual demands) to verify the devices' functionality on demand. An observation period lacking a suitable number of activations is not considered valid for demonstrating fault-free operation [12].

I.8. Performance Analysis of SIS

I.8.1. Analytical approach

This section discusses the application of analytical formulas to estimate the Probability of Failure on Demand (PFD) for Safety Instrumented Systems (SIS), showcasing a range of formulas available in the literature.

I.8.1.1. IEC 61508 approach

The IEC 61508 standard, particularly in Part 6, outlines analytical formulas for calculating the average Probability of Failure on Demand (PFDavg) for various configurations of Safety Instrumented Systems (SIS), which are comprehensively detailed in Table I.5.

Table I.5: Analytical formulas based on IEC 61508

Architecture	PFD_{avg} according to IEC 61508 Part 6
1001	$(\lambda_{DU} + \lambda_{DD})t_{CE}$
1002	$2\left((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right)^2 t_{CE}t_{GE} + \beta_D\lambda_{DD}MTTR + \beta\lambda_{DU}\left(\frac{\tau}{2} + MRT\right)$
1003	$6\left((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right)^3 t_{CE}t_{GE}t_{G2E} + \beta_D\lambda_{DD}MTTR + \beta\lambda_{DU}\left(\frac{\tau}{2} + MRT\right)$
2002	$2(\lambda_{DU} + \lambda_{DD})t_{CE}$
2003	$6\left((1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right)^2 t_{CE}t_{GE} + \beta_D\lambda_{DD}MTTR + \beta\lambda_{DU}\left(\frac{\tau}{2} + MRT\right)$

where:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{\tau}{2} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D}MTTR \text{ and } t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{\tau}{3} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D}MTTR$$

$$t_{G2E} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{\tau}{4} + MRT\right) + \frac{\lambda_{DD}}{\lambda_D}MTTR$$

MTTR (Mean Time To Repair): Mean time to restore a dangerous detected failure.

MRT (Mean Repair Time): Mean time to repair of dangerous undetected failure.

The standard assumes MTTR = MRT and $\beta_{DU} = \beta$and$\beta_{DD} = \beta_D$.

The standard does not take into account CCF for series architecture like the 2002 configuration.

I.8.1.2. ISA approach

ISA-TR84.00.02 [13] details the methodology for calculating the Probability of Failure on Demand (PFDavg) for Safety Instrumented Functions (SIFs) based on the ANSI/ISA-84.01-1996 guidelines. These formulas notably include the impact of systematic failures on safety integrity. A significant difference from the IEC 61508 standard is the treatment of detected dangerous (DD) failures. Under IEC 61508, DD failures are assumed to leave a channel in a failed state until it is repaired, thereby influencing the PFD during the restoration period. Conversely, the ISA standard posits that a DD failure triggers the Safety

Instrumented System (SIS) to bring the process to a safe state, thus omitting DD failures from the PFD calculations. This approach is elaborated in Oliveira and Abramovitch [14]. Table I.6 presented below delineates the ISA formulas for different SIF configurations.

Table I.6: Analytical formulas based on ISA-TR84.00.02-2002

Architecture	PFD_{avg} according to ISA-TR84.00.02-2002
1001	$\left(\lambda_{DU} \cdot \frac{\tau}{2}\right) + \left(\lambda_F^D \cdot \frac{\tau}{2}\right) \approx \lambda_{DU} \cdot \frac{\tau}{2}$
1002	$\left(\lambda_{DU}^2 \cdot \frac{\tau^2}{3}\right) + (\lambda_{DU} \cdot \lambda_{DD} \cdot MTTR \cdot \tau) + \beta\lambda_{DU} \cdot \frac{\tau}{2}$
1003	$\left(\lambda_{DU}^3 \cdot \frac{\tau^3}{4}\right) + (\lambda_{DU}^2 \cdot \lambda_{DD} \cdot MTTR \cdot \tau^2) + \beta\lambda_{DU} \cdot \frac{\tau}{2}$
2002	$(\lambda_{DU} \cdot \tau) + (\beta\lambda_{DU} \cdot \tau)$
2003	$(\lambda_{DU}^2 \cdot \tau^2) + (3 \cdot \lambda_{DU} \cdot \lambda_{DD} \cdot MTTR \cdot \tau) + \beta\lambda_{DU} \cdot \frac{\tau}{2}$

where:

λ_F^D is the dangerous systematic failure rate.

τ is the time interval between manual functional tests of the component.

I.8.1.3. The PDS method

The PDS method, developed by SINTEF and grounded in the principles of IEC 61508 and 61511, is widely adopted within the Norwegian petroleum industry. It diverges from the IEC standards in how it calculates the Probability of Failure on Demand (PFD) by incorporating a specialized Common Cause Failure (CCF) model called the multiple beta-factor model. This model is particularly designed for different types of voting systems used in safety configurations. It accounts for the impact of CCF rates and introduces a specific formula for the beta-factor in an M-out-of-N (MooN) voting logic, denoted as $\beta(MooN) = \beta C_{MooN}$, where M is less than N. The diagram below, based on research by Hokstad and Corneliussen [15] , illustrates the C_{MooN}values for various voting configurations.

Voting	1002	1003	2003	1004	2004	3004
C_{MooN}	1.0	0.3	2.4	0.15	0.8	4.0

Table I.7: C_{MooN} factors based on system voting logic (adapted from [15]).

Based on the data provided in the preceding figure, PFD formulas for several common configurations have been derived. These formulas are simplified and generalized in Table I.8, which distills the more detailed calculations found in Table I.7. This simplification process excludes contributions from detected failures and the beta factor, facilitating a more streamlined approach to calculation.

Table I.8: Analytical formulas based on PDS method (adapted from [15])

Architecture	PFD_{avg} according to PDS method
1001	$\lambda_{DU} \cdot \frac{\tau}{2} + \lambda_{DD} \cdot MTTR$
1002	$(1-\beta)^2 \lambda_{DU}^2 \cdot \frac{\tau^2}{3} + 2(1-\beta)\lambda_{DD} \cdot \lambda_{DU} \cdot MTTR \cdot \frac{\tau}{2} + \beta\left(\lambda_{DD} \cdot MTTR + \lambda_{DU} \cdot \frac{\tau}{2}\right)$
1003	$0.3\left[\beta \cdot \lambda_{DD} \cdot MTTR + \beta\lambda_{DU} \cdot \frac{\tau}{2}\right] + \frac{1}{4}[(1-1.7\beta)\lambda_{DU} \cdot \tau]^3 + 3(1-1.7\beta)\lambda_{DD} \cdot MTTR \cdot \beta\lambda_{DU} \cdot \frac{\tau}{2}$
2002	$(2-\beta)\left(\lambda_{DU} \cdot \frac{\tau}{2}\right) + \beta \cdot \lambda_{DD} \cdot MTTR$
2003	$2.4 \cdot \beta\lambda_{DU} \cdot \frac{\tau}{2} + [(1-1.7\beta)\lambda_{DU} \cdot \tau]^2 + 3(1-1.7\beta)\lambda_{DD} \cdot MTTR \cdot \beta\lambda_{DU} \cdot \frac{\tau}{2}$
SINTEF does not use the normal β factor model for CCF. The coefficient β for CCF is the same for both detected and undetected $\beta_{DU} = \beta_{DD} = \beta$.	

I.8.1.4. Other authors approaches

Oliveira and Abramovitch [14] expanded upon the ISA-TR84.00.02-2002 PFD equations by generalizing them for use in any K-out-of-N (KooN) architecture, particularly those systems featuring higher redundancy. The formula they presented for KooN configurations is as follows:

$$\begin{aligned} PFD_{KooN} = \; & C_N^{N-K+1}((1-\beta)\lambda_{DU})^{N-K+1}\tau^{N-K}\left(\frac{\tau}{N-K+2} + MRT\right) + C_N^{N-K+1}\left((1-\beta_D)\lambda_{DD}MTTR\right)^{N-K+1} \\ & + \sum_{i=1}^{N-K} C_N^i (f_{DU}(i) \times \lambda_{DU})^i \times \tau^{i-1}\left(\frac{\tau}{i+1} + MRT\right) \times C_{N-i}^{N-K+1-i}(f_{DD}(N-K+1-i)) \\ & \times (\lambda_{DD}MTTR)^{N-K+1-i} + \beta_{DU}\left(\frac{\tau}{2} + MRT\right) + \beta_D\lambda_{DD}MTTR \end{aligned} \quad (5)$$

In the equation, the first term represents the contributions from $n-k+1 n-k+1$ DU failures, while the second term corresponds to contributions from DD failures. The third term accounts for the contributions from all possible combinations of DU and DD failures totaling $n-k+1 n-k+1$ failures. Finally, the fourth and last term quantifies the contribution from Common Cause Failures (CCFs) affecting both DU and DD failures.

The functions $f_{DU}(i)$and $f_{DD}(N-K+1-i)$ are binary functions representing the independent failure coefficients or Common Cause Failures (CCFs). The objective is to express the Probability of Failure on Demand (PFD) equation in a concise format. The specific functions are defined as follows:

Table I.9: PDS simplified analytical formulas for PFD_{avg} of KooN architecture (adapted from [7]).

Voting	Common cause contribution	Contribution fromindependentfailures
1001	-	$\lambda_{DU} \cdot \tau/2$
1002	$\beta \cdot \lambda_{DU} \cdot \tau/2$	$+[\lambda_{DU} \cdot \tau]^2/3$
2002	-	$2 \cdot \lambda_{DU} \cdot \tau/2$
1003	$C_{1oo3} \cdot \beta \cdot \lambda_{DU} \cdot \tau/2$	$+[\lambda_{DU} \cdot \tau]^3/4$
2003	$C_{1oo3} \cdot \beta \cdot \lambda_{DU} \cdot \tau/2$	$+[\lambda_{DU} \cdot \tau]^2$
3003	-	$3 \cdot \lambda_{DU} \cdot \tau/2$
MooN; N=2, 3, …	$C_{1ooN} \cdot \beta \cdot \lambda_{DU} \cdot \tau/2$	$+\frac{1}{N+1} \cdot [\lambda_{DU} \cdot \tau]^N$
MooN, M<N; N=2,3, …	$C_{MooN} \cdot \beta \cdot \lambda_{DU} \cdot \tau/2$	$+\frac{N!}{(N-M+2)! \cdot (M-1)!} \cdot [\lambda_{DU} \cdot \tau]^{N-M+1}$
MooN; N=1,2,3, ...	-	$N \cdot \lambda_{DU} \cdot \tau/2$

$$f_{DU}(x) = \begin{cases} 1, & \text{for } x = 1 \\ (1-\beta), & \text{for } x > 1 \end{cases} \text{ and } f_{DD}(x) = \begin{cases} 1, & \text{for } x = 1 \\ (1-\beta_D), & \text{for } x > 1 \end{cases} \quad (6)$$

In the formula, x denotes the number of failures, classified as DU and DD respectively. Table I.9 presents the PFD formulas for selected configurations as developed by Oliveira and Abramovitch [14] using MAPLE software.

Innal et al. [16] provide a generic formulation for thePFD_{KooN} configurations, accounting for scenarios where dangerous detected failures are either repaired instantaneously or not. The following equation incorporates the rates for dangerous detected failures ($\lambda_{DD} > 0$) and common cause failures, with $\lambda_{DU}^{(c)} = \beta\lambda_{DU}$ and $\lambda_{DD}^{(c)} = \beta_D\lambda_{DD}$. Table I.10 illustrates the application of this methodology, also known as the binomial approach, which is founded on the specified formulas:

$$\begin{aligned} PFD_{\text{Koon}} = \; & C_N^{N-K+1} \times \lambda_D^{(i)N-K+1} \times \prod_{i=1}^{N-K+1} MDT_{1ooi} + \lambda_{DU}^{(c)} \times \left(\frac{\tau}{2} + MRT\right) + \lambda_{DD}^{(c)} \times MTTR \\ & = C_N^{N-K+1} \times \prod_{i=1}^{N-K+1} \left(\lambda_{DU}^{(i)} \times \left(\frac{\tau}{i+1} + MRT\right) + \lambda_{DD}^{(i)} \times MTTR\right) + \lambda_{DU}^{(c)} \\ & \times \left(\frac{\tau}{2} + MRT\right) + \lambda_{DD}^{(c)} \times MTTR \end{aligned} \quad (7)$$

Table I.10: Selected configurations for formula by Oliveira and Abramovitch [14]

Architecture	PFD_{avg} according to Oliveira and Abramovitch [14]
1001	$(1-\beta)\lambda_{DU}\left(\frac{\tau}{2}+MRT\right)+(1-\beta_D)\lambda_{DD}MTTR+\beta\lambda_{DU}\left(\frac{\tau}{2}+MRT\right)+\beta_D\lambda_{DD}MTTR$
1002	$(1-\beta)^2\lambda_{DU}^2\tau\left(\frac{\tau}{3}+MRT\right)+(1-\beta_D)^2\lambda_{DD}^2MTTR^2+2\lambda_{DU}\left(\frac{\tau}{2}+MRT\right)\lambda_{DD}MTTR+\beta\lambda_{DU}\left(\frac{\tau}{2}+MR$ $+\beta_D\lambda_{DD}MTTR$
1003	$(1-\beta)^3\lambda_{DU}^3\tau^2\left(\frac{\tau}{4}+MRT\right)+(1-\beta_D)^3\lambda_{DD}^3MTTR^3$ $+3\lambda_{DU}\left(\frac{\tau}{2}+MRT\right)(1-\beta_D)^2\lambda_{DD}^2MTTR^2$ $+9(1-\beta)^2\lambda_{DU}^2\tau\left(\frac{\tau}{3}+MRT\right)\lambda_{DD}MTTR+\beta\lambda_{DU}\left(\frac{\tau}{2}+MRT\right)+\beta_D\lambda_{DD}MTTR$
2002	$2(1-\beta)\lambda_{DU}\left(\frac{\tau}{2}+MRT\right)+2(1-\beta_D)\lambda_{DD}MTTR+\beta\lambda_{DU}\left(\frac{\tau}{2}+MRT\right)+\beta_D\lambda_{DD}MTTR$
2003	$3(1-\beta)^2\lambda_{DU}^2\tau\left(\frac{\tau}{3}+MRT\right)+3(1-\beta_D)^2\lambda_{DD}^2MTTR^2+6\lambda_{DU}\left(\frac{\tau}{2}+MRT\right)\lambda_{DD}MTTR+\beta\lambda_{DU}\left(\frac{\tau}{2}+M$ $+\beta_D\lambda_{DD}MTTR$
The coefficient β is for CCF of DU failures and β_D is for DD failures. The functions $f_{DU}(x)$ and $f_{DD}(x)$ have been expressed in the equation in terms of $(1-\beta)$ and $(1-\beta_D)$.	

where $C_n^k=\frac{n!}{(n-k)!k!}$, $\lambda_{DU}^{(i)}=(1-\beta)\lambda_{DU}$ and $\lambda_{DD}^{(i)}=(1-\beta_D)\lambda_{DD}$ (8)

Table I.11: Selected configurations for formula by Innal et al. [16]

Architecture	PFD_{avg} according to Innal et al. [16]
1001	$(1-\beta)\lambda_{DU}\left(\frac{\tau}{2}+MRT\right)+(1-\beta_D)\lambda_{DD}MTTR+\beta\lambda_{DU}\left(\frac{\tau}{2}+MRT\right)+\beta_D\lambda_{DD}MTTR$
1002	$\left((1-\beta)\lambda_{DU}\left(\frac{\tau}{2}+MRT\right)+(1-\beta_D)\lambda_{DD}MTTR\right)\left((1-\beta)\lambda_{DU}\left(\frac{\tau}{3}+MRT\right)\right.$ $\left.+(1-\beta_D)\lambda_{DD}MTTR\right)+\beta\lambda_{DU}\left(\frac{\tau}{2}+MRT\right)+\beta_D\lambda_{DD}MTTR$
1003	$\left((1-\beta)\lambda_{DU}\left(\frac{\tau}{2}+MRT\right)+(1-\beta_D)\lambda_{DD}MTTR\right)\left((1-\beta)\lambda_{DU}\left(\frac{\tau}{3}+MRT\right)\right.$ $\left.+(1-\beta_D)\lambda_{DD}MTTR\right)\left((1-\beta)\lambda_{DU}\left(\frac{\tau}{4}+MRT\right)+(1-\beta_D)\lambda_{DD}MTTR\right)$ $+\beta\lambda_{DU}\left(\frac{\tau}{2}+MRT\right)+\beta_D\lambda_{DD}MTTR$

2002	$2 \cdot (1-\beta)\lambda_{DU}\left(\frac{\tau}{2}+MRT\right)+2 \cdot (1-\beta_D)\lambda_{DD}MTTR+\beta\lambda_{DU}\left(\frac{\tau}{2}+MRT\right)+\beta_D\lambda_{DD}MTTR$
2003	$3 \cdot \left((1-\beta)\lambda_{DU}\left(\frac{\tau}{2}+MRT\right)+(1-\beta_D)\lambda_{DD}MTTR\right)\left((1-\beta)\lambda_{DU}\left(\frac{\tau}{3}+MRT\right)+(1-\beta_D)\lambda_{DD}MTTR\right)+\beta\lambda_{DU}\left(\frac{\tau}{2}+MRT\right)+\beta_D\lambda_{DD}MTTR$
The coefficient β for CCF is the same for both detected and undetected $\beta_{DU}=\beta_{DD}=\beta$.	

I.9. Conclusion

In conclusion, this chapter provides a comprehensive exploration of Safety Instrumented Systems (SIS) in relation to their crucial role in risk management within process industries. The discussion traversed definitions, functionalities, safety standards, risk assessments, Safety Integrity Level (SIL) requirements, and systematic and operational challenges. It illuminated how SIS functions as critical safeguards against potentially catastrophic failures, elaborating on their design, operational checks such as diagnostic coverage and valve stroke tests, and compliance with the rigorous demands of IEC 61508 and IEC 61511 standards.

Particularly notable is the focus on the safety lifecycle which underpins the systematic implementation and operation of SIS, emphasizing continuous improvement from system conception to decommissioning. Moreover, the chapter underscores the importance of precise SIL allocation and robust safety requirements specifications to ensure that SIS meet both current and future safety demands.

Analytical models and real-world applications provide a solid framework for understanding the probabilistic performance of SIS components, which is essential for validating their effectiveness and reliability. The concepts of proven in use and prior use offer pathways for integrating and verifying component reliability in line with established safety standards, ensuring that the systems are fit for purpose.

CHAPTER II

OPTIMIZATION OF PREVENTIVE MAINTENANCE FOR SIS THROUGH EFFECTIVE TESTING STRATEGIES

This chapter explores the importance of maintenance strategies in maintaining the performance of Safety Instrumented Systems (SIS) during the operational phase of the safety lifecycle. It highlights the key factors influencing SIS performance, such as redundancy, overall failure rates, diagnostic coverage, common failure modes, proof testing intervals, and repair times. A significant focus is placed on the importance of conducting tests on SIS during their operational phase, which are generally categorized into Diagnostic, Proof, and Partial tests. The chapter particularly underscores the importance of proof testing, which is essential for detecting faults and preventing failures that could increase the probability of failure on demand (PFDavg). Various methods for testing SIS are presented, ranging from automatic and semi-automatic to manual approaches. Additionally, the chapter contributes to the mathematical modeling of imperfect partial proof tests, enhancing understanding of their impact on SIS performance.

This chapter is dedicated to optimize the preventive maintenance of Safety Instrumented Systems (SIS) by integrating a spectrum of testing strategies that are vital for enhancing the reliability of these systems throughout their operational phase.Effective maintenance of Safety Instrumented Systems (SIS) hinges on a robust testing program—it encompasses diagnostic, functional, and proof tests, each serving a distinct purpose in maintaining the system's operational integrity. Specifically, proof testing is indispensable as it is designed to identify latent failures that could potentially affect the system's ability to perform its essential safety functions when they are most needed. These tests go beyond routine evaluations; they are rigorous assessments intended to ensure that SIS are capable of handling real-world emergencies by effectively simulating conditions that might trigger system failures.

Maintaining SIS presents various challenges due to the complexity of these systems, which require specialized knowledge and sophisticated maintenance protocols. These challenges are compounded by the logistical difficulties involved in conducting exhaustive tests without disrupting ongoing operations. Moreover, staying abreast of technological advancements and managing the requisite resources are essential for ensuring adherence to evolving safety standards.

Testing of Safety Instrumented Systems is mandated by such standards as IEC 61508 [4] and IEC 61511 [1], with a primary focus on safeguarding the safety and reliability of these systems within industrial processes. This testing, typically outlined during the planning phase, involves a series of thorough checks and validations to confirm that the SIS operates correctly under diverse conditions, particularly in emergency or failure scenarios. The objective is to validate that the system can effectively prevent accidents, mitigate risks, and maintain safe operations.

Regular proof testing of SIS is critical to detect "Dangerous Undetected" faults [4] [17]. In the absence of these periodic tests, it becomes challenging to verify the reliability and effectiveness of an SIS, thereby significantly increasing the risk of system failure when it is most needed. Thus, regular proof testing is not merely a compliance requirement but a fundamental safety measure to ensure that the SIS performs its protective functions adequately on demand.

Testing a Safety Instrumented System involves simulating the system's response to conditions similar to real emergencies. This comprehensive simulation covers all subsystems and channels, aiming to uncover various types of dangerous failures, including those typically undetectable during normal operations. The primary goal is to ensure that the SIS behaves as expected in real emergency situations, thus upholding the safety it is designed to provide.

An important aspect of this testing is its role in shaping effective maintenance strategies. By pinpointing potential failure points—whether they necessitate repairs or complete replacements—testing informs the planning of effective maintenance activities. This is essential for preventing frequent failures and for maintaining the designated Safety Integrity Level (SIL) of the system. SIL is a measure of the reliability of the SIS in performing its safety functions, consistent testing and maintenance are crucial to preserve this level of integrity and performance.

Furthermore, testing a Safety Instrumented System provides crucial data for maintenance teams helping to implementcorrective, preventive, and predictive maintenance measures. This data, derived from detailed simulations of emergency scenarios, not only identifies existing failure points but also potential future vulnerabilities. This enables maintenance to be strategically tailored, focusing on immediate repairs and incorporating long-term strategies to preemptively tackle issues before they arise. Such a proactive maintenance approach significantly enhances the SIS's reliability and extends its operational lifecycle, directly contributing to its effectiveness in risk mitigation and ensuring ongoing protection against industrial hazards [18][19].

This chapter explores various testing strategies that can be customized to boost the effectiveness of SIS maintenance. It examines how different testing methods—automatic, semi-automatic, and manual—along with their scheduling, whether sequential, simultaneous, or staggered, can significantly impact maintenance outcomes. These strategies are pivotal not only in maintaining system reliability but also in optimizing the system's performance and standing its operational lifecycle.

An essential component of this chapter is the mathematical modeling of testing strategies, particularly the modeling of imperfect partial proof tests. These models provide valuable insights into the quantitative impacts of various testing regimes on the system’s reliability, guiding the optimization of maintenance schedules and strategies. Additionally, the chapter addresses the economic implications of SIS maintenance, presenting a cost-benefit analysis framework to help maintenance managers and engineers for assessing the financial impact of various maintenance strategies.

II.1. Current challenges in SIS maintenance

Maintaining a Safety Instrumented System (SIS) involves several common challenges, each requiring careful management and strategic planning. The process involves navigating the complexities inherent to sophisticated safety systems that demand specialized knowledge and technical skills. These challenges are exacerbated by the need for conducting rigorous and comprehensive testing without disrupting ongoing operations, keeping pace with rapid technological advancements, and managing the significant

resources necessary for effective maintenance. Additionally, ensuring compliance with constantly evolving safety standards further complicates the maintenance landscape. Each of these factors necessitates a strategic and well-considered approach to maintain the operational integrity and reliability of SIS.

Here's an analysis of these challenges:

1. **Complexity of systems**: SIS are often complex, involving intricate components and sophisticated software. Understanding and maintaining these systems requires specialized knowledge and skills. The complexity can make diagnosing issues and implementing repairs time-consuming and challenging.
2. **Regular testing and calibration**: SIS components require regular testing and calibration to ensure that they are functioningproperly. This process can be labor-intensive and may require temporary system shutdowns, which can disrupt normal operations.
3. **Keeping up with technological advances**: As technology evolves, SIS components can become outdated. Upgrading or integrating new technology with existing systems can be challenging, both technically and financially.
4. **Environmental conditions**: Extreme environmental conditions, such as high temperatures, humidity, or corrosive environments, can impact the performance and integrity of SIS components. Regular maintenance should take in consideration these conditions to prevent premature failure.
5. **Compliance with safety standards and regulations**: SIS must comply with various safety standards and industry regulations, which can change over time. Keeping up with these changes and ensuring system compliance can be a significant challenge.
6. **Human error**: The risk of human error in operating, testing, and maintaining SIS is a constant challenge. Proper training and clear maintenance protocols are necessary to minimize these risks.
7. **Software updates and cybersecurity**: With the increasing integration of digital technologies, It is crucial to ensure that the software components of SIS are up to date and secured from cyber threats is crucial. This requires regular updates and vigilant cybersecurity measures.

8. **Resource allocation**: Allocating sufficient resources, including skilled personnel and budget, for the maintenance of SIS can be challenging, especially for organizations with limited resources.
9. **Documentation and record keeping**: Accurate and up-to-date documentation of maintenance activities, system modifications, and operational procedures is essential. Poor documentation can create gaps in maintenance activities, misunderstanding of system changes, and compliance issues.
10. **Aging equipment and obsolescence**: Over time, components of SIS can become obsolete, making hard to find spare parts and increasing the risk of system failure. Planning for upgrades or replacement is essential but can be expensive and time-consuming.
11. **Integration with other systems**: Ensuring seamless integration between the SIS and other control systems within a facility can be complex. Incompatibilities can lead tomalfunctions or failures.
12. **Balancing maintenance with production demands**: Conducting thorough maintenance often requires system downtime, which can conflict with production demands. Finding the balance between maintaining safety and meeting production targets is a challenging concern.

In summary, maintenance of SIS requires navigating a range of complex and interrelated challenges. These include technical complexities, compliance requirements, environmental factors, resource management, and the need for full vigilance against human error and technological obsolescence. Effective maintenance strategies must address these challenges to ensure the ongoing reliability and effectiveness of the SIS.

II.2. Maintenance strategies' effect on SIS performance

Redundancy (KooN), overall failure rate (λ), diagnostics coverage rate (DC), proportion of common failure modes (β), proof testing intervals, and Mean Time To Repair (MTTR) are all critical factors that influence the performance of Safety Instrumented Systems (SIS).

- **Redundancy (KooN):** This refers to the number of redundant components or subsystems in the SIS. Higher redundancy typically enhances system reliability by providing backup options in case of a component failure.

- **Overall failure rate (λ):** Expressed in failures per hour or as the inverse of the Mean Time Between Failures (MTBF), this rate indicates how often components within the SIS are likely to fail. A lowerfailure rate means a more reliable system.

$$\lambda_D = \lambda_{DD} + \lambda_{DU} = DC.\lambda_D + (1 - DC).\lambda_D \quad (9)$$

- **Diagnostics coverage rate (DC):** This is the percentage of potential failure modes that can be detected by the system's diagnostic functions. Higher DC rates imply better system monitoring and early detection of issues, reducing the risk of undetected failures.
- **Proportion of common failure modes (β):** Represented as a percentage of total failures, this factor accounts for failures that affect multiple components or systems simultaneously. High β values can indicate vulnerabilities in the system where a single issue might lead to widespread failures.
- **Proof testing intervals:** These are the scheduled times at which the system undergoes comprehensive testing to ensure all components and functions are operating correctly. Longer intervals might increase the risk of undetected failures, while more frequent testing can enhance system reliability.

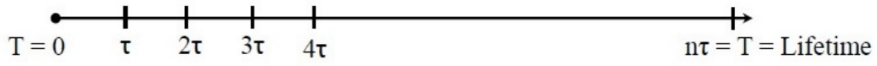


Figure II.1: Proof Test Interval, where a test is carried out at each $n\tau$

- **Repair time (MTTR):** This is the average time required to repair and restore the SIS after a failure. Shorter MTTR helps in minimizing downtime and maintaining system availability.

The concept of maintenance strategies for Safety Instrumented Systems (SIS) is crucial in ensuring their optimal performance during their operational phase. This importance stems primarily from the potential to identify faults or failures during this phase. Alessandro Birolini, in his 2017 publication, emphasizes the necessity of implementing both preventive and corrective maintenance. Preventive maintenance is conducted at predetermined intervals to forestall potential issues, while corrective maintenance is a response to identified faults.

The effectiveness of these maintenance strategies is not merely theoretical; they have quantifiable impacts on the performance of SIS. The various strategies include corrective, preventive, predictive, and proactive maintenance, each with its distinct effect on system performance.

- **Corrective maintenance:** This strategy is fundamentally reactive. It comes into play after a fault has been identified. While necessary, it can negatively impact SIS performance. This is because the system may experience increased downtime while repairs are made, and there is a high risk of failure during this period. The performance impact can be measured using metrics like Mean Time Between Failures (MTBF), which typically shows a decrease in this scenario.
- **Preventive maintenance:** This approach is more proactive, involving routine checks and repairs at scheduled intervals, regardless of whether a fault has been detected. The primary benefit of preventive maintenance is the reduction of unexpected system failures. This leads to an improved Safety Integrity Level (SIL), which is a measure of risk reduction provided by the SIS, and a lower failure rate. By addressing potential issues before they become problems, preventive maintenance enhances the overall reliability of the SIS.
- **Predictive maintenance:** This strategy involves continuously monitoring the condition of the SIS to predict when maintenance should be performed. This approach minimizes downtime and enhances the system's reliability. Predictive maintenance allows for maintenance to be scheduled at the most opportune time, rather than at predetermined intervals. Its effectiveness is assessed through metrics such as Mean Time to Repair (MTTR) and reduced failure rates.
- **Proactivemaintenance:** Regarded as the most comprehensive strategy, proactive maintenance involves a holistic approach to maintaining the SIS. It goes beyond mere scheduled checks or condition monitoring; it includes the implementation of systemic changes to improve the overall performance and reliability of the system. This strategy has the most positive impact on SIS performance, leading to higher SIL ratings and maintaining extremely low failure rates. Proactive maintenance is essentially about ensuring that the system is always at its best, thereby guaranteeing safety.

The term "failures" in the context of Safety Instrumented Systems (SIS) encompasses two primary types: safe failures and dangerous failures. Understanding the distinction between them and their implications is critical for maintaining the reliability and safety integrity of an SIS.

- **Safe failures:** These are failures that lead to spurious trips. In other words, they cause the SIS to activate when it's not actually needed. While these failures can be inconvenient and may lead to unnecessary downtime or interruption in operations, they don't directly compromise safety. Instead, they err on the side of caution, triggering safety responses even in the absence of a real hazard.

- **Dangerous failures:** These are far more critical as they prevent the SIS from functioning correctly when it's really required. A dangerous failure means that the system fails to respond in a situation where it should, causing a risk to safety.

A significant concern within these failure types is the occurrence of undetected failures, particularly undetected dangerous failures. These failures are critical because the system's diagnostic functions fail to identify them, leaving the system compromised without the knowledge of the operators. The probability of such failures occurring, and remaining undetected, tends to increase over time. This increase affects the Probability of Failure on Demand (PFDavg), a key metric in assessing SIS performance.

PFDavg is a measure of the likelihood that the SIS will fail to perform its safety function when required. As undetected dangerous failures accumulate, the PFDavg increases, indicating a decline in system reliability. To manage this, proof testing is conducted. Proof testing involves a thorough examination of the SIS to detect and rectify any failures that went unnoticed during normal operations. This process is crucial as it helps to uncover and address undetected failures, thereby reducing the PFDavg and enhancing the system's reliability.

The calculation of PFDavg is a fundamental aspect of determining whether an SIS can achieve the required level of risk reduction. This calculation takes into account various factors, including maintenance activities and the effectiveness of proof testing in identifying and rectifying undetected dangerous failures. The goal of this calculation is to ensure that the SIS meets the desired level of risk reduction.

Safety Integrity Level (SIL) is a key concept when discussing the reliability of safety instrumented systems. SIL is a measure of the level of risk reduction provided by the SIS. It is determined through the calculation of PFDavg, among other factors. The higher SIL means lower probability that the SIS will fail to perform its required safety functions.

Common Cause Failures (CCF) are a critical concept in the field of redundant systems, which are designed to enhance reliability and safety by using multiple components to perform the same function. The idea behind redundancy is that even if one component fails, others can continue to function, ensuring that the overall system remains operational. However, CCFs present a unique challenge in this setup. They occur when two or more components of the system fail simultaneously or in quick succession due to a shared cause. This shared cause could be anything from design flaws, manufacturing defects, to environmental factors or external events like power outages or fires. The occurrence of CCFs defeats the

purpose of redundancy, as it leads to the simultaneous failure of multiple backup components, resulting in the loss of the desired function of the system.

To understand and mitigate the impact of CCFs on system reliability, various models have been developed. Among these, the β-factor model stands out for its simplicity and effectiveness, making it a popular choice in reliability engineering. This model is also recommended by the IEC 61508 standard, a widely recognized international standard for the functional safety of electrical, electronic, and programmable electronic safety-related systems. The β-factor model provides a way to quantify the impact of CCFs on the overall failure rate of the system. It operates by dividing the total failure rate of a component (denoted as λ) into two distinct categories: independent failures and dependent failures due to CCFs. Independent failures are those that occur solely due to the component's own characteristics, unrelated to external factors or the state of other components. In contrast, dependent failures are those directly influenced by common causes that can affect multiple components.

$$\lambda = \lambda^{ind} + \lambda^{CCF} = (1-\beta).\lambda + \beta.\lambda \quad (10)$$

In practice, using the β-factor model involves determining the proportion of the total failure rate that can be attributed to common causes. This proportion is represented by the β-factor, a value between 0 and 1. A higher β-factor indicates a greater likelihood that failures will occur due to common causes, hence suggesting a higher risk of CCFs in the system. This model aids in analyzing and designing redundant systems by providing insights into how much of the system's unreliability can be attributed to CCFs. By understanding this, engineers can implement targeted strategies to reduce the risk of CCFs, such as diversifying designs, implementing varied manufacturing processes, or incorporating environmental protection measures. The β-factor model thus plays a crucial role in enhancing the reliability and safety of redundant systems, ensuring they can effectively perform their intended functions even in the presence of potential common causes of failure.

II.3. Testing strategies for SIS

Figure II.2 illustrates a comprehensive approach for testing Safety Instrumented Systems (SIS), showcasing various methods designed to detect different types of failures. Key among these methods are diagnostic tests, which are adept at identifying dangerous detected failures (DD). These are failures that the system's self-monitoring capabilities can recognize. In contrast, proof tests focus on uncovering dangerous undetected failures (DU) – failures that diagnostic tests may not have detected. Proof tests

themselves vary and can be either full or partial, and perfect or imperfect, depending on their scope and thoroughness.

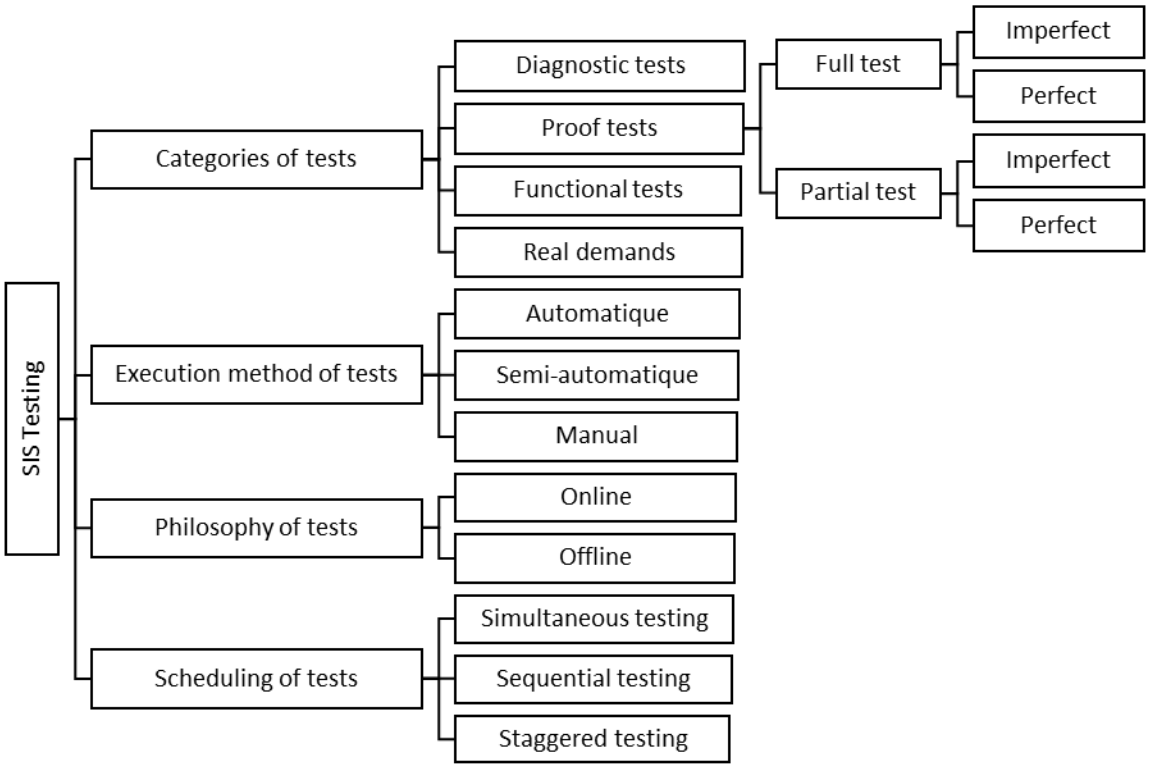


Figure II.2: SIS testing approach

Additionally, functional tests play a critical role in SIS evaluation. They are considered the most realistic form of testing, superior to both proof and diagnostic tests, particularly in ensuring the correct operation of the safety loop. Functional tests are akin to proof tests, especially in systems where there are no redundant groups in the safety loop, and where each subsystem relies on a single component to perform the required safety function.

The testing methodologies for SIS can be categorized into Automatic, Semi-Automatic, and Manual approaches. Automatic tests, such as diagnostic tests, are pre-programmed and run without human intervention. Semi-Automatic tests combine manual initiation (like turning a switch) with automated processes, and Manual tests are entirely human-driven, from initiation to execution.

Moreover, testing philosophy can be divided into online and offline categories. Online tests are performed while the Equipment Under Control (EUC) is operational, allowing for continuous system operation. In contrast, offline tests are conducted when the EUC is not in operation, necessitating a temporary shutdown.

Lastly, the scheduling of these tests can be strategized through Sequential, Simultaneous, or Staggered Testing. Each strategy offers different benefits and is chosen based on the specific requirements and operational contexts of the SIS. This multi-faceted approach to SIS testing, as detailed in the works of [20][21][22][23] and [17], ensures a comprehensive evaluation of system safety and reliability.

II.3.1. Proof testing: according to IEC61508 [4] a proof test is a "periodic test performed to detect dangerous hidden failures in a safety-related system so that, if necessary, a repair can restore the system to an “as new” condition or as close as practical to this condition", this definition means that the proof test is a routine examination conducted on safety-related systems to uncover latent, potentially hazardous failures that are not immediately observed during normal operation. This test aims to ensure that these systems are functioning as intended and to maintain a high level of safety. If any hidden defects are found, the system can be repaired to either return it to its original, "as new" state or to a state as close as possible to that, thereby ensuring the system's reliability and effectiveness in preventing accidents or malfunctions.

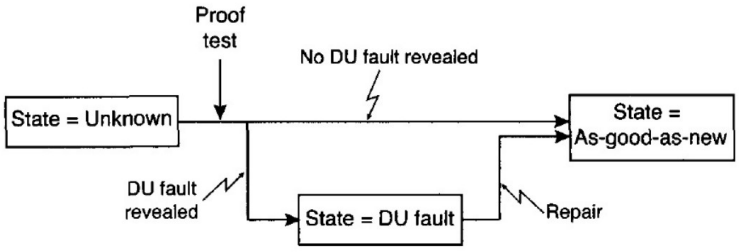


Figure II.3: The process of proof testing [24]

Proof tests are categorized into two main types: full and partial.

II.3.1.1. Full proof tests: These involve a comprehensive examination of the entire safety-related system to ensure every component and function operates as intended. Full proof tests are thorough, checking all aspects of the system to detect any hidden failures. This type of test often requires shutting down the system entirely, as it involves an exhaustive inspection of all parts, software, and operational capabilities. The goal is to confirm that the system can perform its safety functions reliably under all expected conditions. Full proof tests are typically more time-consuming and resource-intensive but offer a higher level of assurance about the system's overall safety and reliability.

II.3.1.2. Partial proof tests: In contrast, partial proof tests focus on specific parts or functions of a safety-related system, rather than the entire system. These tests are less comprehensive and are used when a full test is impractical, too disruptive, or unnecessary for certain system components. Partial proof tests

are useful for ongoing maintenance and monitoring, as they can be conducted more frequently and with less impact on system operation. They help in early detection of potential issues in critical components of the system. However, since they do not cover the entire system, they might miss failures in untested parts.

Proof test coverage (PTC) is a critical metric in safety engineering, used to evaluate the effectiveness of proof tests in identifying potential failures within a safety-related system. Essentially, PTC quantifies how thoroughly a proof test can uncover hidden failures that might prevent the system from performing its essential safety functions when they are most needed. This metric is expressed as a percentage and indicates the proportion of all possible hidden failures that the proof test is capable of detecting. For instance, a proof test with a PTC of 90% means it can identify 90% of the potential hidden failures within the system. The remaining 10% represents the portion of failures that the test may not detect, which constitutes a residual risk.

The impact of a proof test on PFDAvg (Average Probability of Failure on Demand) is significant in the context of safety-critical systems. When a proof test is conducted, it can detect hidden failures in the system that would otherwise increase the risk of a safety function not being performed when needed. By identifying and rectifying these hidden failures, proof tests effectively reduce the PFDAvg, meaning they lower the probability that the system will fail when called upon.

The effectiveness of the proof test, as measured by the Proof Test Coverage (PTC), directly influences the extent to which PFDAvg is reduced. A higher PTC means a more effective proof test, capable of detecting a larger percentage of potential failures, thus leading to a greater reduction in PFDAvg. Conversely, a proof test with lower PTC might leave more undetected failures, resulting in a smaller reduction in PFDAvg.

Mean test time (MTT) of a proof test refers to the average duration required to perform a proof test on a safety-related system. This metric is crucial in safety engineering, as it helps in planning and resource allocation for the maintenance of these systems. MTT encompasses the time taken to inspect, test, and verify all components and functions of the system to ensure they are operating correctly and can perform their safety functions when needed. A shorter MTT is generally desirable as it implies less downtime and disruption to the system's operation. However, it's important to balance the need for efficiency with the thoroughness of the test, as a hastily conducted proof test might overlook critical issues. MTT is a key factor in scheduling maintenance and safety checks. It provides a practical benchmark for organizations to assess the operational impact of safety maintenance activities.

Mean repair time (MRT) in the context of proof testing is a critical indicator that quantifies the average time taken to repair and restore a safety-related system to its fully functional state following the identification of a failure during a proof test. This measure includes all the time spent from the moment a failure is detected until the system is repaired, tested, and confirmed to be operational again. MRT is a vital aspect of system reliability and safety management, as it directly impacts the system's availability and readiness. A shorter MRT is generally preferable, as it minimizes the duration during which the system is not fully operational, thereby reducing the risk of unavailability in case of an emergency or demand. However, it's crucial that repairs are thorough and effective, ensuring that once the system is back online, it can perform its safety functions reliably. MRT is a key consideration in maintenance planning and resource allocation. It serves as an indicator of the efficiency and effectiveness of the maintenance processes and can drive improvements in repair strategies and resource management.

II.3.2. Diagnostic testing:

Diagnostic testing is an essential process for ensuring the continuous integrity and safety of these critical systems. These tests are largely automated and are designed as a form of self-testing within various components of the SIS. The primary aim of diagnostic testing is to regularly check and verify the integrity and functionality of each part of the system, from sensors and logic solvers to actuators. By doing so, these tests can identify potential issues, such as component malfunctions or degradation, before they escalate into major failures. This proactive maintenance approach helps in preempting system breakdowns, thereby enhancing overall safety. The automated nature of diagnostic tests allows them to be conducted frequently and efficiently, minimizing the need for extensive manual intervention and ensuring that the SIS remains in a constant state of readiness.

The results obtained from diagnostic tests in systems like Safety Instrumented Systems (SIS) are invaluable for guiding maintenance strategies and enabling timely interventions. By continuously monitoring and assessing the conditions of various system components, these tests can detect early signs of wear, degradation, or malfunction. This early detection is crucial, as it allows maintenance teams to address issues before they evolve into significant failures that could compromise system integrity and safety. For instance, if a diagnostic test reveals a sensor drifting out of calibration, maintenance can recalibrate or replace the sensor before it leads to incorrect readings and potentially unsafe conditions. This proactive approach not only ensures the continuous reliability and safety of the system but also can lead to more efficient maintenance practices. It allows for repairs to be scheduled at convenient times, reducing unplanned downtime and high-cost emergency interventions. The insights provided by

diagnostic tests play a pivotal role in maintaining the optimal performance of critical safety systems, thereby safeguarding both the equipment and the personnel relying on these systems.

Diagnostic test coverage (DTC) quantifies the effectiveness of diagnostic tests in identifying potential faults within a system. Expressed as a percentage, DTC measures the extent to which the system's self-testing capabilities can detect and report failures or anomalies. A high DTC value indicates that a large proportion of possible faults can be uncovered by the system's diagnostic tests, enhancing the reliability and safety of the system. For example, a DTC of 80% means that the diagnostic tests can detect 80% of all potential faults, providing a significant level of assurance regarding the system's operational integrity. DTC helps in evaluating the effectiveness of the diagnostic capabilities of a system and guides improvements in system design and maintenance strategies.

II.3.3. Functional testing:

Functional Testing involves verifying the operational capability and reliability of the entire SIS. This type of testing is designed to simulate actual conditions under which the SIS would be required to perform its safety functions. During a functional test, various components of the SIS, such as sensors, logic solvers, and actuators, are rigorously evaluated to ensure they respond appropriately to simulated hazard scenarios. The goal is to confirm that the system can detect and react to potential dangers effectively, thereby preventing accidents or mitigating their consequences. Functional Testing differs from diagnostic testing, which focuses on individual component conditions; instead, it assesses the entire SIS under realistic conditions.

II.3.4. Real demands serving as tests

Real Demands in the context of a Safety Instrumented System (SIS) refer to actual, unplanned operational scenarios where the SIS is required to perform its safety functions as it would in a real emergency. Unlike planned diagnostic, proof, or functional tests that are conducted under controlled conditions, real demands occur spontaneously during normal operation, providing a unique and authentic test of the system's effectiveness. These real-life scenarios are critical because they test the SIS in the exact conditions for which it was designed, including all operational variables and environmental factors that might not be fully replicable in a simulated test environment. The way the SIS responds to these real demands—such as activating alarms, shutting down processes, or initiating other safety measures—offers invaluable insights into its actual performance and reliability. This form of testing helps in validating the practical effectiveness of the SIS, ensuring that it is capable of protecting people, the

environment, and assets in real-world situations. Real demands serving as tests are thus an essential aspect of assessing and maintaining the overall integrity and readiness of a Safety Instrumented System.

II.3.5. Various methods to execute tests

The testing of Safety Instrumented Systems (SIS) encompasses a range of methods, each varying in the degree of human involvement and the operational status of the Equipment Under Control (EUC). These testing methods are essential to maintain and ensure the reliability of the SIS and are broadly categorized into Automatic, Semi-Automatic, and Manual Tests.

II.3.5.1 Automatic test: In this type of testing, the process is fully automated and embedded within the system's components. These tests run independently without the need for human intervention, thereby significantly minimizing the risk of human error. A common example of automatic testing is diagnostic tests, which continuously monitor the system and automatically perform checks to ensure all parts are functioning correctly. This type of testing is crucial for ongoing system health assessment and is especially valuable in high-availability environments.

II.3.5.2. Semi-automatic tests: Semi-automatic tests blend automated processes with human initiation or intervention. Typically, a person will start the test, like activating a switch or pressing a button, after which the test proceeds automatically. This approach allows for human control over the timing and circumstances of the test while still benefiting from the precision and consistency of automated procedures. It's particularly useful in situations where some level of human judgment or oversight is desirable before commencing the test.

II.3.5.3. Manual tests: These tests are entirely human-driven and do not rely on automated software or systems. Manual tests, such as proof tests and partial proof tests, require personnel to physically inspect, operate, and evaluate the various components and functions of the SIS. While this method can be more time-consuming and subject to human error, it is essential for comprehensive system evaluation and for situations where automated testing is not feasible or available.

II.3.6. Philosophy of tests

Online Tests and Offline Tests are two distinct approaches to test Safety Instrumented Systems (SIS) that differ based on the operational state of the Equipment Under Control (EUC).

II.3.6.1. Online tests: These tests are conducted while the EUC is fully operational and active. The primary advantage of online testing is that it allows the SIS to be tested without disrupting the normal operations of the EUC. This means that the production or process that the EUC controls can continue

running without interruption, ensuring no loss of productivity or downtime. Online tests are particularly valuable in continuous process industries or in scenarios where shutting down the EUC is either impractical or costly. These tests often involve automated diagnostic checks that can monitor the conditions and functionality of the SIS components without interfering with their operation.

II.3.6.2. Offline tests: In contrast, offline tests are carried out when the EUC is not in operation. During these tests, the EUC is typically shut down, and the SIS is isolated for safety reasons. This approach allows for a more thorough and in-depth examination of the SIS, as testers can safely access and evaluate all components and functions without the risk of affecting the EUC's operation or compromising safety. While offline tests are more disruptive, requiring a halt in the EUC's operations, they are crucial for conducting comprehensive evaluations, particularly for aspects of the SIS that cannot be tested during normal operations.

Both online and offline tests are essential for a holistic and effective maintenance strategy of SIS. Online tests provide continuous monitoring and immediate detection of potential issues while maintaining operational continuity. In contrast, offline tests allow for detailed inspections and more complex testing procedures, ensuring the overall integrity and reliability of the SIS. The choice between online and offline testing depends on various factors, including the nature of the EUC, the criticality of the process, and the specific requirements of the safety system.

II.3.7. Scheduling of tests

The scheduling of tests for Safety Instrumented Systems (SIS) is a critical process in maintaining their reliability and functionality. It requires careful consideration of both the operational needs of the Equipment Under Control (EUC) and the safety requirements of the system. There are three primary strategies for scheduling SIS tests: Simultaneous Testing, Sequential Testing, and Staggered Testing.

II.3.7.1. Simultaneous testing:

Simultaneous Testing in the context of Safety Instrumented Systems (SIS) is a testing approach where all redundant channels of a subsystem are tested at the same time. The primary implication of this method is that during the test, the safety function of the system becomes unavailable. This unavailability poses a significant risk and may even necessitate the temporary shutdown of the Equipment Under Control (EUC), potentially leading to operational disruptions. The major disadvantages of Simultaneous Testing include the loss of safety functionality during the test, potential for production loss, and an overall increased risk. These drawbacks make it generally the least preferred option among testing strategies for

SIS. However, it is employed in specific circumstances where the temporary unavailability of the SIS can be tolerated or managed effectively, such as in systems with less stringent operational continuity requirements or where alternative safety measures can be temporarily deployed. Despite its challenges, Simultaneous Testing can be useful in certain scenarios, particularly where a comprehensive, all-at-once assessment of redundant channels is needed.

II.3.7.2. Sequential testing:

Sequential Testing is a methodical approach for testing Safety Instrumented Systems (SIS) where each item or channel in the subsystem is tested individually, one after the other. The primary advantage of this approach is that it allows the safety function of the system to remain available, albeit in a degraded mode, throughout the testing process. This method enables the Equipment Under Control (EUC) to continue operating without the need for a complete shutdown, making it more reliable and less disruptive compared to simultaneous testing. The process involves thoroughly testing and restoring one channel before proceeding to the next, ensuring at least a basic level of safety function is consistently available. This step-by-step method minimizes the risk of complete system failure during testing and is particularly beneficial in environments where even a temporary total shutdown could have significant implications. Due to its balanced approach that offers a blend of safety and operational continuity, Sequential Testing is a popular choice in many industries, especially those where maintaining continuous system operation is crucial.

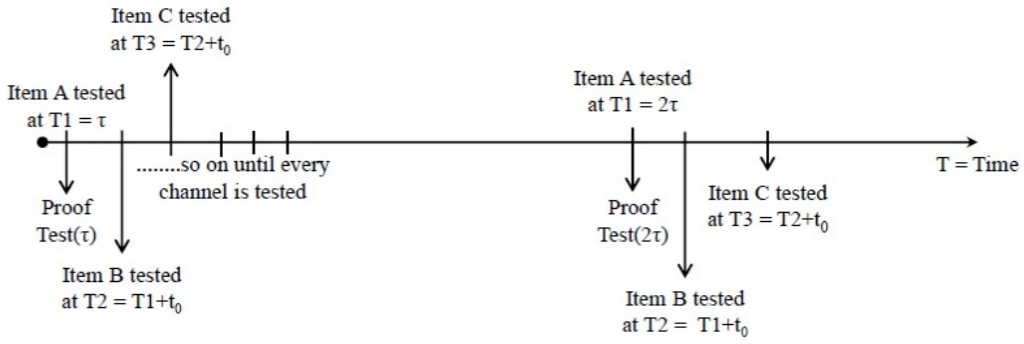


Figure II.4: Sequential testing of redundant channels at the starting/end of each proof test τ

II.3.7.3. Staggered testing:

Staggered Testing is a strategic approach for testing Safety Instrumented Systems (SIS) where redundant components are tested at different intervals, rather than all at once. This method involves sequentially testing each component over the total test interval, allowing for continuous and uninterrupted operation

of the safety loop. The primary advantage of Staggered Testing is that it does not adversely affect the production and safety functionality of the Equipment Under Control (EUC). By testing components at different times, this approach enhances the overall reliability of the SIS and significantly reduces the risk of Common Cause Failures (CCFs). Additionally, it allows for the distribution of testing responsibilities among different teams, potentially decreasing the likelihood of human errors. This distribution of testing tasks also aids in managing workload and resources more efficiently. Staggered Testing is often favored in various industries due to its ability to maintain operational continuity while ensuring comprehensive and thorough testing of the system's components. This balance makes it a highly preferred method for ensuring the effectiveness and reliability of safety-critical systems.

The choice of test scheduling strategy for an SIS depends on several factors, including the criticality of the system, the operational requirements of the EUC, and the risk tolerance of the organization. Staggered testing is generally favored for its ability to maintain continuous system operation while ensuring thorough testing of all components. Sequential testing offers a compromise, providing some level of continuous operation but with reduced redundancy during testing. Simultaneous testing, while less preferred due to its higher risk, might be suitable in situations where temporary unavailability of the SIS is manageable.

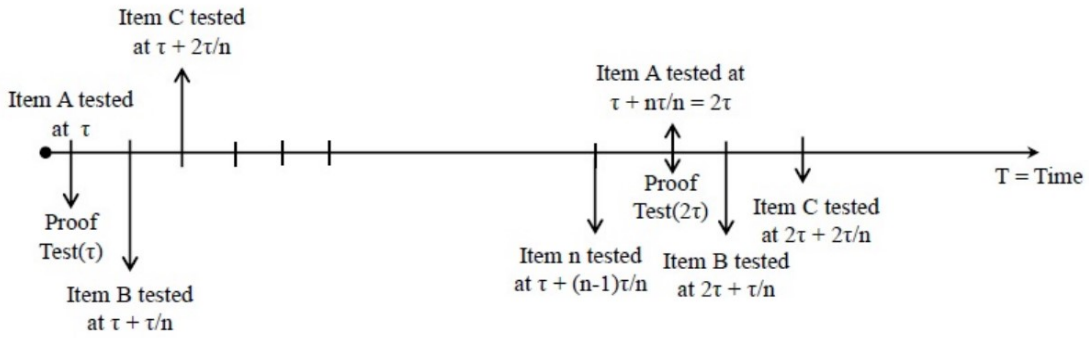


Figure II.5: Staggered testing of n redundant channels at equal parts of the proof test interval τ

II.4. Modeling of an imperfect partial proof test

Full and partial proof tests are essential maintenance strategies for Safety Instrumented Systems (SIS). A full proof test involves a comprehensive examination of the entire system, ensuring that all components and subsystems of the SIS are functioning correctly and as intended. This type of test is thorough and aims to uncover any hidden failures or performance issues that might compromise safety. In contrast, partial proof tests are more targeted, focusing on specific subsystems or components within the SIS.

These tests are used to identify potential failures or deficiencies in certain areas of the system, allowing for focused corrective actions. Both full and partial proof tests are critical in maintaining the reliability and safety of SIS, as they help to detect and rectify issues before they lead to hazardous situations.

This section seeks to enhance the model originally presented by [25], incorporating the concept of imperfect partial proof tests. The original model, while comprehensive, did not fully account for the potential limitations and imperfections inherent in partial proof tests conducted on safety systems. Recognizing that these tests may not always detect every failure or issue, the reformulated model aims to integrate this reality into its calculations and predictions. This is showed in equation 11, which has been modified to include parameters or factors representing the imperfect nature of partial proof tests. By doing so, the model becomes more realistic and practical, offering a better understanding and assessment of the reliability and effectiveness of safety systems under conditions where partial proof tests might not be fully effective in identifying all potential failures or shortcomings.

$$PFD_{Avg} \approx \frac{1}{\tau}\sum_{i=1}^{m}\sum_{j=0}^{n-k}\binom{n}{j}\tau_i((1-\gamma_1\gamma_2)\lambda_{DU}t_{i-1})^j\frac{(n-j)!((\lambda_{DU}\tau_i)^{n-j-k+1})}{(n-j-k+2)!(k-1)!} + \frac{1}{\tau}\sum_{i=1}^{m}\sum_{j=n-k+1}^{n}\binom{n}{j}\tau_i((1-\gamma_1\gamma_2)\lambda_{DU}t_{i-1})^j \quad (11)$$

Additionally, if the imperfect partial tests are conducted at regular intervals of $\tilde{\tau}$, where, $\tau_i = \tilde{\tau}$ for all $i, t_i = i.\tilde{\tau}$ and $\tilde{\tau} = \tau/m$ with γ_1 is the partial proof test coverage and γ_2 is the imperfect partial proof test coverage or efficiency of partial proof test coverage; then the formula for average Probability of Failure on Demand $\mathrm{PFD_{Avg}}$ can be simplified to:

$$PFD_{Avg} \approx \frac{1}{m}\sum_{i=1}^{m}\sum_{j=0}^{n-k}\binom{n}{j}((i-1)((1-\gamma_1\gamma_2)\lambda_{DU})\tilde{\tau})^j\frac{(n-j)!((\lambda_{DU}\tilde{\tau})^{n-j-k+1})}{(n-j-k+2)!(k-1)!} + \frac{1}{m}\sum_{i=1}^{m}\sum_{j=n-k+1}^{n}\binom{n}{j}((i-1)((1-\gamma_1\gamma_2)\lambda_{DU})\tilde{\tau})^j \quad (12)$$

The use of partial proof test coverage and imperfect partial proof test coverage serve as the primary tools for the entire assessment, ultimately resulting in the desired Average Probability of Failure on Demand (PFDavg) for the assumed KooN subsystem.

II.5. Economic aspects of optimized SIS maintenance

II.5.1. Cost-benefit analysis framework for optimized maintenance

The Cost-Benefit Analysis (CBA) Framework for Optimized Maintenance of Safety Instrumented Systems (SIS) is a structured approach used to evaluate the financial and operational effectiveness of various maintenance strategies. This framework is vital for ensuring that maintenance activities not only enhance the safety and reliability of the SIS but also do so in a cost-effective manner. The goal is to find an optimal balance where the benefits of maintenance, in terms of safety and reliability, outweigh the associated costs.

In the first stage of this framework, all potential costs associated with the maintenance of the SIS are identified and quantified. These costs include direct expenses such as labor, spare parts, and tools, as well as indirect costs like downtime, potential production losses, and administrative expenses. For a comprehensive analysis, long-term costs such as the impact of maintenance on the lifecycle of the SIS components, and the cost of potential safety incidents due to system failures, should also be considered. It's important to note that the cost calculation should consider not just the immediate expenses but also the long-term financial implications.

Once the costs are clearly understood, the next step is to assess the benefits of various maintenance strategies. These benefits are often less tangible and more challenging to quantify but are crucial for a balanced analysis. Benefits include increased system reliability and availability, reduced likelihood of unplanned downtime, improved safety and compliance with regulatory standards, and the prevention of costly accidents or safety incidents. In some cases, optimized maintenance can also lead to improvements in operational efficiency and energy savings.

The final stage involves comparing these costs and benefits to determine the net value or return on investment (ROI) of each maintenance strategy. This comparison helps in making informed decisions about which strategy provides the best balance of cost, safety, and operational efficiency. It is essential to adopt a long-term perspective, as some benefits, particularly those related to improved safety and reduced risk of catastrophic failures, may result over time. The chosen strategy should align with the organization's overall safety objectives, risk tolerance, and financial constraints. By applying this framework, organizations can ensure that their SIS maintenance practices are not only effective in maintaining safety and reliability but also in optimizing financial performance.

II.5.2. Long-term financial implications of preventive maintenance optimization

The long-term financial implications of optimizing preventive maintenance for Safety Instrumented Systems (SIS) are significant and multifaceted. Preventive maintenance, by design, is a proactive approach, focusing on performing maintenance tasks at regular intervals regardless of whether a fault is apparent. When optimized effectively, this approach can have profound financial benefits for an organization.

Reduction in unscheduled downtime and associated costs: One of the most direct benefits of optimized preventive maintenance is the reduction in unscheduled downtime. SIS are critical for the safe operation of many industrial processes, and their failure can lead to unplanned shutdowns, which are often costly. By regularly maintaining these systems, the likelihood of unexpected failures is significantly reduced. This proactive approach helps in avoiding the high costs associated with emergency repairs, including expedited shipping for parts, overtime labor, and, the most important, loss of production. Over the long term, consistent preventive maintenance can lead to more predictable and stable operational costs.

Extension of equipment life and capital cost savings: Regular maintenance keeps equipment in optimal condition, which can prolong its operational life. This means that the capital investment in SIS can be amortized over a longer period, delaying the need for costly replacements or upgrades. In the long run, this can result in substantial capital cost savings. By extending the life of the equipment, organizations can get more value out of their initial investment, reducing the overall total cost of ownership.

Improved safety and compliance, leading to indirect cost savings: An optimized preventive maintenance plan not only maintains the functionality of the SIS but also ensures compliance with safety standards and regulations. This compliance is crucial, as non-compliance can lead to hefty fines, legal liabilities, and reputational damage, all of which have significant financial implications. Moreover, a well-maintained SIS enhances overall safety, which can reduce the likelihood of accidents and incidents. The financial benefits here, though indirect, are substantial, as they include avoiding costs related to accidents, such as injury, claims, property damage, and potential litigation.

II.6. Conclusion

In conclusion, the chapter "Optimization of Preventive Maintenance for SIS Through Effective Testing Strategies" has thoroughly explored the relationship between preventive maintenance and testing strategies in the context of Safety Instrumented Systems (SIS). The chapter effectively demonstrates that the optimization of preventive maintenance, when integrated with well-planned testing strategies,

significantly enhances the reliability and safety of SIS. This optimization is not only crucial for the technical robustness of the systems but also for ensuring compliance with international standards and reducing the risk of unexpected failures.

The detailed analysis presented in this chapter highlights the importance of a systematic approach to preventive maintenance. By incorporating rigorous testing strategies into the maintenance schedule, the chapter showcases how potential faults can be identified and rectified in a timely manner, thereby preventing costly downtime and ensuring continuous safe operation. This approach underscores the necessity of understanding the specific requirements of SIS and tailoring maintenance activities to meet these needs. The integration of functional, performance, and safety tests within the preventive maintenance program is shown to be a key factor in maintaining the integrity and effectiveness of SIS.

Lastly, this chapter contributes significantly to the field of maintenance optimization for safety-critical systems. The insights gained from this study are invaluable for industry practitioners and researchers alike, providing a framework for enhancing SIS performance and reliability. The chapter not only adds to the existing body of knowledge but also paves the way for future research in this area, particularly in the development of more advanced testing techniques and tools. The optimization strategies discussed here are essential for organizations aiming to achieve the highest standards of safety while also managing operational costs effectively, thereby striking a balance between economic efficiency and uncompromised safety.

CHAPTER III

PROPOSED SPN MODEL FOR SIS PERFORMANCE AND COST OPTIMIZATION

This chapter proposes a sophisticated model using Stochastic Petri Nets (SPN) to assess and optimize the performance and cost-efficiency of Safety Instrumented Systems (SIS) during their operational phase. It elaborates on the integration of Stochastic Petri Nets with Monte Carlo simulations to analyze the dynamic and probabilistic behaviors of these systems, thereby enhancing their reliability and effectiveness in real-world scenarios. The chapter incorporates a series of innovative models, including SPN models for single component with partial imperfect and perfect proof testing, which simulate the real-time dynamics of component failures and the efficacy of testing protocols. Additionally, the chapter presents an SPN model for redundant components, addressing the challenges of common cause failures in systems with multiple backup components. A novel approach for Reliability-Based Spare Parts Optimization is introduced, optimizing procurement strategy to enhance system uptime and efficiency. The chapter also details the integration of sensors, logic solvers, and actuators into SPN models to accurately calculate the Probability of Failure on Demand (PFDavg) for system components. Moreover, specific SPN applications for PFD calculations of Safety Instrumented Functions (SIFs) are elaborated, showcasing how SPNs can track and improve the reliability of critical safety functions. These models collectively advance the understanding of SIS behavior under various conditions, providing a robust framework for enhancing reliability and safety through precise and targeted interventions.

The traditional approaches to safety system analysis, such as fault tree analysis and reliability block diagrams, provide static snapshots of system reliability and fail to capture the dynamic interactions within the system components and between the system and its environment. Moreover, the increasing complexity of modern industrial systems, coupled with their stringent safety requirements, calls for more sophisticated analysis techniques that can model system behavior over time and under varying operational conditions.

Stochastic Petri Nets (SPN) have emerged as a powerful tool for modeling and analyzing complex systems where concurrency, synchronicity, and stochasticity play crucial roles. Developed from the classic Petri Nets invented by Carl Adam Petri in the 1960s, SPNs add the capability to handle stochastic timing of events, making them particularly suitable for simulating and analyzing systems with random and concurrent events. The graphical nature of Petri Nets aids in visualizing complex process flows and interactions, while their mathematical foundation supports rigorous analysis and simulation.

The integration of SPN with Monte Carlo simulations represents a significant methodological advancement in the analysis of SIS. Monte Carlo methods are known for their power in handling random variables and stochastic processes, providing a means to simulate thousands of scenarios based on probability distributions. By combining SPN with Monte Carlo simulations, this research leverages the strengths of both methods: SPN for structural and behavioral modeling, and Monte Carlo simulations for the probabilistic analysis of these behaviors over numerous simulated runs.

This chapter details several innovative SPN models tailored for specific components and functions within an SIS:

1. **SPN Models for Single Component with Imperfect and Perfect Proof Testing:** These models simulate the effects of both perfect and imperfect testing on component reliability, addressing the practical challenges of test imperfections that can lead to undetected failures.
2. **Redundant Components Model:** This model focuses on systems with multiple backup components and explores the impact of common cause failures—a critical aspect in systems where redundancy is supposed to enhance reliability but can also introduce new failure modes.
3. **Reliability-Based Spare Parts Optimization:** This novel approach uses SPN to manage and optimize spare parts expenses, directly linking inventory levels to system reliability and operational downtime, thus driving cost efficiency alongside reliability.

The models developed and discussed herein are expected to make substantial contributions to the field of safety engineering, particularly through their ability to enhance the understanding of complex dynamic and stochastic system behaviors. This research not only provides a more nuanced understanding of the probabilistic nature of failures and their detection but also facilitates more informed decision-making regarding the design, operation, and maintenance of SIS.

Furthermore, these advancements are anticipated to help in the development of guidelines and standards for the design and operation of safety systems, reflecting a deep integration of theoretical modeling with practical operational needs. Ultimately, the adoption of these models could lead to significant improvements in the safety and cost-efficiency of industrial operations, potentially setting new benchmarks in safety system performance and reliability.

As industries continue to evolve and as their operational complexities grow, so does the need for innovative safety analysis techniques. This chapter's exploration into SPN and Monte Carlo simulations reflects a timely response to these challenges, promising not only to enhance the safety and efficiency of SIS but also to provide a robust framework for future research and application in safety system analysis and optimization. This comprehensive approach ensures that safety systems are not only designed to meet current safety standards but are also adaptable to future changes in technology and industry practices.

III.1. Analyzing SIS performance during operational phase

SIS performance analysis in operational phase involves a comprehensive evaluation of how Safety Instrumented Systems (SIS) function in real-world conditions once they are fully operational. The performance analysis is crucial for ensuring that the SIS meets its designed safety objectives and operates within established parameters. It encompasses monitoring system responses to real conditions, assessing reliability and effectiveness in detecting and mitigating risks, and ensuring compliance with safety regulations. Additionally, this phase includes the examination of maintenance records, incident reports, and system modifications to identify trends or recurring issues. The insights gained from the performance analysis are invaluable for continuous improvement, helping to identify areas for enhancement in both the system and maintenance protocols, thereby ensuring the ongoing safety and efficiency of the operational environment.

III.1.1. Stochastic Petri nets and Monte Carlo simulation approach

According to [26], and as referenced in the standards [1] and [4], the combination of Monte Carlo simulation techniques and Petri net modeling is recognized as a highly effective approach for assessing the performance of Safety Instrumented Systems (SIS). This integrative method is crucial because it capitalizes on the strengths of both Monte Carlo simulations and Stochastic Petri Nets (SPN) to address the complexities inherent in industrial systems.

Stochastic Petri Nets are particularly adept at modeling the behavior of systems. They offer a structured way to represent concurrent, asynchronous, distributed, parallel, nondeterministic, and stochastic system behavior. This makes them ideal for mapping out the intricate and varied operations of SIS, which often include a range of conditional and concurrent processes. On the other hand, Monte Carlo simulations excel in handling random variables, which are a core aspect of industrial systems. This includes simulating occurrences like equipment failures and repair times, which are inherently random and crucial to understanding SIS performance.

The integration of these two methodologies provides a powerful tool for system analysis. It allows for the simulation of complex, large-scale industrial systems, including those not amenable to Markov process-based modeling. This synergy is particularly pertinent given the advancements in computational capabilities. With the evolution from mere dozens of FLOPS to capabilities reaching giga, tera, and even peta FLOPS, Monte Carlo simulations have become increasingly feasible and essential for accurate system analysis. This enhanced computational power enables the handling of the vast number of calculations required for Monte Carlo simulations, making it an indispensable tool in the realm of SIS performance assessment. Consequently, this combined approach not only offers a more nuanced understanding of SIS behavior but also supporting informed decision-making, leading to improved safety and efficiency in industrial operations.

III.1.1.1. Stochastic Petri nets modeling approach

Carl Adam Petri's development of Petri Nets (PNs) in the 1960s marked a significant advancement in the field of reliability engineering, particularly for analyzing real-system performance. As detailed by [26], Petri Nets provide a framework for building finite state automations that closely replicate the behavior of the system under study. This method has evolved to be an invaluable tool in modeling and understanding complex system dynamics.

A Stochastic Petri Net (SPN), a variant of the traditional Petri Net, is composed of three key parts: static, dynamic, and scheduling components, each playing a crucial role in the system's representation.

1. **Static Part:** This includes the fundamental elements of the Petri Net.
   - **Places:** Represented as circles, places denote potential states within the system.
   - **Transitions:** Shown as rectangles, these symbolize possible events or changes in the system.
   - **Arcs:** These connect places and transitions, illustrating the flow within the net. Upstream arrows validate the transitions, and downstream arrows indicate the consequences of transitions being fired.
2. **Dynamic Part:** This illustrates how the system evolves over time.
   - **Tokens:** Small black circles that move between places. These tokens represent resources or entities within the system. Their distribution across places (known as Petri net marking) indicates the current state of the system.
3. **Scheduling Part:** It involves the timing aspects of the system.
   - **Stochastic Delays:** Represent random delays before events occur.
   - **Deterministic Delays:** Signify known, fixed time intervals before events take place.

The operational rules of a Petri Net are quite straightforward but critical for its functioning. A transition is considered valid (i.e., it can occur) if all its upstream places contain the requisite number of tokens as defined by the weights of the upstream arcs, and all associated conditions or predicates are true. When these conditions are met and the required time has elapsed (activation duration), the transition is activated and then fired.

The process of firing a transition is what dynamically changes the state of the system. Duringthis process:

- Tokens are removed from upstream places, in quantities matching the weights of the upstream arcs.
- Tokens are added to downstream places, according to the weights of the downstream arcs.
- Assertions or conditions within the system are updated to reflect these changes.

This dynamic nature of SPNs, as mentioned by [27], allows them to effectively model complex systems, capturing both their state and the stochastic nature of events and processes within them. This makes

SPNs particularly useful in reliability engineering, where understanding the probabilistic behavior of systems is essential.

III.1.1.2. Monte Carlo simulation approach

Simulating dynamical systems using Stochastic Petri Nets (SPNs) demands a method that can accurately capture the system's probabilistic behavior. Monte Carlo simulation stands out as the most effective approach in this context. This method relies on generating a large number of histories, which are essentially individual instances of the system's operation under different conditions. By observing the outcomes of these numerous histories, we can simulate the overall behavior of the system.

The reason Monte Carlo simulation is so powerful is that it allows for the application of classical statistics to the results. This statistical analysis can compute relevant probabilistic parameters with high precision. For instance, parameters like reliability and availability of the system can be more accurately predicted using this method, as noted by [26]. This precision in prediction is crucial for understanding and optimizing the performance of dynamical systems represented by SPNs.

For any given parameter X that we wish to simulate, basic statistical methods are applied to the collected data (represented as a sample Xi). These methods include calculating the mean, variance, and the confidence interval of Xi. Such calculations are especially important when dealing with a large number of simulations, which can pose challenges in terms of calculation accuracy.

The basic statistics used for this purpose include:

- Mean: The average value of the sample Xi, which provides a central tendency of the simulated data.

$$\bar{x} = \sum_i^n x_i \Big/ n \tag{13}$$

- Variance: This measures the spread of the sample data around the mean, offering insight into the variability within the simulated outcomes.

$$\sigma^2 = \sum_i^n (x_i - \bar{x})^2 \Big/ n \tag{14}$$

- Confidence Interval: This is a range within which the true value of the parameter is likely to fall, with a certain level of confidence (e.g., 90% confidence level corresponds to E=1.6449).

$$CI = \left[x - E.\left(\sigma / \sqrt{n} \right).\bar{x} + E.\left(\sigma / \sqrt{n} \right) \right] \tag{15}$$

These statistical measures are invaluable in understanding the behavior and reliability of the simulated system. They provide a quantitative basis for evaluating the performance of the system under various conditions, thereby facilitating more informed decisions in the design and analysis of such dynamical systems.

III.2. Methodology Proposed for Assessing the Performance of Safety Instrumented Systems (SIS)

A Safety Instrumented System (SIS) is a critical component in many industries, designed to provide necessary safety functions to prevent or mitigate hazardous events. The behavior and performance of an SIS can be complex, often involving interactions between various components and reactions to different operational scenarios. To accurately model and analyze this complexity, Stochastic Petri Nets (SPNs) are proposed [28].

III.2.1. SPN models for single component with imperfect and perfect proof testing

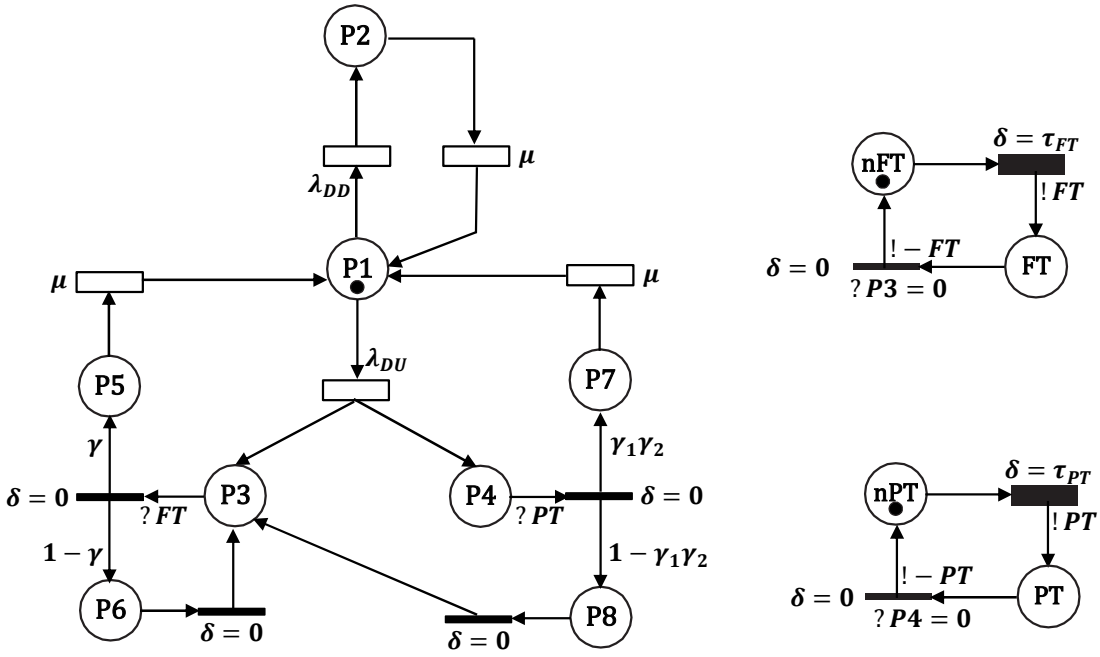


Figure III.1: SPN for single component with full and partial imperfect proof testing

Figure III.1 presents the Petri net (PN) model for a single component subjected to both full and partial imperfect testing, which captures the transitions between various operational states of the component. The model identifies several key states :

1. **Working (Good Operating State)**: Represented by the component being operational with a token placed in P1, indicating normal functionality without any detected issues.
2. **Dangerously Failed Detected (DD)**: In this state, failures are detected and identified, necessitating repairs. The component in this state has tokens in places P2, P5, and P7, indicating that the system has recognized the failure and is waiting for corrective action.
3. **Dangerously Failed Undetected (DU)**: This state occurs in two scenarios—
    - Places P3 and P4 represent failures that have occurred but remain undetected due to inherent limitations in the detection mechanisms.
    - Places P6 and P8 indicate failures undetected due to the imperfections in both full and partial testing procedures, showcasing a critical risk where failures go unnoticed possibly affecting the overall system performance.

The transitions between these states are influenced by the component's performance and the effectiveness of the testing protocols employed. The model underscores the impact of imperfect testing in failing to detect certain types of failures, which can have serious operational implications. This diagram serves as a tool to analyze the reliability and risk factors associated with the component in a dynamic operating environment.

If a dangerously detected failure (DD) occurs in the system, the token currently in place P1, representing the component in a working state, transitions to place P2. This transition occurs over a period defined by the failure rate λ_{DD}, quantifying the likelihood of moving to a failure state per unit time. Once the failure is detected and repairs commence, the token is moved back to place P1, symbolizing a return to the operational state. The duration of this repair process is determined by the repair rate μ_{DD} = 1/MTTR, where MTTR (Mean Time To Repair) represents the average time required to repair the component.

In the scenario of a dangerously undetected failure (DU), the token in place P1 is shifted to places P3 and P4, reflecting a state where the component has failed but the failure has not been detected. The transition to these places is governed by the failure rate λ_{DU}, which measures the frequency of undetected failures occurring per unit time. The token's movement to multiple places illustrates the

potential ambiguity and complications in diagnosing and addressing undetected failures within the system.

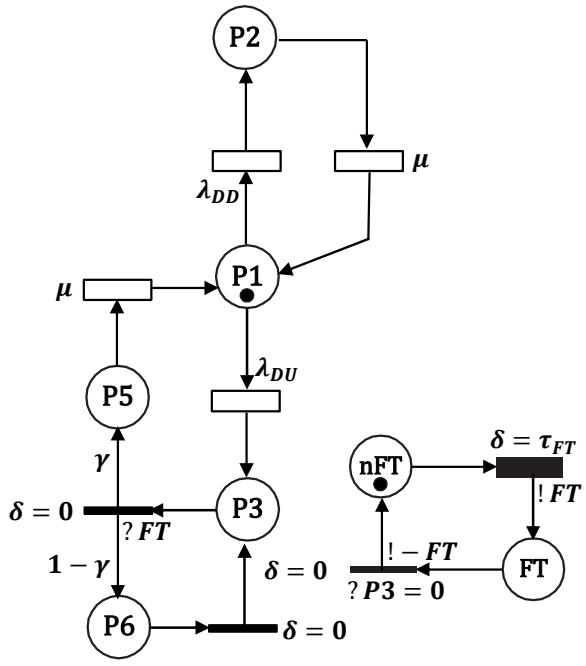


Figure III.2: Proposed SPN model for single component with full imperfect proof testing

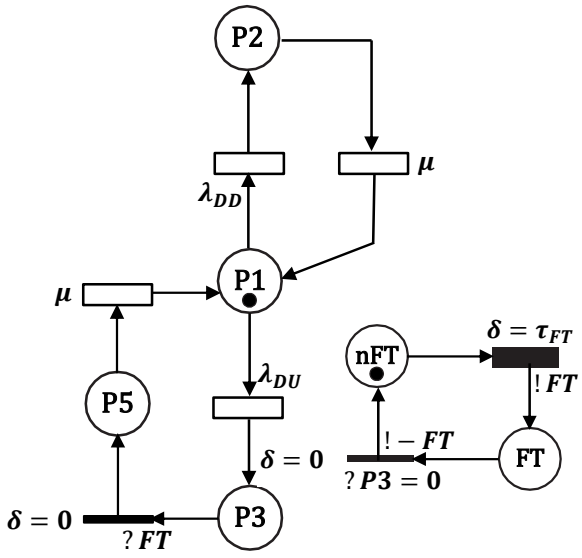


Figure III.3: Proposed SPN model for single component with full perfect proof testing

When a component undergoes a full perfect test, the assignment **!FT** (which signifies **!full_test = true**) and the guard condition **?FT** (equivalent to ?**full_test = true**) play pivotal roles. Specifically, a token initially located at **nFT** (representing no Full Test) is transitioned to the **FT** (Fully Tested) state during the full test interval, denoted by $\delta = \boldsymbol{\tau}$FT. Concurrently, if a token is present at P3, indicating a "dangerously failed undetected (DU)" state, it is moved to P5, which represents a "dangerously failed detected (DD)" state, where it awaits repair.

Subsequently, the token transitions back to P1 (the working state) during the designated repair period, represented by μ_{DD_F}. However, this repair process can only commence if the failure is successfully detected within the duration of the full perfect test, again indicated by $\delta = \boldsymbol{\tau}$FT. This mechanism ensures that the component only returns to a functional state after undergoing both detection and successful repair of any detected failures.

Otherwise,If the assignment !–FT (equivalent to full_test=false) is met and the guard ?P3=0, indicating that there are no tokens in place P3, the system then redirects the token from the full test place (FT) back to the non-full test place (nFT). This transition initiates a new period for conducting a full test, resetting the testing process to ensure continuous monitoring and evaluation of the component's status. This mechanism is designed to cycle through testing phases efficiently, maintaining rigorous scrutiny over the component's operational integrity.

When the component undergoes a full imperfect test, the likelihood of detecting failures is incorporated as a test coverage factor, denoted by the probability γ. This factor represents the probability that the full test successfully detects failures. Conversely, with a probability of $(1-\gamma)$, the test may fail to detect existing failures. These undetected failures could potentially be identified in a subsequent full test, reflecting the inherent imperfectness of the testing process.

In the model's dynamics, if a failure is not detected during the initial test, the token representing the component's state is moved from place P3 to place P6, indicating the presence of an undetected failure. If the failure remains undetected in subsequent testing, the token may cycle back to place P3. This cycle between places P3 and P6 illustrates the potential for repeated failure detection attempts due to the imperfect nature of the full test.

The Petri net (PN) model for the full proof test is designed to encapsulate the system's testing process through two distinct states. Initially, the system resides in the "no full test" (nFT) state, representing the

condition before any full proof test is carried out. This state serves as the starting point in the testing cycle, indicating that the system has yet to undergo rigorous evaluation. Upon completion of the full proof test, if the system meets the established criteria and passes the test, it moves to the "full tested" (FT) state. This transition reflects the successful verification of the system's operational integrity and compliance with safety or performance standards, confirming its readiness for continued or enhanced operational duties.

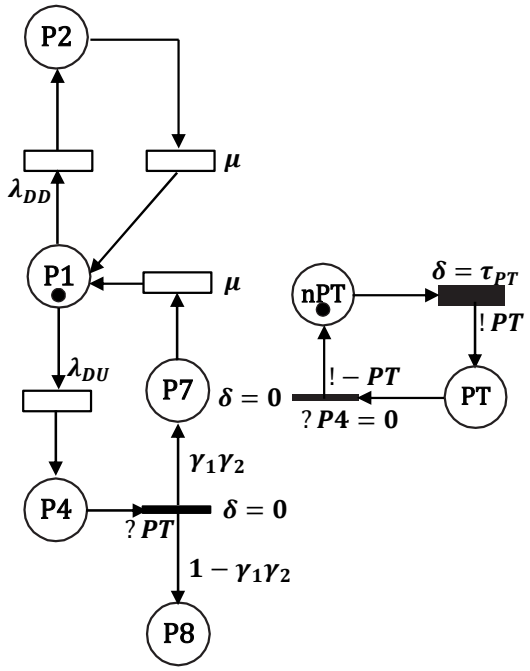


Figure III.4: Proposed SPN model for single component with partial imperfect proof testing

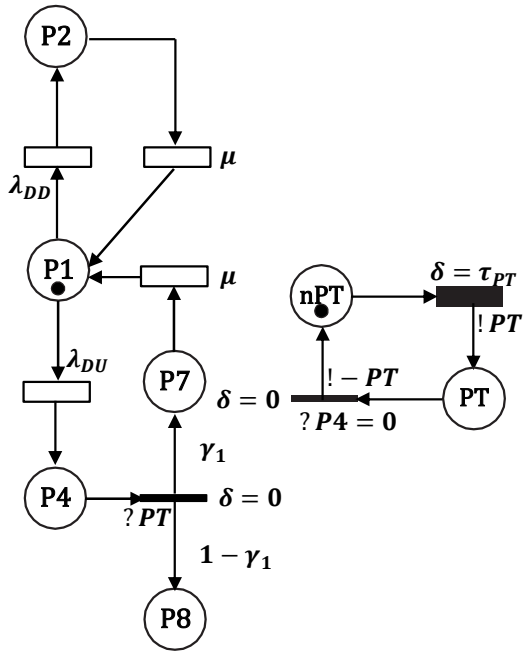


Figure III.5: Proposed SPN model for single component with partial perfect proof testing

When the component undergoes a partial perfect test, the assignments **!PT** (indicating **!partial_test=true**) and the guard **?PT** (equivalent to **?partial_test=true**) play critical roles in the model's dynamics, respectively mean that the token initially at **nPT** (No Partial Test) is moved to place **PT** (Partial Tested) over the duration of the partial test interval, denoted as δ = **τ**PT, and the token initially placed at P4 (indicating a "dangerously failed undetected" (DU) state) is moved to P7 (representing a "dangerous detected (DD) failure", awaiting repair). This transition occurs with a probability γ1, which serves as the coverage factor for the partial proof test, reflecting the likelihood that the test will detect the failure.

After detection, the token is then moved back to P1 during the repair process, which is quantified by the repair rate μ_{DD_P}. This return to the operational state (P1) signifies the completion of the repair cycle. Importantly, this repair process is contingent upon the detection of the failure during the partial perfect test interval (δ = **τ**PT), highlighting the interdependence of detection and subsequent repair actions in maintaining the system's reliability and safety.

Otherwise, If the assignment **!–PT** (equivalent to **partial_test = false**) is met and the guard condition **?P4=0** is satisfied, indicating that there are no tokens in place P4, the system triggers a transition. In this case, the token is transferred from place PT back to place nPT. This transition effectively resets the state,

initiating a new period for partial testing. This mechanism ensures that the component undergoes repeated partial testing until the conditions for moving to a different state are fulfilled.

When the component undergoes a partial imperfect test, the test's effectiveness is quantified by a coverage factor, represented as a probability γ2 of detecting failures. This setup allows for the partial test to successfully detect failures with a probability of γ1γ2. Conversely, it fails to detect failures with a probability of 1-γ1γ2. Failures undetected by the partial test might be identified during a subsequent full test, reflecting the inherent imperfection of the testing process. In this scenario, tokens may be transferred from place P4 to P8 and subsequently returned to P3.

Furthermore, these partial tests, characterized by their imperfect detection capabilities, are conducted at regular intervals. Here, γ1 represents the coverage of the partial proof test, while γ2 indicates the extent to which this partial proof test is imperfect. This model underscores the dynamic and probabilistic nature of the testing process, as it attempts to manage and mitigate the risks of undetected failures within the system.

The Petri net (PN) model for the partial proof test is comprised of two distinct states that delineate the system's progression through the testing process. The initial state, labeled as "no partial test" (nPT), represents the system before the commencement of the partial proof test. This state captures the baseline condition of the system, prior to any intervention. Upon successful completion of the partial proof test, the system transitions to the second state, known as "partial tested" (PT). This state indicates that the system has undergone and passed the partial proof test, reflecting its compliance with specific operational standards or safety requirements. This model effectively outlines the transformation of the system's status from untested to verified through the partial testing procedure.

III.2.2. SPN models for redundant components with full and partial imperfect proof testing

Figure III.6presents a Petri net (PN) model designed to capture the dynamics of common cause failures (CCF) in redundant components. This model encompasses four distinct states to simulate the transition of components under the influence of CCF. Initially, the system is in a stable state without any CCF, as represented by a token in place P9. Upon the occurrence of a CCF, the model shifts to more critical states based on the nature and detection of the failure.

The subsequent states include:

- "Dangerous undetected (DU) failure" located in place P11, which represents a failure that has occurred but has not been detected by the system's monitoring processes.
- "Dangerous detected (DD) failures" depicted in place P10, indicating failures that are recognized by the system. Components in this state are queued for repair, represented by place P12.

Once repairs are completed, or if the undetected failure becomes apparent and is subsequently addressed, the component transitions back to the original state of no CCF (P9). This model allows for a detailed analysis of how components under common cause failures move between detection, repair, and stable states, providing insights into the reliability and maintenance needs of systems with redundant components.

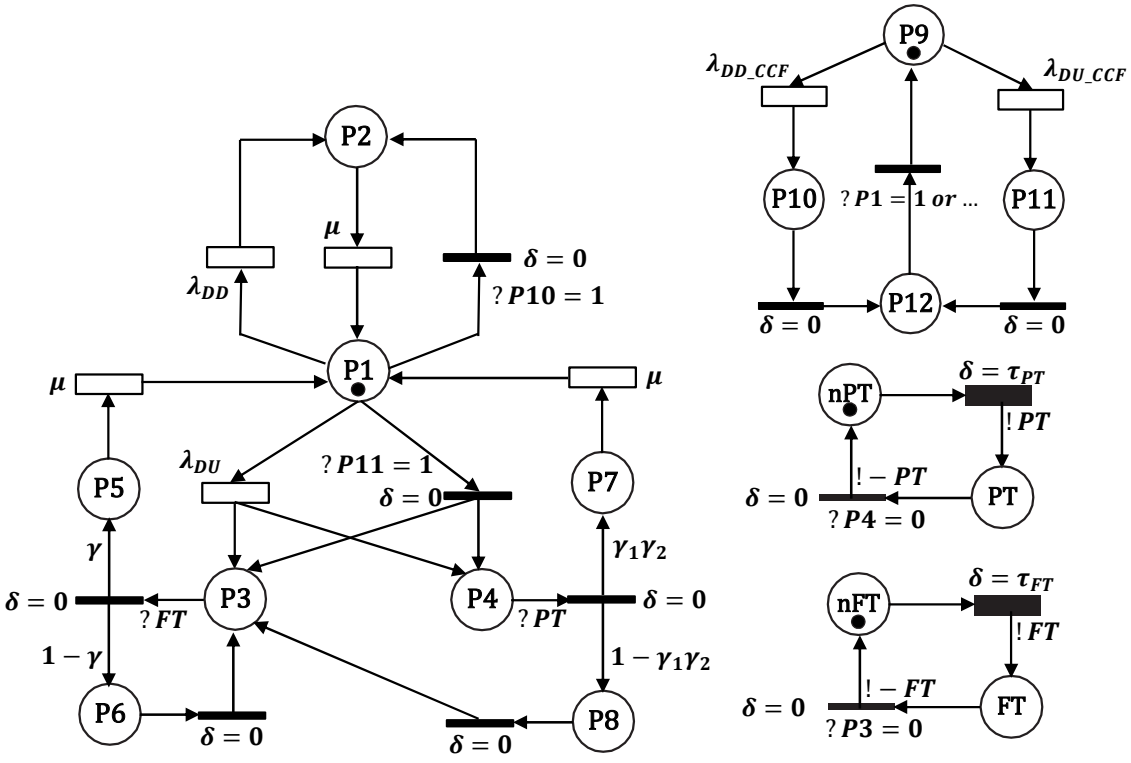


Figure III.6: Proposed SPN model for redundant components with full and partial imperfect proof testing

III.2.3. SPN model for reliability-based spare parts optimization

Figure III.7introduces an enhancement to the proposed Petri net (PN) model with the addition of a designated place for managing the spare parts inventory, labeled as "SP." This modification aims to optimize the inventory of spare parts essential for system repairs. The SP place functions as a strategic repository, enabling effective monitoring and allocation of spare parts. This is crucial for maintaining system uptime and ensuring timely repairs. By integrating this inventory management feature into the PN model, the system's overall efficiency in handling repairs and minimizing downtime due to spare parts shortages is significantly improved.

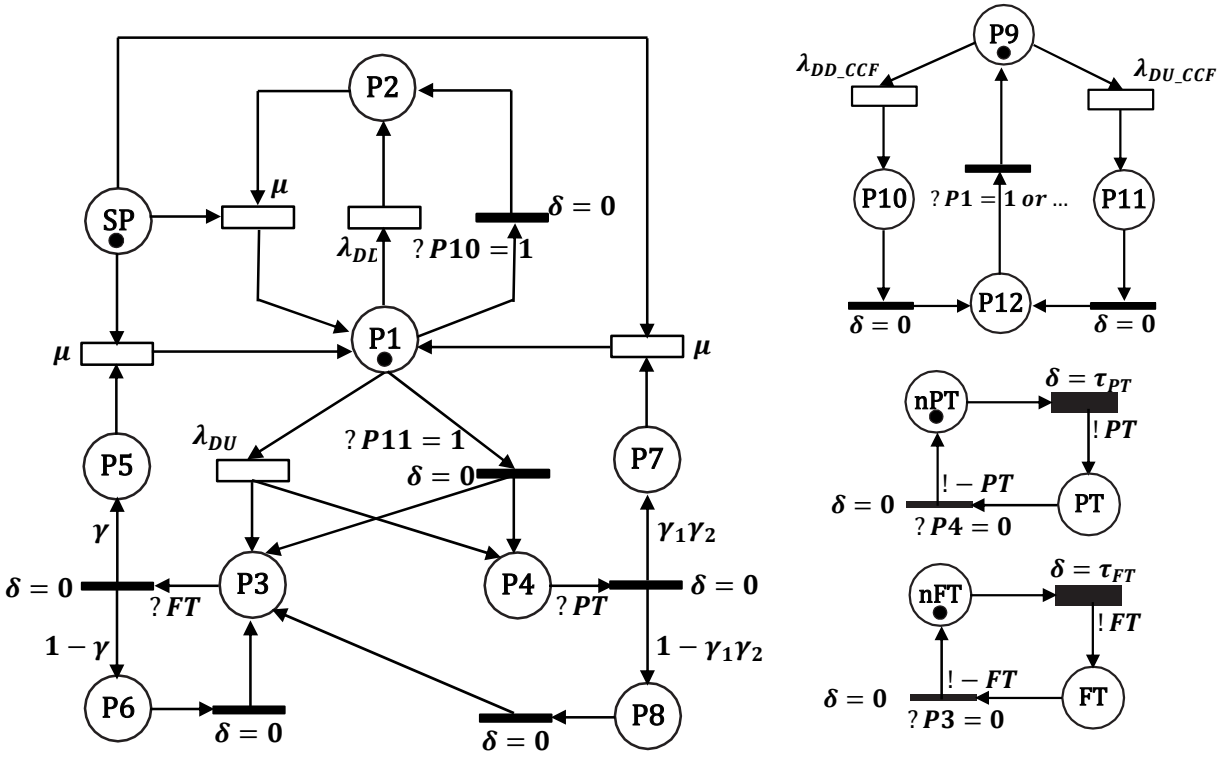


Figure III.7: Proposed SPN model for reliability-based spare parts optimization

III.2.4. SPN models to calculate the Probability of Failure on Demand (PFDavg)

The Probability of Failure on Demand (PFDavg) quantifies the reliability of a system and is derived from the mean marking of the "working" state in a Petri net model. Specifically, PFDavg is defined as the ratio of the total time that a system operates in the "working" state (indicated by the presence of a token in the corresponding place) to the overall operational duration, represented by TT. This metric is essential

for assessing the likelihood that the system will fail to perform its intended function upon demand. It provides a crucial indicator of the system's operational safety and efficiency, particularly in scenarios where reliability is critical.

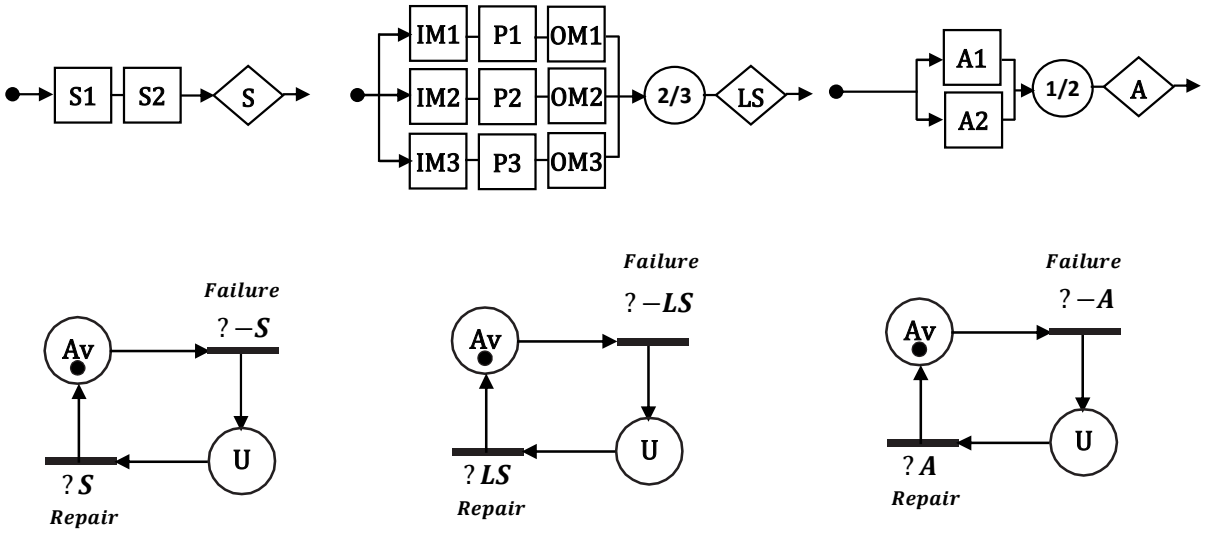


Figure III.8: Use of sensors, logic solver and actuator reliability block diagrams to build SPN for PFD calculations

Figure III.8 presents a Stochastic Petri net (SPN) model designed to represent the key components of a safety instrumented system, which includes sensors (S), logic solvers (LS), and actuators (A). This model extends to accommodate common cause failures (CCFs) in instances of component redundancy, enhancing the fidelity of the simulation in reflecting potential real-world operational issues.

The modeling challenge primarily relieson effectively mapping the components according to the logic prescribed by the reliability block diagram. This diagram details the layout and interconnections of the components, serving as a critical reference for constructing an accurate model. By adhering to this blueprint, the SPN can replicate the operational logic and interdependencies of the system components.

Once the system is accurately modeled, the average Probability of Failure on Demand (PFDavg) can be calculated. This is done by determining the mean marking of a specifically designated place within the Petri net model, which correlates to the system's reliability at that point. Through this approach, the Petri net model becomes an invaluable tool for in-depth analysis of system reliability and safety, offering quantifiable insights into the system’s performance under various conditions. This capability is particularly important for ensuring the integrity and operational safety of complex systems where reliability is paramount.

Utilizing messages labeled Ci significantly facilitates the interconnection of components, allowing for the construction of detailed and structured assertions. These messages serve as communication links, ensuring seamless integration and interaction among different parts of the system. By employing Ci messages, developers can define clear and precise conditions or rules that govern the behavior and responses of the system under various operational scenarios. This method not only enhances the clarity and efficiency of the system architecture but also aids in maintaining consistency and reliability throughout the network of components. Thus, the use of Ci messages plays a pivotal role in building robust and adaptable frameworks necessary for complex systems management and operation.

Based on the established framework, the following detailed assertions can be formulated to guide our analysis and understanding of the system's dynamics:

$$S = S1.S2 \tag{16}$$

$$\begin{aligned} LS = &\left(IM1.P1.OM1\right).\left(IM2.P2.OM2\right) + \left(IM1.P1.OM1\right).\left(IM3.P3.OM3\right) \\ &+ \left(IM2.P2.OM2\right).\left(IM3.P3.OM3\right) \end{aligned} \tag{17}$$

$$A = A1 + A2 \tag{18}$$

Figure III.9 depicts a sub-Petri net that models the operational states of a Safety Instrumented Function (SIF). The SIF is deemed to be functioning properly and is considered available (Av) if, and only if, all components—sensors, logic solver, and actuator—are in a true state, indicating that they are operating correctly. Conversely, if any of these components fail to meet their required conditions, the SIF becomes unavailable (U). This representation in the Petri net is used to explicitly track and visualize the availability status of the SIF, highlighting its dependency on the coordinated performance of its constituent components. The transitions between these states are critical for understanding the reliability and safety mechanisms within the system.

The calculation of the Probability of Failure on Demand (PFD) is a critical measure in safety systems, focusing primarily on the states of availability (Av) and unavailability (U). This analysis hinges on the functioning status of key system components: sensors, a logic solver, and actuators. The system is deemed unavailable when the combined state of these components is false, indicating a failure. Conversely, when the combined state becomes true, the system is restored to availability.

This transition between available and unavailable states is modeled to determine the PFD. The mean marking of Av, in this context, represents the average system availability. This is calculated as the

proportion of time the system remains in the available state over the observed period. Similarly, the mean marking of U denotes the system's average unavailability. It reflects the proportion of time the system remains in the unavailable state, effectively quantifying the system's PFD average.

This analysis provides a clear and quantitative understanding of system reliability and safety, crucial for optimizing and ensuring operational integrity.

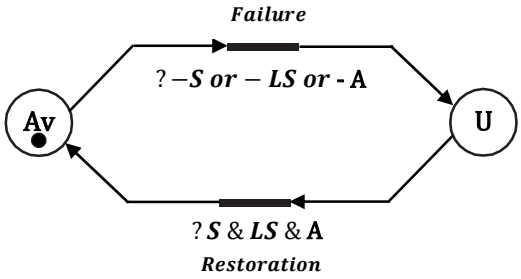


Figure III.9: Using Petri Net for PFD calculations of SIFs

III.3. Conclusion

In this chapter, we have explored the innovative integration of Stochastic Petri Nets (SPN) with Monte Carlo simulations to enhance the reliability and efficiency of Safety Instrumented Systems (SIS) during their operational phase. This approach not only facilitates a deeper understanding of dynamic and probabilistic system behaviors but also enhances decision-making processes for safety and performance improvements.

The deployment of SPN models for single component under both partial and full proof testing conditions has provided profound insights into the intricacies of system failure mechanisms and their detection. Moreover, the modeling of redundant components has addressed the critical challenges posed by common cause failures, crucial for systems relying on multiple backup components.

Further, the introduction of a Reliability-Based Spare Parts Optimization model represents a strategic advance in inventory management, optimizing the allocation of critical spare parts to enhance system uptime and reduce downtime costs.

The methodologies and models developed and discussed in this chapter contribute substantially to the field of system safety engineering. They offer robust frameworks for not only understanding but also significantly improving the reliability and operational safety of complex industrial systems. Through

continuous application and refinement, these models hold the potential to set new standards in the safety and efficiency of Safety Instrumented Systems, ensuring that they meet both current and future challenges in industrial safety management.

CHAPTER IV

CASE STUDY - EMERGENCY SHUTDOWN SYSTEMS (ESDs)

This chapter focuses on Emergency Shutdown Systems (ESD) which are crucial for risk management in industrial processes, particularly gas compression. It covers the emergency shutdown and depressurization philosophy through various safety levels, details the ESD components and architecture within the compression section, and explains how the activation of the ESD system are triggered by various emergency scenarios in order to protect personnel and equipment. The performance of ESDs is assessed using Petri Nets and Monte Carlo simulations, which analyze the impact of both full and partial tests on system integrity. This evaluation highlights the challenges of achieving perfect tests and suggests strategies for optimizing maintenance and associated spare parts costs through reliability analysis. Ultimately, the chapter underscores the importance of implementing effective maintenance strategies to maintain industrial operation integrity, reduce risks, minimize costs, and ensure compliance with international functional safety standards IEC 61508 and IEC 61511.

Process safety, functional safety, and safety instrumented systems (SISs) are interrelated concepts within the field of safety engineering. Process safety deals with risk management in complex industrial processes across all industry sectors, with its origins dating back to the 1960s when it was first established as a field of research and safety management in the oil and chemical industries [29]. Process safety encompasses measures and protocols designed to prevent, control, and mitigate incidents such as fires, explosions, and toxic gas releases that could result from the operation of industrial processes.

On the other hand, functional safety is specifically concerned with ensuring the reliability of safety instrumented systems over their lifecycle. It involves various stages such as process hazards analysis (PHA), developing safety requirements specifications (SRS), and implementing measures to achieve the required level of risk reduction. Functional safety standards, such as IEC 61508 and IEC 61511, provide comprehensive guidelines for achieving and maintaining a proper functional safety management system. These standards outline methodologies for assessing risks, determining safety integrity levels (SIL), and designing and implementing safety instrumented functions (SIFs) within SISs.

Safety instrumented systems (SIS) are fundamental in achieving risk reduction within the process industry. SISs comprise sensors, logic solvers, and final elements, and they are designed to detect hazardous process deviations and take appropriate actions to prevent these events or mitigate their consequences [30][31][32] [5] [4]. SISs operate independently of the process control systems and are capable of initiating a safe shutdown or initiating other necessary safety measures in response to predefined hazardous conditions. They are crucial components in maintaining process safety and preventing catastrophic incidents in industrial facilities.

Despite safety being a top priority in Algerian gas facilities, the ongoing task of optimizing the performance and maintenance costs of Safety Instrumented Systems (SISs) consistently presents a challengingconcern. The dynamic nature of these facilities, coupled with the intricate complexities inherent in process systems, underscores the critical need for a comprehensive analysis of the current state of SISs and the pinpointing of potential areas for improvement.

By tackling these challenges head-on, companies operating within the Algerian gas sector can significantly promote their process safety measures, control operational risks, and mitigate the financial strain associated with ongoing systems maintenance.

Proof tests are conducted to detect potential faults or failures of Safety Instrumented Systems (SIS) and repair them to ensure the proper functioning of the SIS. These tests are broadly categorized into two

types: full tests and partial tests. Each type presents its own set of advantages and disadvantages, and the choice between them necessitates careful consideration of various factors, including system reliability and cost-effectiveness. However, achieving a perfect proof test is often challenging. There may be cases where the system is not thoroughly tested or fails to perform as anticipated during the test. Consequently, the likelihood of the SIS failing to execute its safety function when required may increase. Hence, it becomes crucial to account for imperfections during SIS proof testing, especially when devising a test strategy during the operational phase [20] [21] [33][34].

In the field of optimizing Safety Instrumented Systems (SISs) performance and maintenance strategies, extensive researches have been carried out. This includes investigations into proof testing, adaptive testing policies, optimal maintenance intervals, diagnostic mechanisms, and modeling and analysis of SIS performance under imperfect testing.

For instance, [35]Developed an adaptive testing approach that adjusts to the condition of multi-state systems, specifically targeting safety-instrumented systems with degrading final elements. Their approach, employing a Markov model, aims to strike a balance between system performance and the number of tests required within the stipulated service duration. It seeks to reduce the number of proof tests needed without compromising safety integrity. Additionally, the study explores various methods and models for reliability analysis and optimization of safety-instrumented systems, underscoring the significance of proof testing and maintenance strategies for SIS.

[36]introduceda novel methodto ensure optimal safety and security barrier maintenance strategy in the chemical facilities. Their approach involves three key steps: scenario building and barrier identification, barrier modeling, and determination of optimal barrier maintenance intervals. Notably, the proposed approach incorporates both safety and security risk sources and accounts for correlations and dependencies between barriers.The study examines how barrier maintenance, correlations between barriers, and consequence assessment affect PFD calculations. Ultimately, the objective is to strike a balance between safety and economic considerations in decision-making processes related to the implementation and maintenance of safety and security barriers.

[37] emphasized the critical role of appropriate device selection and configuration within Safety Instrumented Systems (SIS) to achieve specific Safety Integrity Levels (SILs) while ensuring safety is not compromised for economic reasons. The study delved into the analysis of systematic errors' contribution to SIS failures within a gas refinery context. Furthermore, the authors presented a formula and practical guideline aimed at enhancing SIL performance while considering systematic failures.

[38] suggested the incorporation of periodic functional testing into the original Markov model for modeling safety instrumentation systems. Their research demonstrated that integrating periodic functional testing into the Markov model enhances its comprehensiveness and aligns it more closely with engineering realities. Additionally, the paper explored the FTA-BN method for safety integrity level grading and verification. It proposed the construction of Markov models that incorporate periodic functional tests and compared the Probability of Failure on Demand (PFDavg) for different redundancy structures, such as one out of one "1oo1", one out of two "1oo2", and two out of three "2oo3". The authors provided failure data and PFDavg calculations specifically for 2oo3 redundancy structures, offering valuable insights into system reliability and performance evaluation.

[39] presented a diagnostic mechanism designed to identify the underlying factors leading to Emergency Shutdown Valve (ESDV) failures, which are recognized as the major common reason for the unavailability of Emergency Shutdown Systems (ESDs). The diagnostic procedure outlined in the paper detailed the sequential steps involved and presented a case study to demonstrate the effectiveness of the approach. Furthermore, the study explored the application of a fuzzy rule-based diagnostic system specifically tailored to address failures within the ESDV subsystem of the Safety Instrumented System (SIS) deployed in gas treatment processes.

[40] Another study delved into the intricacies of designing and maintaining Safety Instrumented Systems (SISs) within the oil and gas industry, with a particular focus on remote and Arctic locations. The paper introduced a comprehensive decision-making framework that encompassed various aspects such as SIS design, maintenance planning, and employee scheduling. Notably, the framework integrated diverse redundancy measures and utilized Markov analysis to model the system's operational behavior accurately. Additionally, the study shed light on workforce planning challenges and employed multi-objective decision-making techniques to strike a balance between investments in system complexity, safety levels, and workforce-related expenditures.

[41] proposed a methodology for determining the optimal proactive maintenance interval (PMI) for instrument devices in oil and gas industries. They discussed various approaches for PMI determination, ranging from periodic visits to advanced programs like predictive and condition-based maintenance. Their approach involved devising a comprehensive and concise formula based on expected utility theory to derive the optimum PMI. These formulas are designed to determine the most cost-effective maintenance plan while ensuring acceptable levels of reliability, availability, and safety in oil and gas industries, addressing an optimal decision-making problem. Through practical implementation in a

typical gas refinery, the authors demonstrated a significant benefit of approximately 41% achieved within one year compared to the previous heuristic maintenance strategy employed over the same duration.

[42] proposed a framework for modeling and analyzing the performance of safety instrumented systems (SIS) under imperfect testing and maintenance strategies. The authors introduced analytical formulas for calculating performance indicators such as the probability of failure on demand (PFD) and the average PFD. This framework provides a valuable tool for evaluating the effectiveness of different maintenance strategies and optimizing the performance of safety instrumented systems in industrial settings.

[43] proposed an optimal maintenance strategy for safety-instrumented systems (SIS) by leveraging observed information during proof tests. They delved into the stochastic degradation process of SIS final elements and elucidated the challenges associated with SIS assessment and maintenance optimization. Moreover, the study calculated key metrics such as the instantaneous unavailability of SIS, PFDavg, and expected cumulative maintenance cost. The method presented in this study offers a valuable framework for optimizing SIS maintenance strategies to align with safety integrity level (SIL) requirements.

[44] introduced a Markov chain model aimed at assessing the unavailability of redundant safety instrumented systems under process demand conditions, encompassing both dangerous detected and undetected failures. The authors provided insights into the principles and mathematical modeling of safety instrumented systems (SIS) commonly utilized in process industries to avoid hazardous events or mitigate their consequences.

[45] proposed an approach to optimize the maintenance schedule of safety instrumented systems (SISs) to enhance their reliability. This method involved formulating the problem of determining optimal time points for maintenance tests as an optimal control problem, with the average probability of failure on demand (PFD) serving as the objective function. Furthermore, the approach could accommodate various types of maintenance tests and redundancy architectures. The study included illustrative examples to demonstrate the applicability and effectiveness of the proposed approach.

Furthermore, recent research [46] has proposed novel formulas for calculating the average probability of dangerous failure on demand (PFD avg) within safety-instrumented systems (SISs), considering both partial and full periodic tests. This approach is based on multi-phase Markov models, providing a comprehensive framework for assessing system reliability.

In a related study, [47] investigated the impact of various testing strategies on the safety performance of individual channels within safety-instrumented systems (SISs) following a detected dangerous (DD) failure. Their findings underscored the importance of testing methodologies in maintaining system integrity and minimizing potential risks.

Additionally, [48] conducted an analysis on the influence of imperfect proof tests on the probability of failure for safety instrumented functions (SIFs) within SISs. Their research emphasized the critical role of proof tests and proof test coverage in accurately evaluating the reliability of safety instrumented systems.

Moreover, another study [25] explored the effect of partial testing on the reliability of safety-instrumented systems (SISs) operating in a low-demand mode. This research effort resulted in the development of simplified formulas for calculating the probability of failure on demand (PFD avg) for SISs subjected to both proof testing and intermediate partial testing, providing valuable insights into system performance under various operational conditions.

Several articles have delved into the application of Stochastic Petri Nets (SPN) and related methodologies in reliability modeling for Safety Instrumented Systems (SISs). For instance, [49] introduced a comprehensive reliability modeling methodology specifically tailored for subsea SISs, which accounts for partial testing and delayed restoration. This methodology was effectively validated using SPN, showcasing its robustness and applicability in real-world scenarios.

Furthermore, [50] utilized Stochastic Petri Net with Predicates and Assertions (SPNPA) to model safety-instrumented systems with time-dependent failure rates. Their study demonstrated how incorporating SPNPA enhances the analysis capabilities of SISs, particularly in scenarios where failure rates vary over time.

In a related work, [51] discussed various challenges and techniques associated with utilizing Petri nets for reliability modeling. They highlighted the significance of graphical rules, modules, predicates, and assertions in making Petri nets more accessible and effective for reliability engineers. Their insights shed light on the practical implementation of Petri nets in reliability analysis.

Moreover, [52] emphasized the user-friendliness and intuitive nature of Stochastic Petri Nets (PN) for system safety analysis. Through a detailed case study, they illustrated how PN can be effectively employed to analyze real-world industrial systems, underscoring its practical utility and relevance in the field.

Furthermore, the study introduced and applied stochastic Petri nets (SPN) for reliability, availability, and safety integrity level (SIL) calculations in industrial systems [53]. It highlighted the effectiveness of SPN in handling complex systems and offered a qualitative advancement in the field. Additionally, another study introduced a stochastic Petri nets model to analyze the behavior of a pressure protection system, comparing it to a Fault Tree model [54]. The research demonstrated that the stochastic Petri nets model provided extended expression and computation power for accurate safety integrity level assessment.

This chapterexplores the power of Stochastic Petri Nets (SPNs) as a valuable modeling tool for evaluating Safety Instrumented Systems (SIS) in the gas processing industry. The utilization of the SPN approach offers a dynamic and adaptable method to analyze the effects of imperfect proof tests. Our study employs the application of Stochastic Petri Nets by not only building upon previous researches but also by demonstrating their effectivenessin addressing challenges related to imperfectness of proof tests for Safety Instrumented Systems.

A comprehensive case study is presented inthis chapter focusing on an existing gas processing facility. We developed and applied a Stochastic Petri Net (SPN) model to assess the influence of imperfect full and partial proof tests on the average Probability of Failure on Demand (PFDavg) related to different Safety Instrumented Functions (SIFs). This approach also aims to minimize spare parts expenses through reliability analysis leading to substantial cost reductions while ensuring that the necessary safety integrity levels (SILs) are maintained.

IV.1. Emergency Shutdown System (ESD)

Every hydrocarbon production process, whether extracting liquids or gases, carries inherent risks to personnel, the environment, and the equipment used. These risks require continuous monitoring and management to ensure the safety and integrity of the operations. Disturbances in process parameters such as temperature, pressure, and level, along with environmental factors like flames and smoke, can pose significant hazards. Consequently, it is essential to implement robust automated safety systems, including the Emergency Shutdown System (ESD), the Fire & Gas System (F&G), the Burner Management System (BMS), and the High Integrity Pressure Protection Systems (HIPPS), to protect and stabilize the process during unsafe conditions.

These systems are designed to respond to any anomalies that result in an immediate loss of control over the compression section’s operations, potentially causing harm to people or equipment damage. These anomalies necessitate swift and decisive corrective actions, primarily managed through the activation of the Emergency Shutdown System (ESD).

The ESD system is designed to detect any operational disturbances or hazardous conditions within the process. Upon detection of such conditions—whether due to fire or gas detection by the F&G system, critically low instrument air pressure, or significant drops in electrical supply voltage—the ESD system initiates a controlled, safe, and automatic emergency shutdown. This shutdown involves the depressurization of the plant, equipment, and machinery to safeguard personnel, the environment, and the infrastructure.

In the event of an emergency, installations are halted both automatically and manually. Automatic emergency shutdowns are facilitated by a lockout sequence triggered by signals from detecting instrument elements. Conversely, manual emergency shutdowns are executed by operators who identify incidents and act promptly to prevent their escalation, emphasizing the importance of effective communication between operators across different plant sections. Understanding the cause and origin of an emergency stop is critical for implementing measures that prevent potential secondary accidents.

IV.1.1. Emergency shutdown and depressurization philosophy (Safety levels)

The architecture of the emergency shutdown system is based on a tiered safety protocol consisting of three progressive safety levels:

- **Level 1 – ESD (Emergency Shut Down):** This level involves a total stop impacting the entire plant. It includes automations that halt the flow of products by stopping rotating machines (pumps, compressors, turbines, etc.) and closing isolation valves known as ESDVs. Triggered by a major incident, an ESD represents the highest level of safety, authorizing the depressurization of all or part of the installation. It ismanaged by a dedicatedsafety PLC (ESD0).
- **Level 2 – PSD (Process Shut Down):** This level affects the specific process involved. It consists of automations that detect process deviations, quickly stopping a process unit or part of installation, and isolating them using isolation valves called SDVs. Triggered by a serious, yet less critical incident than an ESD, a PSD may initiate depressurization of the isolated equipment (e.g., a compressor) but never results in a general plant depressurization. It ismanaged by a safety PLC (PSD1, PSD2).
- **Level 3 – USD (Unit Shut Down):** This level pertains to stopping a specific unit or isolated equipment. It involves functions that shut down a section or part of equipment without engaging safety elements (ESDV or SDV). USD stops are triggered by minor incidents and are typically managed to keep production running by starting backup equipment or utilizing temporary

solutions. USD stops are controlled by the centralized control system (DCS) and not by a safety PLC (PSD3).

The ESD system, the focus of this chapter, is responsible for handling emergency shutdowns and depressurizations as well as unit stops. It integrates safety logic, depressurization logic, and unit stop logic into common controllers, ensuring a comprehensive response to detected fire or gas events (inside or outside the premises) through digital outputs from the Fire and Gas (F&G) system wired into the ESD inputs.

IV.1.2. ESD System Description

The process control system (DCS) and the ESD system are two different and independent systems, designed to ensure maximum reliability and safety. The ESD system processes data from the site or other systems (DCS, F&G, packages) and executes programmed logics based on predefined safety standards.

The ESD system utilizes Triconex programmable safety PLCs, which are compliant with the international standards IEC 61508 and 61511 for functional safety. Thesesystems are characterized by theirrobustness and reliability:

- **General Characteristics of Triconex:** The triple architecture of TRICON enhances system availability and maintains the same level of safety during repairs with hot-swappable card changes and automatic configuration recognition. This architecture prevents unplanned unit shutdowns and contributes to safety by avoiding the initiation of transient sequences, which are more prone to malfunctions than a stable state.
- **Triple Architecture:**Triconex systems are fault-tolerant, majority-voting systems designed for critical automation and control applications in industries such as oil, chemical, energy, and rotating machinery. They are engineered to ensure continuous operation even in the event of component failure, transparently to the operator.

The ESD system employs advanced communication strategies to ensure reliable and continuous operation across different interfaces:

- **Triconex / DCS Communication**: The Triconex Programmable Logic Controller (PLC) is intricately connected to the Distributed Control System (DCS) through a communication card. This setup includes redundancy in the connections, which is crucial for maintaining the reliability and ensuring the uninterrupted operation of safety systems in critical scenarios.

- **Triconex / PC Tristation Communication**: Although not redundant, the Ethernet network connecting the PCs to the Triconex system is strategically configured to maximize communication reliability. This configuration is crucial for maintaining effective communication channels, facilitating timely updates and interventions, and ensuring that the Tristation PC can reliably access and manage system parameters even in demanding operational environments.

IV.2. Supervision System

The Supervision System of the Emergency Shutdown (ESD) encompasses various components designed to ensure seamless and efficient management of safety operations. Here's a detailed overview of each element within the system:

- **ESD Safety Panel**: Centrally located in the control room, this panel consolidates all emergency stop buttons, strategically providing operators with rapid access to critical emergency controls. This setup is essential for enabling quick responses in urgent situations, thereby enhancing the overall safety of the operations.
- **ESD Bypass Panel**: This panel assembles all the bypass selectors in a single location, facilitating flexible control over the system during periods of maintenance or non-emergency operations. The layout of this panel allows for easy adjustments to the system's operational parameters without compromising safety, offering operators the ability to fine-tune processes while ensuring that essential safety measures are readily accessible.
- **Operator and Engineer Stations**: The integration between the ESD and the Distributed Control System (DCS) is achieved through a robust communication bus. This setup utilizes the DCS's supervision consoles and printers, serving as the primary operator interface. This arrangement ensures that operational data and controls are relayed efficiently, maintaining high levels of system performance and safety. Additionally, the TRISTATION—dedicated to system maintenance and programming—is a pivotal component of the supervision system. Running on a PC platform with Windows XP, the TRISTATION is equipped with a suite of software tools designed for various tasks:
  - **Application Program Development**: Facilitates the creation and modification of custom safety applications tailored to specific operational needs.

- **Event Logging**: Captures and records significant system events, providing a detailed audit trail that is essential for troubleshooting and understanding the sequence of events leading up to any incidents.
- **Sequence of Events Analysis**: Offers analytical capabilities that help decipher the sequence and timing of events, crucial for diagnosing system issues and improving future responses.
- **DDE Server**: Enhances data exchange and operational oversight, allowing for real-time data communication and integration with other systems.

This comprehensive approach to system supervision ensures not only the operational integrity of the ESD but also enhances its maintainability, reliability, and adaptability to changing operational demands.

IV.3. Description of the Emergency Shutdown of the Compression Section

The Algerian Edjeleh field's Flared Gases Recovery unit (AEGR), inaugurated in March 2005, serves a multifaceted purpose. Its primary objective is to recover, compress, dehydrate, and transport gases that were conventionally flared from the field's ten (10) oil separation units. This recovered gas plays a crucial role in gas-lift injections, facilitating the activation of existing oil wells to either enhance oil production or sustain a consistent flow rate. Additionally, AEGR significantly contributes to mitigating air pollution by curbing gas emissions, aligning with the stipulations of the Global Gas Flaring Reduction Initiative [55].

The installed Emergency Shutdown Systems (ESDs) within the compression section of The Flared Gases Recovery unit represent a critical component of Safety Instrumented Systems (SIS). These systems are mainly designed to address hazardous situations effectively by bringing the process into a controlled and safe state, thus safeguarding personnel, equipment, and the environment.

The ESDs contain various elements, starting with input devices situated in the field, including sensors like transmitters and detectors. These sensors continuously monitor essential physicochemical parameters such as temperature, pressure, and level. Upon detecting deviations beyond predetermined thresholds in any of these parameters, they generate demand signals, which serve as indications of potential unsafe conditions.

These demand signals are then transmitted to the logic unit, which serves as the central controller. Specifically, the logic unit, often in the form of a programmable controller such as the Triconex Trident, interprets the incoming signals and executes predefined cause-and-effect algorithms. Based on these

algorithms, the logic unit activates specific outputs, initiating the necessary actions to mitigate the identified risks and restore the system to a safe state.

Basically, the integration of input elements, logic units, and output actions forms a robust framework for proactive emergency response and risk mitigation within the compression section of The Flared Gases Recovery unit. This systematic approach ensures a rapid and efficient response to potential hazards, minimizing the impact of emergencies and ensuring the continued safety and integrity of the operation.

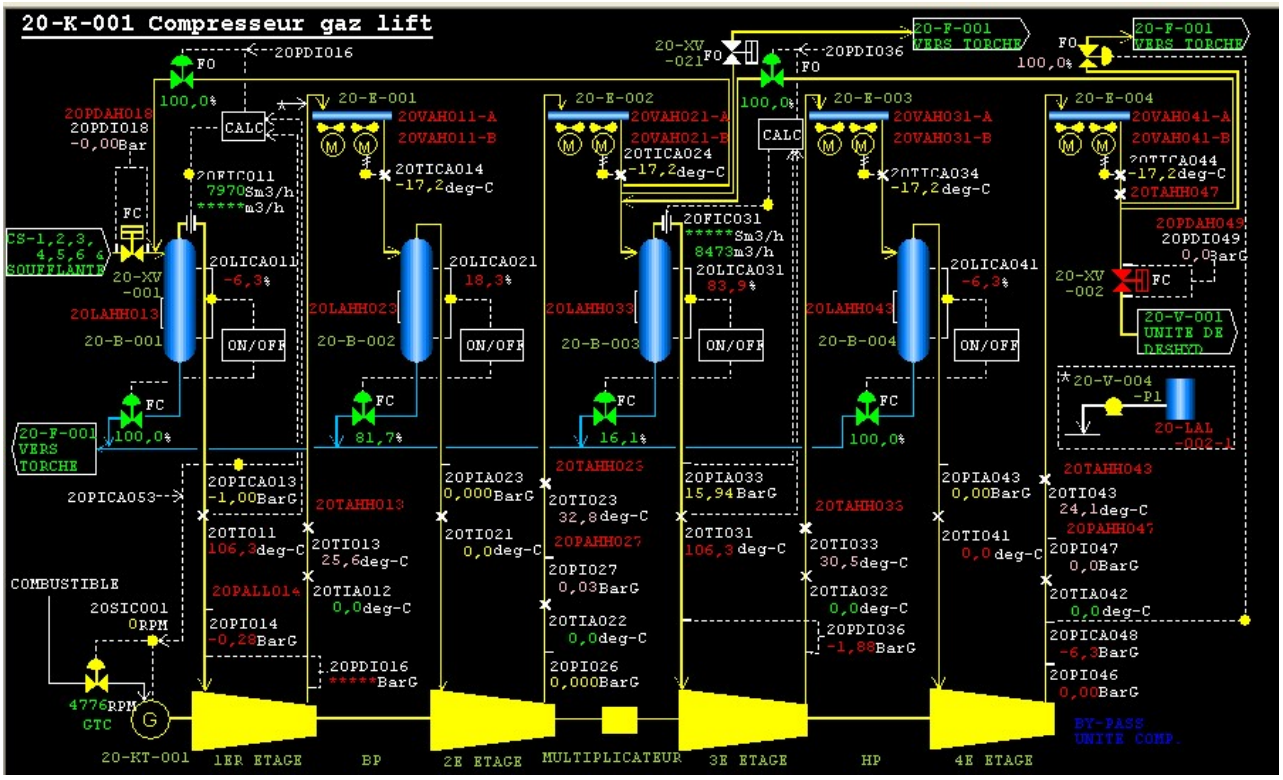


Figure IV.1: synoptic scheme of recovery unit (Compression section)

IV.3.1. ESD System Components for the Compression Section

The logical unit architecture is grounded on Triple-Modular Redundant (TMR) redundancy, wherein three identical, parallel, and isolated processing modules are interconnected by a single card responsible for diagnostics across all modules.

Table IV.1 provides a comprehensive overview of the architecture (KooN type) for each component of the ESD system, delineating the definition of its process functions.

Table IV.1: ESD components architectures and functions

Component	Architecture	Description
20-LSHH-013	1001	Level switch high/high in vessel 20_B_001
20-LSHH-023	1001	Level switch high/high in vessel 20_B_002
20-LSHH-033	1001	Level switch high/high in vessel 20_B_003
20-LSHH-043	1001	Level switch high/high in vessel 20_B_004
20-LSHH-053	1001	Level switch high/high in vessel 20_B_005
20-LSLL-262	1001	Low pressure seal oil level switch low/low
20-LSLL-272	1001	High pressure seal oil level switch low/low
20-TSHH-013	1001	1st compressor discharge temperature high/high
20-TSHH-023	1001	2nd compressor discharge temperature high/high
20-TSHH-033	1001	3rd compressor discharge temperature high/high
20-TSHH-043	1001	4th compressor discharge temperature high/high
20-PSLL-014	1001	1st stage compressor suction pressure low/low
20-PSHH-027	1001	2nd compressor discharge pressure high/high
20-PSHH-047	1001	3rd compressor discharge pressure high/high
20-PSLL-256	1001	lube oil pressure low/low
XV-001	1001	Emergency Shutdown Valve (ESDV) compressor 20-K-001 aspiration
XV-002	1001	ESDV compressor 20-K-001 discharge

IV.3.2. Architecture of the ESD System for the Compression Section

Figure IV.2 illustrates the safety logic diagram of the Emergency Shutdown System (ESD). The diagram provides clear labeling of components and their connections, facilitating a comprehensive understanding of the system's organization and functionality.

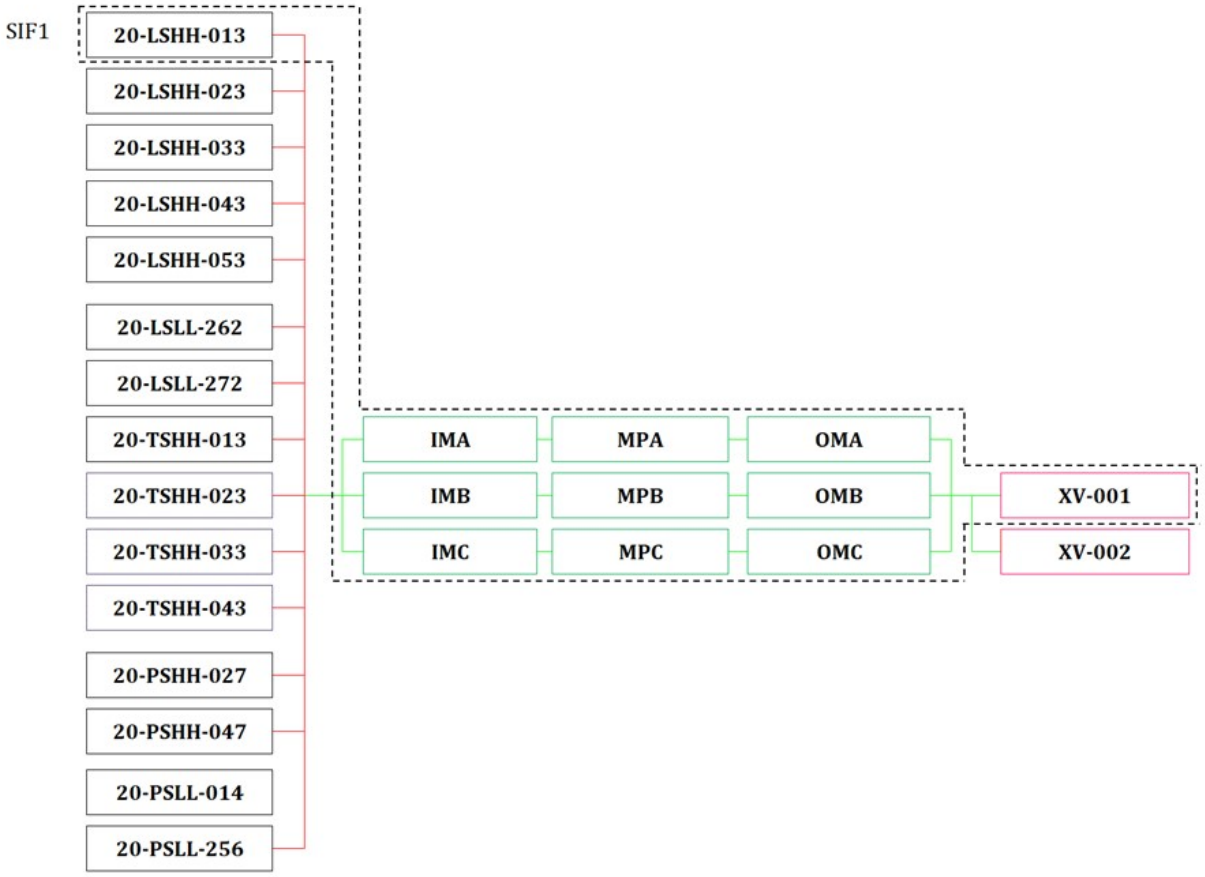


Figure IV.2: Simplified logic diagram of ESD

IV.3.3. Activation of the ESD System

The Emergency Shutdown system (ESD) serves as a critical safety mechanism, activated by various scenarios to safeguard the operation of the compression section. These scenarios involve high/high liquid levels in compressor separation vessels (20-B-001, 20-B-002, 20-B-003, and 20-B-004), high/high liquid level in dehydration inlet gas demister separator (20-B-005), low/low compressor 1st suction pressure, high/high 1st, 2nd, 3rd, or 4th compressor discharge temperatures, high/high 2nd or 4th compressor discharge pressure, low/low lube oil manifold pressure, and high/high oil level in LP or HP compressor sealing oil tank.

In the event of a trip of the centrifugal compressor (20-K-001) and gas turbine (20-KT-001), proper measures are in place to isolate and depressurize the compression section. However, the lubricating oil and sealing oil system of 20-K-001/20-KT-001 will remain in continuous operation to cool down the equipment, unless if there is failure of thelubricating oil and sealing oil system or

powerloss.Furthermore, as a safety precaution, the fuel gas supply to 20-KT-001 and 20-V-001 will be automatically shut off.

IV.4. ESDs performance assessment of the Compression Section

In this section, we delve into the evaluation of Emergency Shutdown Systems (ESDs) within the compression section. The performance assessment is essential for ensuring the safety and reliability of the compression processes.

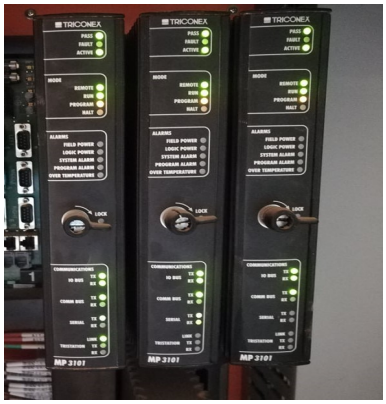
IV.4.1. Modeling of the ESD system using Petri Nets coupled with Monte Carlo simulation

Through the integration of Petri Nets and Monte Carlo Simulation, we aim to achieve a robust and accurate representation of the ESD system, facilitating thorough performance assessment and risk analysis.

By leveraging advanced modeling and simulation techniques, we can gain valuable insights into the ESD system's behavior, enabling informed decision-making to implement proper proactive measures in order to mitigate risks and ensure the integrity of the compression section.

Figure IV.3 represents real site pictures for different components of ESD (sensor, logic solver, and actuator).

Level Switch High/High sensor



TRICONEX Logic Solver

Simple Effect ESDV

Figure IV.3: Example of ESD components from the gas recovery unit.

IV.4.1.1. Modeling of the sensor subsystem

This part presents the models established for the level sensors (LSHH) specifically designed for monitoring liquid levels within the separation vessels across various maintenance strategies.

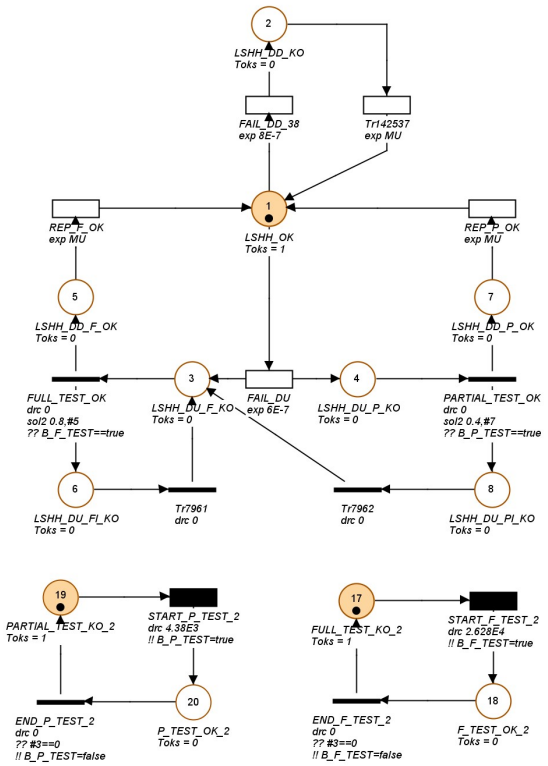


Figure IV.4: LSHH Full & Partial Imperfect tests

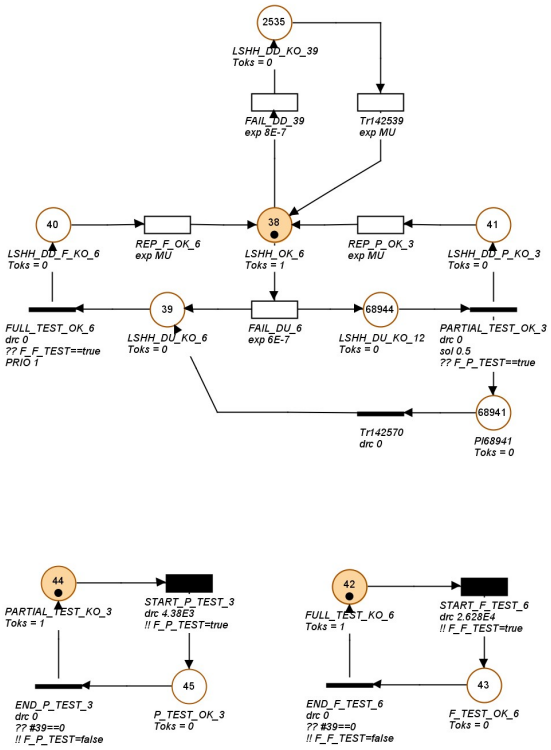


Figure IV.5 LSHH Full & Partial Perfect tests

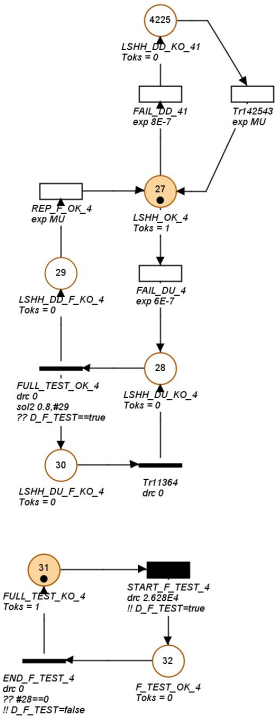


Figure IV.6: LSHH Full & Imperfect Test

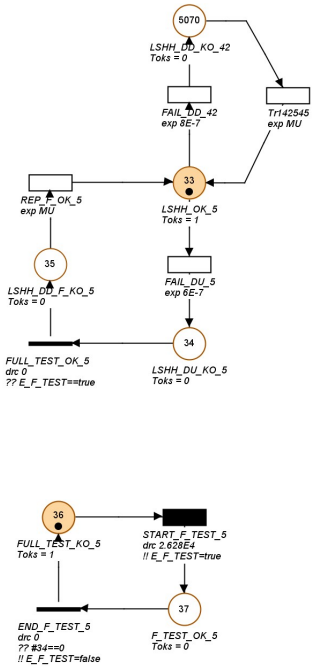
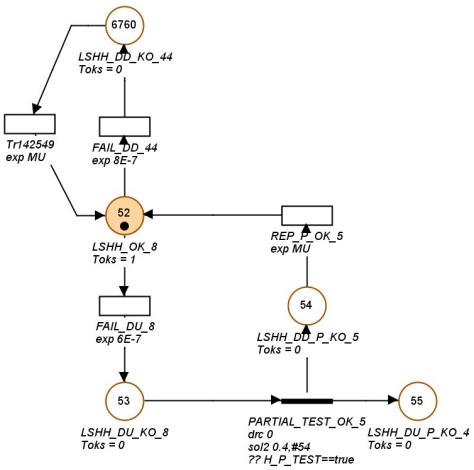
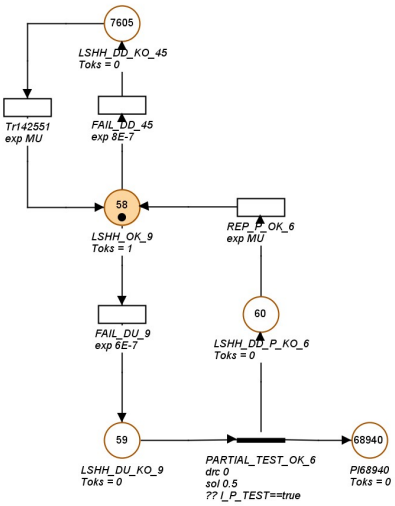
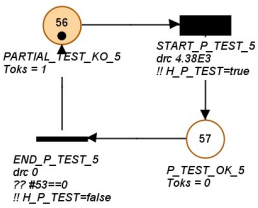


Figure IV.7: LSHH Full & Perfect Test







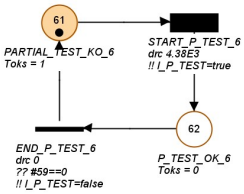


Figure IV.8: LSHH Partial Imperfect test

Figure IV.9: LSHH Partial Perfect test

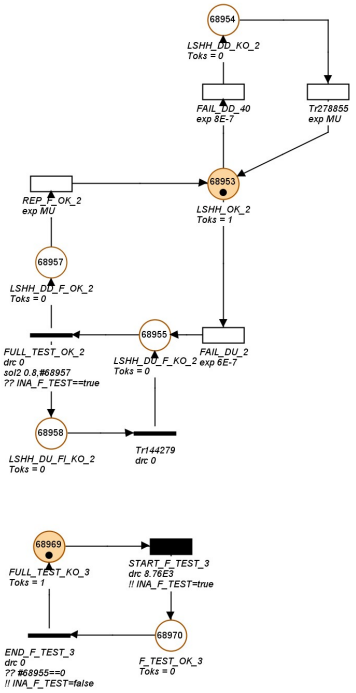
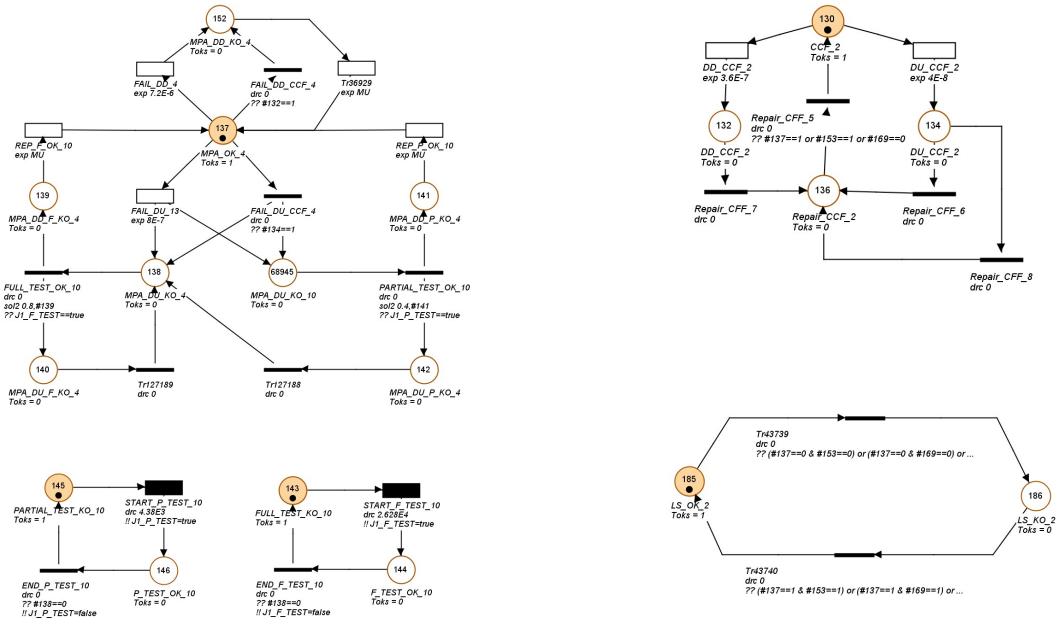


Figure IV.10: LSHH Full Imperfect tests

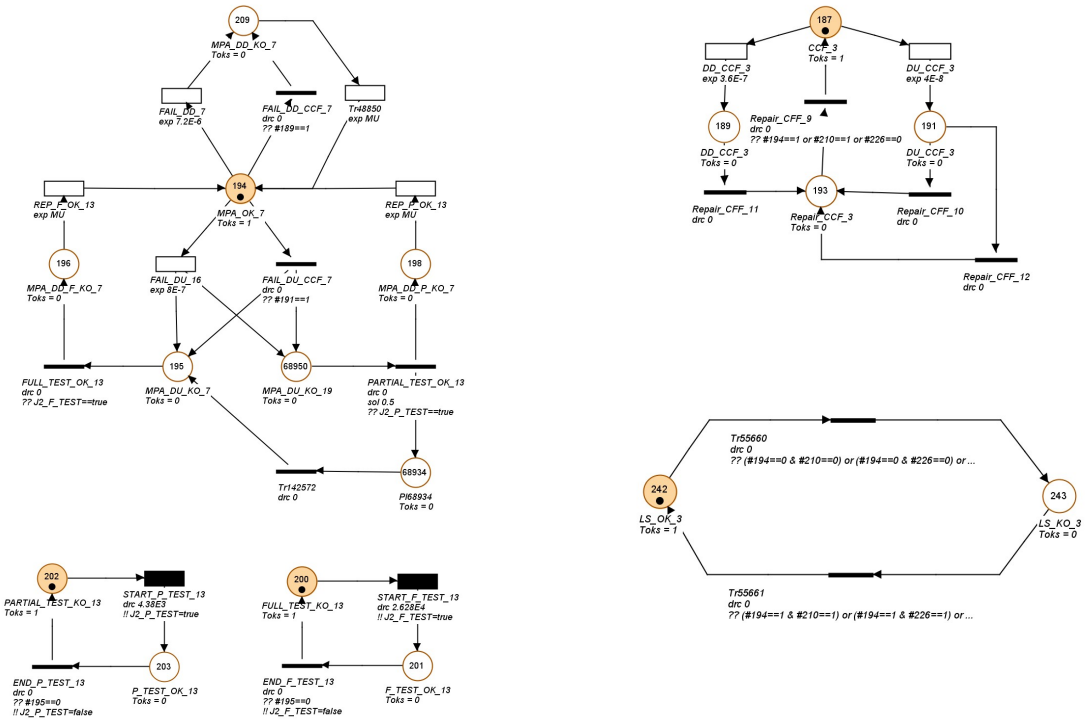
IV.4.1.2. Modeling of the logic solver (LS) subsystem

This section provides the models developed for the logic solver TRICONEX of the ESDs (Emergency Shutdown Systems) corresponding to various maintenance strategies:



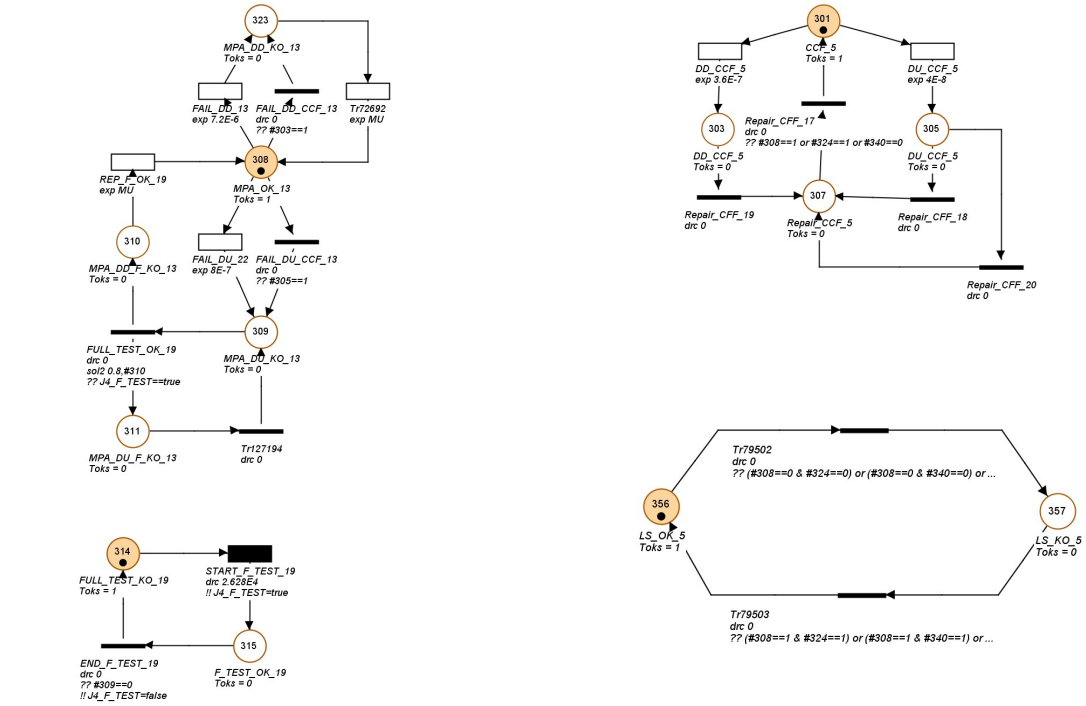
NB: MPA is similar to MPB and MPC

Figure IV.11: TRICONEX Full & Partial Imperfect tests



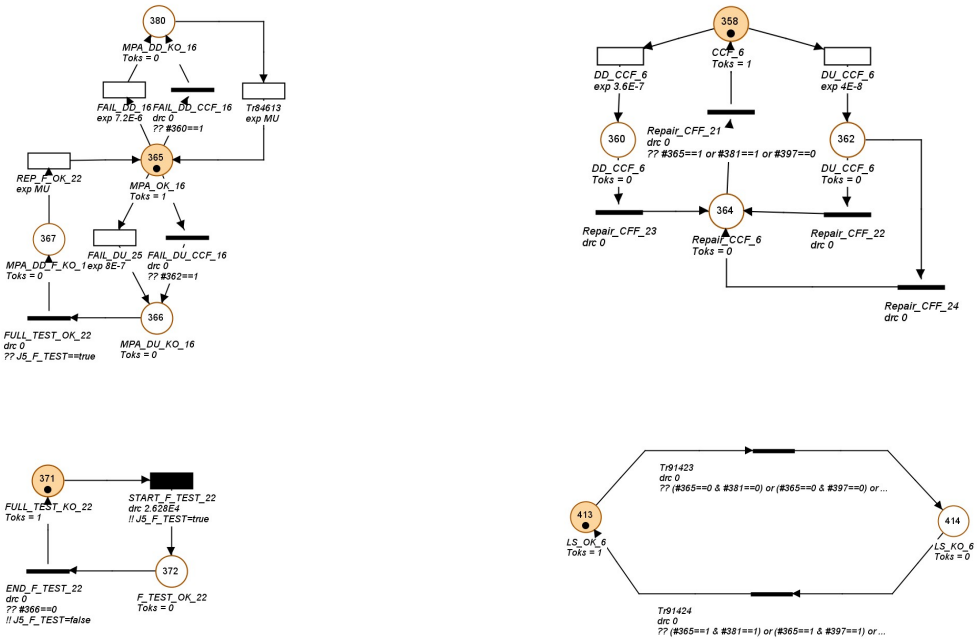
NB: MPA is similar to MPB and MPC

Figure IV.12: TRICONEX Full & Partial Perfect tests



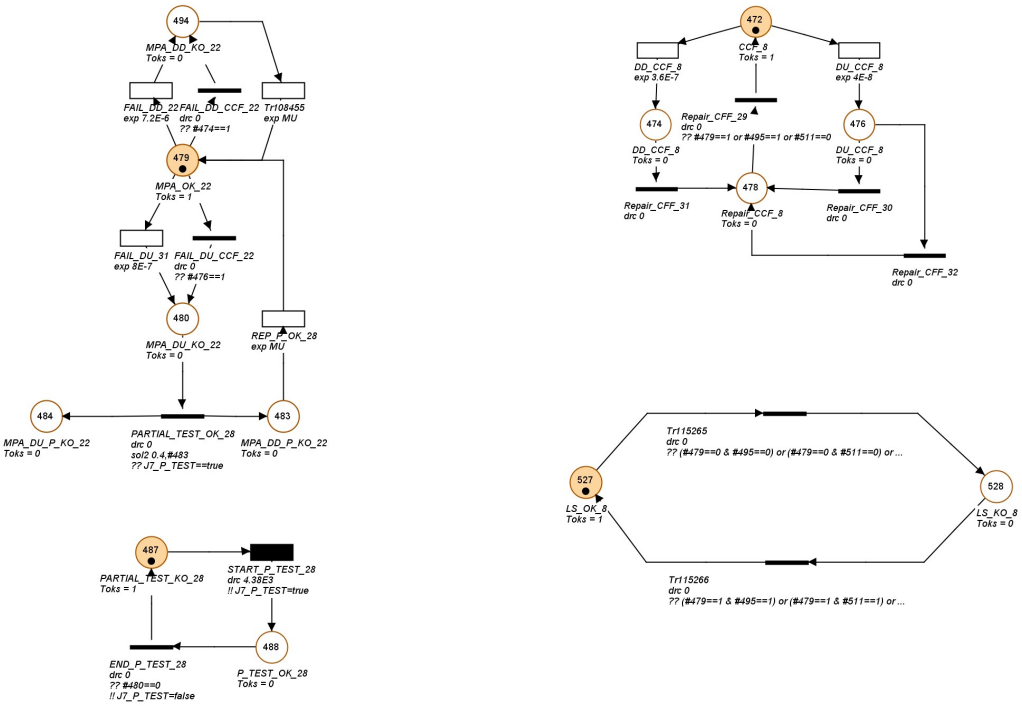
NB: MPA is similar to MPB and MPC

Figure IV.13: TRICONEX Full & Imperfect test



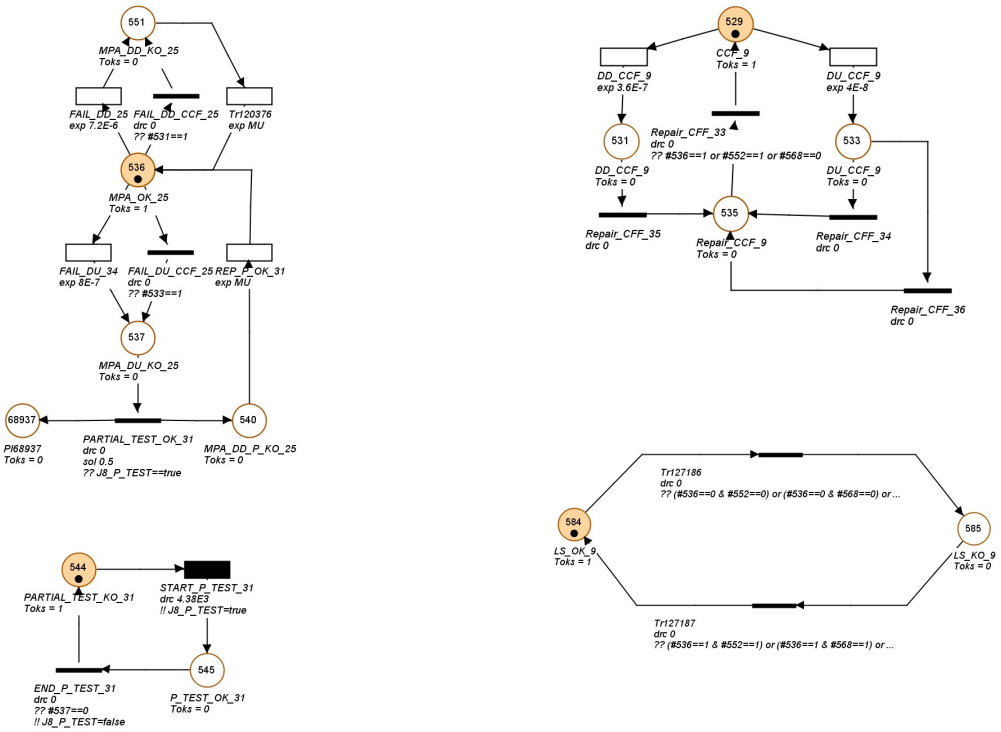
NB: MPA is similar to MPB and MPC

Figure IV.14: TRICONEX Full & Perfect test



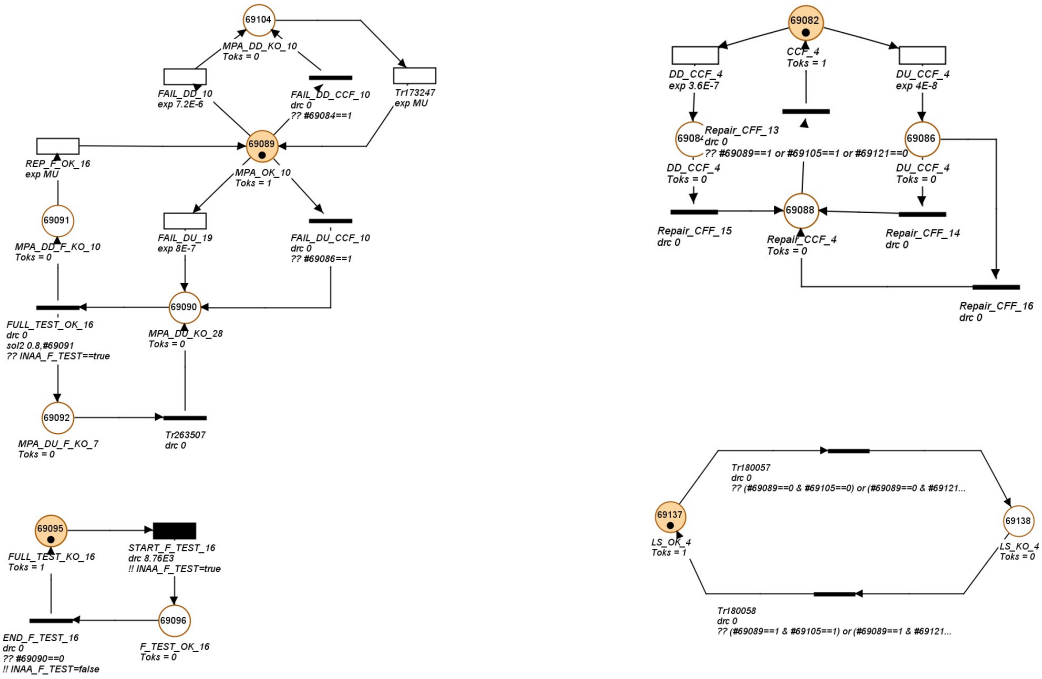
NB: MPA is similar to MPB and MPC

Figure IV.15: TRICONEX Partial Imperfect test



NB: MPA is similar to MPB and MPC

Figure IV.16: TRICONEX Partial Perfect test



NB: MPA is similar to MPB and MPC

Figure IV.17: TRICONEX Full Imperfect tests

IV.4.1.3. Modeling of the final element (FE) subsystem

This part presents the models established for the Emergency Shutdown Valves (ESDVs) corresponding to different maintenance strategies.

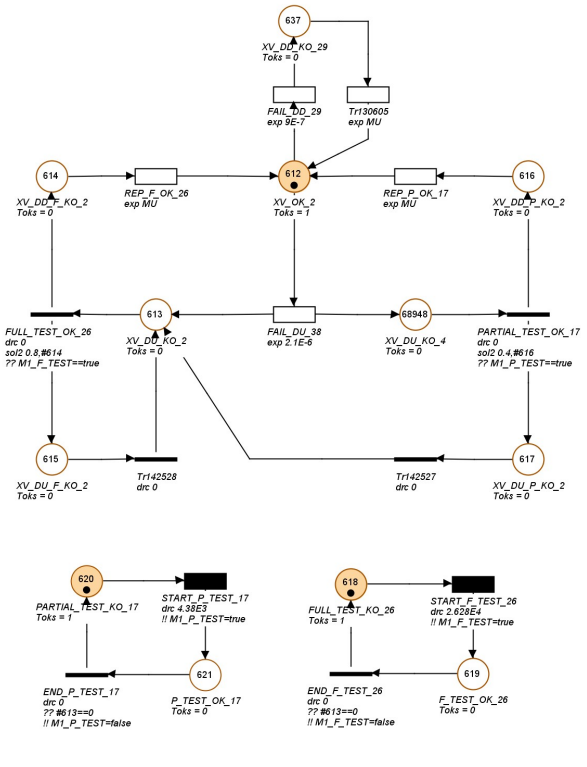


Figure IV.18: XV Full & Partial Imperfect tests

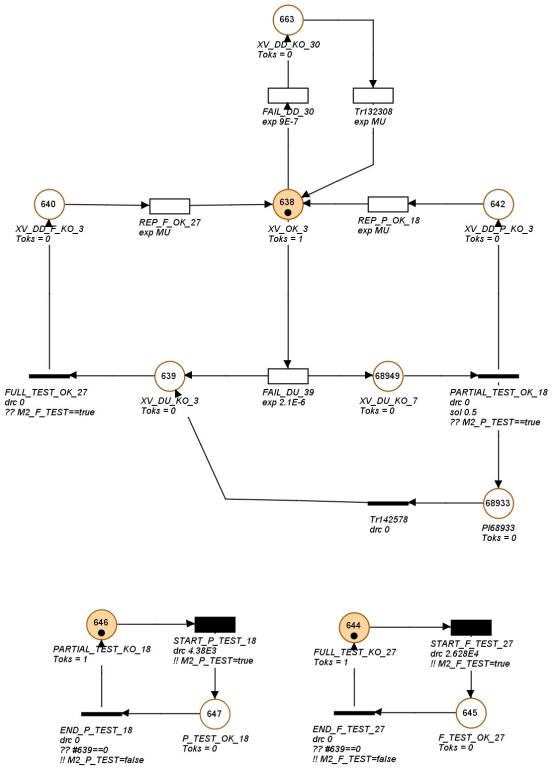


Figure IV.19: XV Full & Partial Perfect tests

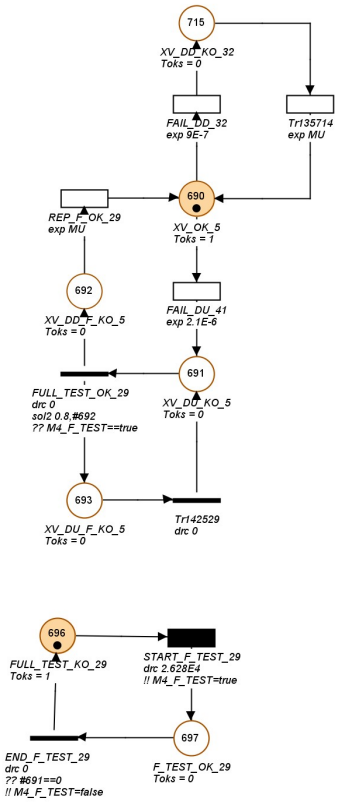


Figure IV.20: XV Full & Imperfect test

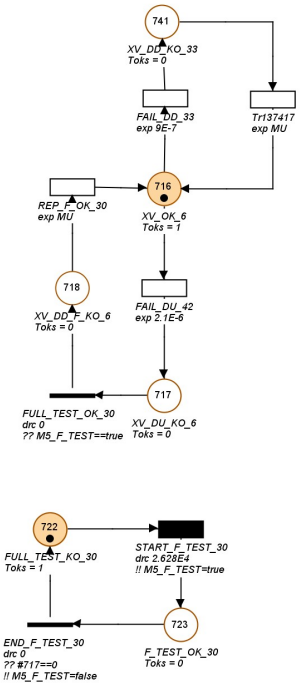


Figure IV.21: XV Full & Perfect test

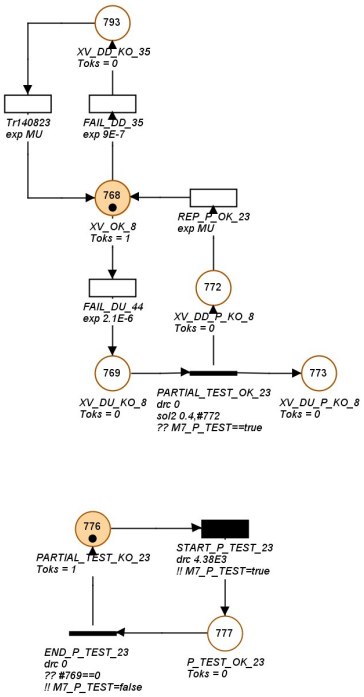


Figure IV.22: XV Partial Imperfect test

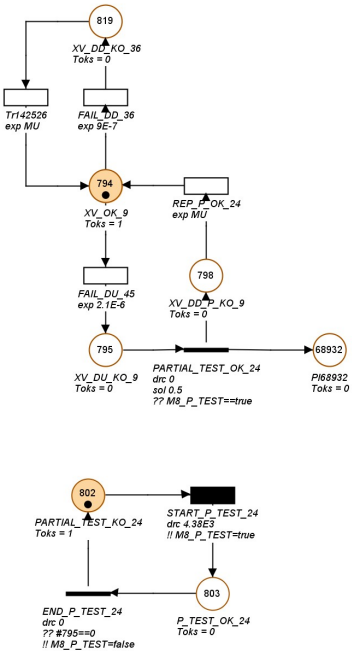


Figure IV.23: XV Partial Perfect test

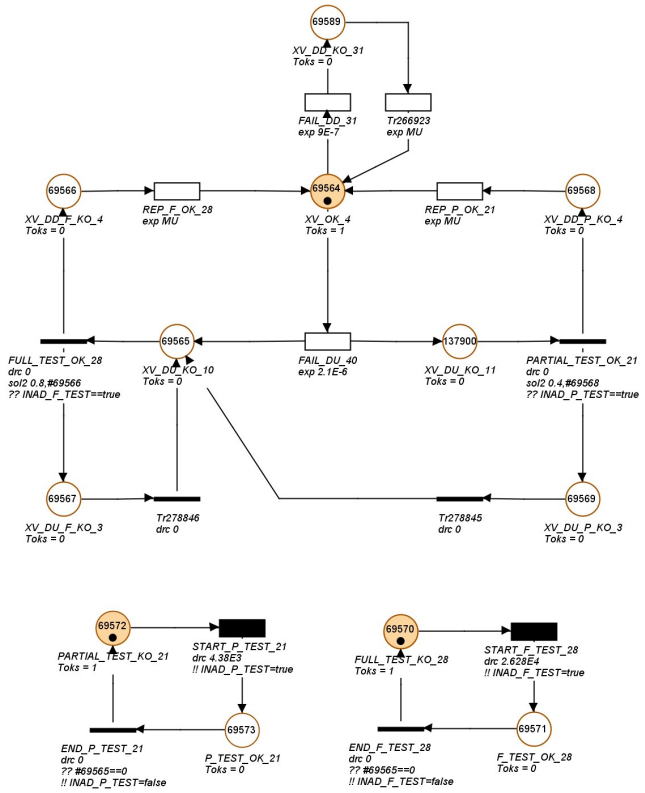


Figure IV.24: XV Full and Partial Imperfect tests

IV.4.2. Results & discussion

The PN models proposed in this study made significant contributionto the performance analysis of the AEGR unit, as shown in Figures III.1-III.9. The analysis was conducted using GRIF (Graphical Interface for Reliability Forecasting), a sophisticated software tool tailored for comprehensive systems analysis. GRIF is specifically designed to evaluate crucial dependability indicators including Reliability, Availability, Performance, and Safety. The utilization of GRIF ensured a thorough assessment of the ESD system's performance under various conditions.

To support the reliability assessment of the ESD system, data from the SINTEF report [56] was utilized. Table IV.2 presents the pertinent data extracted from the SINTEF report, which served as a crucial resource in evaluating the reliability aspects of the ESD system.

Table IV.2: Data used for assessing the reliability of the ESD System

	λ_{DD} (h-1)	λ_{DU} (h-1)	DC (%)	Full test interval (h)	Partial test interval (h)	β-factor	γ	γ_1	γ_2
20-LSHH-013 20-LSHH-023 20-LSHH-033 20-LSHH-043 20-LSHH-053 20-LSLL-262 20-LSLL-272	8,00E-07	6,00E-07	60%	2,63E+04	4,38E+03	/	80%	50%	80%
20-TSHH-013 20-TSHH-023 20-TSHH-033 20-TSHH-043	4,00E-07	3,00E-07	60%	2,63E+04	4,38E+03	/	80%	50%	80%
20-PSLL-014 20-PSHH-027 20-PSHH-047 20-PSLL-256	3,00E-07	2,00E-06	15%	2,63E+04	4,38E+03	/	80%	50%	80%
IMA IMB IMC	1,44E-06	1,60E-07	90%	2,63E+04	4,38E+03	0,05	80%	50%	80%
MPA MPB MPC	4,32E-06	4,80E-07	90%	2,63E+04	4,38E+03	0,05	80%	50%	80%
OMA OMB OMC	1,44E-06	1,60E-07	90%	2,63E+04	4,38E+03	0,05	80%	50%	80%
XV-001 XV-002	9E-07	9,00E-07	30%	2,63E+04	4,38E+03	/	80%	50%	80%

The intervals for conducting full tests for sensors and full and partial tests for ESDVs specified below are based on real data from the applied maintenance strategy on the examined ESDs:

- The sensors are fully tested every 12 months or after 8760 hours of operation.
- The logic solvers are fully tested every 12 months or after 8760 hours of operation.
- The shutdown valves are fully tested every 3 years or after 26280 hours of operation. Additionally, partial tests are conducted every 6 months or after 4380 hours of operation, with an efficiency rate of 50%.

The Stochastic Petri Net (SPN) model proposed in this study serves as a pivotal tool for conducting the intricate calculations essential for establishing the Safety Integrity Levels (SILs) of the Emergency Shutdown systems (ESDs). This modeling approach enables a comprehensive analysis of the system's reliability and safety performance under stochastic conditions.

The investigation primarily concentrates on diverse safety instrumented functions (SIFs) integral to the ESDs. These functions encompass a range of critical operations aimed at ensuring the integrity and effectiveness of the shutdown systems. To facilitate clarity and coherence in the analysis, SIFs sharing identical configurations of sensors, logic solvers, and actuators have been categorized as belonging to the same group. This classification scheme streamlines the evaluation process, allowing for a more structured and efficient assessment of the ESDs' performance across various scenarios and operational contexts.

The Safety Instrumented Functions (SIFs), denoted as SIF1, encompass a comprehensive setup within the system. Each separation vessel (20-B-001, 20-B-002, 20-B-003, 20-B-004, and 20-B-005) is equipped with a solitary high/high liquid level sensor (LSHH), a TRICONEX processing logic unit, and an emergency shut-off valve, designated as 20-XV-001.

Additionally, the Temperature SIFs (SIF2) are configured with a single temperature transmitter (TAHH), a TRICONEX processing logic unit, and an emergency shut-off valve, specifically 20-XV01.

Conversely, the Pressure SIFs (SIF3) are designed with either a single low/low-pressure transmitter (PALL) or a single high/high pressure transmitter (PAHH), in conjunction with a TRICONEX processing logic unit and an emergency shut-off valve, namely 20-XV01.

The proposed model underwent implementation involving one million iterations (1E+6 trials) utilizing Monte Carlo simulation techniques to mimic the behavior of the Emergency Shutdown System (ESD) over a duration of 132,000 hours. This extensive simulation rigorously scrutinized the performance and reliabilityof the ESDs across diverse conditions and scenarios. The statistical analysis conducted was both

robust and precise, owing to the substantial sample size of one million iterations. As a result, the simulation outcomes yielded invaluable insights into the behavior and performance of the ESD system, facilitating a more precise assessment of its reliability and safety.

Through the statistical analysis of this extensive sample, a comprehensive estimation was derived, furnishing crucial information pertinent to the functional safety management and maintenance of the ESD system.

Table IV.3: SPN-MC simulation results

	PFDavg	Availability (%)	SIL
LSHH (1001): Full and Partial Imperfect Tests	5,67E-03	99,433	SIL2
LSHH (1001): Full and Partial Perfect Tests	4,48E-03	99,552	SIL2
LSHH (1001): Full Imperfect Test	1,09E-02	98,910	SIL1
LSHH (1001): Full Perfect Test	7,90E-03	99,210	SIL2
LSHH (1001): Partial Imperfect Test	2,39E-02	97,610	SIL1
LSHH (1001): Partial Perfect Test	2,02E-02	97,980	SIL1
LSHH (1001): Full Imperfect Test (Real maintenance strategy)	3,93E-03	99,607	SIL2
Logic solver (2003): Full and Partial Imperfect Tests	3,16E-04	99,968	SIL3
Logic solver (2003): Full and Partial Perfect Tests	2,29E-04	99,977	SIL3
Logic solver (2003): Full Imperfect Test	7,77E-04	99,922	SIL3
Logic solver (2003): Full Perfect Test	4,59E-04	99,954	SIL3
Logic solver (2003): Partial Imperfect Test	3,93E-03	99,607	SIL2
Logic solver (2003): Partial Perfect Test	2,78E-03	99,722	SIL2
Logic solver (2003): Full Imperfect Test (Real maintenance strategy)	1,11E-04	99,989	SIL3
ESDV (1001): Full and Partial Imperfect Tests	1,83E-02	98,170	SIL1
ESDV (1001): Full and Partial Perfect Tests	1,45E-02	98,550	SIL1
ESDV (1001): Full Imperfect Test	3,70E-02	96,300	SIL1
ESDV (1001): Full Perfect Test	2,72E-02	97,280	SIL1
ESDV (1001): Partial Imperfect Test	8,07E-02	91,930	SIL1
ESDV (1001): Partial Perfect Test	6,82E-02	93,180	SIL1

ESDV (1001): Full and Partial Imperfect Tests (Real maintenance strategy)	1,84E-02	98,160	SIL1
SIF 1: Full and Partial Imperfect Test	3,14E-02	96,860	SIL1
SIF 1: Full and Partial Perfect Test	2,77E-02	97,230	SIL1
SIF 1: Full Imperfect Test	4,81E-02	95,190	SIL1
SIF 1: Full Perfect Test	3,52E-02	96,480	SIL1
SIF 1: Partial Imperfect Test	1,05E-01	89,500	-
SIF 1: Partial Perfect Test	8,90E-02	91,100	SIL1
SIF 1 (Real maintenance strategy)	2,69E-02	97,310	SIL1
SIF 2 (Real maintenance strategy)	2,32E-02	97,680	SIL1
SIF 3 (Real maintenance strategy)	3,73E-02	99,433	SIL1

Table IV.3 outlines the results of the calculations carried out to evaluate the reliability of different Safety Instrumented Functions (SIFs) under various maintenance strategies, including the one currently applied in the AEGR unit. The results indicate that the safety integrity levels of all SIFs are negatively impacted by the interval between tests of the emergency shut-off valves, which are performed every three years during the planned shutdown. This recommends that more frequent partial testing of the shut-off valves may be required to maintain the required SILs.

It is important to note that the results presented in Table IV.3 are based on specific assumptions and conditions, and may vary depending on the specific context and operating conditions of the system being evaluated. However, they provide valuable insights into the potential impact of testing intervals on system reliability, and emphasize the importance of ongoing SISs monitoring and maintenance.

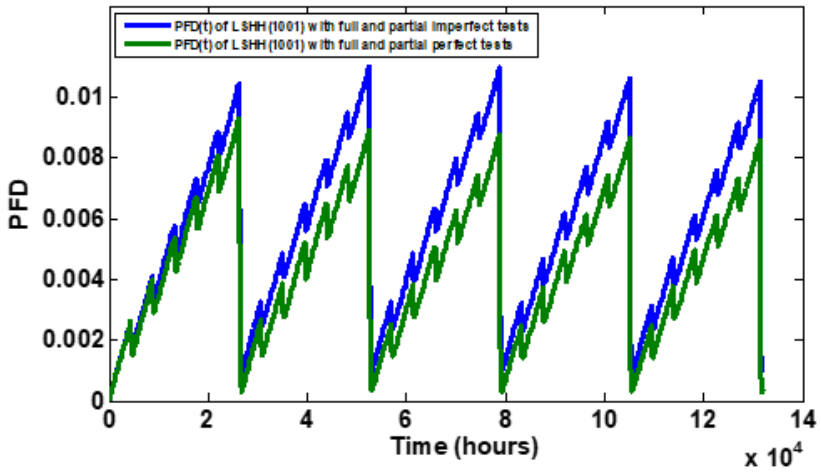


Figure IV.25: PFD(t) of LSHH (1001): Full and Partial Imperfect Tests vs Full and Partial Perfect Tests

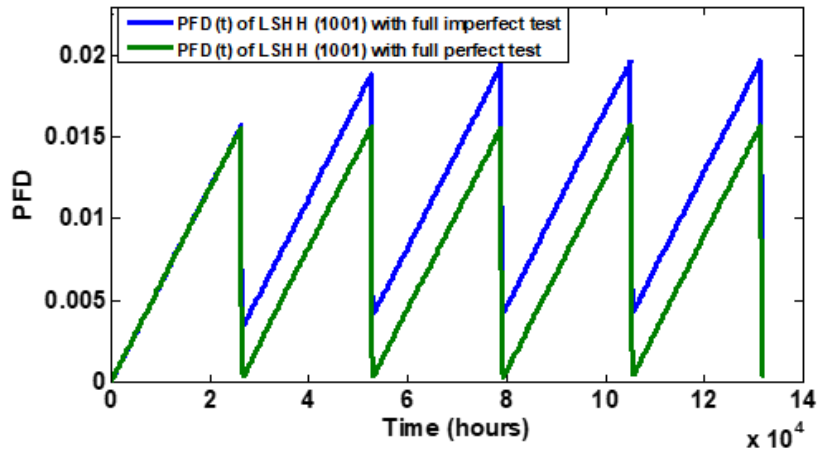


Figure IV.26: PFD(t) of LSHH (1001): Full Imperfect Test vs Full Perfect Test

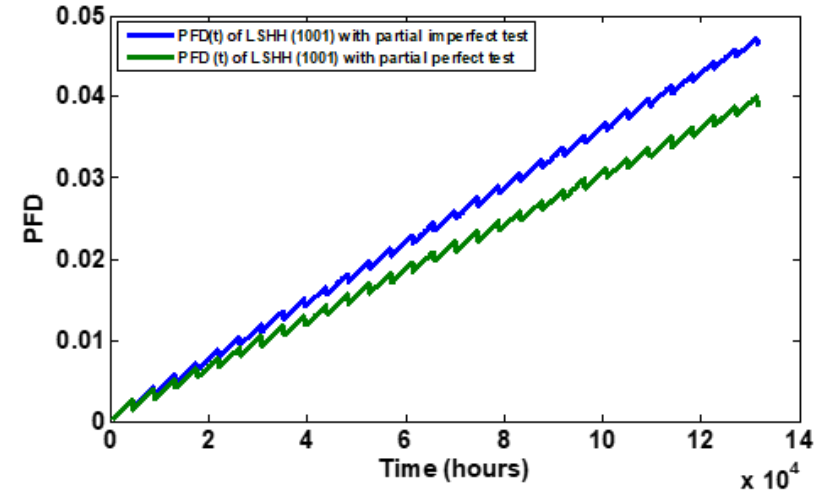


Figure IV.27: PFD(t) of LSHH (1001): Partial Imperfect Test vs Partial Perfect Test

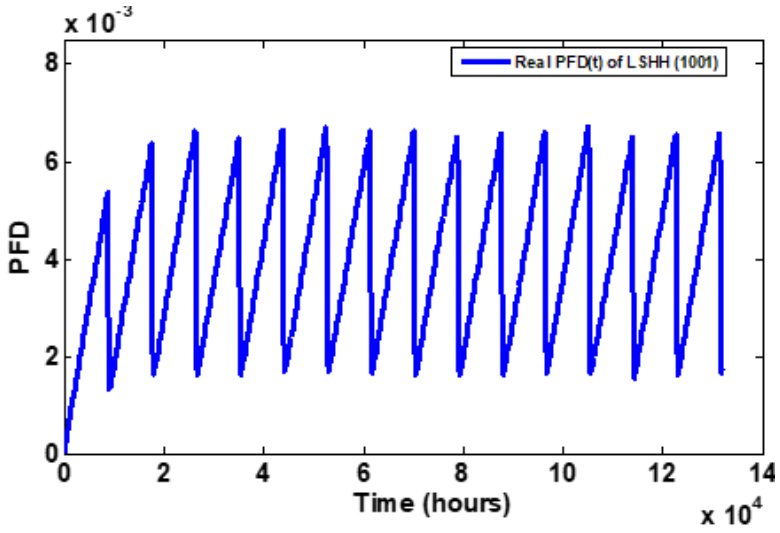


Figure IV.28: Real PFD(t) of LSHH (1001): Full Imperfect Test

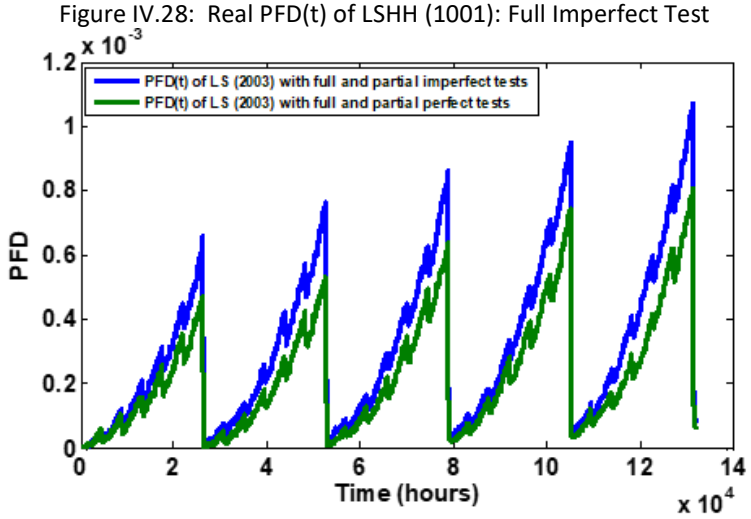


Figure IV.29: PFD(t) of the logic solver (2003): Full and Partial Imperfect Tests vs Full and Partial Perfect Tests

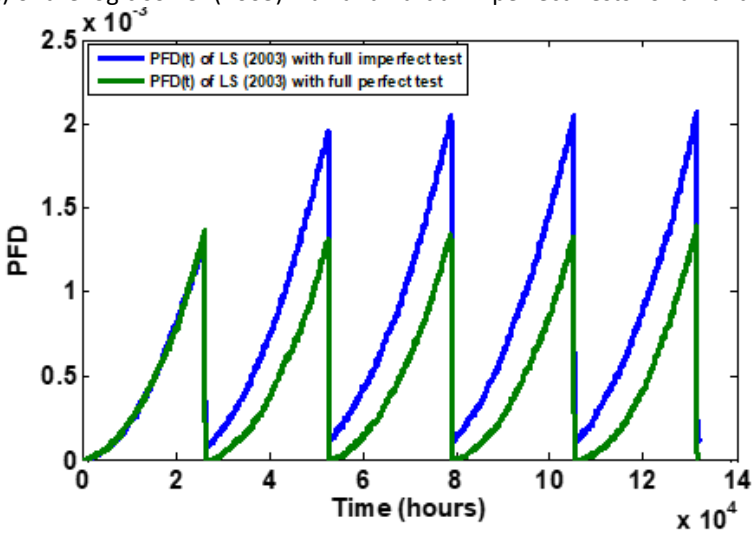


Figure IV.30: PFD(t) of the logic solver (2003): Full Imperfect Test vs Full Perfect Test

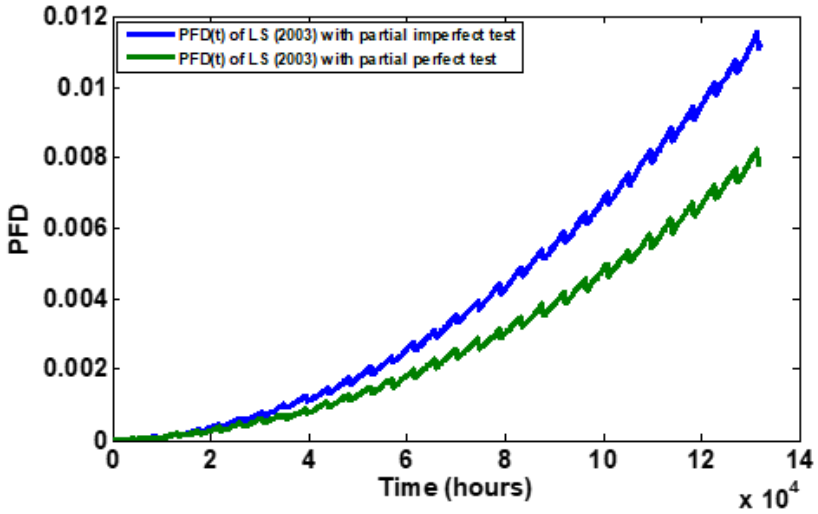


Figure IV.31: PFD(t) of the logic solver (2003): Partial Imperfect Test vs Partial Perfect Test

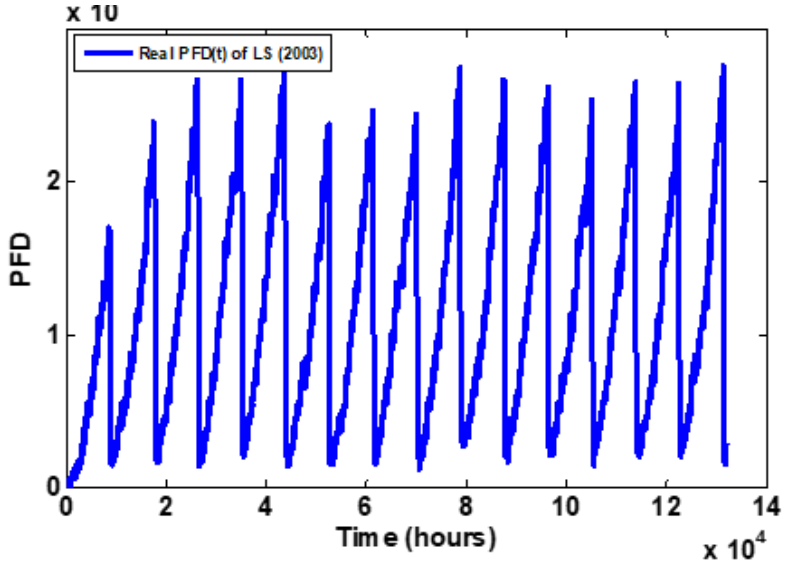


Figure IV.32: Real PFD(t) of the logic solver (2003): Full Imperfect Test

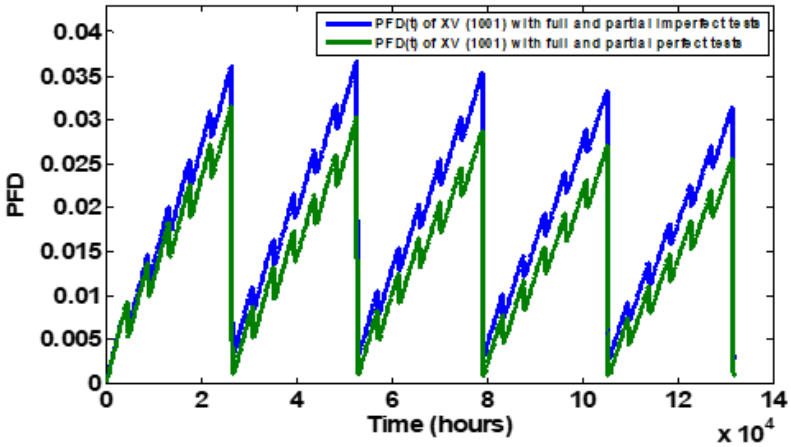


Figure IV.33: PFD(t) of ESDV (1001): Full and Partial Imperfect Tests vs Full and Partial Perfect Tests

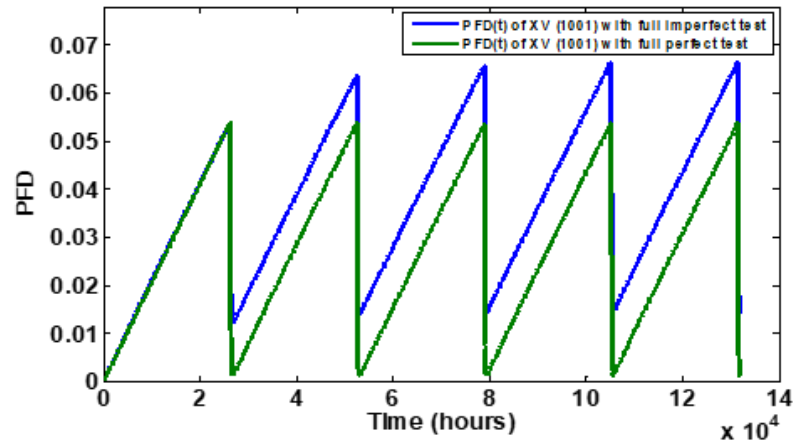


Figure IV.34: PFD(t) of ESDV (1001): Full Imperfect Test vs Full Perfect Test

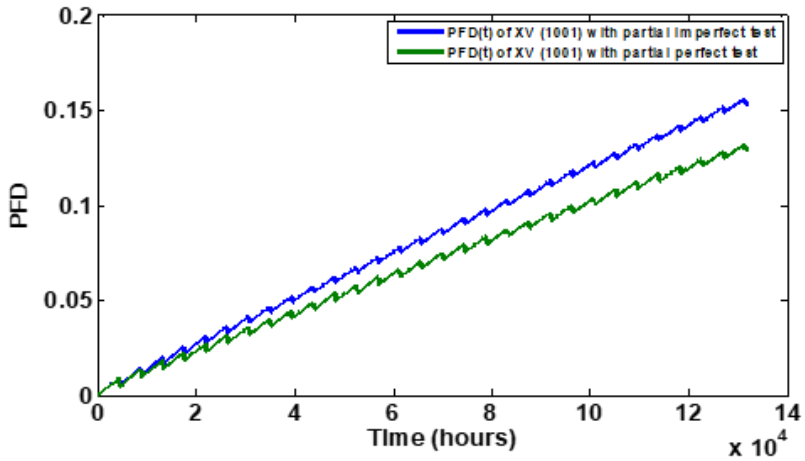


Figure IV.35: PFD(t) of ESDV (1001): Partial Imperfect Test vs Partial Perfect Test

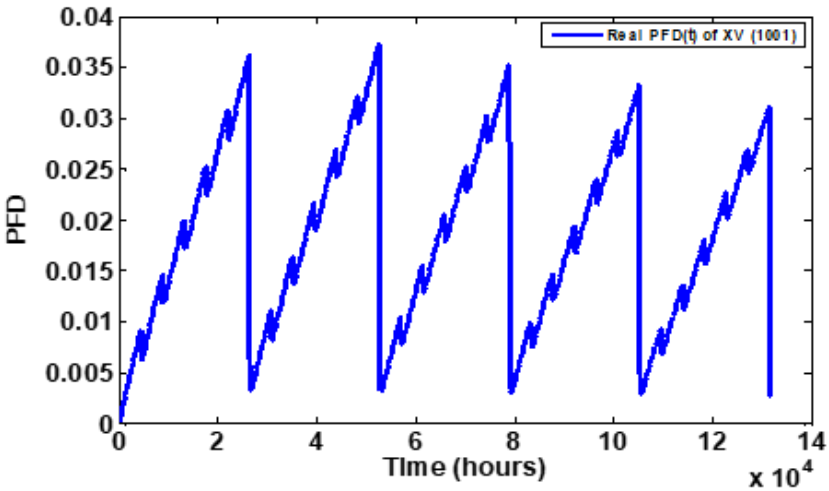


Figure IV.36: Real PFD(t) of ESDV (1001): Full and Partial Imperfect Tests

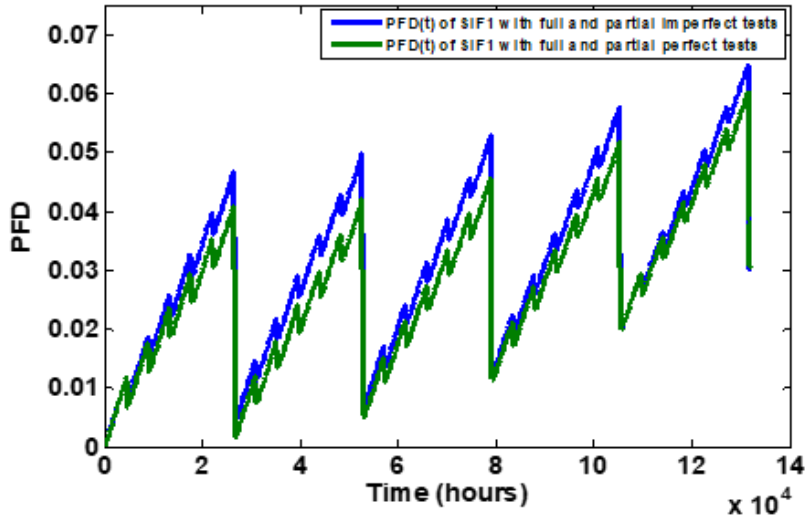


Figure IV.37: PFD(t) of SIF 1: Full and Partial Imperfect Test vs Full and Partial Perfect Test

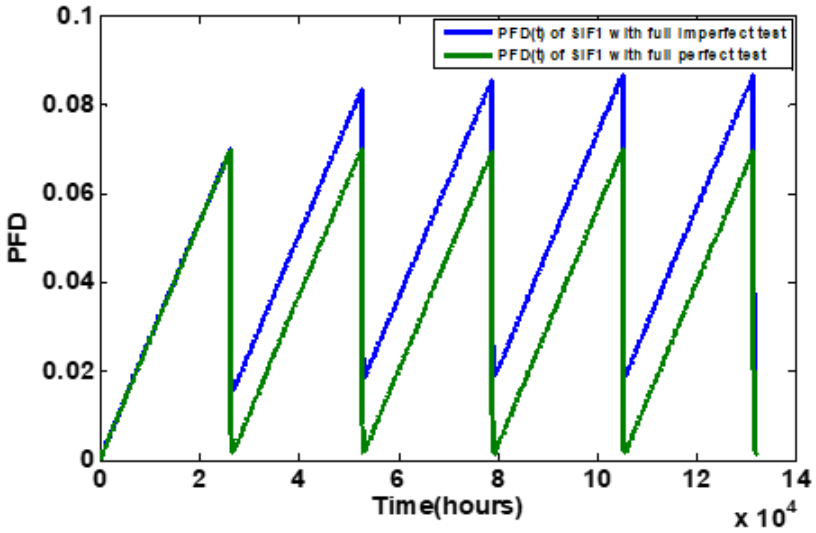


Figure IV.38: PFD(t) of SIF 1: Full Imperfect Test vs Full Perfect Test

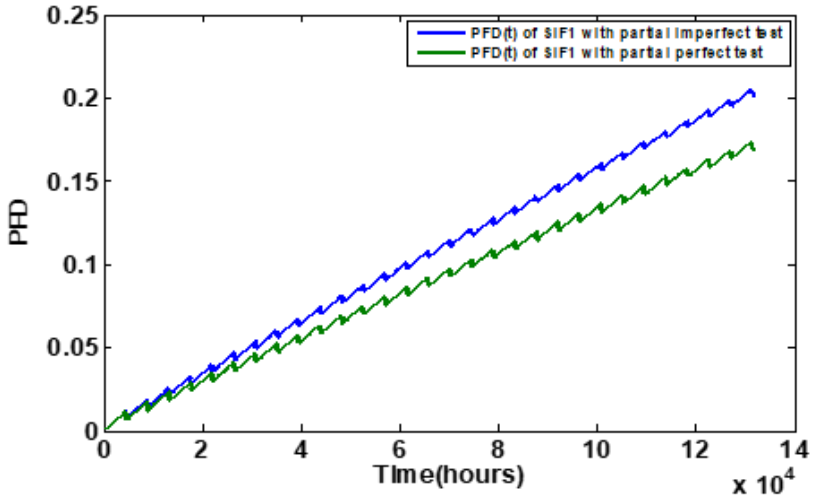


Figure IV.39: PFD(t) of SIF 1: Partial Imperfect Test vs Partial Perfect Test

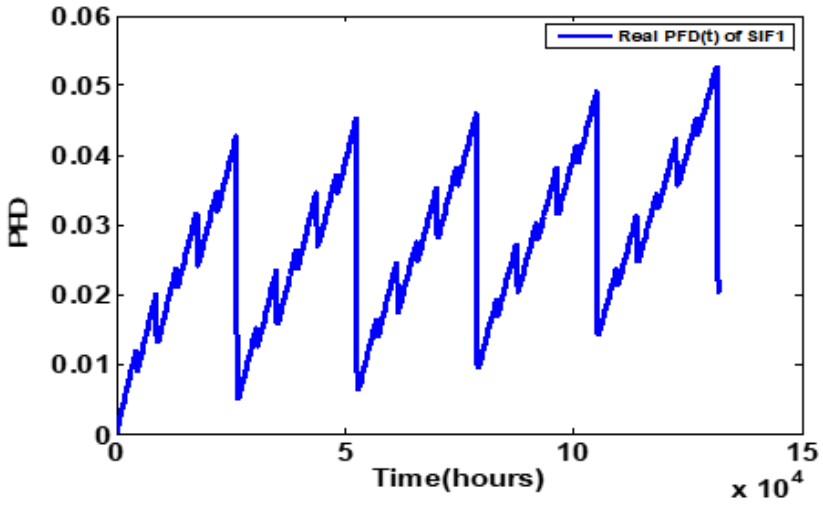


Figure IV.40: Real PFD(t) of SIF 1

IV.4.2.1. Full and partial proof tests impact

Figures IV.25, IV.29, IV.33, IV.36, IV.37, and IV.40 demonstrate the significant impact of implementing both partial and full tests on the Probability of Failure on Demand (PFDavg) and Safety Integrity Levels (SILs) of Safety Instrumented Functions (SIFs) under consideration. These figures illustrate that the incorporation of partial tests alongside with full tests leads to a reduction in PFDavg and an increase in SILs, improving system reliability.

Partial tests are particularly effective in identifying certain potential failures that contribute to the overall reliability of the system. By detecting these failures, the partial tests contribute to a decrease in PFDavg, thereby enhancing the safety and dependability of the system. As such, the combination of full and

partial tests emerges as a crucial strategy for sustaining the desired SIL over time by identifying and addressing the maximum potential failures that could compromise system integrity.

While partial proof testing is indeed less comprehensive than full proof testing, it still holds significant value in identifying potential faults or failures, ultimately enhancing the overall reliability of the system, as shown by the findings presented in Figures IV.27, IV.31, IV.35, and IV.39. Moreover, partial proof testing offers advantages over full proof testing in terms of reduced downtime and cost-effectiveness. Consequently, both testing methodologies are indispensable in maintaining the ongoing reliability of Safety Instrumented Systems (SIS).

Figures IV.26, IV.30, IV.34, and IV.38 provide clear evidence of the substantial effects of conducting a full perfect proof test on the Safety Instrumented System (SIS) performance. These figures demonstrate that performing such tests can effectively restore the Probability of Failure on Demand (PFDavg) to zero by detecting and rectifying any potential faults or failures. This outcome signifies that the system has undergone comprehensive testing and has returned to its initial phase of reliability.

This underscores the critical importance of conducting thorough and effective full proof testing to uphold the reliability of the system. By identifying and addressing any issues through rigorous testing procedures, organizations can ensure the continued functionality and dependability of their Safety Instrumented Systems.

However, there are some restrictions to conduct a full proof test. The test can be time-consuming, resulting in loss of production due to the shutdown of the process. Despite these challenges, the benefits of performing a full proof test, such as increased Safety Instrumented System (SIS) reliability and availability, and reduced likelihood of unplanned shutdowns or process interruptions, make it an important strategy to maintain the required Safety Integrity Level (SIL).

While full-proof testing can provide more assurance of reliability for SIS than partial-proof testing, the last one can be an effective option when full-proof testing is not possible or practical. The effectiveness of partial proof testing depends on the specific components tested, the frequency of testing, and the applicable standard requirements. It is crucial to carefully select the components to be tested and to ensure that partial proof testing provides sufficient failure coverage of the entire SIS.

As a result, the choice between full and partial proof testing involves a trade-off between system reliability and cost-effectiveness. Regardless of the type of proof testing performed, ensuring that the SIS

performance is maintained and potential faults and failures are detected and repaired promptly is essential.

IV.4.2.2.Imperfectness impact in full and partial proof tests

Achieving a perfect proof test poses significant challenges due to the inherent difficulty in detecting all potentially dangerous undetected failures within the system. One primary reason for this challenge is that the system may not undergo testing under normal operating conditions during a proof test, thus allowing certain types of failures to remain undetected. Additionally, the impulse lines of the system may not be thoroughly tested for blockages, which can further contribute to system failure. Moreover, the system's complexity and limitations of testing equipment can exacerbate the difficulty of achieving a perfect proof test.

In response to these challenges, this research study proposes a Petri Net (PN) model that incorporates the impact of imperfect testing while calculating the average Probability of Failure on Demand (PFDavg). Figures IV.25- IV.40 illustrate the time-dependent evolution of the Probability of Failure on Demand (PFD(t)) for various maintenance strategies, including the actual strategy implemented for Safety Instrumented Functions (SIFs) and their components. It is observed that when the imperfectness of full and/or partial proof tests is taken into account, the PFD(t) increases, directly affecting the Safety Integrity Levels (SILs) of the SIFs under consideration. Put simply, when the proof test is imperfect and certain failures remain undetected, the overall reliability of the SIF decreases, resulting in a lower SIL.

Ensuring proper execution of proof testing is crucial to mitigate the risk of undetected failures and uphold the desired SIL. By doing so, the reliability of the SIF can be maintained at the required level over time, thereby enhancing overall safety and performance.

IV.4.2.3.Financial impact of full Proof Tests

Proof tests can have a significant financial impact on oil and gas companies, both directly and indirectly. Direct costs typically include the cost of repair teams (manpower) and equipment needed to perform tests, such as calibration materials and test devices, as well as transportation costs. On the other hand, indirect costs include production losses and gas flaring tax, the unit amount specified in the Algerian hydrocarbons law [57].

Optimizing proof test intervals and scheduling full tests during planned plant shutdowns, for regular inspections of pressure equipment every three (03) years in accordance with executive decree N°21-261

[58], is the key approach for managing the economic impact associated with proof testing. This approach enhances the protection provided by various safety instrumented functions (SIFs) and thus improves the reliability of emergency shutdown systems (ESDs).

For example, performing a full proof test requires shutting down the unit, resulting in 8 hours of production losses and the payment of the flaring gas tax. Table IV.4 lists the losses incurred per test for a single SIF.

Table IV.4: Direct and indirect costs

Production losses	**-**	**-**
flaringgastax	€2667,99 per hour	€21 343,92 per 8 hours
Repair team costs	2 people at €6 per hour	€72 (12 manhours)
Testing equipment's and calibration materials costs	€340 per year	€340 per year
Transportationcosts	€34 per day	€34 per day

It's evident that the costs associated with conducting a full proof test for a single Safety Instrumented Function (SIF) are estimated to be approximately €22,235.92, with the flaring gas tax constituting a staggering 99.13% of the total costs. However, it's imperative to highlight that the expenses incurred due to not conducting proof tests can far outweigh the costs of conducting them. A malfunctioning SIS can lead to severe incidents, equipment damage, environmental harm, and even loss of life. The financial impact of such incidents can be immense, including fines, legal expenses, compensation payouts, and reputational harm.

Essentially, if proof tests can be carried out without significant interruptions to flare gas recovery, more frequent partial testing may be both feasible and advantageous. Nonetheless, it's crucial to strike a careful balance between testing costs and the imperative to uphold safety and reliability, taking into account factors such as flaring gas tax and maintenance expenses. By doing so, oil and gas producers can optimize the performance of their SIS, mitigate the costs associated with failures, and enhance production efficiency.

IV.4.2.4.Reliability-Based Spare Parts Optimization

The utilization of reliability analysis techniques to manage the procurement strategy of spare parts for a specific system or equipment is commonly referred to as reliability-based spare parts optimization. This process aims to determine the optimal quantity of spare parts required to uphold system reliability while minimizing the risk of stockouts [59], [60], [61], [62], [63] and [64].

This approach incorporates reliability engineering methodologies to evaluate failure rates of individual system components and their impact on overall system performance. In the context of this thesis, the proposed Petri net model serves as a tool to optimize spare parts forecasting during the operational phase of an existing gas processing facility.

As depicted in Figure IV.41, the results of the Monte Carlo simulation based on the proposed Petri net model illustrate the considerations of spare parts requirements at varying percentages over a two-year operational period for different Safety Instrumented Functions (SIFs). The simulation outcomes offer valuable insights into the optimal requisition of spare parts for the Safety Instrumented System (SIS), thereby contributing to maintaining high levels of system reliability while concurrently reducing maintenance costs.

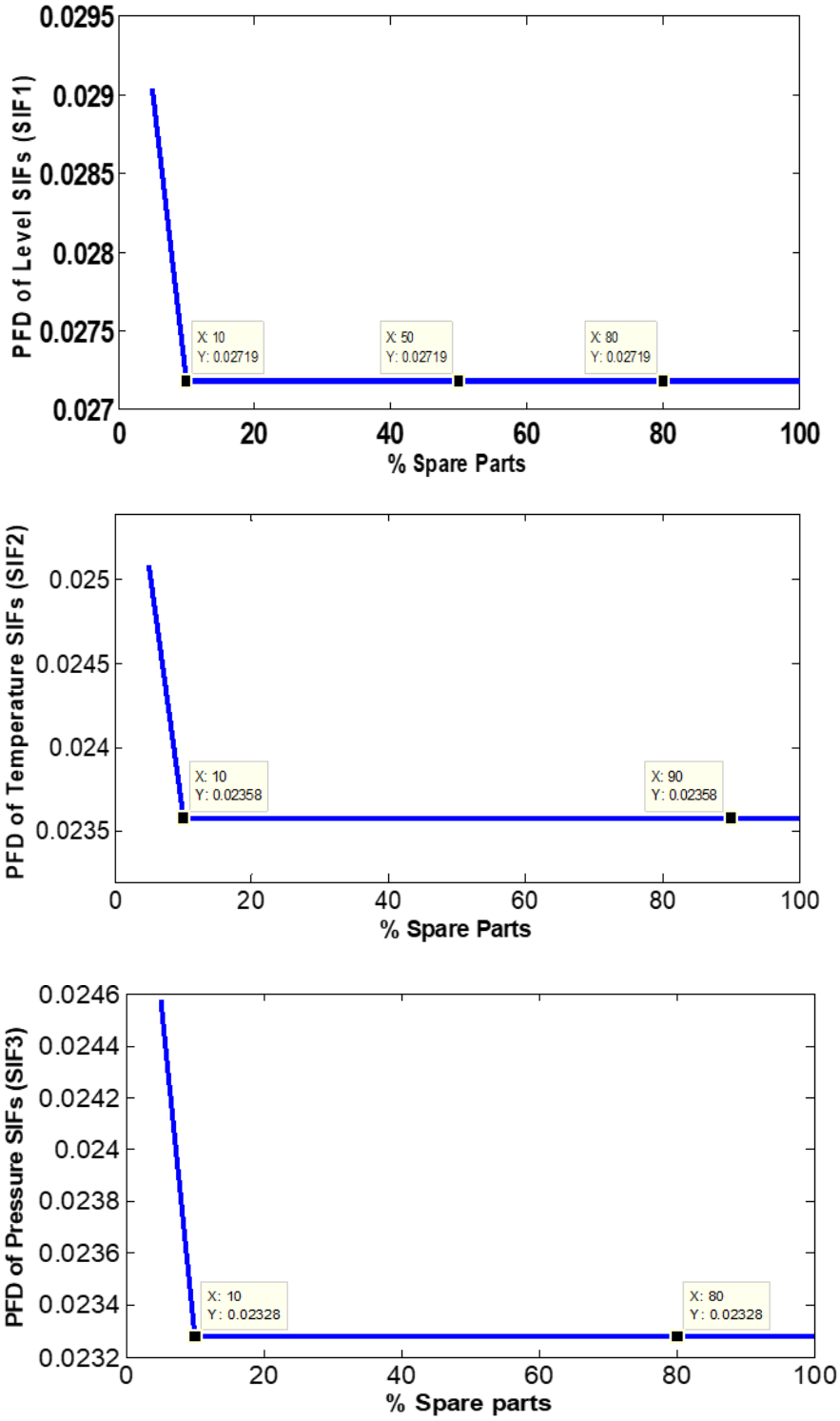


Figure IV.41: Reliability-Based Spare Parts Optimization

Moreover, the simulation results illustrated in Figure IV.41 indicate that allocating 10% of spare parts, equivalent to 37,105.68 €, is adequate for sustaining two years of system operation. Furthermore, the simulation demonstrates that the reliability of the Safety Instrumented Systems (SISs) remains consistent

when the spare parts quantity surpasses 10%. Thus, surpassing a certain threshold of spare parts does not notably enhance system reliability.

Currently, the spare parts requisition is established at 25% for two years of system operation, entailing an estimated cost of 92,764.20 €. This implies that the current spare parts requisition percentage exceeds the optimal percentage determined by the Petri Net (PN) model simulation. Consequently, there is an opportunity to reduce expenses by adjusting the spare parts procurement strategy based on the reliability analysis provided by the model.

The PN model simulation facilitates optimization of spare parts procurement grounded on reliability considerations, potentially leading to a cost reduction of 55,658.52 € (equivalent to a 60% benefit). Suchoptimization has the potential to yield substantial cost savings while upholding system reliability. Hence, the model emerges as a valuable tool for fine-tuning spare parts procurement strategies and upholding SIS reliability in gas processing facilities.

IV.5.Conclusion

Achieving the delicate balance between safety and cost presents an ongoing challenge within the oil and gas industry, particularly considering that the maintenance of Safety Instrumented Systems (SISs) can prove to be financially burdensome, especially in the context that most of Algerian gas processing plants are located in remote areas. In this chapter, we delve into the development and application of a stochastic Petri Net model to an operational flared gas recovery unit. Our aim is to investigate the performance of SISs, thereby determine the optimal maintenance strategies and practices essential for ensuring the operational integrity of gas processing facilities.

Proof testing emerges as a pivotal maintenance strategy for controlling SIS performance indicators such as the average Probability of Failure on Demand (PFDavg). The decision between full and partial proof testingnecessitates a careful consideration of the trade-off between system reliability and cost-effectiveness. Partial testing holds the potential to identify failures and support system reliability, while full proof testing offers a high level of failure detection with moreexpenses of time and resources.

In summary, while the implementation of full proof testing for SISs can present a significant financial impact on oil and gas companies, the consequences of not running this test could be catastrophic if the SIS fail to shut down the facility in case of hazardous situations. Hence, it is imperative to weigh the costs and benefits of proof testing, ensuring the implementation of an appropriate testing program (full or partial) in order to keep optimal process safety.

We recommend a combination approach between both tests wherein full tests are scheduled during planned shutdowns, typically conducted every three years in accordance with local regulations. Simultaneously, the frequency of partial tests should be increased to maximize the detection of potential failures and faults.

Furthermore, a reliability-based spare parts analysis was conducted to define the optimal order quantity for maintaining the required Safety Integrity Level (SIL) overall the SIS lifecycle. Using financial data provided by maintenance and procurement departments, our model demonstrated a significant reduction in spare parts expenses, from €92,764.20 to €37,105.68 in two years, equal to a 60% benefit.

In summary, the findingsof this chapter are aligned with fundamental principles of safety and risk engineering, highlighting the importance of evaluating, analyzing, optimizing, and managing safety systems within gas processing facilities. It offers invaluable insights into maintenance strategies, performance analysis, and cost optimization of SISs which present paramount factors for promoting safety and mitigating risks within oil and gas sector.

This research represents a significant contribution to the field of process safety and risk engineering, offering substantial findings for optimizing performance and reducingSIS maintenance costs in Algerian gas processing facilities. These outcomes hold practical implications across various phases, including design, engineering, procurement, construction, and operational phases.

General conclusion and perspectives

In wrapping up this work, it's clear that a comprehensive and integrated approach is vital for improving the performance and reliability of Safety Instrumented Systems (SISs). This thesis has made significant strides in developing and validating Petri Net models that incorporate the imperfections of proof tests and evaluate various maintenance strategies related to SIS, using an Emergency Shutdown System (ESD) in a Flared Gases Recovery Unit as a practical case study. Our research not only underscores the importance of these systems in mitigating undesired events but also highlights the financial impact of proof testing.

By applying Stochastic Petri Net (SPN) models to analyze the effects of both full and partial proof tests on Safety Instrumented Functions (SIFs), we demonstrated that optimizing test intervals and schedules can substantially reduce costs and improve the reliability of SIS. Specifically, the proposed model showed significant cost savings, achieving around a 60% benefit over two years compared to existing procurement process while maintaining the required safety integrity levels (SILs). This result validates our approach, emphasizing that realistic modeling of SIS maintenance strategies can effectively minimize spare parts expenses and inventory, ensuring timely availability and smooth plant operations efficiency.

These findings provide a foundation for refining these models further and expanding their application across different industries. Decision-makers can gain significant benefits from this work to develop robust maintenance strategies that enhance SIS reliability and cost-efficiency while ensuring seamless operations. Ultimately, this research establishes a strong basis for more reliable, and efficient safety systems in the oil and gas industry and beyond, offering a solid framework for future studies in SIS performance optimization and reliability.

The first chapter provided a comprehensive overview of Safety Instrumented Systems (SISs), detailing their essential components and performance criteria. Key concepts, such as safety instrumented functions, safety integrity levels, and failure classifications weredefined. Standards like IEC 61508 and IEC 61511 were explored to emphasize the importance of a structured safety lifecycle for effective hazard identification, risk analysis and reduction. Diagnostic coverage was reviewed through Full and Partial Stroke Tests, while proven and prior use cases underscored the practical reliability of SIS. Finally, performance analysis methods, including IEC 61508, ISA, and PDS approaches, offered comparative

insights, laying a solid foundation for understanding SIS performance and paving the way for further in-depth analysis in subsequent chapters.

The **second chapter** examined strategies for optimizing preventive maintenance of Safety Instrumented Systems (SISs). It addressed challenges in SIS maintenance and explored how various maintenance strategies can affect its performance. We reviewed different testing strategies such as proof testing (full and partial), diagnostic, and functional testing, emphasizing their roles in ensuring system reliability. The chapter also outlined different scheduling approaches and philosophies, like simultaneous and staggered testing.

The economic aspect was considered through a cost-benefit analysis framework, highlighting the financial implications of optimizing preventive maintenance. Our model of imperfect partial proof tests demonstrated how balancing test thoroughness and availability can minimize costs while maintaining performance. Overall, effective testing strategies integrated with economic insights can enhance SIS effectiveness and reliability while reducing long-term maintenance expenses.

In **chapter three**, we proposed a comprehensive model using Stochastic Petri Nets (SPN) and Monte Carlo simulation to optimize the performance and cost efficiency of Safety Instrumented Systems (SISs). The methodologies included models for different system configurations, from single component to redundant components with perfect and imperfect proof testing. A model for reliability-based spare parts optimization has been proposed.

Our SPN models effectively integrates Monte Carlo simulation to account for uncertainties, providing accurate predictions for performance and cost over the system's lifecycle. This allows in-depth analysis of both component and system reliability, offering strategic insights into planning of maintenance activities, and resources allocation. These models lay the groundwork for optimizing SIS performance and cost management, ensuring their effective role in safeguarding critical industrial processes.

In the**fourth chapter**, the developed Petri Net (PN) models coupled with Monte Carlo (MC) simulations had been applied to evaluate the system's performance, focusing on the sensor, logic solver (LS), and final element (FE) subsystems. Our analysis explored the effects of full and partial proof tests, assessed the impact of imperfect testing, and evaluated the financial implications of full proof testing. Additionally, we proposed a reliability-based optimization strategy for spare parts management to enhance system efficiency. Ultimately, the insights gained from this case study provide a valuable framework for optimizing ESD performance, reducing costs, and improving reliability in high-stakes industrial environments.

Furthermore, this research is a significant step forwardbut there is much more to explore, and several perspectives for future investigation are:

1. **Integration of Artificial Intelligence and Machine Learning**: Future research could focus on integrating artificial intelligence (AI) and machine learning (ML) techniques into SIS performance analysis. These technologies can significantly improve predictive maintenance strategies by analyzing vast amounts of operational data to identify failure patterns, predict potential failures, and optimize maintenance schedules. This proactive approach would minimize downtime and reduce maintenance costs while enhancing system reliability.
2. **Enhancing Reliability-Based Spare Parts Optimization**: Further studies could explore the application of AI/ML in spare parts management by dynamically predicting component failures and ensuring the availability of critical spare parts. This would reduce excess inventory and streamline the supply chain, cutting costs while maintaining system integrity.
3. **Cybersecurity Measures**: With increased reliance on digital technologies, future work should also focus on integrating cybersecurity measures into SIS design. Research could explore how to protect these safety systems from cyber threats, ensuring data integrity and reliable operation even in the face of targeted attacks.

Together, these research perspectives would pave the way for next-generation SIS solutions that are more efficient, intelligent, and resilient.

In conclusion, this thesis significantly contributes to the understanding and improvement of preventive maintenance strategies for Safety Instrumented Systems through the effective use of Stochastic Petri Nets coupled with Monte Carlo Simulation.

Bibliography

[1] *Functional safety – Safety instrumented systems for the process industry sector*, IEC61511, 2016.

[2] M. Qi, Y. Kan, X. Li, X. Wang, D. Zhao, and I. Moon, "Spurious activation and operational integrity evaluation of redundant safety instrumented systems," *Reliability Engineering & System Safety,* vol. 197, p. 106785, 2020/05/01/ 2020, doi: https://doi.org/10.1016/j.ress.2019.106785.

[3] I. v. B. ; and W. M. Goble, *Safety Instrumented System Design Techniques and Design Verification*. ISA, 2018.

[4] *Functional safety of electrical/electronic/programmable electronic safety-related systems*, IEC61508, 2010.

[5] J. V. Bukowski, "Modeling and analyzing the effects of periodic inspection on the performance of safety-critical systems," *IEEE Transactions on Reliability,* vol. 50, no. 3, pp. 321-329, 2001, doi: 10.1109/24.974130.

[6] A. C. Torres-Echeverría, S. Martorell, and H. A. Thompson, "Multi-objective optimization of design and testing of safety instrumented systems with MooN voting architectures using a genetic algorithm," *Reliability Engineering & System Safety,* vol. 106, pp. 45-60, 2012/10/01/ 2012, doi: https://doi.org/10.1016/j.ress.2012.03.010.

[7] S. Hauge, M. A. Lundteigen, P. Hokstad, and S. Håbrekke, "Reliability prediction method for safety instrumented systems–pds method handbook, 2010 edition," *SINTEF report STF50 A,* vol. 6031, p. 460, 2013.

[8] D. J. Smith, *Reliability, maintainability and risk: practical methods for engineers*. Butterworth-Heinemann, 2021.

[9] H. Jin, M. A. Lundteigen, and M. Rausand, "Uncertainty assessment of reliability estimates for safety-instrumented systems," *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability,* vol. 226, no. 6, pp. 646-655, 2012/12/01 2012, doi: 10.1177/1748006X12462780.

[10] M. Lundteigen and M. Rausand, *The effect of partial stroke testing on the reliability of safety valves*. 2007.

[11] S. S. Misra, "Safety and reliability in safety instrumented systems for offshore oil and gas production facility ", FACULTY OF ENGINEERING AND SUSTAINABLE DEVELOPMENT

Department of Electrical Engineering, Mathematics and Science University of Gävle, Sweden, 2022.

[12] N. O. A. GAS;, *070 – NORWEGIAN OIL AND GAS - APPLICATION OF IEC 61508 AND IEC 61511 IN THE NORWEGIAN PETROLEUM INDUSTRY (Recommended SIL requirements)*. Norskolge&gass, 2018.

[13] *ISA-TR84.00.03, Safety instrumented functions sif—safety integrity level (sil) evaluation technique: Determining the sil of a sif via markov analysis.*, 2002.

[14] L. F. Oliveira and R. N. Abramovitch, "Extension of ISA TR84.00.02 PFD equations to KooN architectures," *Reliability Engineering & System Safety,* vol. 95, no. 7, pp. 707-715, 2010/07/01/ 2010, doi: https://doi.org/10.1016/j.ress.2010.01.006.

[15] P. Hokstad and K. Corneliussen, "Loss of safety assessment and the IEC 61508 standard," *Reliability Engineering & System Safety,* vol. 83, no. 1, pp. 111-120, 2004/01/01/ 2004, doi: https://doi.org/10.1016/j.ress.2003.09.017.

[16] 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, doi: https://doi.org/10.1016/j.ress.2014.10.001.

[17] Y. Liu and M. Rausand, "Reliability effects of test strategies on safety-instrumented systems in different demand modes," *Reliability Engineering & System Safety,* vol. 119, pp. 235-243, 2013/11/01/ 2013, doi: https://doi.org/10.1016/j.ress.2013.06.035.

[18] M. Lintala and J. Ovtcharova, "Enhancing System Lifecycle Processes by Integrating Functional Safety Information from Practice into Design Requirements," *International Journal of Advanced Robotic Systems,* vol. 10, no. 10, p. 376, 2013/10/01 2013, doi: 10.5772/56850.

[19] D. J. Smith, *Reliability, Maintainability and Risk*. Butterworth-Heinemann, Oxford, OX5 1GB, UK, eighth edition., 2011.

[20] S. Sachdeva, "Imperfect Testing and its Influence on Availability of Safety Instrumented Systems," internationalMaster's degree program, Norwegian University of Science and Technology, 2015.

[21] E. S. Ocheni, "Impact of partial and imperfect testing on reliability assessment of safety instrumented systems," MASTER, Department of Production and Quality Engineering, Norwegian University of Science and Technology, 2015.

[22] J. V. Bukowski and I. v. Beurden, "Impact of proof test effectiveness on safety instrumented system performance," in *2009 Annual Reliability and Maintainability Symposium*, 26-29 Jan. 2009 2009, pp. 157-163, doi: 10.1109/RAMS.2009.4914668.

[23] 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, doi: https://doi.org/10.1016/j.ress.2008.09.006.

[24] M. Rausand, *Reiability of Safety-Critical Systems: Theory and Applications*. Wiley, Hoboken, NJ., 2014.

[25] H. Jin and M. Rausand, "Reliability of safety-instrumented systems subject to partial testing and common-cause failures," *Reliability Engineering & System Safety,* vol. 121, pp. 146-151, 2014/01/01/ 2014, doi: https://doi.org/10.1016/j.ress.2013.08.006.

[26] C. Djeddi, A. Hafaifa, M. Guemana, and B. Nail, "Reliability assessment of complex safety instrumented systems using stochastic Petri nets," in *2sd International Conference on Applied Automation and Industrial Diagnostics (ICAAID*, 2017.

[27] D. René and A. Hassane, *Discrete, Continuous, and Hybrid Petri Nets*. Springer Science & Business Media, 2010.

[28] B. Rabah, R. Younes, C. Djeddi, and L. Laouar, "Optimization of safety instrumented system performance and maintenance costs in Algerian oil and gas facilities," *Process Safety and Environmental Protection,* vol. 182, pp. 371-386, 2024/02/01/ 2024, doi: https://doi.org/10.1016/j.psep.2023.11.081.

[29] P. Amyotte *et al.*, "Process safety for the 21st century and beyond," *ICS.*

[30] T. Kerin, "Managing Process Safety. In The Core Body of Knowledge for Generalist OHS Professionals. 2nd Ed. ," Tullamarine, VIC: Australian Institute of Health and Safety., 2019.

[31] *PSM* 2022.

[32] *KPIs PSM*, 2022.

[33] A. Birolini, *Reliability Engineering: Theory and Practice*. Springer, Berlin, 2017.

[34] IEC61511, *Functional safety - Safety instrumented systems for the process industry sector*. Geneva: International Electrotechnical Commission, 2016.

[35] A. Zhang, S. Wu, D. Fan, M. Xie, B. Cai, and Y. Liu, "Adaptive testing policy for multi-state systems with application to the degrading final elements in safety-instrumented systems," *Reliability Engineering & System Safety,* vol. 221, p. 108360, 2022/05/01/ 2022, doi: https://doi.org/10.1016/j.ress.2022.108360.

[36] S. Yuan, G. Reniers, M. Yang, and Y. Bai, "Cost-effective maintenance of safety and security barriers in the chemical process industries via genetic algorithm," *Process Safety and*

Environmental Protection, vol. 170, pp. 356-371, 2023/02/01/ 2023, doi: https://doi.org/10.1016/j.psep.2022.12.008.

[37] R. Abbasinejad, F. Hourfar, D. Kacprzak, A. Almansoori, and A. Elkamel, "SIL calculation in gas processing plants based on systematic faults and level of maturity," *Process Safety and Environmental Protection,* vol. 174, pp. 778-795, 2023/06/01/ 2023, doi: https://doi.org/10.1016/j.psep.2023.04.044.

[38] P. Chen, Q. Lin, and X. Han, "Taking 2oo3 as an example to study the improvement of Markov model considering periodic function test," *Journal of Physics: Conference Series,* vol. 2264, no. 1, p. 012008, 2022/04/01 2022, doi: 10.1088/1742-6596/2264/1/012008.

[39] O. Bensmaine, R. Nait-Said, and F. Zidani, "Failure Diagnostic of Emergency Shutdown Valve (ESDV) Based on Fault-Symptom Tree and Fuzzy Inference System: A Case Study," *Journal of Failure Analysis and Prevention,* vol. 22, no. 2, pp. 785-800, 2022/04/01 2022, doi: 10.1007/s11668-022-01359-z.

[40] Y. Redutskiy, C. M. Camitz-Leidland, A. Vysochyna, K. T. Anderson, and M. Balycheva, "Safety systems for the oil and gas industrial facilities: Design, maintenance policy choice, and crew scheduling," *Reliability Engineering & System Safety,* vol. 210, p. 107545, 2021/06/01/ 2021, doi: https://doi.org/10.1016/j.ress.2021.107545.

[41] R. Abbasinejad, F. Hourfar, and A. Elkamel, "Optimum Maintenance Interval Determination for Field Instrument Devices in Oil and Gas Industries Based on Expected Utility Theory," *Computers & Chemical Engineering,* vol. 152, p. 107362, 2021/09/01/ 2021, doi: https://doi.org/10.1016/j.compchemeng.2021.107362.

[42] H. Srivastav, A. Barros, and M. A. Lundteigen, "Modelling framework for performance analysis of SIS subject to degradation due to proof tests," *Reliability Engineering & System Safety,* vol. 195, p. 106702, 2020/03/01/ 2020, doi: https://doi.org/10.1016/j.ress.2019.106702.

[43] A. Zhang, T. Zhang, A. Barros, and Y. Liu, "Optimization of maintenances following proof tests for the final element of a safety-instrumented system," *Reliability Engineering & System Safety,* vol. 196, p. 106779, 2020/04/01/ 2020, doi: https://doi.org/10.1016/j.ress.2019.106779.

[44] S. Alizadeh and S. Sriramula, "Unavailability assessment of redundant safety instrumented systems subject to process demand," *Reliability Engineering & System Safety,* vol. 171, pp. 18-33, 2018/03/01/ 2018, doi: https://doi.org/10.1016/j.ress.2017.11.011.

[45] D. Martynova and P. Zhang, "Optimization of Maintenance Schedule for Safety Instrumented Systems," *IFAC-PapersOnLine,* vol. 50, no. 1, pp. 12484-12489, 2017/07/01/ 2017, doi: https://doi.org/10.1016/j.ifacol.2017.08.1928.

[46] F. Innal, M. A. Lundteigen, Y. Liu, and A. Barros, "PFDavg generalized formulas for SIS subject to partial and full periodic tests based on multi-phase Markov models," *Reliability Engineering &System Safety,* vol. 150, pp. 160-170, 2016/06/01/ 2016, doi: https://doi.org/10.1016/j.ress.2016.01.022.

[47] Y. Liu and M. Rausand, "Proof-testing strategies induced by dangerous detected failures of safety-instrumented systems," *Reliability Engineering & System Safety,* vol. 145, pp. 366-372, 2016/01/01/ 2016, doi: https://doi.org/10.1016/j.ress.2015.06.016.

[48] J. Jin, L. Pang, B. Hu, and X. Wang, "Impact of proof test interval and coverage on probability of failure of safety instrumented function," *Annals of Nuclear Energy,* vol. 87, pp. 537-540, 2016/01/01/ 2016, doi: https://doi.org/10.1016/j.anucene.2015.09.028.

[49] S. Wu, L. Zhang, W. Zheng, Y. Liu, and M. A. Lundteigen, "Reliability modeling of subsea SISs partial testing subject to delayed restoration," *Reliability Engineering & System Safety,* vol. 191, p. 106546, 2019/11/01/ 2019, doi: https://doi.org/10.1016/j.ress.2019.106546.

[50] S. Wu, L. Zhang, M. A. Lundteigen, Y. Liu, and W. Zheng, "Reliability assessment for final elements of SISs with time dependent failures," *Journal of Loss Prevention in the Process Industries,* vol. 51, pp. 186-199, 2018/01/01/ 2018, doi: https://doi.org/10.1016/j.jlp.2017.12.007.

[51] J.-P. Signoret, Y. Dutuit, P.-J. Cacheux, C. Folleau, S. Collas, and P. Thomas, "Make your Petri nets understandable: Reliability block diagrams driven Petri nets," *Reliability Engineering & System Safety,* vol. 113, pp. 61-75, 2013/05/01/ 2013, doi: https://doi.org/10.1016/j.ress.2012.12.008.

[52] J. R. Müller, T. Ständer, and E. Schnieder, "Improving System Safety Modelling in accordance to IEC 61508 by using Monte Carlo Simulations," *IFAC Proceedings Volumes,* vol. 42, no. 5, pp. 193-197, 2009/06/01/ 2009, doi: https://doi.org/10.3182/20090610-3-IT-4004.00038.

[53] J.-P. Signoret, "Dependability & safety modeling and calculation: Petri nets," *IFAC Proceedings Volumes,* vol. 42, no. 5, pp. 203-208, 2009/06/01/ 2009, doi: https://doi.org/10.3182/20090610-3-IT-4004.00040.

[54] 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, doi: https://doi.org/10.1016/j.ress.2008.03.024.

[55] B. Svensson and S. Djumena, "GLOBAL GAS FLARING REDUCTION INITIATIVE, World Bank Group in collaboration with the Government of Norway," 2001.

[56] S. Hauge, *Reliability Data for Safety Instrumented Systems*: SINTEF Report A13502, 2010.

[57] *Law No. 19-13 of 14 Rabi Al-Thani 1441 corresponding to December 11, 2019 regulating hydrocarbon activities.,* O. J. O. T. A. R. N. 79., 2019.

[58] *Executive Decree No. 21-261 of 2 Dhou El Kaada 1442 corresponding to June 13, 2021, regulating pressure vessels (ESP) and electrical equipment intended to be integrated into installations belonging to the hydrocarbon sector.,* O. J. O. T. A. R. N. 49., 2021.

[59] B. Ghodrati and U. Kumar, "Reliability and operating environment-based spare parts estimation approach," *Journal of Quality in Maintenance Engineering,* vol. 11, no. 2, pp. 169-184, 2005, doi: 10.1108/13552510510601366.

[60] D. Louit, R. Pascual, D. Banjevic, and A. K. S. Jardine, "Optimization models for critical spare parts inventories—a reliability approach," *The Journal of the Operational Research Society,* vol. 62, no. 6, pp. 992-1004, 2011. [Online]. Available: http://www.jstor.org/stable/20868941.

[61] A. Barabadi, B. Ghodrati, J. Barabady, and T. Markeset, "Reliability and spare parts estimation taking into consideration the operational environment — A case study," in *2012 IEEE International Conference on Industrial Engineering and Engineering Management*, 10-13 Dec. 2012 2012, pp. 1924-1929, doi: 10.1109/IEEM.2012.6838081.

[62] N. Z. Kontrec, G. V. Milovanović, S. R. Panić, and H. Milošević, "A Reliability-Based Approach to Nonrepairable Spare Part Forecasting in Aircraft Maintenance System," *Mathematical Problems in Engineering,* vol. 2015, p. 731437, 2015/05/07 2015, doi: 10.1155/2015/731437.

[63] K. Nataša and P. Stefan, "Spare Parts Forecasting Based on Reliability," in *System Reliability*, V. Constantin Ed. Rijeka: IntechOpen, 2017, p. Ch. 6.

[64] A. Nouri Qarahasanlou, R. ShakorShahabi, and N. Fallahnejad, "Assessment of Spare Parts Requirement by Reliability: A Case Study," (in en), *International Journal of Reliability, Risk and Safety: Theory and Application,* vol. 5, no. 1, pp. 9-19, 2022, doi: 10.30699/IJRRS.5.1.2.