الجمهورية الجزائرية الديمقراطية الشعبية
Republic Algerian Democratic and Popular
وزارة التعليم العالي والبحث العلمي
Ministry of Higher Education and Scientific Research
جامعة وهران 2 محمد بن أحمد
University of Oran 2 Mohamed Ben Ahmed
معهد الصيانة والأمن الصناعي
Institute of Maintenance and Industrial Safety

Department of Industrial Safety and Environment

MEMORY

For the master's degree

Sector: Industrial Security
Speciality: Industrial Safety and Environment

Theme

Reliability analysis of a safety instrumented system

SIS

Presented and publicly supported by:

GHEZZAL Mohammed Aymen & HADJ DIDA Abdennour

In front of the jury composed of:

Name and surname	Grade	Establishment	Quality
Talbi Zahéra	MCB	IMSI	**President**
Benomar Fatima	MCB	IMSI	**Framer**
Aouimer Yamina	MCB	IMSI	**Examiner**

September 2025

Acknowledgments:

At the end of this work, we would like to express our deepest gratitude to all the people who contributed, directly or indirectly, to the completion of this memoir.

First and foremost, we thank Almighty God for granting us health, patience, and the determination needed to accomplish this work.

Our thanks to ***Mrs. Benomar Fatima,*** *our academic supervisor, for her guidance, constant support, and valuable advice, which were essential to the success of this memory.*

We would also like to thank ***Mr. Yacine Korti,*** *Intervention Engineer,* ***Mr. Walid Megherbi,*** *Prevention Engineer,* ***Mr. Mnaouer,*** *SNCC Engineer,* ***Mr. Shami****, Intervention Technician,* ***Mr. Azuz****, DCS Control Room Operator, as well as* ***Mrs. K. Malek, Laboratory*** *Technician, for their invaluable assistance, availability, and technical explanations that greatly guided and enriched us throughout this project.*

Dedication

We dedicate this work with love and gratitude:

To my dear parents, ***Leila and Djamel****, whose constant support and guidance have been the foundation of my journey.*
To my ***grandmother****, whose prayers and encouragement have always been a source of strength, I owe my deepest gratitude.*
To my ***aunt*** *and her husband,* ***B. Kamel****, for their encouragement and unwavering belief in me.*

And to my beloved parents, ***Fatiha*** *and* ***Abdelkader****, whose sacrifices, love, and endless encouragement have shaped who I am today.*
To my dear ***brother, Mohamed,*** *and my* ***sister Sara****, for their affection, inspiration, and constant motivation that remind me to always move forward with hope and determination.*

This work is as much yours as it is mine.

الملخص

شكل أنظمة السلامة المؤتمتة **(SIS)** حاجزاً أساسياً لحماية الأفراد والمنشآت والبيئة من الأحداث الخطرة ضمن إطار السلامة الصناعية. يتناول الجزء الأول من هذا العمل الأسس النظرية لأنظمة **SIS**، بما في ذلك مستويات السلامة الوظيفية **(SIL)**، ووظائف السلامة المؤتمتة **(SIF)**، إضافة إلى المعايير الدولية المنظمة لتطبيقها وضمان فعاليتها.

أما الجزء الثاني فيعرض طرق تحليل المخاطر، ولا سيما **تحليل شجرة الأعطال (FTA)** و**الشبكات البايزية(BN)** ، حيث توفر هذه المنهجيات مقاربات تكميلية لتقييم كفاءة الأنظمة ونمذجة الصناعات الخطرة.

وقد تم تطبيق هذه الدراسة على **مجمع GP2/Z في أرزيو**، المتخصص في معالجة وتخزين **الغاز البترولي المسال(GPL)** ، وذلك بغرض تحديد أنماط الفشل الحرجة، وتقييم احتمالية حدوثها، ومقارنة فعالية منهجيتي **FTA**و**BN**.

أظهرت النتائج أهمية الدمج بين هذه التقنيات في إجراء تقييم شامل للمخاطر واقتراح توصيات لتحسين كفاءة أنظمة **SIS**وزيادة موثوقيتها وتوافرها في التطبيقات الصناعية.

الكلمات المفتاحية :السلامة الصناعية، SIS، SIL، SIF، FTA، الشبكات البايزية، GPL، GP2/Z، تحليل المخاطر.

Résumé

Les Systèmes Instrumentés de Sécurité (SIS) constituent une barrière essentielle pour protéger les individus, les installations et l'environnement contre les incidents dangereux dans le cadre de la sécurité industrielle. Ce mémoire présente dans une première partie les fondements des SIS, tels que les Niveaux d'Intégrité de Sécurité (SIL), les Fonctions Instrumentées de Sécurité (SIF), ainsi que les normes internationales qui régissent leur mise en œuvre.

La deuxième partie décrit les méthodes d'analyse de risques, notamment l'Arbre de Défaillances (FTA) et les Réseaux Bayésiens (BN), qui offrent des approches complémentaires pour l'évaluation de la fiabilité des systèmes et la modélisation des risques industriels.

Une étude de cas a été réalisée au sein du complexe GP2/Z d'Arzew, spécialisé dans le traitement et le stockage du GPL. L'analyse a permis d'identifier les modes de défaillance critiques, d'évaluer leur probabilité d'occurrence et de comparer l'efficacité des approches FTA et BN.

Les résultats soulignent l'importance de la combinaison de ces deux techniques pour affiner l'évaluation des risques et proposer des recommandations visant à améliorer la fiabilité et la

disponibilité des SIS dans les applications industrielles.
Mots-clés : Sécurité industrielle, SIS, SIL, SIF, FTA, Réseaux Bayésiens, GPL, GP2/Z, Analyse de risques.

Abstract

Safety Instrumented Systems (SIS) are the fundamental protection to safeguard individuals, facilities, and the environment against hazardous incidents in industrial safety. In this thesis, the fundamentals of SIS, including Safety Integrity Levels (SIL), Safety Instrumented Functions (SIF), and the international standards governing their implementation, are introduced.

The second part outlines risk analysis methods, namely Fault Tree Analysis (FTA) and Bayesian Networks (BN), which provide complementary approaches for system reliability assessment and industrial risk modeling.

A case study was carried out at the GP2/Z plant in Arzew, which specializes in LPG processing and storage. The analysis identified critical failure modes, assessed their probability of occurrence, and compared the effectiveness of FTA and BN methodologies.

The results highlight the importance of combining the two techniques to refine risk assessment and propose recommendations for improving the reliability and availability of SIS in industrial applications.

Keywords: Industrial Safety, SIS, SIL, SIF, FTA, Bayesian Networks, LPG, GP2/Z, Risk Analysis.

Acronyms

ALARP As Low As Reasonably Practicable

BPCS, Base Process Control System

DCS Distributed Control System

IEC, International Electrotechnical Commission

E/E/PE, systèmes électriques, électroniques et programmables E/E/EP

ESD Emergency Shut Down

EUC, Equipment Under Control

HS, Hand Switch

ISO, International Standardization Organization

LT, Level Transmitter

MDT, Mean Down Time

MTBF Mean Time Between Failures

MTTF Mean Time to Failure

MTTR Mean Time to Repair

NCS, Networked Control System

OHSAS, Occupational Health and Safety Assessment Series

RV, Relief of the safety Valve

PES, Programmable Electronic System

PFD Probability of Failure on Demand

PFH, Probability of a dangerous Failure per Hour

PFS, Probability of Failure to Safe

PIC, Pressure Indicator Controller

PT, Pressure Transmitter

PV, Pressure control Valve

PY, Pressure signal Converter calculator

RAMS, Reliability, Availability, Maintainability, and Safety

RFF, Risk Reduction Factor

SIF, Safety Instrumented Function

SIL, Safety Integrity Level

SIS, Systèmes Instrumentés de Sécurité

SFF, Safe Failure Fraction

SRS, Safety-related systems

XV, Shut off valve

Contents Table

الملخص 4

Résumé 4

Abstract 5

Chapter 1: 13

I. Introduction 14

I 1. SAFETY INSTRUMENTED SYSTEMS (SIS): 14

I 2. Safety Integrity Level (SIL): 17

I 3. Safety instrumented function (SIF): 22

I.4. SIL /SIF /SIS : 23

I 4.1. Summary of SIL, SIF, and SIS Implementation 23

I 4.2. Implementation Steps: 24

1. Risk Assessment & SIL Assignment: 24

2. Design Safety Functions (SIFs): 24

3. SIS Design & Integration: 24

4. Verification & Validation 24

5. Installation & Commissioning: 24

6. Operation & Maintenance: 24

I 5. Systems for safety applications: 24

I 6. FUNCTIONAL SAFETY: 25

I . 6.1Hazard concept 25

Definitions: 25

I . 6.2 Notion of risk 26

I 6.3 Risk classification 27

I 6.4 Acceptable risk 28

I . 6.5 Major risk 29

I . 6.6 Industrial risk 29

I . 6.7 Notion of safety 30

I . 6.8 General principles of protection 30

I . 6.8.1 Passive safety features 30

I . 6.8.2 Active safety features 30
I . 7. Standards relating to safety instrumented systems: 31
I 7.1 IEC 61508 standard: 31
I . 7.2 The IEC 61511 standard: 33
I . 7.3 The IEC 61513 standard 35
I . 7.4 The IEC 62061 standard 35
I . 7.6 ISO 26262 standards: 36
I 8 Conclusion: 36
Chapter 2: 37
II.1 Introduction 38
II.2 Definition: 38
Types of Risk Analysis: 38
II.3 Fault tree analysis (FTA): 40
II.3.1 Fault tree analysis symbols: 41
II.3.2 Fault tree analysis steps: 44
II.4 Limits of FTA: 49
II.5 Bayesian networks (BN): 50
II.5.2 Bayes rule: 53
II.5.3Transformation of FTA to BN: 54
Conclusion: 56
Chapter 3: 57
III.1 PRESENTATION OF THE GP2Z COMPLEX: 58
III.2 Technical sheet of the complex: 59
III.3 Main facilities of the complex: 60
III.4 History of the GP2Z complex: 60
III.5 GENERAL INFORMATION ON LPG: 62
III.6 THE ORGANIZATION OF THE COMPLEX: 63
III.7 PRINCIPLE OF THE GP2-Z PROCESS: 65
III.7.1 The main sections of the complex: 65
III.7.2 Description of the manufacturing process: 65
III.7.2.1 LPG reception and storage sections: 65

III.7.2.2 DEHYDRATION: 66
III.7.2.3 SEPARATION: 66
III.7.2.4 REFRIGERATION: **67**
Vapor compression: 69
Anti-pumping system: 69
III.7.2.5 STORAGE: 70
Chapter 4: 71
IV.2 Fault Tree Analysis: 74
IV.2.1 Qualitative analysis: 76
IV.2.3 Interpretation: 78
IV.3 Bayesian Network: 81
Prior probability: 84
Posteriori probability: 85
References: 89

Prelude

Industrial plants are no longer concerned solely with system performance in terms of quality, productivity, and profitability, but also with safety. Specific systems known as safety instrumented systems are used to reduce the risk of hazardous events occurring in these plants by guaranteeing the protection of equipment, people, the environment, and property.

These risks reflect both the severity and the frequency of occurrence. Hazardous event. The severity scales comprise several levels, which are assessed according to the consequences of the hazardous event on people, the environment, and property.

Safe installation can involve several means of achieving a situation where all risks are reduced to a tolerable level. Unambiguous criteria must be defined for tolerable risk levels. Measures to ensure process safety are dedicated to each specific type of protection. The design of the process, the choice of plant devices and equipment.

Action on basic process control systems (BPCS), which are used to optimize process conditions to maximize quality and production, can also help to reduce risks. Reduce risks. However, these actions are sometimes insufficient, and it is necessary to introduce other safety systems to further reduce risk to an acceptable level further.

The instrumented safety systems (SIS) are introduced to meet this need and respond to dangerous situations when the process finds itself in such situations.

This memoir delves into the intricate aspects of Safety Instrumented Systems, structured into four key chapters. The first chapter introduces SIS, defining fundamental concepts and laying the groundwork for subsequent discussions. This includes an exploration of their architecture, functions, and regulatory frameworks that govern their implementation.

Building upon this foundation, the second chapter examines various risk analysis methods employed in assessing SIS effectiveness. Techniques such as Fault Tree Analysis (FTA) and

Bayesian Networks provide insight into potential failure modes, enabling a systematic approach to risk mitigation.

The third chapter navigates the complexities associated with system selection and design types of SIS configurations, emphasizing their suitability for specific industrial applications. The decision-making process behind choosing an appropriate system is examined, considering factors such as redundancy, fault tolerance, and response time.

Finally, the fourth chapter focuses on quantifying SIS performance. This section presents calculations and evaluations related to reliability, availability, and dependability, ensuring compliance with functional safety standards. Through rigorous assessment, the effectiveness of SIS is determined, reinforcing its pivotal role in safeguarding industrial operations.

The work presented in this memoir aims to evaluate the performance in terms of reliability and dependability of safety instrumented systems equipped with functional safety standards.

The performance of a safety function can be expressed as the probability of failure on demand PFD and the probability of safe failure PFS. These two attributes are important for safety, and their values represent, respectively, a measure of the level of safety achieved (SIL) and the financial loss (frequent production stoppages) caused by the safety system due to nuisance tripping. The PFD value is a requirement to meet the safety integrity level of IEC 61508. For the PFS value, there are currently no prescriptions in the international safety world, although users require the PFS value to be as low as possible.

Chapter 1:

Safety Instrumented Systems (SIS)

I. Introduction

Safety assessment is nowadays an integral part of the strategy of a company, apart from quality, productivity, and profitability. Understanding the process of safety is the first step for minimizing the level of risk. Different mechanical instruments, such as basic process control system (BPCS) and safety instrumented system (SIS), are used to protect the company from undesirable events, where SIS is among the best instruments used to reduce the severity of consequences. Three essential parts: sensor, logic solver, and final element are necessary to carry out SIS functions.

Safety Instrumented Systems (SIS) play a critical role in industrial processes, ensuring the protection of personnel, assets, and the environment from hazardous events. These systems serve as a last line of defense, mitigating risks associated with process failures and enhancing overall operational safety. Given their importance, a comprehensive understanding of SIS, from foundational principles to performance evaluation, is essential. Furthermore, many companies, especially oil and gas industries, rely on the SISs to protect the workers, environment, and properties in case of undesirable events.

First, we will introduce the concept of the Safety Instrumented System (SIS) along with its key components and concepts related to Safety Instrumented Functions (SIF) and Safety Integrity Levels (SIL), explaining their operation, potential failures, and overall organization. Then, we will clarify essential terms frequently used in this field, such as system, hazard, risk, risk reduction, safety, and functional safety. Next, we will explore the regulatory framework governing SIS, with a particular focus on IEC 61508 and its sector-specific derivative standards.

I.1. Safety Instrumented Systems (SIS):

IEC 61508 [26] is concerned with functional safety, achieved by safety-related systems that are primarily implemented in electrical and/or electronic and/or programmable electronic (E/E/PE) technologies, i.e., E/E/PE safety-related systems. The standard is generic in that it applies to these systems irrespective of their application.

An E/E/PE safety-related system covers all parts of the system that are necessary to carry out the safety function (i.e., from sensor, through control logic and communication systems, to final actuator, including any critical actions of a human operator). [61508-0]

IEC 61511 [24] defines a safety instrumented system SIS*:*

" Instrumented system used to implement one or more SIFs

A SIS is composed of any combination of sensor (s), logic solver (s), and final elements. It also includes communication and ancillary equipment (e.g., cables, tubing, power supply, impulse lines, heat tracing).

A SIS may include software, and may also include human action as part of a SIF."

A SIS consists of any combination of:

S Sensor: a piece of equipment that delivers, from a physical quantity, another quantity, often electrical (voltage, current, resistance), which is a function of the first and can be directly used for measurement or control. [26]

LS (Logic Solver): part of either a BPCS or SIS that performs one or more logic functions.

In IEC 61511 terms, logic solvers are used: electrical logic systems for electro-mechanical technology, PE logic systems for programmable electronic systems. [26]

Examples are electrical systems, electronic systems, programmable electronic systems, pneumatic systems, and hydraulic systems. Sensors and final elements are not part of the logic solver.

FE (Final Element): final element part of the BPCS or SIS that implements the physical action necessary to achieve or maintain a safe state. [26]

Examples are valves, switch gear, and motors, including their auxiliary elements (such as a solenoid valve and actuator used to operate a valve).

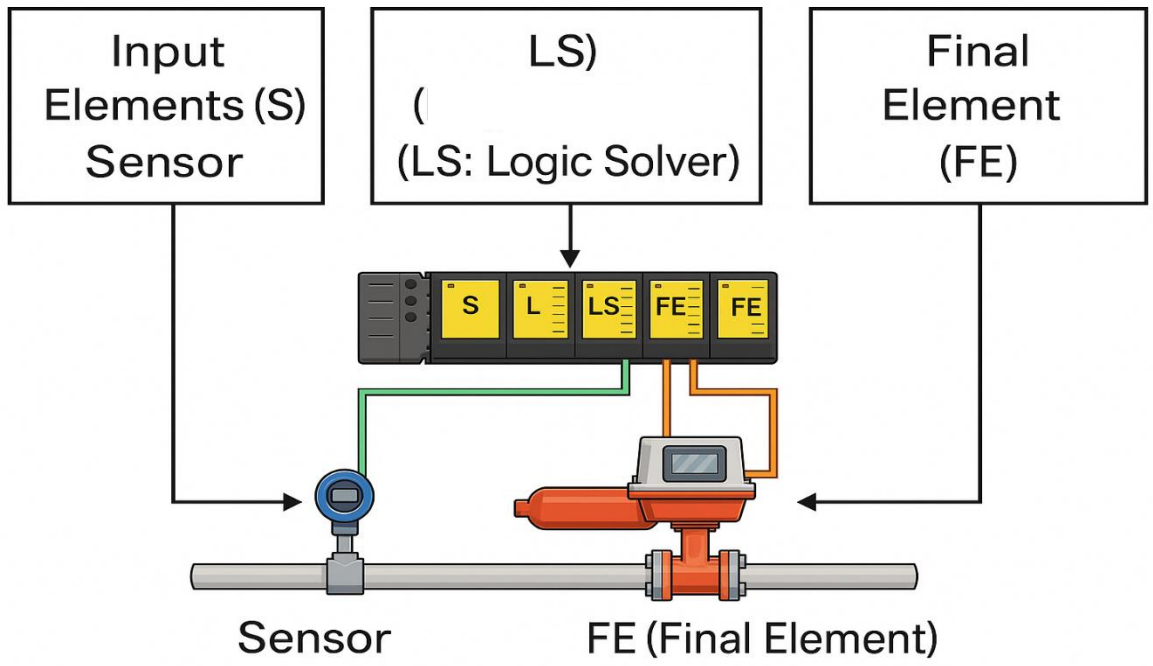


Figure 1.1: An example of SIS.

The "processing" function can be complex. It can be as simple as receiving an all-or-nothing signal from a sensor and triggering an actuator. It can also acquire several quantities measured by sensors, compare them, and activate the control of one or more actuators based on a combinatorial function of the information received. Processing units can be classified into two categories according to their technology:

- Wired technologies, based on elementary logic components (relays), linked together electrically (or pneumatically).

- Programmed technologies, based on acquisition or alarm control units, programmable logic controllers (PLCs), and programmable safety controllers (PSCs).

Actuators (motors, servomotors, etc.) transform a signal (electrical or pneumatic) into a physical phenomenon, enabling them to control the starting of a pump, the closing or opening of a valve, etc. Depending on the driving energy, they are referred to as pneumatic, hydraulic, or electrical actuators. They are coupled to terminal elements.

Terminal elements are elements controlled by an actuator. These include valves, rotating machines (pumps, compressors, etc.), and audible and visual alarms. It should be borne in mind that the

purpose of the safety function fulfilled by the SIS is to detect the dangerous phenomenon and to put these elements in their final safety position (open/closed, stop/start).

Finally, the processing unit is connected to the sensors and actuators by transmission means. These may be electric cables, telephone lines, Hertzian waves (walkie-talkie transmission, etc.), or pipes (pneumatic or hydraulic transmission).[38]

I.2. I Safety Integrity Level (SIL):

Safety Integrity Level (SIL) [37] is a measure used to determine the reliability of safety systems in reducing risks associated with hazardous industrial processes. Simply put, SIL quantifies the effectiveness of safety measures, providing a standardized way to assess whether a system can effectively mitigate risks to acceptable levels.

SIL is part of the functional safety framework, a set of standards designed to ensure that safety systems perform their intended functions even under fault conditions. These levels are assigned based on how likely a failure in a safety system might be and how severe the consequences of that failure could be. This serves as a key guide to how systems should be designed, implemented, and maintained to minimize hazards in high-stakes environments.

Importance of SIL Level

The safety integrity level plays a key role in safety and compliance. Benefits of SIL include:

- **Risk Reduction:** SIL levels help companies evaluate the effectiveness of safety systems, essential for protecting workers, avoiding costly shutdowns, and preventing environmental damage.
- **Industry Standardization:** SIL levels provide a universal language across sectors, simplifying communication between engineers, safety auditors, and decision-makers.
- **Compliance and Implementation:** SIL standards bridge regulatory requirements and practical application, ensuring that safety systems meet both compliance and functional expectations.

- **Benchmarking Safety Performance:** SIL levels serve as a benchmark, allowing organizations to align their safety practices with industry standards and maintain reliable safety systems.

Safety Integrity Levels Explained

When discussing Safety Integrity Levels (SIL), I often remind folks that these levels aren't arbitrary—they're structured to provide a tiered approach to safety, each level representing a step up in the reliability of a system to reduce risks. Depending on the potential consequences of a system failure, each SIL level dictates the amount of risk reduction required for a particular function.

SIL Level 1

SIL 1 is where most systems start, and for some lower-risk applications, it's often sufficient. When evaluating a SIL 1 system, look at risk reduction that is effective but not overly complex or costly. For instance, if a system failure has minor consequences, SIL 1 provides a basic level of safety assurance without over-engineering.

Systems at this level are reliable, but they're not intended to handle catastrophic failure situations. In practice, a SIL 1 system might be adequate for functions that, if they fail, wouldn't pose serious harm but still need some level of reliability.

SIL Level 2

SIL 2 steps up the risk reduction by requiring a higher degree of reliability. When we move to SIL 2, it's because the potential consequences of a failure are more severe, and we can't afford even a low failure rate. A SIL 2 system is often used in environments where failures could lead to significant financial loss, downtime, or environmental impact.

For instance, in a chemical plant, a SIL 2 safety system could oversee a pressure valve to prevent medium-risk failures. This level requires tighter controls and more frequent testing than SIL 1, making it a standard choice for medium-risk functions.

SIL Level 3

SIL 3 is where things get critical—this level is applied when a system failure could result in severe consequences, such as loss of life or major environmental hazards. SIL 3 systems are more complex and require rigorous design, testing, and maintenance to ensure they meet higher reliability standards. If a process needs a SIL 3 safety function, you can work with engineers to implement strict testing schedules and redundant systems.

For example, in the oil and gas industry, SIL 3 is commonly applied to emergency shutdown systems that prevent catastrophic events. Achieving SIL 3 compliance is no small feat—it requires significant investment, but for high-stakes operations, it's often a non-negotiable.

SIL Level 4

SIL 4 is the highest and rarest level, reserved for situations where failure is absolutely not an option. In my experience, SIL 4 systems are found in environments like nuclear facilities, where any error could have catastrophic consequences on a large scale. A SIL 4 rating demands an extreme level of reliability, achieved through complex redundancies, fail-safe mechanisms, and continual testing.

Due to the complexity and cost, SIL 4 isn't practical for most applications. However, when human life or critical infrastructure is at stake, this level provides the confidence needed for ultra-critical functions. Think of it as the "gold standard" of risk reduction—it's costly and intricate, but for the highest-risk scenarios, it's indispensable.

SIL Level Chart

Safety Integrity Level	Probability of Dangerous Failure per hour
SIL 4	$\geq = 10^{-9}$ to 10^{-8}
SIL 3	$\geq = 10^{-8}$ to 10^{-7}
SIL 2	$\geq = 10^{-7}$ to 10^{-6}
SIL 1	$\geq = 10^{-6}$ to 10^{-5}

Figure 1.2: Safety integrity requirements: average frequency of dangerous failures of SIF[22]

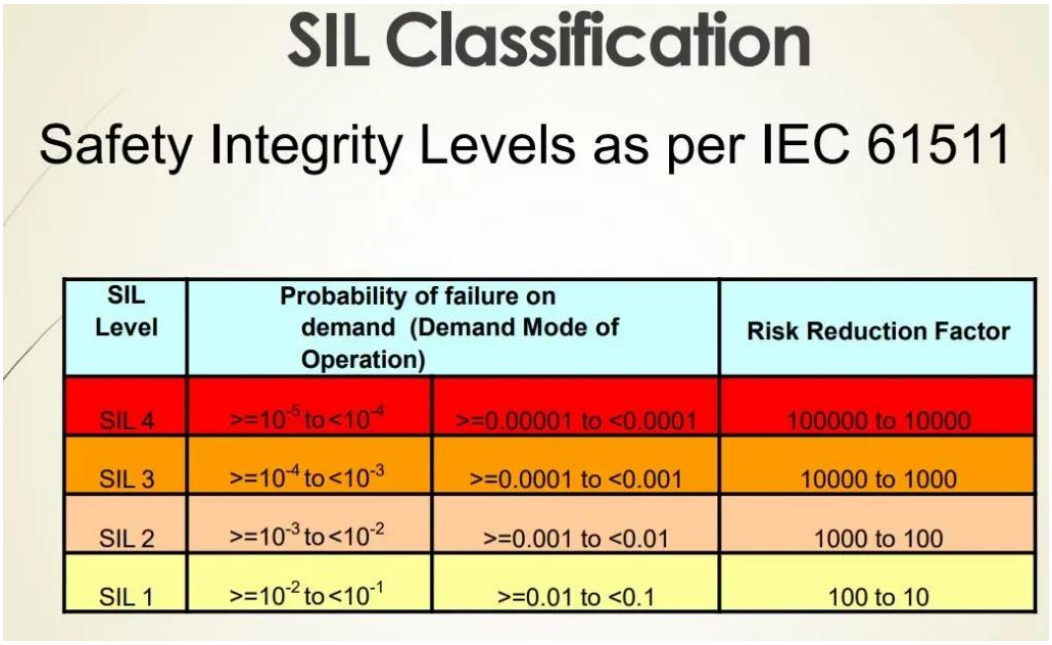


Figure 1.3: Safety integrity requirements: PFDavg[22]

The SIL Level Chart, as shown above, provides a quick reference to understand the reliability required for each SIL level, where:

- **probability of dangerous failure on demand PFD**: *safety unavailability (see IEC 60050-192)* [20] *of an E/E/PE safety-related system to perform the specified safety function when a demand occurs from the EUC or EUC control system* [IEC 61508-4]

This metric reflects the likelihood that a safety system might fail when it's called upon. A lower PFD means a higher level of reliability. For instance, a SIL 1 system has a PFD range between 0.1 and 0.01, meaning it has a higher chance of failure than a SIL 2 or SIL 3 system, which has progressively lower PFDs. [22]

- **average probability of dangerous failure on demand PFDavg**: *mean unavailability (see IEC 60050-192)* [20] *of an E/E/PE safety-related system to perform the specified safety function when a demand occurs from the EUC or EUC control system.*

Two kinds of failures contribute to PFD and PFDavg: the dangerous undetected failures that occurred since the last proof test and genuine on-demand failures caused by the demands (proof tests and safety demands) themselves. The first one is time-dependent and characterized by its dangerous failure rate $\lambda DU(t)$, whilst the second one is dependent only on the number of demands and is characterized by a probability of failure per demand (denoted by γ).

- **average frequency of a dangerous failure per hour PFH**:

The term "Probability of Dangerous Failure per Hour" (PFH) was introduced in the first edition of IEC 61508. This term is inappropriate because a probability is always unitless and therefore cannot be expressed "per hour". In fact, PFH is not a probability but a frequency. For this reason, in the second edition of IEC 61508, the PFH was redefined as "Mean Hazardous Failure Frequency per Hour". The abbreviation PFH was then kept for reasons of continuity, but the term "probability of a dangerous failure per hour" should no longer be used.

'Average frequency of a dangerous failure of an E/E/PE safety-related system to perform the specified safety function over a given period of time'

PFH is used instead of PFDavg when safety functions are not under low load (i.e., high or continuous load). PFH is defined by an average failure frequency (hazardous). A failure frequency is equivalent to an "unconditional failure intensity" and should not be confused with a "failure rate". To put it simply, when the values are constant, the unconditional intensity of

failure is the inverse of the Mean Time Between Failures (MTBF), while the failure rate is the inverse of the mean time to failure (MTTF). That is to say, the former takes the Mean Time To Restoration (MTTR) into account, while the latter does not.

When the E/E/PE safety-related system is the ultimate safety layer, the PFH should be calculated from its unreliability F(T)=1-R(t) (see "failure rate" above). When it is not the ultimate safety-related system, its PFH should be calculated from its unavailability U(t) (see PFD above). PFH approximations are given by F(T)/T and 1/MTTF in the first case and 1/MTBF in the second case.

- **Risk Reduction Factor (RRF):** This is the inverse of PFD and shows how much the system reduces the risk of a hazardous event. A higher RRF means the system offers greater risk reduction. For example, SIL 3 has an RRF between 1,000 and 10,000, meaning it reduces risk by that factor compared to having no safety system in place.

In practice, this chart is a key decision-making tool for safety officers, engineers, and risk managers. For example, if a process has the potential to cause serious harm, a higher SIL level (like SIL 3 or SIL 4) might be mandated to minimize the risk to an acceptable level.

On the other hand, for lower-risk scenarios, a SIL 1 or SIL 2 might be sufficient. It's a guide that translates risk management principles into actionable levels of system reliability, helping us design systems that match the safety demands of each unique industrial environment.

I.3. . I Safety instrumented function (SIF):

Definition :(SIF) [16] It is a safety measure that senses a potentially hazardous condition and automatically performs an action to return the process to a safe condition.

A SIF is implemented as a functional combination of sensors, a logic solver, and one or more final elements. A SIF will typically interrupt a chain of events, starting with a process upset and leading to a potentially hazardous situation. For a given SIF, this chain of events is referred to as the SIF-scenario (although the SIF in question might not be the only safety measure featured in this scenario). A typical example of SIF is a high-level protection comprising one or more level detectors, a programmable logic controller (PLC), and one or more valves in the feed line that will be closed when the liquid level reaches the trip point. Another example might be a high-pressure

protection on a reactor that initiates an action to stop the reaction when the temperature in the reactor reaches the trip point. This action can be closing a valve or stopping a pump in the feed line, opening a valve in an emergency dump line, or opening a valve to inject a killing agent to stop the reaction.

Risks introduced by the SIF. When a SIF is activated, it automatically performs one or more actions (e.g., closing or opening valves, starting or stopping motors, etc.). These actions are intended to stop the SIF scenario, but sometimes can create a (new) hazardous situation. For example, closing a valve can cause a fluid hammer or a deadheading pump. The risks of the action(s) by SIF should have been identified, and additional measures should be taken to manage these risks.

I.4. SIL /SIF /SIS :

The **Safety Integrity Level (SIL), Safety Instrumented Function (SIF)**, and **Safety Instrument System (SIS)** are three terms that often get lumped together but serve distinct purposes in functional safety. Each plays a critical role in safeguarding industrial processes, and understanding their differences can help you see the bigger picture of risk management.

To put it all together: **SIL** is the standard for reliability, **SIF** is the specific function that reduces the risk, and **SIS** is the entire system making sure these functions work as intended. Understanding these distinctions isn't just theory; it's practical knowledge that can make or break the safety and effectiveness of high-stakes processes. Each plays a part in a bigger risk management strategy, ensuring that safety mechanisms are both functional and reliable when it matters most. [4]

I.4.1. . I Summary of SIL, SIF, and SIS Implementation :

• SIL (Safety Integrity Level) defines the required performance of safety functions based on risk analysis and determines the necessary reliability of the system.

• SIF (Safety Instrumented Function) refers to a specific safety task or action that is designed to mitigate hazards, and each SIF is assigned a SIL based on the risk and required performance.

• SIS (Safety Instrumented System) is the system that incorporates multiple SIFs, ensuring that each safety action is taken when needed to reduce the risk to an acceptable level. [4]

I.4.2. . Implementation Steps:

1. Risk Assessment & SIL Assignment: Determine the safety integrity level for each safety function based on risk.

2. Design Safety Functions (SIFs): Define the safety actions and select components to meet the required SIL.

3. SIS Design & Integration: Design the overall safety system to implement SIFs and ensure system redundancy, diagnostics, and fault tolerance.

4. Verification & Validation: Perform functional testing, reliability analysis, and SIL validation to ensure that the system meets safety requirements.

5. Installation & Commissioning: Install the SIS, integrate SIFs, and validate the system's performance.

6. Operation & Maintenance: Monitor the system's performance, perform periodic proof testing, and maintain the SIS throughout its lifecycle.

By following these steps, you ensure that the safety system remains reliable, effective, and capable of meeting the required safety integrity levels throughout the lifecycle of the project.

I.5. . Systems for safety applications:

An E/E/PE (electrical/electronic/programmable safety electronics) system for safety applications comprises all the system elements required to fulfill the safety function. In other words, from the sensor, through the control logic and communication systems, right up to the final actuator, including critical operator actions.

Safety systems are defined in terms of the absence of unacceptable risk of injury or damage to people's health. Damage to people may be direct or indirect, such as damage to property or the environment. Some systems may be primarily designed to protect against failures with major economic implications. This means that, with comparable or identical technical objectives, there is no difference between a safety system and a control system. IEC 61508 [IEC61508, 2010] [21] and IEC 61511 [IEC61511, 2017] [9] can therefore be used to develop any I/O/PE system with critical functions, such as protection of equipment, property, or productivity.

I.6. FUNCTIONAL SAFETY :

DÉFINITION:

According to the IEC 61508 standard [26], functional safety represents a subset of overall safety and is based on the proper functioning of a system or equipment in response to its inputs.

The IEC 61508 standard defines functional safety as a subset of overall safety, closely connected to the machine and the control system. It depends on the proper functioning of electrical safety control systems, which may be composed of other technologies and third-party risk reduction devices. [21]

Functional safety, therefore, aims to prevent unacceptable risks that could:

- Cause injury.
- Directly or indirectly affect human health.
- Neglect the environment.
- Damage property. It also applies to products and systems that incorporate protective solutions based on different technologies, including:
- Mechanical, hydraulic, pneumatic, electrical, electronic, programmable electronic, optical, etc.
- Or a combination of these technologies.

I.6.1Hazard concept

Definitions:

According to [Desroches, 1995] [1] and theIEC61508 safety standard [IEC61508, 2010] [22], the danger does means potential harm that may affect property (deterioration or destruction), the environment, or people, Hazards can have a direct impact on people, through physical injury or death or ill health, or indirectly, through damage to the environment.

According to the OHSAS18001 standard [OHSAS18001, 1999] [35], a hazard is a source or situation that may result in injury or damage to health, property, or the environment

or a combination of these.

It’s worth noting that many terms are used, depending on the standard or the author, to describe the notion of danger and its ambiguity.

Furthermore, dictionaries often associate the term “danger” with “risk”.

In fact, several dictionaries propose “risk” as a synonym for the term “danger”.

Synonymous with the term danger, which explains why so many people use the term

Even official documents and texts conflict between danger and risk.

I.6.2 Notion of risk

The perception of potential damage associated with a dangerous situation is related to the notion of risk. The term risk has many meanings. Similarly, risks can be very varied in nature, and many classifications have been proposed.

The definitions of two-dimensional risk are quite similar. According to [Villemeur, 1998] [2], risk is a measure of a hazard, combining a measure of the occurrence of an undesirable event and a measure of its effects or consequences.

And according to the OHSAS 18001 standard [OHSAS18001, 1999] [35], a risk is the combination of probability and consequence(s) of occurrence.

However, there are slightly more complex definitions than those of [Villemeur, 1998] [2] and the OHSAS 18001 standard [OHSAS18001, 1999], in which a third dimension appears: risk acceptability, the threshold below which the existence of a hazard is accepted, even though its severity and probability of occurrence are not zero. It should also be noted that Périlhon [Périlhon, 1998] [36] proposes a logical method for highlighting most of a facility’s risks: the organized systemic risk analysis method or MOSAR. It involves breaking down the facility into sub-systems and systematically investigating the hazards presented by each of them. These sub-systems are then linked together to reveal major risk scenarios. The process may continue with a detailed analysis of the operational safety type. It ends with the construction of intervention plans.

Risk can be modeled in a general and elementary way by measuring its criticality C, which is a function of its severity G and its probability of occurrence P: C =P G (2) In general, risk refers to the pair (severity, probability). In most cases, this is the product of the severity of an accident and

its probability of occurrence. Farmer has classified risk into two categories: acceptable risk and unacceptable risk, based on the function G = f(P), as shown by the curve in Fig. 2



Figure 1.4: Risk Acceptability Curve Based on Probability and Severity

I.6.3 Risk classification

There are several classifications of risk in the literature. According to [Tanzi and Delmer, 2003] [42], risk analysis enables us to classify risks into five main categories:

- natural risks: floods, forest fires, avalanches, storms, earthquakes, etc.

- technological hazards: man-made, including industrial, nuclear, biological, and dam-break hazards; public transport hazards (people, hazardous materials) are also considered technological hazards.

- everyday risks: domestic accidents, road accidents, etc.

- conflict-related risks.

One of the most widespread classifications of hazards is that of natural and man-made.

According to this classification, risks can be natural in the sense that they relate to an event with no proven direct human cause. Assumed direct or indirect causes should not alter this distinction.

Risks linked to human activity cover a range of different risk categories:

- technical, technological, industrial, and nuclear risks;

- transport-related risks

- health risks;

- economic, financial, and managerial risks;

- media risks.

- professional risks.

Finally, we can characterize the operation of risk classification by the following two types of classification:

- Subjective" classification by individuals, based on their idea of risk and their experience and knowledge, or 'objective' classification, based on statistical data, surveys, etc.

- Qualitative" ranking characterized by the establishment of a system of comparative or 'quantitative' order based on the calculation of probabilities.

I.6.4 Acceptable risk

The notion of risk is essential to characterize the confidence attributed to a system. Indeed, while we often accept severe damage as potential, it is only their low probability of occurrence that makes us accept them [Lamy et al., 2006; Simon et al., 2007] [30] [41]. For example, we continue to fly despite possible accidents because the probability of a crash resulting in the death of passengers is extremely low. We usually make this trade-off in relation to the risks we might otherwise incur, such as those induced by natural phenomena like earthquakes, avalanches, or floods.

According to the OHSAS 18001 standard [OHSAS18001, 1999] [35], acceptable risk is a risk that has been reduced to a tolerable level for an organization in terms of its legal obligations and its own occupational health and safety policy.

According to ISO/IEC Guide 51 [ISO, 1999] [27], acceptable risk is a risk that is accepted in a given context, based on current societal values.

It should be noted that acceptability refers to the risk, and not to the severity of the damage or its probability of occurrence considered separately. These definitions also underline the fact that acceptability depends on the current values of our society, often based on data associated with natural phenomena. For example, we accept the risk of dying by flying if the probability of death from this cause is the same or even lower than the probability of death from an earthquake or heart attack (for a healthy body) [Beugin, 2006] [5].

The definitions also specify that acceptability is a function of context. This context may firstly characterize the state of knowledge about practices or the implementation of technology.

I.6.5 Major risk

A major hazard is characterized by the number of victims, the cost of material damage, and the impact on the environment [Tanzi and Delmer, 2003] [42]. Major risk is characterized by two criteria that define its frequency and severity:

- low frequency.

- high severity (many deaths and injuries)

I.6.6 Industrial risk

Industrial risk is characterized by an accident occurring on an industrial site that could have serious consequences for personnel, the population, property, the environment, or the natural surroundings [34].

Actions to prevent major industrial risks are based on knowledge of the feared phenomena, notably through hazard studies. This prevention is based on four main principles.

- Risk control at source.

- Controlling urban development.

- Emergency organization.

- Preventive information and consultation.

I.6.7 Notion of safety

Safety is often defined by its opposite: the absence of danger, risk, accident, or disaster.

According to [Desroches et al., 2003] [15], safety relates to the non-occurrence of events that could diminish or damage the integrity of the system throughout the entire duration of the system's activity, whether this activity is successful, degraded, or has failed.

According to the ISO/IEC 73 guide [ISO, 2002] [28] drawn up by the ISO (International Organization for Standardization) on risk management terminology, safety is the absence of unacceptable risk, injury, or damage to people's health, directly or indirectly, resulting from damage to equipment or the environment.

It should be noted that in the context of industrial installations, we speak of the safety of installations regarding accidents and safety regarding voluntary external attacks (such as malicious acts or terrorist attacks), malicious intrusions, and internal malicious acts.

I.6.8 General principles of protection

We can distinguish between passive and active safety measures [34].

I.. 6.8.1 Passive safety features

Passive safety refers to all the elements brought into play to reduce the consequences of an accident when it cannot be avoided. It acts by its very presence, without human intervention or energy requirements (e.g., containment building, retention basin, etc.). However, passive safety must not be reduced to limiting the consequences of accidents (electrical insulation is a passive, preventive measure).

I.. 6.8.2 Active safety features

Active safety refers to all elements used to prevent accidents. It requires action, energy, and maintenance (e.g., detectors, valves, etc.).

The safety of an installation is based on the use of these two modes of action. Preference is given to the passive mode whenever technically possible. Quality criteria are required for the active

mode, notably tolerance to the first failure: doubling the safety device (redundancy). Functional safety remains one of the most important ways of addressing risks. Other means of reducing or eliminating risk, such as design-integrated safety, are also essential.

I.7. I standards relating to safety instrumented systems:

Instrumented safety systems are not new. It has long been the practice to fit protective systems to industrial process plants where there is a potential threat to life or the environment, should something go wrong. These systems are independent of the normal process control and take some action to render the plant safe in the event of a malfunction.

Until recently, such systems have generally been designed according to established practice within the company concerned, or in accordance with local codes of practice. Some of the necessary equipment, for example, shutdown control systems, was available, designed, and certified for safety applications, but much of the peripheral equipment was not. Designers and installers had to do the best they could with the equipment that was available.

This situation is now changing rapidly. The broad acceptance of the IEC 61508 standard is giving safety equipment suppliers and users a common framework on which to design products and systems for safety-related applications.

I.7.1 IEC 61508 standard:

The IEC 61508 standard addresses the functional safety of electrical/electronic/programmable electronic systems to perform safety-related instrumented functions in most industrial sectors. This standard, whose foundation is based on functional safety management, is based on a life cycle bringing together all the stages, ranging from the identification of dangers, the creation of the system, to its removal.

This voluminous standard gives a lot of information concerning both hardware and software methods for achieving the required level of security. One of the key points of this standard is the approach in terms of quantification of failures corresponding to the four safety integrity levels (SIL).[39]

The Structure of IEC 61508

The overall title of IEC 61508 is “Functional safety of electrical, electronic and programmable electronic (E/E/PE) safety-related systems”. The Parts are as follows:

• Part 0: Functional safety and IEC 61508. Note: This has the status of a Technical Report and is purely informative.

• Part 1: General Requirements.

• Part 2: Requirements for electrical, electronic, and programmable electronic systems.

• Part 3: Software Requirements.

• Part 4: Definitions and abbreviations.

• Part 5: Examples of methods for the determination of safety-integrity levels.

• Part 6: Guidelines on the application of Parts 2 and 6.

• Part 7: Overview of techniques and measures.

Since its creation, several derivatives of this standard (called daughter standards) have emerged. Each time, these daughter standards were created to make EN 61508 applicable for the different sectors concerned. [21]

These sectoral standards are as follows:

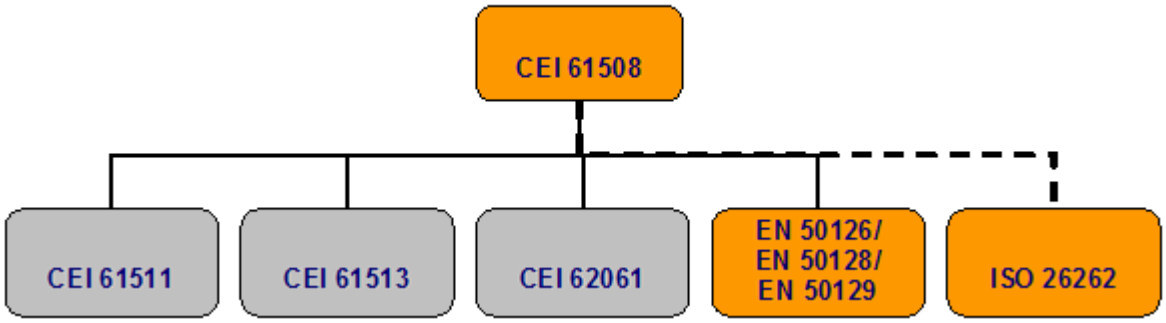


Figure 1.5: IEC 61508 standard

The IEC 61511 standard, created in 2003, is the standard adapted from the IEC 61508 standard for industrial processes.

The IEC 61513 standard, created in 2001, is the standard adapted from the IEC 61508 standard for the nuclear sector.

The IEC 62061 standard, created in 2005, is the standard adapted from the IEC 61508 standard for machine safety.

The EN 50126/EN 50128/EN 50129 standards, created respectively for the latest versions, in 1999/2001/2003, are standards adapted from the IEC 61508 standard for the railway sector.

The ISO 26262 standard is currently being produced, and its release is planned for 2009. This is the adaptation of the IEC 61508 standard for the automotive sector. [13]

I.7.2 The IEC 61511 standard:

The IEC 61511 [9] standard concerns functional safety for safety instrumented systems (SIS) applications in Process Industries. The standard requires carrying out process hazard and risk assessment to deduce SIS specifications. Two main concepts, which are fundamental according to the application, are underlined: safety lifecycle and safety integrity levels.

Part 1 – This is the only normative part of the series. She understands the terminology and requirements

Part 2 – This is an informative guide to Part 1.

Part 3 – informative part of the series which provides information on the methods available for carrying out a Hazard and Risk Assessment (H&RA) to determine integrity requirements, i.e., Safety Integrity Level (SIL).

Part 4 – This is actually a technical report. It contains explanations and justifications for the changes made between edition 1 and edition 2.

The IEC 61511 [10] standard is one of the variations of the IEC 61508 standard. SIS constitutes the main subject of these two standards, but they are considered differently depending on the professions they are aimed at

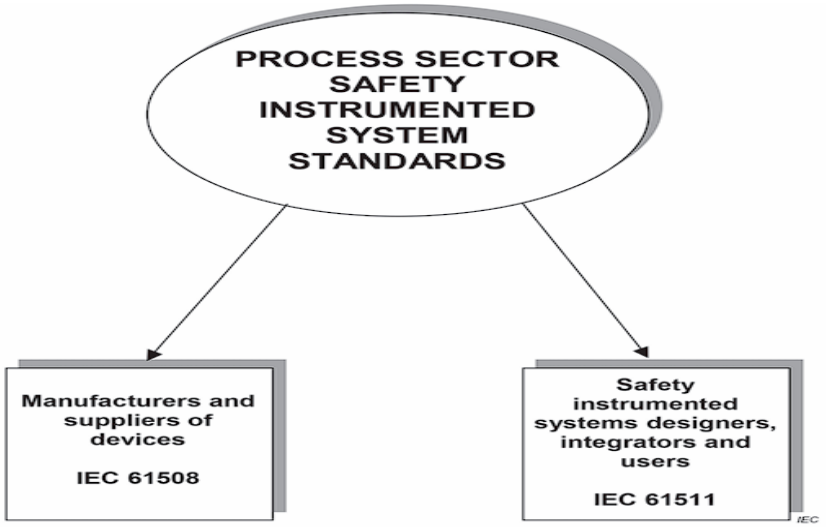


Figure 1.6: Relationship between IEC 61511 and IEC 61508

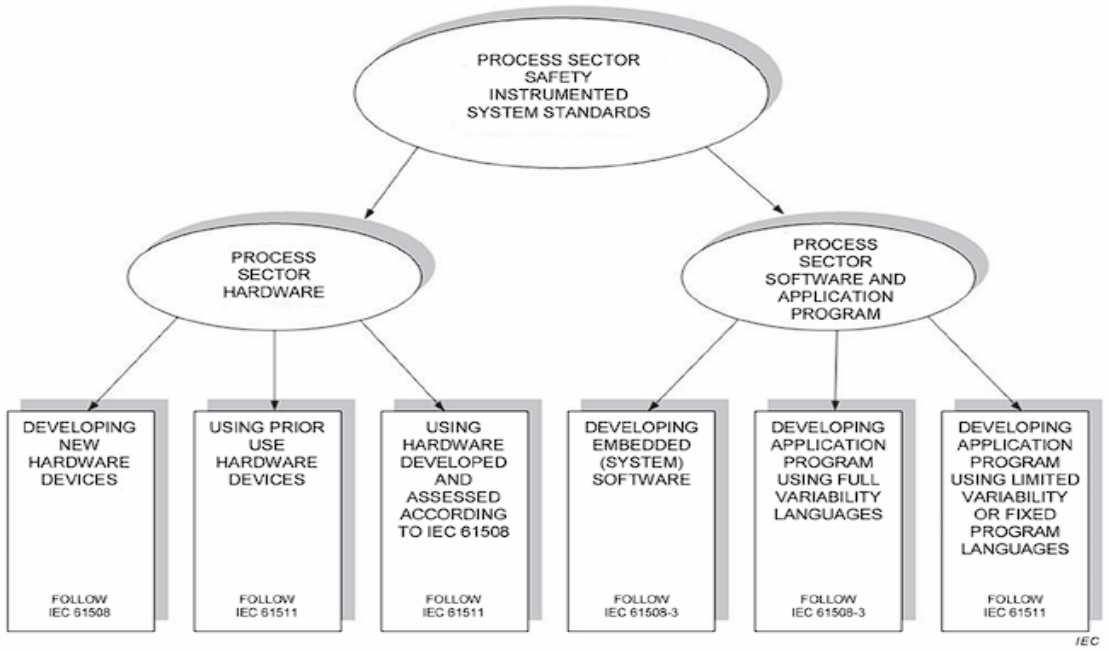


Figure 1.7: Detailed Relationship between IEC 61511 and IEC 61508

IEC 61508 is a complex standard, difficult to implement, and it is intended especially for manufacturers and suppliers of E/E/EP systems, while the standard IEC 61511 is easier to use; it presents a simplification of IEC 61508 by limiting it to the elements necessary for the process industry.

I.7.3 The IEC 61513 standard

IEC 61513 [25] concerns the safety sector of nuclear power plants. She presents the requirements relating to the control systems used to accomplish the safety functions of nuclear power plants. The design of control systems can be achieved using a combination of traditional hardwired components and computer components. Compliance with IEC 61513 facilitates compatibility with the requirements of IEC 61508 as they have been interpreted in the nuclear industry.

I.7.4 The IEC 62061 standard

IEC 62061 [23] is based on the same concepts as those of IEC 61508. She is intended for use by machine designers and manufacturers of electronic control systems, controls relating to machine safety. It concerns the specification of requirements and makes recommendations for the design, integration, and validation of these systems.

I.7.5 Standards EN 50126/EN 50128/EN 50129 :

- **The EN 50126 standard** – "Specification and demonstration of reliability, availability, maintainability and safety" **[6]:**

This standard makes it possible to implement a coherent approach to managing reliability, availability, maintainability, and security called RAMS. This standard can be applied in the railway sector throughout the life cycle because it integrates the RAMS requirements specific to this area.

- **The EN 50128 standard** – "Signaling, telecommunications and processing systems" **[7]:**

This standard deals with the methods that must be used to provide software that meets the safety integrity requirements applied to the railway sector. The integrity of software is distributed over five SIL levels, ranging from SIL 0 to SIL 4. These SIL levels are defined by association in the management of risk, frequency, and consequence of a dangerous event. To precisely define the SIL level of software, techniques and measures are defined in this standard.

- **The EN 50129 standard –** "Railway applications – Electronic safety systems for signaling" [8]:

This standard addresses all points related to the approval process of individual systems, whether software or hardware, and which may exist as part of an overall system. This standard defines the evidence to be provided for the acceptance of each individual system based on its SIL integrity level.

I.7.6 ISO 26262 standards :

The ISO 26262 standard, also called ISO/CD 26262, is currently being drafted and should be released in 2009. This new standard redefines the five SIL (Safety Integrated Level) integrity levels of the IEC 61508 standard into four ASIL (Automotive Safety Integrated Level) integrity levels ranging from ASIL A to ASIL D. The ASIL level is determined by a risk analysis considering the evaluation severity, controllability, and relative exposure to feared events. [11]

I.8 Conclusion:

In the realm of industrial safety, **Safety Instrumented Systems (SIS)** stand as a critical line of defense, ensuring that risks are mitigated and operations remain secure. By integrating **functional safety principles** and adhering to industry standards like **IEC 61508,** precisely the **IEC 61511,** organizations can systematically reduce the probability of failures and their potential consequences. Understanding these systems, their components, and their role in risk reduction is the first step toward building a resilient safety strategy.

However, identifying safety measures alone is not enough. To truly safeguard industrial processes, we must delve deeper into **risk analysis methods** and the systematic approaches that allow us to assess, quantify, and manage potential hazards. In the next chapter, we will explore the methodologies used to evaluate risk, understand its classifications, and determine how to implement effective safety measures tailored to specific industrial challenges.

Chapter 2:

Risk analysis methods

II.1 Introduction

The necessity of expertise for tackling the complicated and multidisciplinary issues of reliability and risk analysis has slowly permeated into all engineering applications, with risk analysis and management gaining a relevant role both as a tool in support of plant design and operation, and as an indispensable means for emergency planning in accidental situations.

Failure is an inevitable aspect of all technological products and systems. From a scientific and engineering perspective, understanding the uncertainty and complexity of failures requires an exploration of a system's functional and physical limits. This involves identifying how, why, and when a device may fail—an approach that complements traditional engineering methods focused on achieving optimal performance.

Managing and mitigating failures effectively is fundamental to ensuring system reliability. Several fields, such as Reliability, Availability, Maintainability, and Safety (RAMS), Risk Management, and Quality Control, revolve around failure analysis and prevention. Within this context, various risk analysis methods have been developed to evaluate hazards and improve system performance. Therefore, in this chapter, the focus will now shift to an in-depth exploration of **FTA, BN, and RBD**, analyzing how they contribute to risk assessment and decision-making in complex engineering systems.

II.2 Definition:

Risk analysis is a multi-step process aimed at mitigating the impact of risks on business operations. Leaders from different industries use risk analysis to ensure that all aspects of the business are protected from potential threats. Performing regular risk analysis also minimizes the vulnerability of the business to unexpected events.

Risk assessment is just one component of risk analysis. The other components of risk analysis are risk management and risk communication. Risk management is the proactive control and evaluation of risks, while risk communication is the exchange of information involving risks. Unlike risk analysis, risk assessment is primarily focused on safety and hazard identification**.**

Types of Risk Analysis :

There are two primary risk analysis methods: qualitative and quantitative.

- **Quantitative Risk Analysis :**

  where we predict the frequency of hardware failures and compare them with some tolerable risk target. If the target is not satisfied, then the design is adapted (e.g., provision of more redundancy) until the target is met **(**Calculates risk using available data)

- **Qualitative Risk Analysis :**

  where we attempt to minimize the occurrence of systematic failures (e.g., software errors) by applying a variety of defenses and design disciplines appropriate to the severity of the tolerable risk target.

  - Easier and more convenient.
  - Rates risks based on perceived severity and likelihood.

Qualitative analysis tools include all root cause analysis (RCA) tools except failure mode and effects analysis, needs assessment, and risk matrix. Common quantitative types include the 3×3, 4×4, and 5×5 risk matrix.

RISK ASSESSMENT MATRIX				
SEVERITY / PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

Figure 2.1: Risk assessment matrix

II.3 Fault tree analysis (FTA):

Definitions:

The IEC 60050-192 [20] defines the Fault tree as 'a *logic diagram showing the faults of sub-items, external events, or combinations thereof, which cause a predefined, undesired event'*

Fault tree analysis is a deductive, top-down approach to determining the cause of a specific undesired event within a complex system. It involves breaking down the root cause of a failure into its contributing factors and representing it through a graphical model called a fault tree, which helps managers and engineers identify potential failure modes—and the probability of each failure mode—for safety and reliability analyses.

Fault tree analysis (FTA) offers one approach to root cause analysis, identifying and analyzing the root of asset issues before equipment breaks down. FTA helps in manufacturing facilities, where understanding the potential causes of system failures is crucial to preventing them.[19]

First developed in the early 1960s by Bell Laboratories to help the US Air Force understand potential flaws in the Minuteman missile system, FTA has been widely used across various industries, including the aerospace, nuclear power, chemical, and automotive sectors, among others.

Maintenance managers might use fault tree analysis to:

- Design and/or install a new system.
- Make changes to existing systems.
- Investigate system safety or system reliability.
- Assess regulatory compliance.
- Optimize maintenance budgets.

As manufacturing environments continue to evolve and become more complex, the need for effective risk management tools like FTA becomes increasingly important. Incorporating fault tree analyses into your organization's safety analyses and reliability engineering practices can help your

organization gain deeper insights into potential causes of system failure. FTA can also help improve overall performance and reduce the likelihood of costly and potentially catastrophic incidents.

II.3.1 Fault tree analysis symbols:

Every industry uses the same set of symbols and naming conventions for fault trees. The fault tree illustrates the link and flow between different activities and is read from top to bottom. Events and gateways (known as gates) are the two categories under which the activities fall. [17]

Event symbols:

Events occur when a system or process fails. The types of events that appear in fault trees have been detailed below.

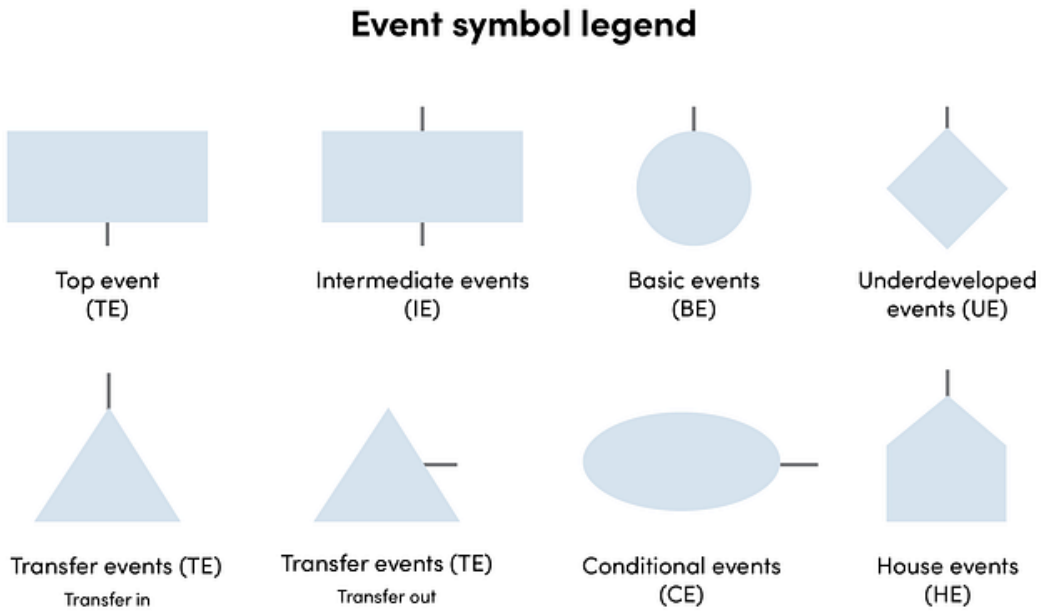


Figure 2.2: Types of event symbols [17]

Below are definitions of each event type illustrated above:

- Top event (TE): These types of events are at the top of the fault tree and prompt an investigation into the system failure. It has a single input but no relative outputs because it is the start of the failure.
- Intermediate events (IE) are located between the lower-level basic events and the top event (the primary undesired event being analyzed). Intermediate events are caused by other events in the fault tree and, in turn, cause other events. They represent higher-level events that can be analyzed further.
- Basic events (BE): events that cannot be further broken down into simpler events are the most fundamental events in a fault tree, representing the lowest level of events you can analyze.
- Underdeveloped events (UE): These events don't have enough information and are placed as a subtree.
- Transfer events (TE): These types of events happen when a fault tree is too long to fit on paper. Larger parts of the tree are hidden with a symbol and expand into a separate tree. There are two types: Transfer-out and transfer-in events. Transfer-out has a triangle and output to the right, and transfer-in events have input on the top of the triangle.
- Conditional events (CE): These events happen as conditions for a type of gate called an inhibit gate.
- House events (HE): These types of events are used to turn an event off and on. If the event is set to 0, it means it will not occur, but if it is set to 1, it means that it will occur. House events are used to allow parts of the fault tree to be included or not included.

Gate symbols

Gates represent the various ways that failures can occur in an asset or system. Sometimes a single event can cause a top-level failure (or catastrophic failure). Sometimes, a combination of different events can cause a top-level failure event.

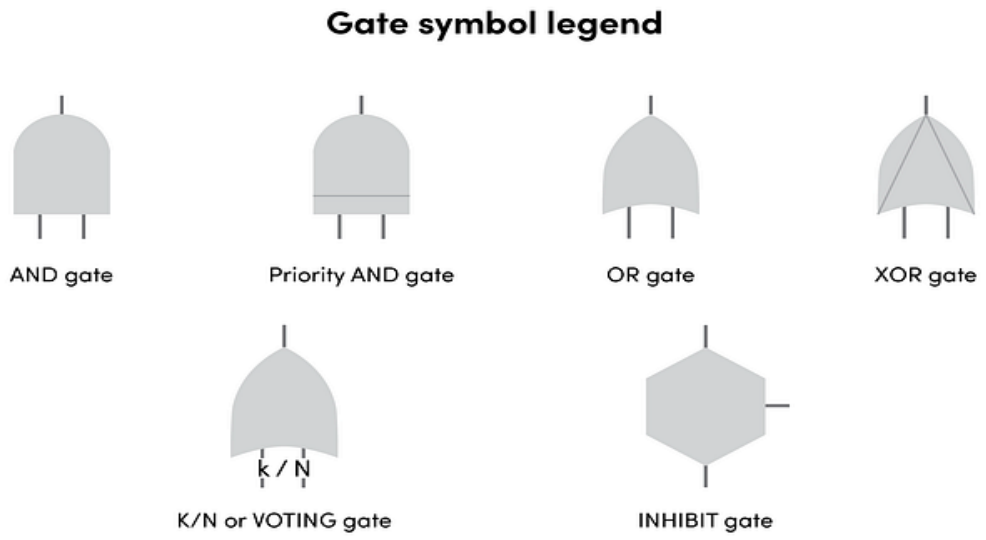


Figure 2.3: types of gate symbols[17]

There are two main types of logic gates used in fault trees: **AND gates** and **OR gates**.

- **AND gates**: Use AND gates when all contributing events must occur simultaneously for the undesired event to occur. For example, if a system failure requires both a component failure and an operator error, an AND gate is used to connect the events in the fault tree.
- **OR gates**: Use an OR gate when any one of the input events is sufficient to cause the output event. In other words, the output event happens if at least one of the input events connected to the OR gate happens. For instance, if a system failure might result from either a component failure or an operator error, an OR gate would be used to connect these events.

Though less commonly used, **NOT gates**, **XOR gates**, **K/N gates**, and **INHIBIT gates** can also help identify specific relationships between input and output events.

- **NOT gates**: NOT gates represent the inverse of an input event. If the input event does *not* occur, the output event will occur. These gates are less common in fault tree analysis, since they model the absence of an event or the occurrence of a complementary event.

- **XOR gates** (Exclusive OR gates): Use an XOR gate when exactly one of the input events must occur for the output event to happen. If none or more than one of the input events occur, the output event will not happen.
- **K/N gates**: K/N gates, also known as voting gates or threshold gates, are used when a specific number of the input events (K) out of all the possible input events (N) must occur for the output event to happen. A K/N gate can help you illustrate more complex relationships in a fault tree analysis.
- **INHIBIT gates**: Like an AND gate, an INHIBIT gate indicates that an output event will occur if both input events and a conditional event (a condition or restriction that can apply to any gate) occur. [19]

II.3.2 Fault tree analysis steps:

Fault tree analysis is often carried out in five steps:

1. Definition of the problem, system, and boundary conditions of the analysis
2. Construction of the fault tree
3. Identification of minimal cut sets
4. Qualitative analysis of the fault tree
5. quantitative analysis of the fault tree.[12]

Fault Tree vs Reliability Block Diagram:

A fault tree may be converted into a reliability block diagram and vice versa, as illustrated below [12].

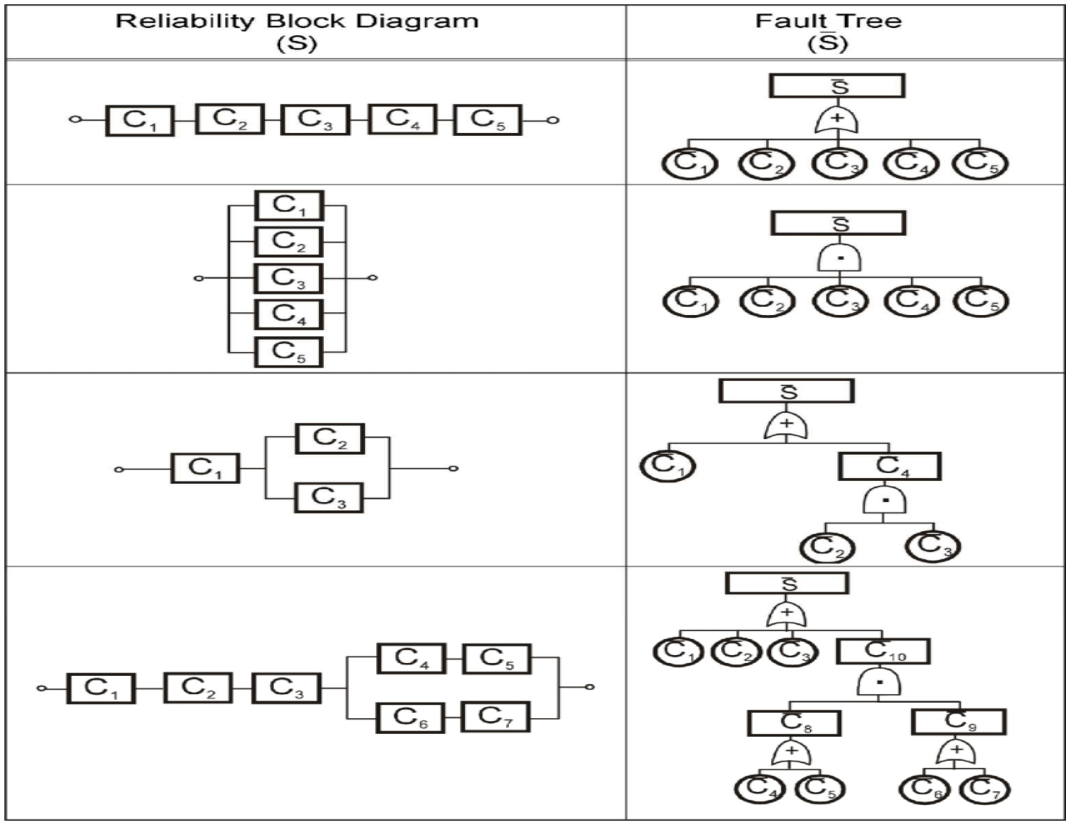


Figure 2.4: Fault Tree to Reliability Block Diagram

Minimal Cut Sets:

Identification of minimal cut sets is one of the most important qualitative analyses of a fault tree.

- Cut set: A cut set in a fault tree is a set of basic events whose (simultaneous) occurrence ensures that the TOP event occurs.
- Minimal cut set: A cut set that cannot be reduced without losing its status as a cut set.

The TOP event occurs if one or more of the minimal cut sets occur. [33]

Qualitative Analysis

Qualitative analysis of the fault tree may include:

- Analysis of minimal cut sets, including:

• To identify and verify any single points of failure?

• To identify those other main contributors (e.g., for minimal cut sets up to order 3) seems correct

- Common cause and dependency analysis:

• This may include checking if logical events connected by local AND-gates are independent

• Review minimal cut sets up to e.g. order 3 to check if there are dependencies and if they must be modelled. [33]

Quantitative Analysis

- The main challenge is therefore to identify the minimal cut sets
- If all minimal cut sets were independent, we could calculate the probability of the top event by:

$$Q_0(t) = 1 - \prod_{j=1}^{k} [1 - Q_j^{\vee}(t)]$$

where $Q_j^{\vee}(t)$ is the failure probability of minimal cut set Cj:

$Q_j^{\vee}(t) = \prod_{i \in C_j} q_i(t)$

Upper Bound Approximation

- In reality, the minimal cut sets will not (normally) be independent, since the same basic event may belong to the several minimal cut sets. [33]
- This type of dependency is called positive dependency, which increases the reliability.
- I This "double counting" of basic events results in a higher failure probability of the TOP event, and consequently, we can claim that the "true" TOP event failure probability will be lower than:

$$Q_0(t) \leq 1 - \prod_{j=1}^{k} [1 - Q_j^{\vee}(t)]$$

And we can therefore use this formula as a conservative approximation for the calculations.

Failure Probabilities at Basic Event Level

Consider the state of the basic event $\boldsymbol{E_i}$ The choice of failure probability is dependent on the following factors:

- **Alternative 1:** The item is in continuous operation and non-repairable.

In this case, we may be interested in the probability that item i has failed at time t, qi(t), which is:

$\boldsymbol{q_i(t)}$**= Pr[** $\boldsymbol{E_i(t)}$**] = Pr(T < t)**

If we assume exponential time to failure, qi(t) becomes:

$\boldsymbol{q_i(t)= 1 - e^{-\lambda_i t}}$

- Alternative 2: The item is in continuous operation and repairable. We assume that the item runs to failure and is then repaired. In this case, we may want to determine the mean unavailability of the item: (stand by)

$\boldsymbol{q_i}$**=MTTRi/ MTTFi + MTTRi≈ λiMTTRi**

where **MTTRi** is the mean time to repair, and **MTTFi** is the mean time to failure.

Note that we here have assumed (again) exponentially distributed time to failure so

that 1/**MTTFi** = **λi**

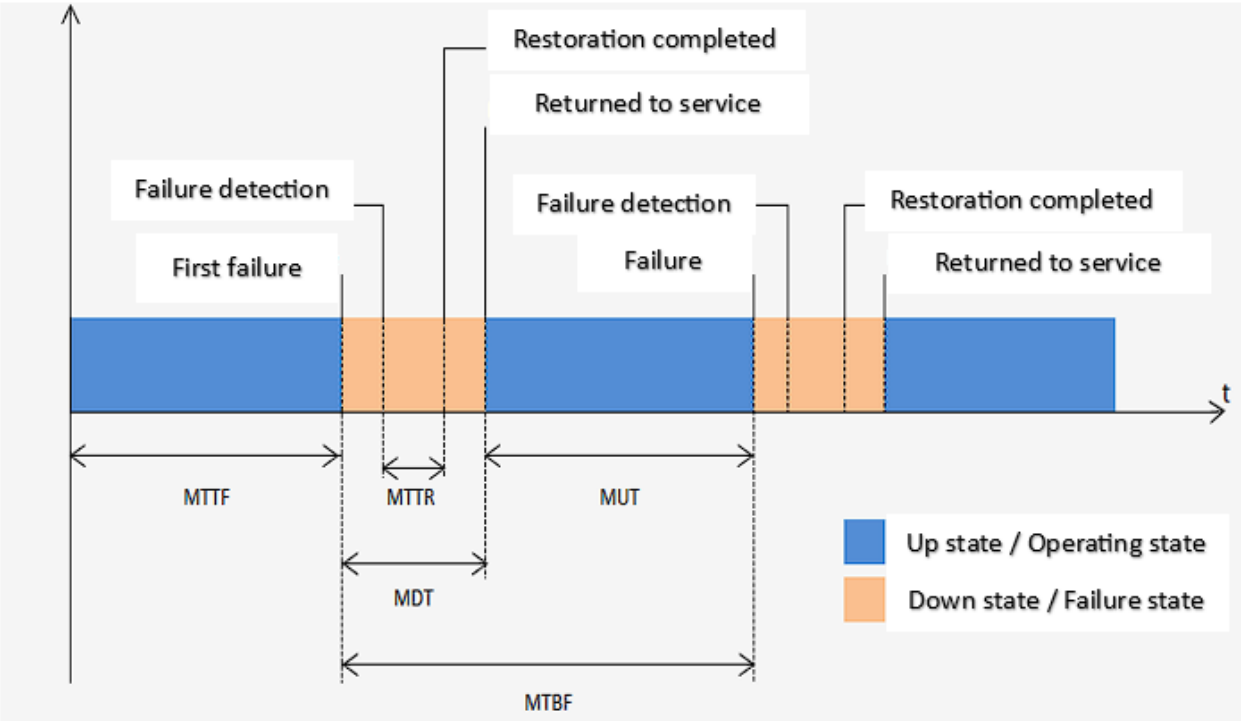


Figure 2.5: Equipment Life Cycle

MTTF: Mean Time to Failure

MTBF: Mean Time Between Failures

MTTR: Mean Time to Repair

MUT: Mean Up Time

MDT: Mean Down Time

- Alternative 3: Periodic testing

Unit I is tested periodically with a test interval τ. A failure may occur at any time in the test interval, but the failure is only detected in a test or if a demand for the unit occurs.

After a test/repair, the unit is assumed to be “as good as new”.

This is a typical situation for many safety-critical units, like sensors and safety valves.

Input data:

►Failure rate λi

►Test interval τi

Basic event probability:

$$q_i(t) \approx \lambda_i \cdot \tau_i / 2$$

II.4 Limits of FTA:

2. Assumes Event Independence

- FTA typically assumes that all basic events are independent.
- In real systems, many failures are interdependent (e.g., a power surge causing multiple components to fail).

2. Static and Non-Recursive

- FTA is static—once the tree is built, it doesn't evolve with new information.
- It cannot model feedback loops or dynamic behaviors in systems.

3. One-Way (Top-Down) Reasoning Only

- FTA works top-down: from a system failure to its causes.
- It doesn't support diagnostic reasoning (e.g., what is the most likely cause given an observed fault).

4. Limited with Uncertainty

- FTA uses fixed probabilities and lacks a natural way to handle uncertain or imprecise data.
- It can't easily deal with missing or evolving data.

5. Poor at Representing Complex Logic

- FTA handles AND/OR gates well but struggles with:
    - Conditional logic (e.g., component A fails *only if* component B also fails)
    - Sequential dependencies (e.g., failure happens if one thing fails *before* another)

6. Inflexible to Updates

- If a system changes, you may need to rebuild the entire fault tree.
- Not ideal for dynamic systems that change over time.

7. No Learning from Data

- FTA does not learn from operational data.
- It's purely analytical, not data-driven.

- The accuracy and effectiveness of FTA rely heavily on the expertise of the analysts, their ability to identify relevant causes of failure, and their understanding of the complexities of the fault tree itself.
- FTA is best suited for smaller system analyses. Large, complex systems typically require large, complex fault trees, making analysis time-consuming and challenging.
- Failure data availability and quality determine the precision of the calculated probabilities in a fault tree.
- Fault tree analysis allows you to examine only one top event at a time. [12]

II.5 Bayesian networks (BN) :

Introduction

Reliability-based design and in-service inspection (or development testing) are two complementary approaches for ensuring the safe performance of structures. Physics-based computational reliability methods are much more cost-efficient for large and complex structures and are tools that could be used when experimental data are difficult to obtain. However, due to the approximations in the computational model and the limited statistical data on the input variables, there may be uncertainty or error in this computation. Therefore, when inspection/test information is available, the results of the two approaches should be combined for a robust re-estimation of the structural reliability. Bayes' theorem, which is used for probabilistic updating, provides an appropriate framework for this purpose.

Definition:

Bayesian networks represent joint probability models among given variables. Each variable is represented by a node in a graph. The direct dependencies between the variables are represented by directed edges between the corresponding nodes, and the conditional probabilities for each variable (that is, the probabilities conditioned on the various possible combinations of values for the immediate predecessors in the network) are stored in potentials (or tables) attached to the dependent nodes. Information about the observed value of a variable is propagated through the network to update the probability distributions over other variables that are not observed directly. Using Bayes' rule, these influences may also be identified in a 'backwards' direction, from dependent variables to their predecessors. [43]

II.5.1 Bayesian approach:

The Bayesian approach to uncertainty ensures that the system remains consistent and provides a way to apply the model to data. Graph theory helps to illustrate and utilize independence structures within interacting sets of variables, hence facilitating the design of efficient algorithms. In many situations, the directed edges between variables in a Bayesian network can have a simple and natural interpretation as graphical representations of causal relationships. This occurs when a graph is used to model a situation where the values of the immediate predecessors of a variable in a network are to be interpreted as the immediate causes of the values taken by that variable.

This representation of causal relationships is probabilistic; the relation between the value taken by a variable and the values taken by its predecessors is specified by a conditional probability distribution.

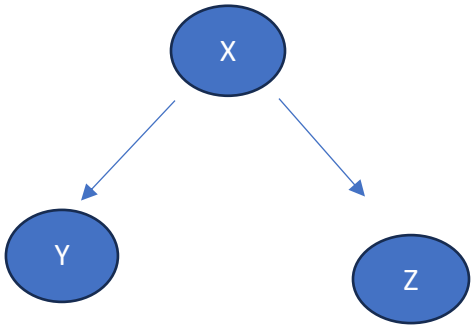
When a graph structure is given and the modelling assumptions permit a causal interpretation, then the estimates of the conditional probability tables obtained from data may be used to infer a system of causation from a set of conditional probability distributions. A Bayesian network is essentially a directed acyclic graph, together with the associated conditional probability distributions.

In general:

A Bayesian network (BN), also known as a Bayesian belief network (BBN), is a *directed acyclic graph* (DAG) formed by the variables (nodes) together with the directed edges, attached by a table of conditional probabilities of each variable on all its parents.

Therefore, it is a graphical representation of uncertain quantities (and decisions) that explicitly reveals the probabilistic *causal* dependence between the variables as well as the flow of information in the model. [40]

independent probability:



X and Z are conditionally independent, so we can say the probability P (X|Y, Z) = P(X|Y)

That is to say that the probability of X depends Only that of Y

- The joint probability of all variables is

P (X, Y, Z) = P(X|Y). P(Y). P(Z|Y)

Concept of causality:

- This is the notion of "causes" and "effects"
- If A and B are in a causal relationship, we connect them by a directed arrow.

Chain types:

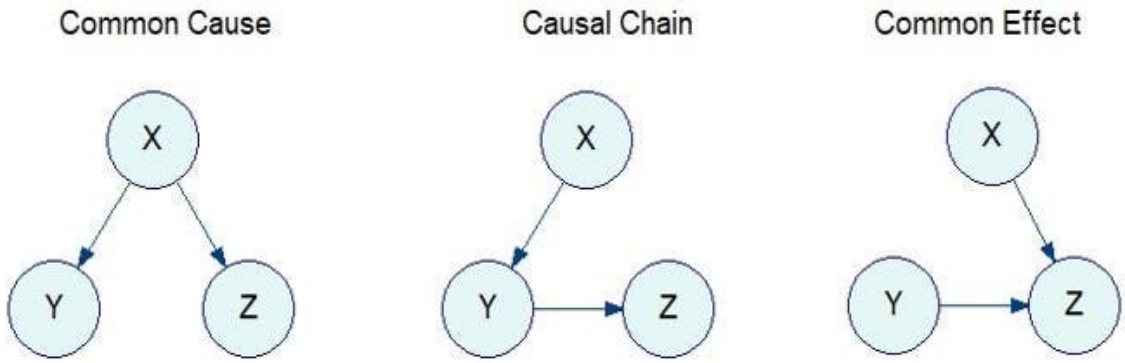


Figure 2.6: chain types in RB

Probability table:

The probability tables, linked to the nodes, are defined by statistics relating to the problem to be solved (can also be determined by experts). Each of the variables has a table of conditional probabilities relating to the causal variables on which it depends.

Concept of causality and relationships between nodes:

In Bayesian Networks, two nodes that represent two different facts can be in a causal relationship without one implying the other. Graphically, each parent affects their sons. The notion of causality plays a very important role in building Network Bayesians.

A Bayesian Network allows several types of nodes to be modeled. We use, in most cases, two types of nodes:

- a discrete node representing a discrete variable.

- a continuous node representing a continuous variable

II.5.2 Bayes rule:

A more instructive form of Bayes' rule is obtained by considering a finite exhaustive set of mutually exclusive hypotheses $\{H_i\}_{i=1}^{m}$ The law of total probability gives for any E:

$$P(E) = \sum_{i=1}^{m} P(H_i)p(E|H_i)$$

and Equation yields for any majoranyH_i

$$P\big((H_i|E)\big) = p(E|H_i)P(H_i)/\sum_{i=1}^{m} P(H_i)p(E|H_i)$$

Here, P(H_i) is the initial or prior probability for a hypothesis, before any evidence E is obtained. The prior probability will have a subjective element, depending on background information and how you interpret this information.

P(H_i) is updated to a new probability, called the posterior probability, based on this new evidence. This update is the key concept of Bayesian learning from experience. [43]

II.5.3Transformation of FTA to BN:

The following figure shows the conversion of an OR and AND logic gate into node equivalents in the RB. The parent nodes A and B are assigned to priori probabilities, and at the child node C, its conditional probability table (TPC). [31]

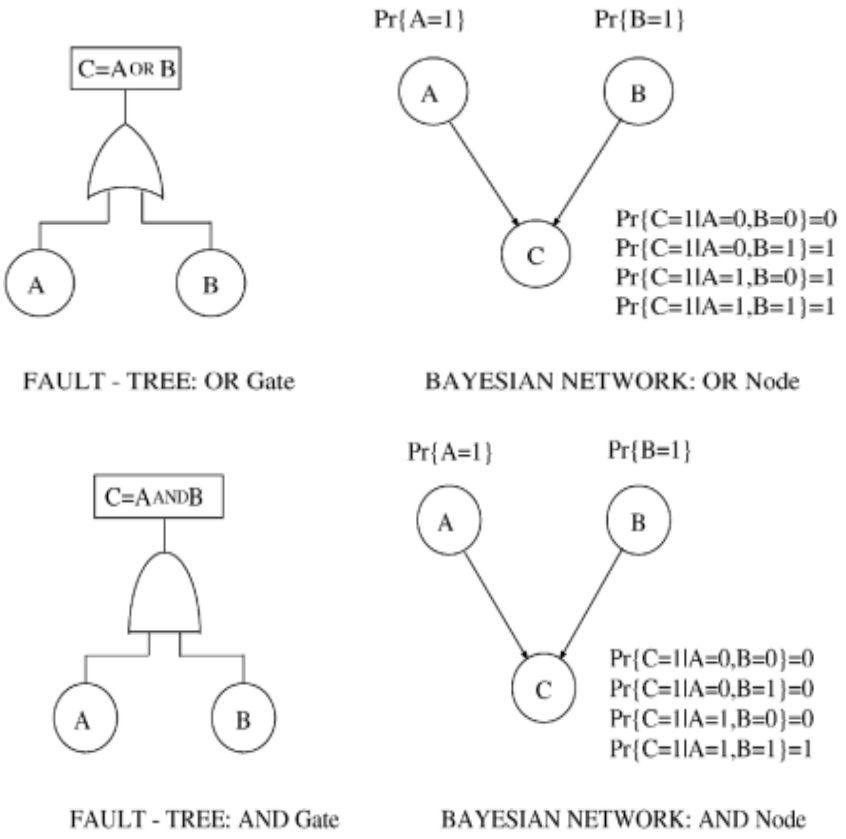


Figure 2.7: Quantitative and qualitative transformation of FTA to BN[31]

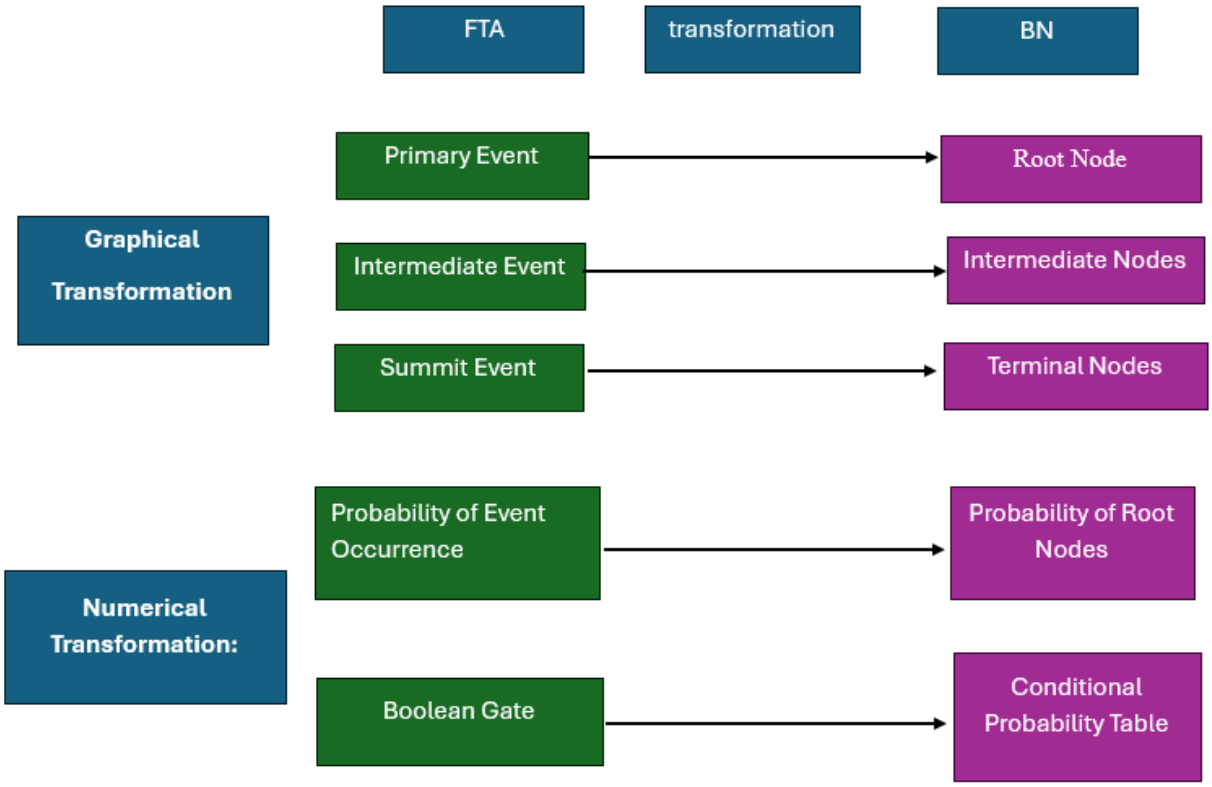


Figure 2.8: Process of FTA transformation to BN

on REX data and/or expert judgment

and/or expert judgment.

Feature	**Fault Tree Analysis**	**Bayesian Network**
Probabilistic Reasoning	Limited	Yes (Bayesian)
Real-time updating	No	Yes
Dependency Modeling	Weak	Strong
Diagnostic Capability	Limited	Excellent
Incomplete Data Handling	Poor	Good

Table 2.1: Comparison between FTA and BN

Conclusion:

Risk analysis is a crucial aspect of engineering and industrial safety, ensuring that potential hazards are identified, assessed, and mitigated effectively. Throughout this chapter, we explored different methods of risk evaluation, with a particular focus on **Fault Tree Analysis (FTA) and Bayesian Networks (BN)**. FTA provides a **structured, logical approach** to tracing failure causes, while BN allows for **probabilistic reasoning**, adapting to real-time data and complex dependencies. Together, these methods form a powerful framework for understanding and managing risks in industrial systems.

However, risk analysis alone is not enough; choosing the right **system architecture** is just as critical in ensuring safety and reliability. In the next chapter, we will focus on **the type of systems used in industrial safety**, with particular attention to **Safety Instrumented Systems (SIS)**.

Chapter 3 :

GP2Z COMPLEX

III.1 PRESENTATION OF THE GP2Z COMPLEX:

The GP2Z complex is one of the liquefaction complexes belonging to the LRP (Liquefaction, Refining, Petrochemicals) activity. The collaboration between SONATRACH and CJB (Constructors John Brown) put the GP2Z complex into operation on 17 March 1973, including the remote processing activity with a capacity of 4 million tons per year of an LPG/condensate mixture. The complex covers an area of 29.5 hectares on the bay of Arzew, about 4 kilometers from the city, and about 40 kilometers east of Oran.

The complex is bounded by:

The north/northwest: a vacant lot and the GL4Z complex

East/North-East: the Mediterranean Sea.

Southeast: FERTALG and FERTIAL petrochemical complexes

South/South-West: RTO

West/Northwest: vacant lot, RA1Zetle refinery CP1Z complex.



Figure 3.1: Satellite map of the location of the GP2Z complex in the industrial zone

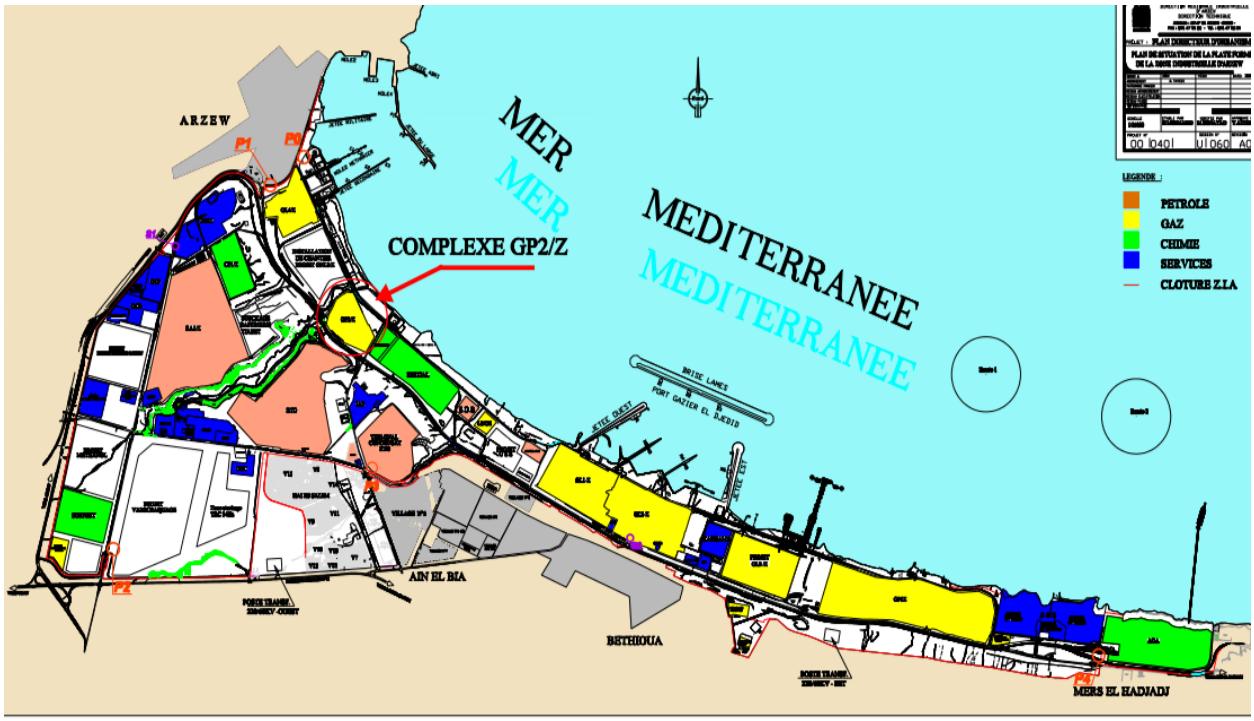


Figure 3.1: Situation plan of the GP2Z complex

The GP2Z Complex is composed of five zones coded as follows: 61, 62, 63, 64, and 65

1. 61: Storage area.
2. 62: Process Area (Dehydration, Separation, and Refrigeration)
3. 63: Utility area.
4. 64: Ship loading area.
5. 65: LPG inlet area.

III.2 Technical sheet of the complex :

1. **Localisation:** ARZEW
2. **Area:** 29.5 hectares.
3. **Staff:** 478 agents.
4. **Target:** Treatment of 1.4 million tons of LPG load
1. **Products:** Commercial propane. / Commercial butane.
2. **Process Used:** Pressure distillation.
3. **Number of Trains:** one train (semi-modular)

4. **Production date:** 19/03/1973
5. **Source of Supply:** Gas from the Hassi R'Mel and Hassi Messaoud gas and oil fields.
6. **Total production capacity:** 1,400,000 tons per year.
7. **Total storage capacity**: - A 70,000 m3 tank for refrigerated butane;
    1. A 70,000 m3 tank for refrigerated propane;
    2. Two spheres of 1220 m3 each, for ambient butane.
    3. Two spheres of 1220 m3 each, for LPG

III.3 Main facilities of the complex:

1. A 70,000 m3 refrigerated propane storage tank.
2. A 70,000 m3 refrigerated butane storage tank.
3. Four spheres: two spheres for LPG buffer storage and two more for ambient butane.
4. An LPG dehydration section.
5. Two LPG Separation Columns.
6. Two oil ovens.
7. A refrigeration section.
8. Une section Boil-off Gaz (BOG).
9. A DCS control room

III.4 History of the GP2Z complex:

The GP2/Z complex is almost forty-nine (49) years old. The construction project was launched in nineteen hundred and seventy (1970) by the English company CJB.

The important dates to remember are:

1973: Commissioning of the complex to process a load of 4 million tons of a condensate/LPG mixture.

1984: Shutdown of the complex following the commissioning of condensate stabilization units at the Hassi R'Mel and Hassi Messaoud fields.

1990: Restart of the complex after the conversion of its reboiling process for the treatment of a capacity of 0.6 million tons per year.

1996: Expansion of the complex to process a capacity of 1.2 million tons of LPG per year. In addition, modification work has been carried out, such as:

1. The conversion of the two (02) condensate/LPG separation columns into depropanisation columns
2. The installation of reboilers at the level of the converted columns and adaptation of their control loops
3. Refurbishment of the dry coolers and compressors of the boil-off system
4. Construction of a new control room and replacement of pneumatic control instruments with the DCS system
5. The renovation of gas turbines, loading arms, air compressors, HV, and MV substations
6. The installation of a new load dehydration unit.

1999: Expansion of the complex's processing capacity to process 1.8 million tons per year. During this extension, several modification works were carried out, such as the replacement of the LPG separation column trays with trays with higher efficiency

The installation of new separator tanks and high-capacity heat exchangers in the refrigeration zone;

 Replacement of heat transfer fluid circulation pumps and LPG charge pumps with larger capacity pumps.

2000: Expansion project: production capacity was to be increased to 2.5 million tons. The scope of the extension project was to be limited to the following achievements:

1. An additional 160 T/h LPG separation unit
2. Installation of a new refrigeration unit
3. Increasing the storage capacity of refrigerated products
4. Extension of the low-voltage electricity network
5. The installation of a new diesel furnace
6. A new dehydration unit.

2003: Project to increase the capacity of the unit to 2.5 MT/a, to allow the complex to be structured into two modular units, each unit will process 1.25 MT/year.

2005: The complex proposed a new extension project that would increase its production to 3.5 MT/year. This project will be carried out by the construction of 02 new storage tanks, with a capacity of 70,000 m3 each, and the rehabilitation of the old columns.

2007: The GP2/Z complex underwent some modifications following the renovation project carried out by IHI (Japanese company), in order to secure the GP2/Z complex while maintaining production at 1.3 MT/year.

2009: Certification ISO 9001/2008 and ISO 14001/2004.

III.5 GENERAL INFORMATION ON LPG:

III.5 .1 Definition

The term LPG, abbreviated liquefied petroleum gas, means a mixture in proportion of propane and butane.

The gas under ambient conditions of temperature and pressure is gaseous, but it has the property of immediately becoming liquid under:

1. V' Pressure at room temperature.
2. V' Atmospheric pressure and low temperature.
3. V' Moderate pressure and partially low temperature.

III.5 .2 Composition of LPG:

The chemical composition of LPG varies according to standards and its uses in different countries. Thus, in France, LPG is made up of 50% propane and 50% butane; in the United States of America, LPG is composed of 95% propane and 5% butane. It may contain propylene, and a small amount of methane, ethylene, pentane, and, exceptionally, flash hydrocarbons such as butadiene or acetylene.

Liquefied petroleum gas (LPG) is a mixture of light hydrocarbons composed mainly of butane (C_4H_{10}) and propane (C_3H_8), stored in a liquid state. LPG is in a gaseous state under normal temperature and pressure conditions, but it can immediately change to a liquid state under the following conditions:

1. High pressure and room temperature.
2. Atmospheric pressure and low temperature.
3. Moderate pressure and medium-low temperature.

LPG is considered to be a clean and more environmentally friendly source of energy, which would make it possible to limit negative impacts on the environment, such as the degradation of the ozone layer or greenhouse gases.

LPG is also used as a fuel for vehicles and in different fields such as power generation and air conditioning.

III.5.3 The characteristics of LPG:

LPG (Liquefied Petroleum Gas) is a mixture of gases consisting mainly of propane and butane in different proportions depending on the nature of the deposits. The average composition in general of Algerian LPGs is around 60% propane and 40% butane, of course, including traces of methane, ethane, and other gases, as well as water. LPGs are gaseous under normal temperature and pressure conditions. The liquefaction of LPGs reduces the space they occupy (1 m3 of liquid LPG occupies a volume of 225 m3 in the gaseous state under normal conditions).

LPG is a gas that is heavier than air. Butane is twice as heavy as air in the vapour phase, i.e., 2.4 g/l as density, and propane is one and a half times heavier than air in the vapour phase, i.e., 1.8 g/l as density, which is why LPGs tend to accumulate in low points. In its liquid state, LPGs are about twice as light as water, i.e., 0.51 kg/l for propane and 0.58 kg/l for butane.

Whether in liquid or gaseous form, LPGs are colorless and odorless, but sulfur-based mercaptans are added to give them a characteristic odor.

LPG is not really toxic; it has at most a slight anesthetic power if inhaled for a long time and causes migraines and stomach aches. It is not corrosive to steel.

LPG is an explosive gas when mixed with air or oxygen; the lower flammability limit of LPG is so low that it is very dangerous; as the flash point of LPG is very low, it ignites easily if there is a leak; the density of propane is 1.5 units and that of n-butane is 2.1 units, As it is heavier than air, the gaseous LPG descends downwards, crawls on the ground and could form an explosive gas mixture

III.6 THE ORGANIZATION OF THE COMPLEX:

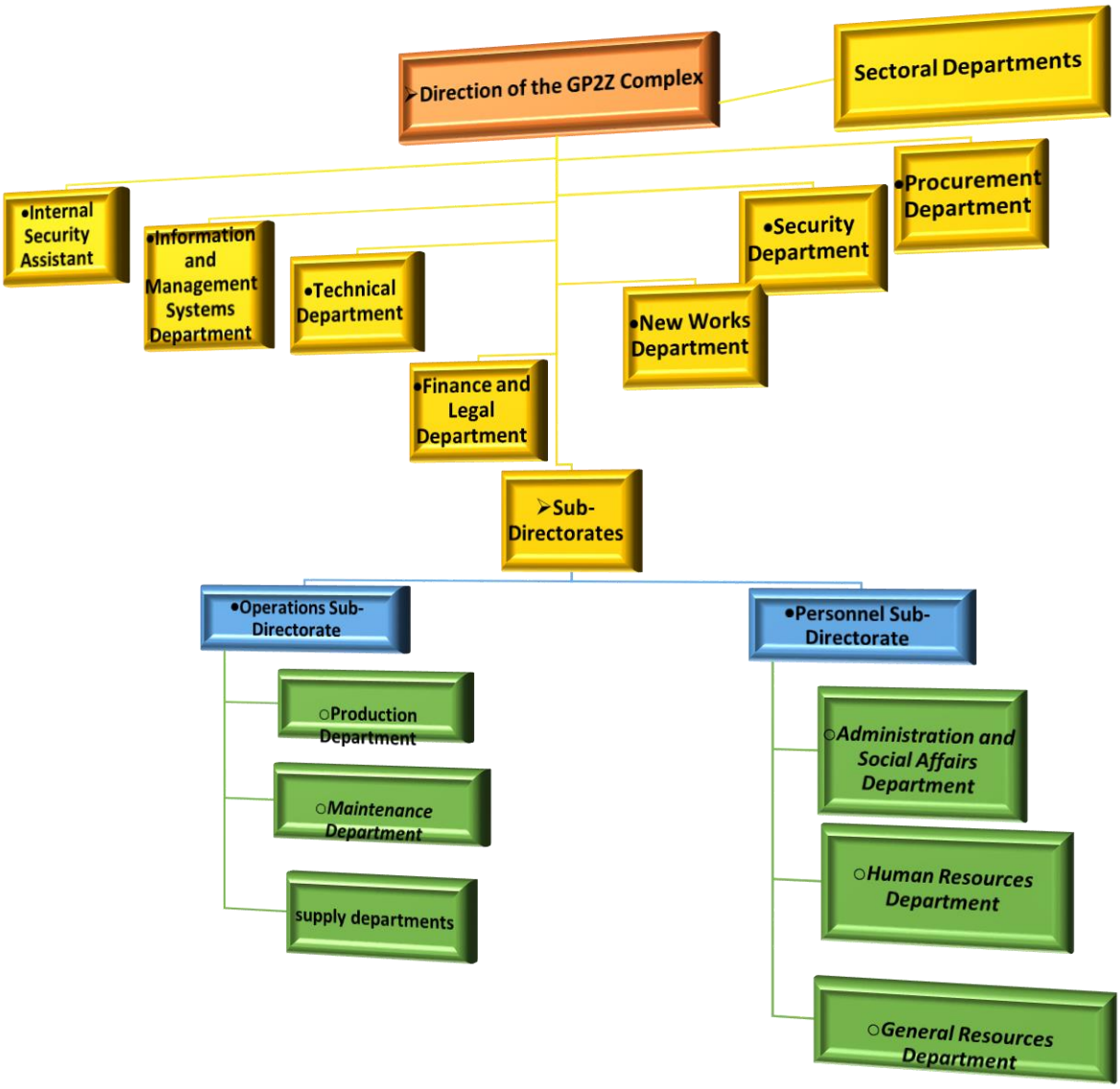


Figure 3.3: GP2Z Organization

III.7 PRINCIPLE OF THE GP2-Z PROCESS:

LPG processing passes through different sections that consist of a closed loop. To process LPG, it must go through the following production line:

III.7.1 The main sections of the complex:

1. A load storage section.
2. A dehydration section.
3. A separation section.
4. A refrigeration section.
5. A storage section for finished products.

III.7.2 Description of the manufacturing process:

III.7.2.1 LPG reception and storage sections:

The LPG comes from the RTO/TRC terminal to the GP2Z complex in a 16-inch diameter pipe, at a pressure of about 20 bar and at room temperature.

An XV-6501 valve activated by the ESD (Emergency Shut Down) system is installed just at the LPG inlet to ensure the safety of the complex.

The LPG feedstock may contain impurities (sand, dust, foreign bodies, etc.). Two filters (440/6502A/B) are installed to remove these materials. Under normal operating conditions, one of the two filters is running, while the other is off. Clogging of the filter elements is detected by the PDI-6501A/B differential pressure indicator to alert the operator to the need for cleaning.

The permutation is done manually by two manual valves, one upstream of the filter and the other downstream.

After the removal of heavy foreign objects, LPG is likely to contain non-condensable gases (light hydrocarbons and inert gases). The removal of these gases is done by means of the deaerator (410/6502) by means of density separation. The light gases are sent to the flare, and the LPG continues its way to reach the storage spheres. The removal of these gases is important both for the correct measurement of the flow rate and for stabilizing the pressure in the LPG storage spheres.

The filtered and degassed LPG will then be stored in two spheres of 1220 m3 each (420/6105 A/G). Under normal operating conditions, both spheres are in operation simultaneously. In the case of

maintenance work, only one sphere will be in use. The LPG load is sent to the dewatering section by the pumps (425/6205 B/C/G). Two pumps are in service while one serves as a reserve.

III.7.2.2 DEHYDRATION:

The aim of the operation:

This very important unit operation, generally used in gas treatment upstream of the separation and refrigeration part, is considered a pre-treatment to avoid:

1. The Risk of Solidification in Cryogenic Processes.
2. Risk of corrosion of pipes (especially in the presence of acid gas)
3. The Risk of Hydrate Formation
4. Biphasic flow and increased pressure drop.
5. Reduction of the calorific value of gas

The LPG product, sucked up by the pumps, is conveyed under flow control to the coalescer, where the greatest amount of free water is removed from the LPG charge by coalescence of suspended water droplets through the filter elements and then separated by gravity.

Then the charge is routed to the adsorbers for the removal of the molecular water. The adsorbent used for drying is the MOLSIV 4A (1/8") UOP molecular sieve. The LPG feedstock from the coalescer passes through the dehydrator (dryer) in the adsorption cycle and flows from top to bottom through the molecular sieve bed. At the outlet of the latter, the water content in the load is less than 1ppm by weight. After completion of the drying operation, the LPG load passes through the 440/6205 A/B filters for the removal of solid particles from the sieve bed.

III.7.2.3 SEPARATION:

The separation section is composed of two trains, each of which is composed of:

1. Separation Column (407/6201)
2. Preheater (405/6201)
3. Reboiler (405/6224)
4. Air condensers (405/6202)
5. Reflux Tank (410/6201)
6. Reflux pumps (425/6202)

The LPG load coming out of the dewatering section is piped 8 inches in diameter to the separation section to be fed into the LPG preheater that heats the LPG before moving to the column. The temperature of the LPG feedstock is controlled by the TIC6213 temperature indicator controller. The setpoint of the latter is set at 50°C in order to maintain the constant temperature of the LPG load.

The butane product from the bottom of the column enters the reboiler, where it is heated, then part is fed back into the column, while the other part is sent to the preheater as a heat source to preheat the LPG load, and then it continues to the sub cooler. The column head vapor is condensed by the dry cooler, and the condensed liquid flows into the reflux tank. The condensed liquid is slightly subcooled to ensure that all the vapor is condensed. Some propane product in the reflux tank is sent to the propane air sub cooler by the FV-6226, controlled by the LIC-6226 reflux tank level controller.

Others are sent to the head of the column by the reflux pumps. Because of the difference between the evaporation temperatures of the two products (propane, butane), the amount of propane sent to the head of the column is used to condense the evaporated butane fractions to separate them from the propane, and the butane introduced into the column after passing through the reboiler is used to evaporate the condensed parts of the propane. In this way, we ensure that we obtain products of the required quality.

In the same way, the butane product, from the two columns, joins upstream of the air cooler, where it is cooled to about 40°C, before being conveyed to the refrigeration section by a line 6 inches in diameter. Thus, another part of butane is conveyed directly from the 405/6214 air condenser to the two ambient butane storage spheres (420/6105E/F) by a line of 6 inches in diameter.

III.7.2.4 REFRIGERATION :

The products from the separation section (Propane and butane) leave the 405/6213 and 405/6214 air condensers to join the refrigeration section, where they will be cooled for later storage.

This section consists of two circuits, namely the commercial product circuit and refrigerant product circuit. The facilities of these two circuits are:

1. Schiller for Propane (405/6205,405/6206,405/6207)
2. Schiller for butane (405/6210, 405/6212)
3. Pure Propane Refrigerant Tank (410/6217)
4. HP (410/6230), MP (410/6205), BP (410/6219) suction drums
5. Drum Quench(410/6218A/B/C)
6. Compressors(430/6201A/B/C)
7. Gas Turbine(430/6203A/B/C)
8. Pure Propane Refrigerant Air Condenser(405/6209A/B).
9. A network of pipes.

Circuit propane commercial :

The propane product is introduced into the Chiller 405/6205 on the beam side, at a temperature of about 40°C, where it will be reduced to about 15°C. The propane reaches the Chiller 405/6206, where the product is cooled to about -14°C, and then passes into the Chiller 405/6207, where its temperature is reduced to -37°C. At the outlet, the product is depressurized in the 410/6106 tank to reach its saturation temperature, which is around -45°C.

Circuit butane commercial :

Similar to propane, commercial butane is piped from 405/6214 air condensers to the refrigeration section. The product is introduced into the Chiller 405/6210 on the beam side at a temperature of around 40°C, knowing that this temperature varies according to the ambient temperature, then it comes out at a temperature of about 14°C, and then it passes to the Chiller 405/6212, where it is cooled to around -11°C. At the outlet, the product is depressurized and sent to storage tank 420/6105.

Refrigerant propane circuit:

Cooling of commercial products (Propane / Butane) is provided by pure propane. The latter is stored in the 410/6217 tank at a pressure of 16 bar and a temperature of around 40°C. Pure propane feeds the grille side of both Chiller 405/6205 and 405/6210 through the LV-6234 and LV-6235 level valves. Downstream of the two LVs, pure propane undergoes expansion, bringing its pressure to about 6 bars and its temperature to 12°C. At the end of this first phase, the vapours produced are conveyed to the HP410/6230 suction tank, and the liquid is conveyed to feed the

second stage chillers, namely the 405/6206 and 405/6212 chillers. The LV-6236 and LV-6237 ensure the expansion of the propane before its introduction into the chillers at a pressure of about 1.8 bar and a temperature of -16°C. At the end of this phase, the refrigerant propane vapours are sent to the MP 410/6205 suction tank, and the 405/6206 chiller feeds the 405/6207 chiller. The LV-6238 ensures the expansion of the refrigerant propane at a pressure of 0.5 bar and a temperature of -40°C before it is introduced into the Chiller 405/6207. In this phase, there is only propane, butane ends its cycle at the level of the second phase. The refrigerant propane vapours are conveyed to the 405/6219 low-pressure suction tank.

Vapor compression:

The vapours are recycled through the turbochargers, each of which consists of a gas turbine and a multi-stage compressor (Dresser).

Each compressor has three intake stages: HP, MP, and LP. The vapours come from the suction tanks. The LP stage vapours are compressed and then mixed with the MP stage inlet vapours; the mixture is compressed and then mixed with the HP stage vapours. At the end, the vapours are discharged at a pressure of about 16 bars, then condensed in the 405/6209 A/B air condenser and then returned to the 410/6217 tank. These compressors can face a pumping problem, so each of the compressors is equipped with an anti-pumping system.

Anti-pumping system :

At the level of the discharges of each compressor, there is a tap to the quench flasks (410/6218A/B/C). At the inlet of each quench Drum, the pressure is monitored and maintained respectively by the PIC-6247A/B/Centre6 pressure indicator controllers at 7 bar.

Pure propane from the 410/6217 tank is injected into the tanks via the TV-6247 A/B/C temperature control valves connected to the TIC-6247A/B/C temperature indicator controllers, allowing the flow of injected pure propane to be controlled.

At each HP, MP and LP suction line of the three compressors (430/6201A/B/C), flow transmitters are installed (FT101/102/103), (FT201/202/203), (FT301/302/303) transmitting a signal to the Flow Control Indicators (FIC101/102/103), (FIC201/202/203), (FIC301/302/303) controlling the flow valves (FV101/102/103), (FV201/202/203) and (FV301/302/303) connected to the 410/6218A/B/C QUENCH drum to compensate for the lack of flow of refrigerant propane vapors from the Suction drum 410/6230, 410/6205,410/6219.

III.7.2.5 STORAGE:

Butane and Propane products will be stored in refrigerated storage tanks with a capacity of 70,000 m3 each, to be marketed later. Part of the butane is stored directly after the separation phase in two storage spheres (420/6105 E/F) under pressure to be subsequently delivered to NAFTAL.

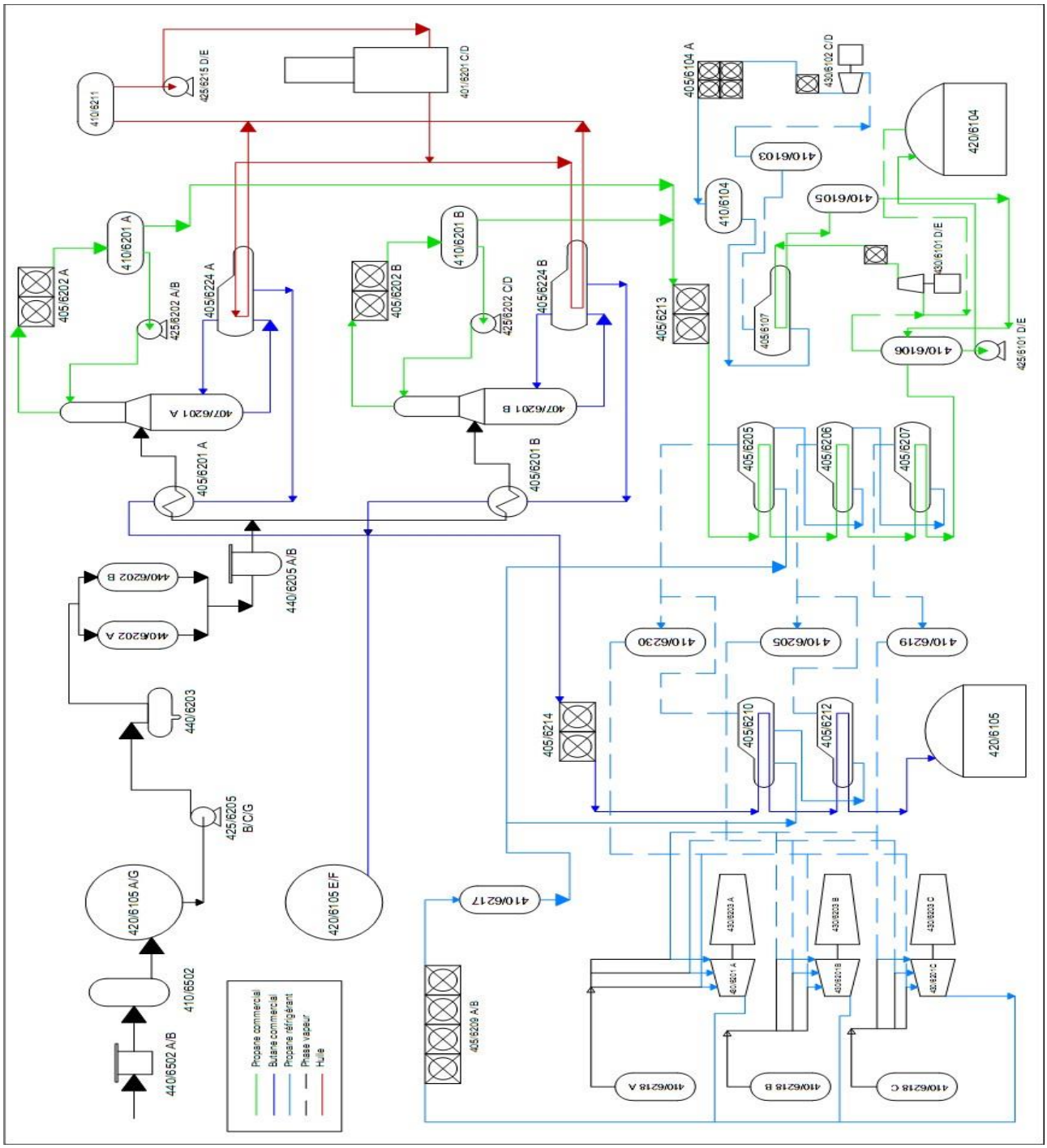


Figure 3.4: block diagram of the production process of the GP2z complex

Chapter 4:

Evaluation of sis

IV.1 Introduction:

We decided to choose the first part of the process, the storage, precisely the storage sphere (420/6105 A/G). Now that we explained above how it works, we're going to focus on the BCPS and SIS parts involved in this section.

The DCS (Distributed Control System) is the first layer of protection, which is connected to all inputs/outputs of the sphere storage.

The DCS Functions in our System: Field Device Monitoring: it reads signals from sensors like LT/LTHH6101 (level), PT6101 (pressure).

It also receives signals from limit switches such as ZSL (on valves HV6102 and HV6103) to confirm valve positions.

Executing Logic Control: Example: If the LPG level becomes too high, the DCS or SIS automatically closes the inlet valve HV6102. It sends open/close commands to valves like HV6103.

Operator Alerts: If a fault or abnormal condition is detected (e.g., level too high, valve doesn't move), DCS triggers alarms on the HMI (screen).

Manual Control Interface: Operators can manually control valves (like HV6103) via the DCS screen (HMI) or local hand switches (e.g., HS6103).

Event and Alarm Logging: All actions, alarms, and events are logged for traceability and analysis.

Now moving to the SIS part, we have 6 paths for safety, starting with:

- Level transmitter LT6105LL: as the level of LPG gets near the instruction, the pump 425/6205 will stop immediately, plus closing the outlet valve HV6103
- Level transmitter LT6101HH: responsible for the inlet valve HV6102
- Valve Openness Switch ZSL, ZSLL:
- Hand switch HS6103: Manual hand closing the valve HV6103
- Relief safety valve RV6104A/B: According to the instruction, the highest value for pressure shouldn't exceed 15.5 bar
- GN line: pressure valve control PV6101A/B
  Pressure signal converter PY6101B: switching from Pneumatic to electric signal

Pressure transmitter PT6101: the instruction is 9,1bar

PIC6101: relating to DCS

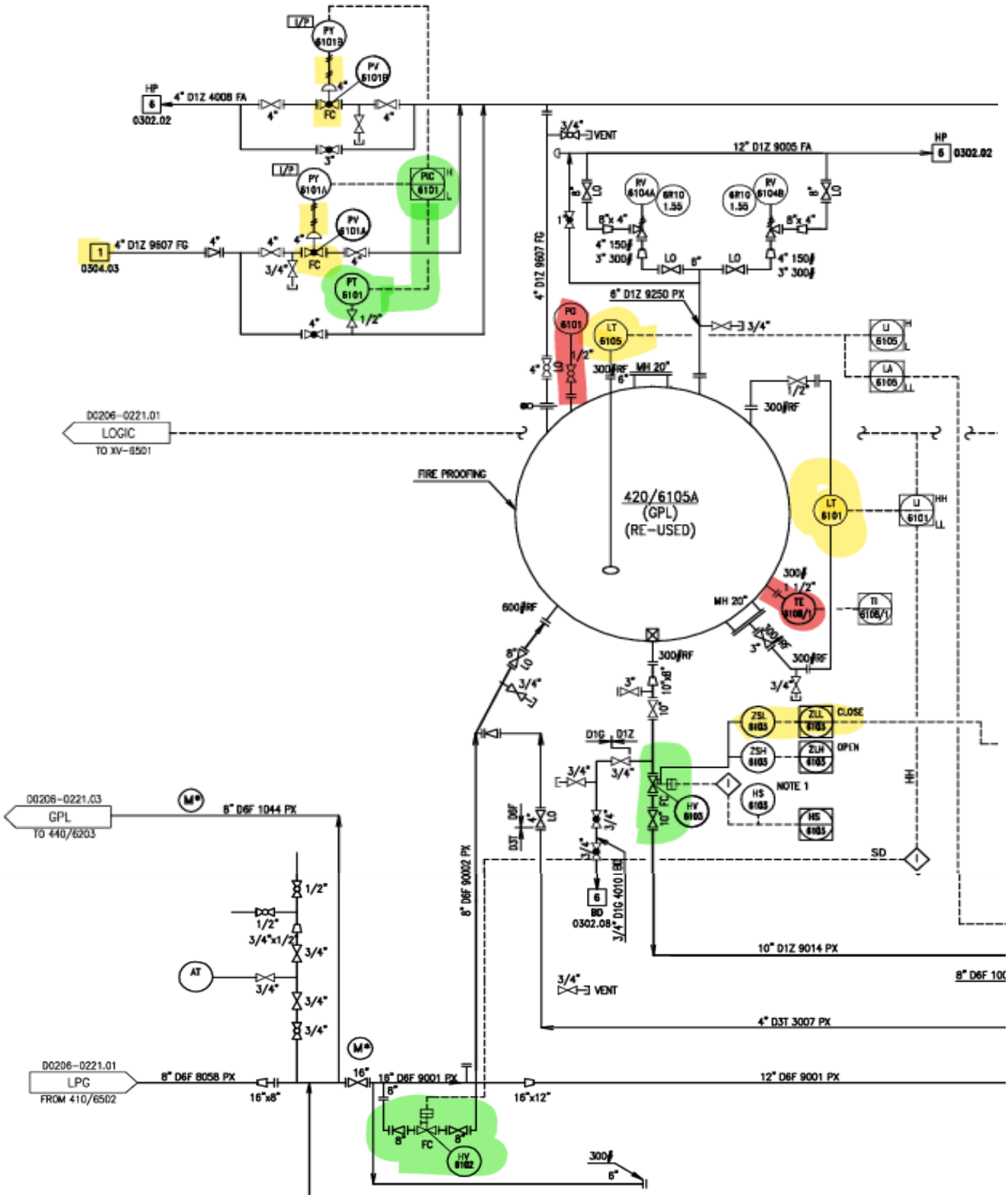


Figure 4.1: PID OF SPHERE

IV.2 Fault Tree Analysis:

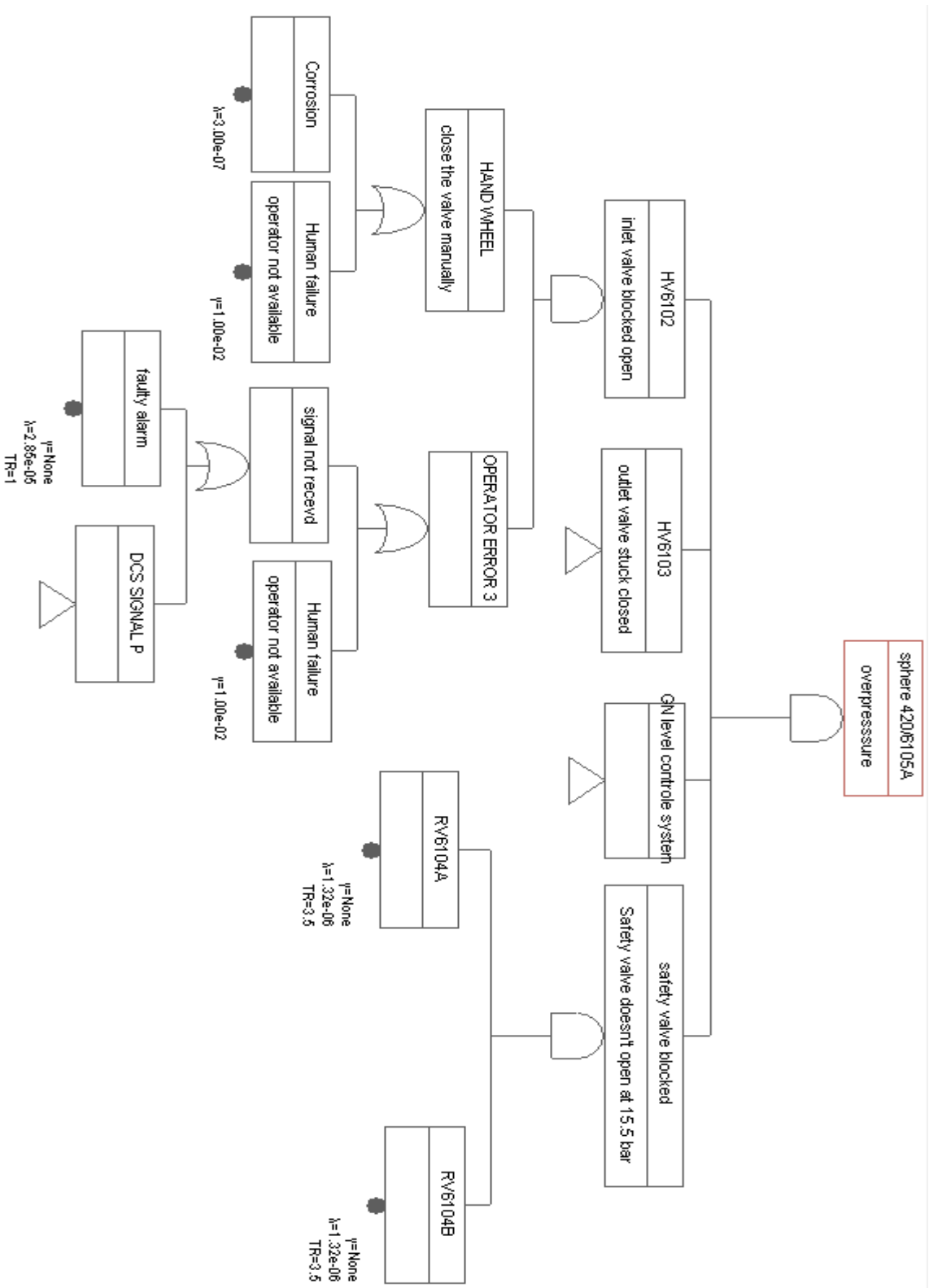


Figure 4.2: Fault Tree Analysis of sphere

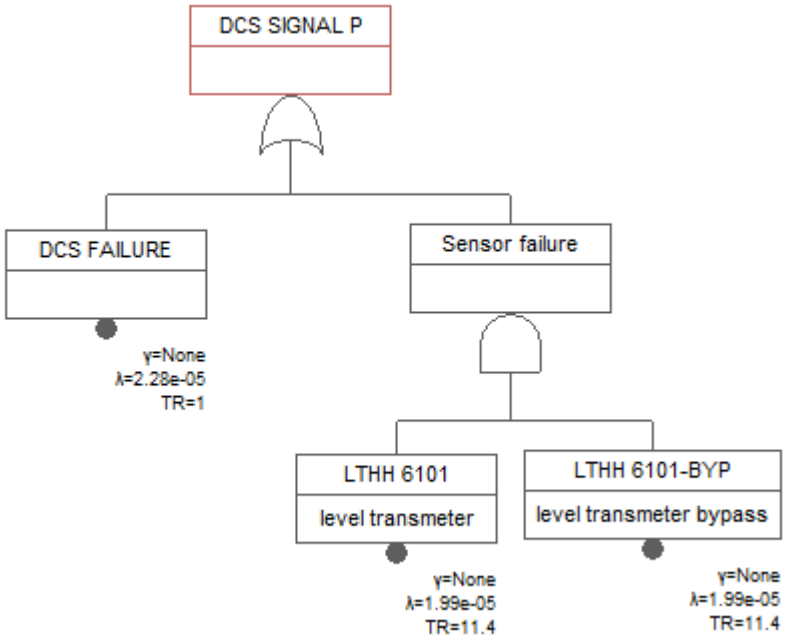


Figure 4.2.1: Fault Tree Analysis of sphere (HV6102) continued.

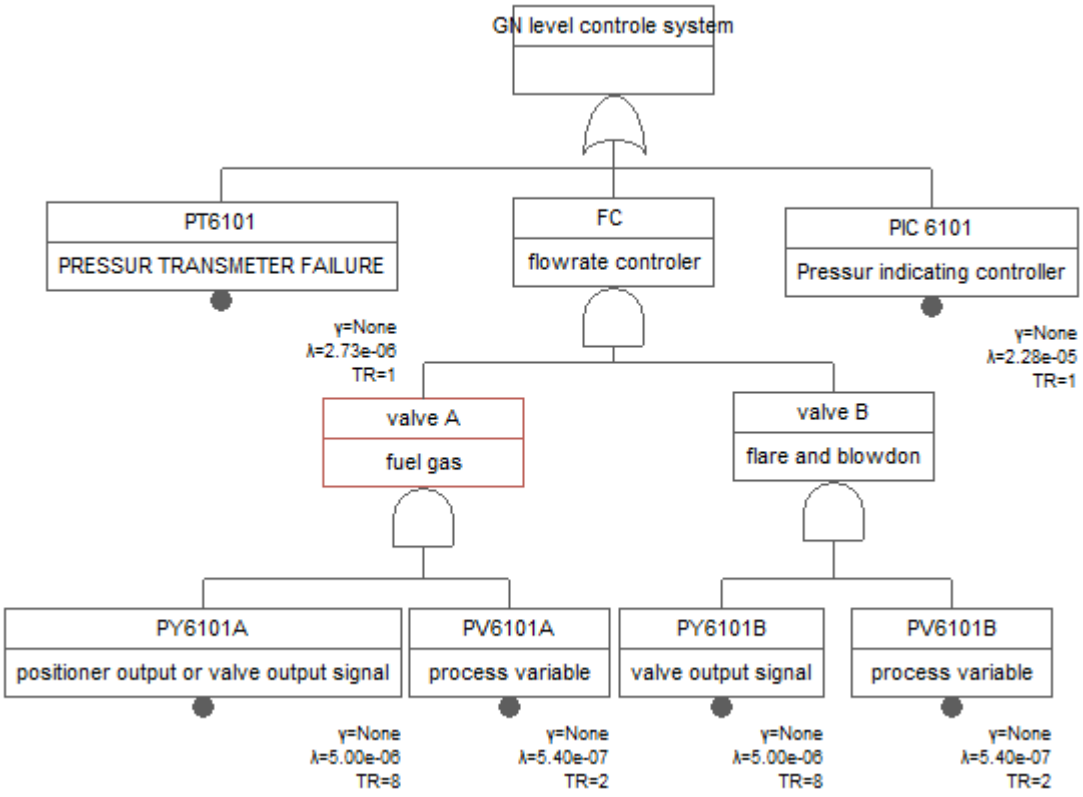


Figure 4.2.2: Fault Tree Analysis of sphere (Gas Level)

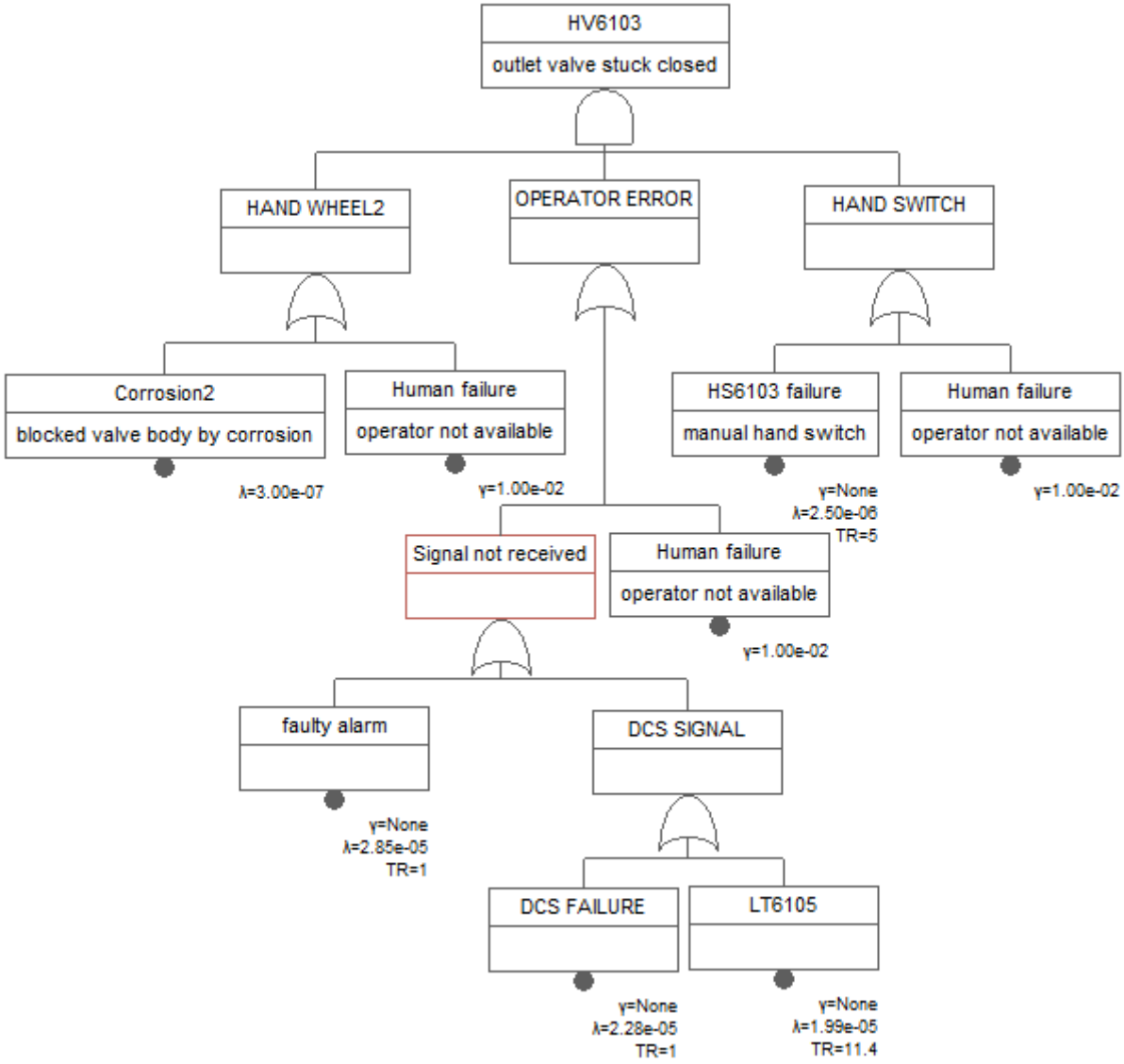


Figure 4.2.3: Fault Tree Analysis of sphere (HV6103)

IV.2.1 Qualitative analysis:

The following table contains the total number of min cuts per order:

Order	Quantity
4	2
7	5
9	2
10	2
12	1

Figure 4.1: minimal cut sets

After calculating, we have:

SO=HF×PIC×RVA×RVB+ HF×PT×RVA×RVB+C1×C2×HS×PIC×RVA×RVB×A+

C1×C2×DCS×HS×RVA×RVB×PIC+C1×C2×HS×PT×RVA×RVB×A+C1×C2×DCS×HS×RVA×RVB×PT+HF×PVA×PVB×PYA×PYB×RVA×RVB+C1×C2×HS×LT×LTH×LTHBY×PIC×RVA×RVB+C1×C2×HS×LT×LTH×LTHBY×PT×RVA×RVB+C1×C2×HS×PVA×PVB×PYA×PYB×RVA×RVB×A+C1×C2×HS×DCS×PVA×PVB×PYA×PYB×RVA×RVB+C1×C2×HS×LT×LTH×LTHBY ×PVA×PVB×PYA×PYB×RVA×RVB.

2 order 4: HF×PIC×RVA×RVB+ HF×PT×RVA×RVB.

5 order 7: C1×C2×HS×PIC×RVA×RVB×A+ C1×C2×DCS×HS×RVA×RVB×PIC+

C1×C2×HS×PT×RVA×RVB×A+C1×C2×DCS×HS×RVA×RVB×PT+
HF×PVA×PVB×PYA×PYB×RVA×RVB.

2 order 9: C1×C2×HS×LT×LTH×LTHBY×PIC×RVA×RVB+

C1×C2×HS×LT×LTH×LTHBY×PT×RVA×RVB

2 order 10:

C1×C2×HS×PVA×PVB×PYA×PYB×RVA×RVB×A+

C1×C2×HS×DCS×PVA×PVB×PYA×PYB×RVA×RVB.

1 order 12:

C1×C2×HS×LT×LTH×LTHBY ×PVA×PVB×PYA×PYB×RVA×RVB.

IV.2.2 Quantitative analysis:

Results	
Probability:	3.13e-08
System unreliability:	1.2e-07
Lambda system:	4.08e-11
Number of failures:	1.2e-07
System MTTR	2291

Figure 4.2: System Basics

Importance factors:

The table below contains the magnitudes of each of the basic factors of events contributing to the dreaded event.

Event	Description	Occurrences	Pr	MIF	CIF	DIF
Human failure	operator not available	3	0.01	3.1e-06	1	1
faulty alarm		3	2.8e-05	2.7e-16	2.5e-13	2.8e-05
DCS FAILURE		3	0.18	2.7e-16	1.6e-09	0.18
LT6105		3	0.16	1.4e-23	7.1e-17	0.16
HS6103 failure	manual hand switch	9	1.2e-05	3.9e-12	1.6e-09	1.3e-05
Corrosion2	blocked valve body by corrosion	9	0.0026	1.9e-14	1.6e-09	0.0026
LTHH 6101-BYP	level transmeter bypass	3	0.00023	9.7e-21	7.1e-17	0.00023
LTHH 6101	level transmeter	3	0.00023	9.7e-21	7.1e-17	0.00023
Corrosion		9	0.0026	1.9e-14	1.6e-09	0.0026
RV6104A		12	0.011	2.7e-06	1	1
RV6104B		12	0.011	2.7e-06	1	1
PT6101	PRESSUR TRANSMETER FAILURE	4	0.024	1.3e-06	1	1
PIC 6101	Pressur indicating controller	4	2.3e-05	1.3e-06	0.00096	0.00099
PY6101B	valve output signal	4	4e-05	6.2e-23	7.9e-20	4e-05
PV6101B	process variable	4	1.1e-06	2.3e-21	7.9e-20	1.1e-06
PV6101A	process variable	4	1.1e-06	2.3e-21	7.9e-20	1.1e-06
PY6101A	positioner output or valve output signal	4	4e-05	6.2e-23	7.9e-20	4e-05

Figure 4.3: event contributions

From above, Malfunction of an Item or Function (MIF) and Occurrences, the most anticipated event is related to RVA and RVB.

DATE	PFDavg
8760	7.9e-09

According to PFDavg, the SIL LEVEL is 4. (The **SIF)** has an **extremely high level of reliability.**

IV.2.3 Interpretation:

Qualitative analysis shows redundancy provided by two safety valves (RVA and RVB) is crucial: a single valve failure does not contribute to the top event, but they do with concurrent failures. The worst scenarios are loss of measurement, loss of control, and valve failures together. Key events associated with the DCS/SIS and level transmitters are mainly the causes of the higher-order minimal cut sets. In numerical terms, the calculated average probability of failure on demand (PFDavg) is 7.9×10^{-9},very low and implying a practically zero probability of failure. According to IEC 61508/61511, this value is in Safety Integrity Level 4 (SIL 4), the highest safety integrity level. This means that the Safety Instrumented Function (SIF) is very dependable with little residual risk. But it requires redundant architecture, regular proof testing, and stringent maintenance practices for the same

IV.2.3.1 Interpretation of SIL 4:

- The Safety Instrumented Function (SIF) is extremely reliable.
- Residual risk is very low.
- Redundant architecture and regular proof testing are essential to maintain this level.

IV.2.3.2 Key Strengths Identified

- Redundant safety valves (RVA and RVB) + PV/PY converters.
- Multiple-level and pressure sensors.
- Integration of DCS/SIS reduces the chance of human error.

IV.2.3.3 Points of Attention / Recommendations

- Even with SIL 4, it is critical to:
    - Maintain and proof-test RVA and RVB regularly (the most critical elements).
    - Verify the calibration of all level and pressure sensors.
    - Test automatic switching between SIS/DCS to ensure reliability.
- Pay attention to scenarios combining sensor failures + control failures, since these appear in high-order cut sets.

IV.2.3.4 Overall Interpretation of the FTA :

- The undesired event depends mainly on safety valves, RVA, and RVB.
- Minimal Cut Sets prove that redundancy and diversity of sensors greatly reduce risk.
- SIL 4 indicates an extremely safe system, appropriate for critical LPG applications.
- Maintenance priority should focus on the safety valves and signal converters, because they are present in almost every critical chain.

IV.3 Bayesian Network:

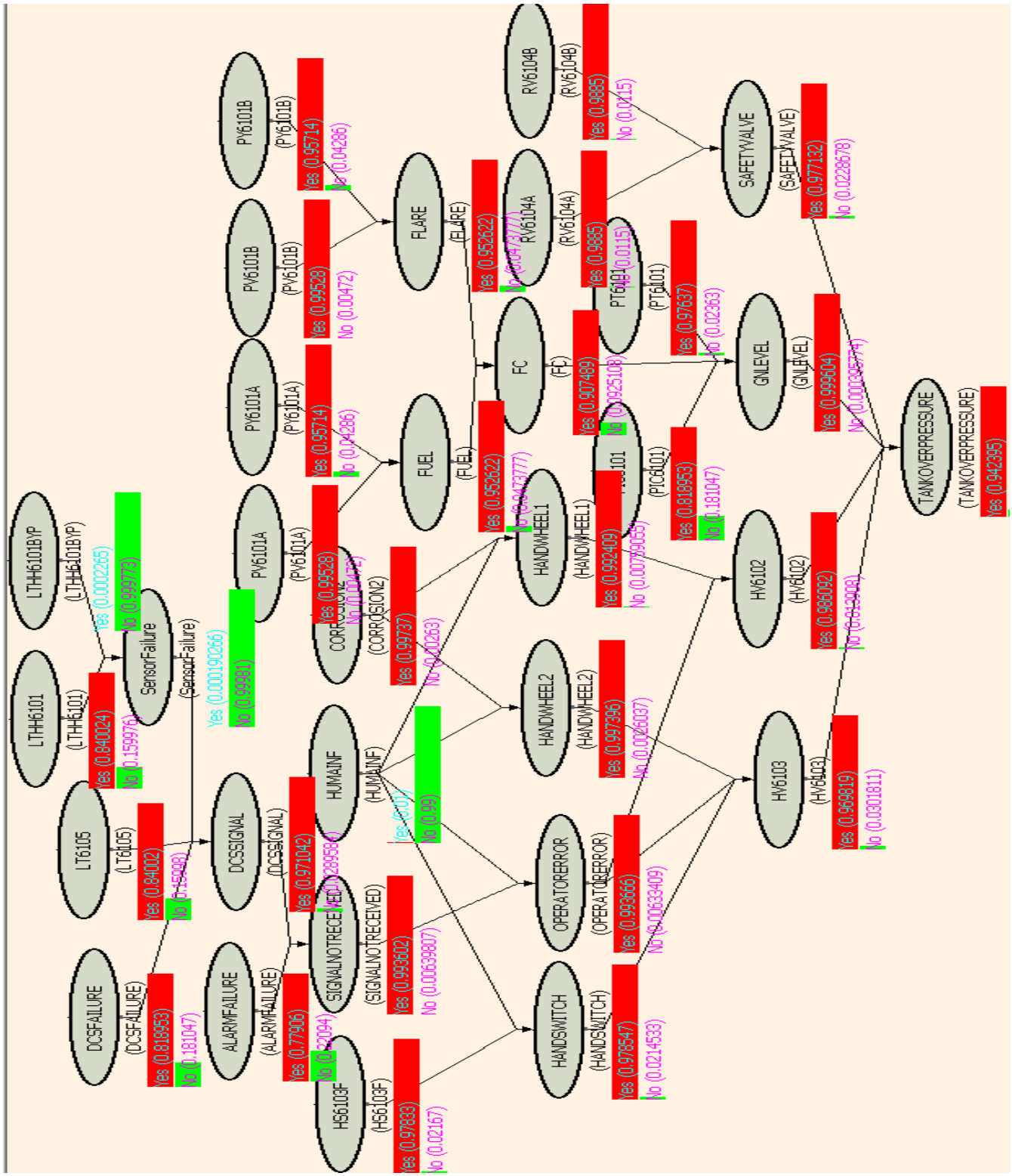


Figure 4.3.1: Bayesian Network of sphere (part 1)

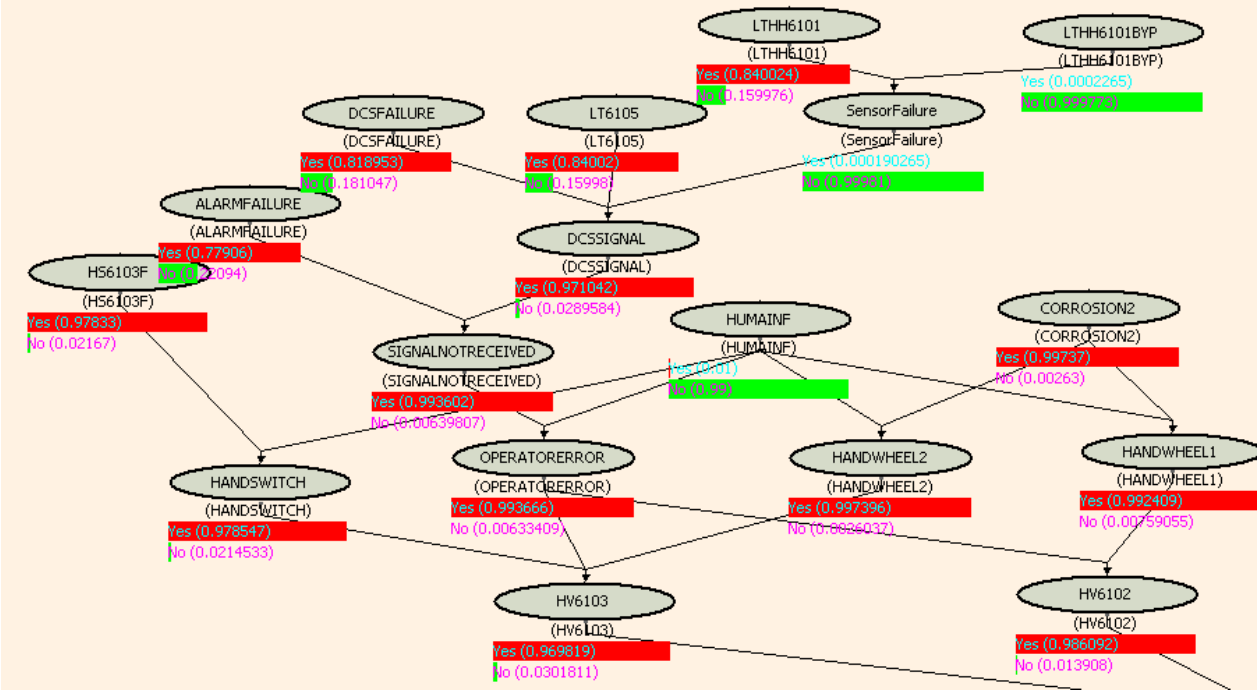


Figure 4.3.1: Bayesian Network of sphere (part 2)

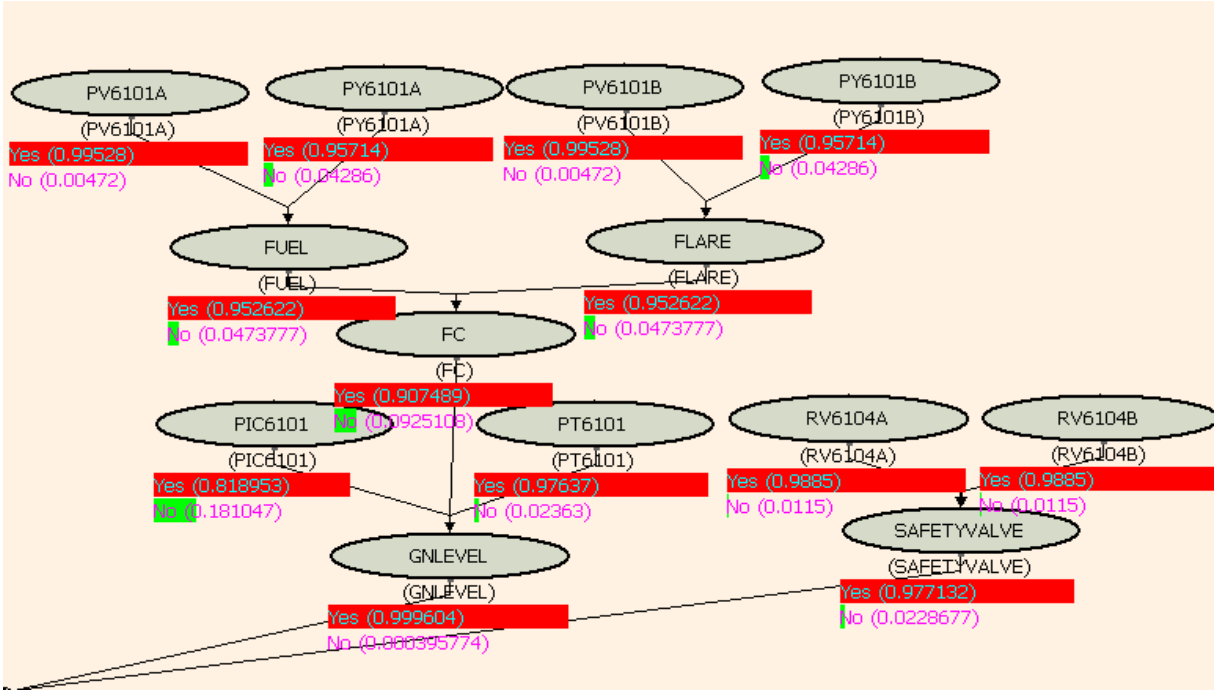


Figure 4.3.1: Bayesian Network of sphere (part 3)

In the Diagram, "Yes" presents availability R (t), and "No" presents unavailability Q(t).

$$\boldsymbol{R_i(t) = e^{-\lambda_i t}}$$

$$\boldsymbol{Q_i(t) = 1 - e^{-\lambda_i t}}$$

Time is 1 year, which equals 8760 h.

For italiclambda, use **OREDA (Offshore Reliability Data)** as a reference.

Equipment	**λ (1/h) × 10^{-6}**	**MTTR (h)**
Level sensor	19,87	11,4
Pressure sensor	2,73	5,3
Signal alarm	28,5	1
DCS	22,8	1
Human error	X	X
Corrosion handwheel (HW)	0,3	8
Valve gate HV03	11,57	10
Valve gate HV02	11,41	10
Valve torch	4,23	4
Valve fuel globe	0,54	2
Relief gate	2,1	9
HS	2.5	5
PSV (RV)	1,32	3,5

Table 4.4: Failure rate (λ) and MTTR of components

And now we use the formula above for the next calculation:

Error	A(t) Availability	Q(t) = 1 -A(t)	λ (t=8760h)
corrosion	0,999737	0,000263	3x10^-7
alarm failure	0,77906	0,22094	2.85x10^-5
DCS failure	0,818934	0,18104	2.28x10^-5
LTH6101/LTHBYP	0,0002265	0.9997735	1.85x10^-5
HS	0,97834	0,02166	2.5x10^-6
Pressure Sensor	0,97636	0,02363	2.73x10^-6
PV(A/B)	0,99528	0,00472	5.4x10^-7
PY(A/B)	0,95714	0,04285	5.1x10^-6
RV(A/B)	0,9885	0,0114	1.32x10^-6

Table 4.5: Availability and Unavailability of Basic Events

Prior probability:

To determine the most undesired events, we use each basic event one time fully operated [R(t)=1]and the other as a failure [R(t)=0]. Here's the table for that: we estimated the marginal importance factors for each basic event using the BIMBURM theory.

Equipment (E)	R(t)=1 P(SP/E=1) (P1)	R(t)=0 (P0)	Difference (P1 - P0)
RV 6104 A/B	0,957668	0	0,957668
PV A/B	0,946672	0,942978	0,003694
PY A/B	0,946819	0,942978	0,003841
PT 6101	0,94703	0,931168	0,015862
PIC 6101	0,94703	0,944959	0,002071
LTH 6101/ BYP	0,947466	0,942394	0,005072
LT 6105	0,946731	0,937322	0,009409
DCS	0,948432	0,938815	0,009617
Alarm failure	0,948432	0,940388	0,008044
Corrosion	0,949125	0,009174	0,939951
HS 6103	0,967515	0,004857	0,962658

Table 4.6: Prior probability continued

WE have 4 undesired events:

- The safety valve: RV6104 A/B
- Corrosion
- Hand switch 6103

Posteriori probability:

Applying Bayes' rule on our system, for example:

$$P\big((LTH|SO)\big) = p(SO|LTH)P(LTH)/P(SO)$$

SO: Sphere overpressure

We have:

$P(SO) = 0{,}946655$

$P(LTH) = 0{,}840024$

$p(SO|LTH)$ =0,947466 so:

$P\big((LTH|SO)\big)$ =0,947466×0,840024/0,946655

$$P\big((LTH|SO)\big) = 0{,}84091$$

We do the same for all basic events:

Equipment (E)	$P((E\|SO))$
RV 6104 A/B	0,99999
PV A/B	0,9952
PY A/B	0,9573
PT 6101	0,9767
PIC 6101	0,8193
LTH 6101/ BYP	0,8409
LT 6105	0,8401
DCS	0,8205
Alarm failure	0,7805
Corrosion	0,99996
HS 6103	0,99988

Table 4.7: Posteriori probability

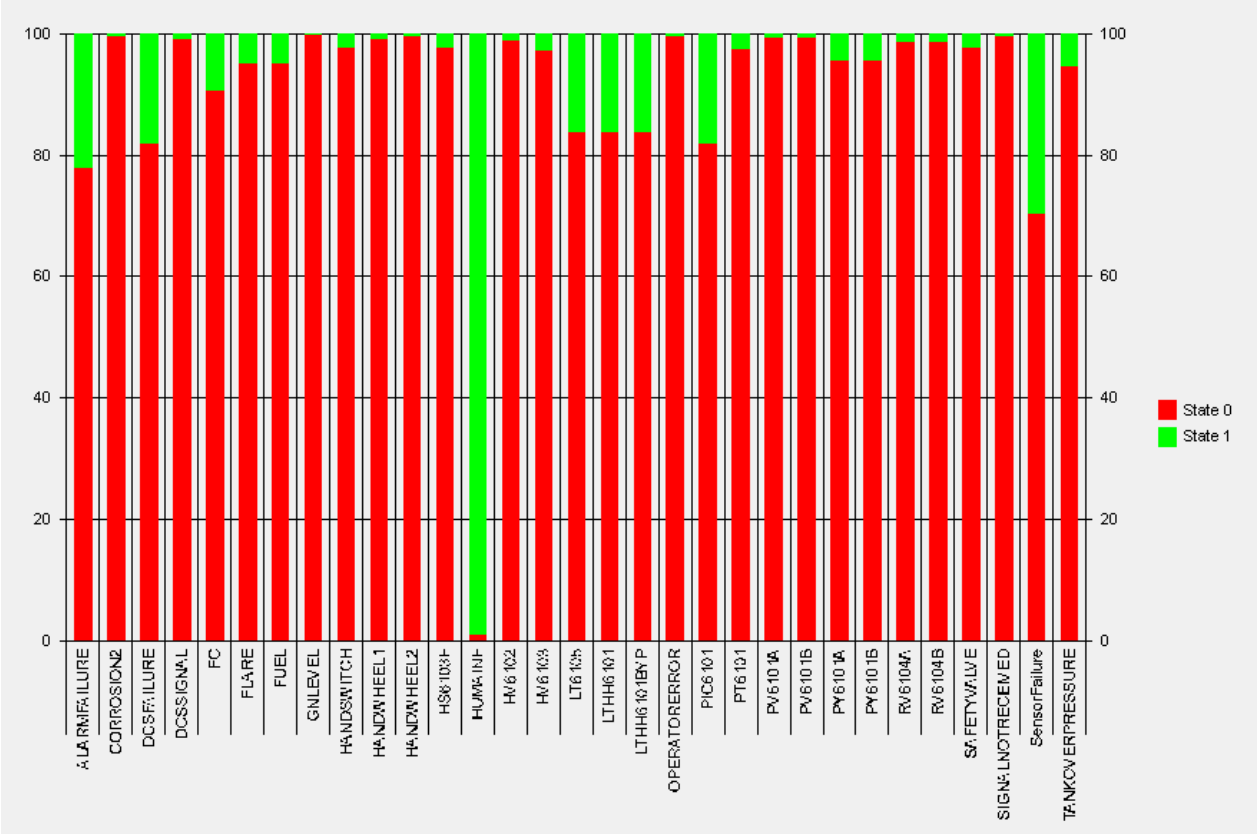


Figure 4.3.2: "Critical Event Probabilities (BN Analysis)"

The figure illustrates the **posterior probabilities of the basic events** obtained from the Bayesian Network analysis. Each bar represents a system component, with **red (State 0)** indicating the probability of failure/unavailability and **green (State 1)** indicating the probability of correct operation. The results highlight that certain events, such as **RV6104A/B (safety valves), HS6103 (hand switch), and corrosion**, show higher failure likelihoods, making them the most critical contributors to the undesired top event. This visualization helps identify the components that require the highest attention in terms of maintenance and reliability improvement.

Comparison between FTA and BN:

This FTA vs. BN comparison brings out a very complementary and interesting point. In fact, the FTA enabled us to identify the least event combinations causing the feared failure (overpressure sphere), and concluded that RV6104 A/B safety valves are the most significant factors with the most decisive effect, with an assessed level of security equal to SIL 4, which is equal to a very high reliability. However, this approach is static and does not straightforwardly involve the event dependencies. However, the Bayesian model enabled us to study dynamically the likelihood of events in terms of the state of the components and time (8760 h). The posterior probability values confirm that the same key factors (RV6104 A/B, corrosion, and HS6103) are most determinant, but also provide an estimate of their relative importance according to different scenarios. The FTA, therefore, provides a qualitative and structured image of the causes, while the BN provides a more realistic and up-to-date opinion on the system reliability.

We use the Arbre-Analyst program for FTA and MSBNX for BN.

General Conclusion:

We concluded this work having examined and evaluated the Safety performance of the Safety Instrumented Systems (SIS) applied on the GP2/Z complex, the 420/6105 A/G storage sphere in particular. The approach utilized combined two risk analysis methods: Fault Tree Analysis (FTA) and Bayesian Networks (BN).

FTA analysis validated the dominant scenarios leading to the predicted failure (sphere overpressure) and determined the central role of the RV6104 A/B safety valves, making the components the most sensitive point in the protection chain. Quantitative results led to SIL 4 designation, which denotes very high reliability of the SIS. However, this static method is still limited by its own assumption of independence and inability to capture the dynamic evolution of the system.

For its part, the Bayesian approach offered a more generalized probabilistic point of view that took into account the interdependence of events and allowed the probabilities to be revised based on new data. This model confirmed the relevance of the same factors (RV6104 A/B, corrosion, and HS6103), while offering a more realistic quantification of their effect under different operating conditions.

In such a manner, the complementarity of FTA and Bayesian Networks demonstrates that through a combination of traditional tools and innovative probabilistic techniques, one can attain a robust and exhaustive appraisal of the reliability of safety systems. The findings obtained stress that rigorous and regular maintenance should be followed as regards safety valves and main equipment so that the overall reliability of the SIS remains at its highest level and people, assets, and the environment are safeguarded.

More generally, this work provides the means to utilize real operating data and feedback (REX) to provide Bayesian models with continuous supply, allowing proactive security management and continuous optimization of SIS performance.

References:

[1] **A. Desroches**. *Concepts et méthodes probabilistes de base de la sécurité*. Lavoisier, France, 1995.

[2] **A. Villemeur**. *Sûreté de fonctionnement des systèmes industriels*. Eyrolles, 1998.

[3] **AN9025-3**. *An introduction to Functional Safety and IEC 61508*, MTL Instruments Group plc 2002

[4] **Arunkumar RS**. *Yours, Instrumentation Engineer* 2024.

[5] **Beugin, J.** *Contribution à l'évaluation de la sécurité des systèmes complexes de transport guidé*. PhD thesis, Université de Valenciennes et du Hainaut-Cambrésis, 2006.

[6] **BS EN 50126-1:2017**. *Railway applications. The specification and demonstration of reliability, availability, maintainability, and safety (RAMS)*. © The British Standards Institution 2017.

[7] **BS EN 50128:2011**. *Railway applications. Communications, signalling, and processing systems. Software for railway control and protection systems*. © The British Standards Institution 2011.

[8] **BS EN 50129:2018**. *Railway applications – Communication, signalling and processing systems – Safety-related electronic systems for signalling*. © The British Standards Institution 2018.

[9] **BS EN 61511-1:2017**. © The British Standards Institution 2017.

[10] **BS EN 61511-2:2017**. © The British Standards Institution 2017.

[11] **BS ISO 26262 1:2018**. © The British Standards Institution 2018.

[12] **CA Ericson, C Ll**. *System Safety Conference*, Orlando, Florida, 1999 - scholar.archive.org.

[13] **clearsy**. *SAFETY solutions designer : La norme CEI 61508 et ses dérivés* 2008.

[14] **David J.Smith & Kenneth G.Simpson**. *Functional Safety*, Second edition 2004.

[15] **Desroches, A., Leroy, A., Vallée, F.** *La gestion des risques : principes et pratiques*. Lavoisier, France, 2003.

[16] **European Commission, Joint Research Centre**. *Safety Instrumented Functions*, 2013.

[17] **Fiix Software**. *Fault Tree Analysis*. 2022[en ligne]. Fiix Software, s.d.

[18] **Florent Brissaud, Didier Turcinovic**. *Sécurité fonctionnelle des systèmes relatifs à la sécurité : 10 erreurs à éviter*. Congrès de Maîtrise des Risques et de Sûreté de Fonctionnement, Institut pour la Maîtrise des Risques, oct. 2016, Saint-Malo, France.

[19] **IBM**. *Fault Tree Analysis*. 2023 [en ligne]. IBM, s.d.

[20] **IEC 60050-192**. *Dependability Edition 1.0 2016-03*, Geneva, Switzerland.

[21] **IEC 61508 Functional safety – Safety instrumented systems for the process industry sector – Part 1**. *Framework, definitions, system, hardware, and application programming requirements® Edition 2.0 2010-04*, Geneva, Switzerland.

[22] **IEC 61508-part4**. ® Edition 2.0 2010-04, Geneva, Switzerland.

[23] **IEC 62061**. *Safety of machinery – Functional safety of safety-related control systems*

Edition 2.0 2021-03

[24] **IEC 61511 (2e édition 2016)**.

[25] **IEC 61513**. *Nuclear power plants – Instrumentation and control important to safety – General requirements for systems* Edition 2.0 2011-08

[26] **IEC TECHNICAL REPORT TR 61508-0:2005**.

[27] **ISO, 1999**. *Aspects liés à la sécurité : Principes directeurs pour les inclure dans les normes*. Organisation internationale de normalisation.

[28] **ISO, 2002**. *Management du risque : Vocabulaire, Principes directeurs pour l'utilisation dans les normes*. Organisation internationale de normalisation.

[29] **Jean-Michel Dranguet, Benjamin Joguet**. *Limites d'application de la norme de sécurité fonctionnelle CEI 61508 dans le cadre d'un projet complexe*. Maîtrise des Risques et Sûreté de Fonctionnement, Lambda-Mu 19, Oct 2014, Dijon, France.

[30] **Lamy, P., Levrat, E., Paques, J-J.** *Méthodes d'estimation des risques machines : analyse bibliographique*. In Lambda Mu, Lille, France, 2006.

[31] **L. Portinalea, A. Bobbioa.** *Improving the analysis of dependable systems by mapping fault trees into Bayesian networks. Reliability Engineering and System Safety 71 (2001)*

[32] **Malak Medkour, Azzedine Bouzaouit, Lakhdar Khochmane, Ouafae Bennis**. *Transformation of Fault Trees into Bayesian Networks Methodology for Fault Diagnosis*. Mechanika, 2017, 23 (6), pp.891-899.

[33] **Marvin Rausand**. *System Reliability Theory Models, Statistical Methods, and Applications*,

Wiley, 2004.

[34] **Mohamed Sallak**. *Évaluation de paramètres de sûreté de fonctionnement en présence d'incertitudes et aide à la conception : application aux Systèmes Instrumentés de Sécurité*. Automatique / Robotique. Institut National Polytechnique de Lorraine - INPL, 2007. Français.

[35] **OHSAS18001**. *Système de management de la santé et de la sécurité au travail - Spécification*. BSI,Afnor,1999.

[36] **P. Périlhon**. *L'analyse des risques : méthode MOSAR*. EDF, 1998.

[37] **Post, H.** *What Is SIL? Safety Integrity Level Meaning and Importance Explained*. TRADESAFE2024.

[38] **ProcessS**. (s.d.). *Les systèmes instrumentés de sécurité* 2013.

[39] **Ron Bell**. *Introduction to IEC 61508*. **ron.bell@hse.gsi.gov.uk**, Health & Safety Executive Bootle, UK 2006.

[40] **S Mahadevan, R Zhang, and N. Smith**. *Structural Safety*, 2001 – Elsevier.

[41] **Simon, C., Sallak, M., Aubry, J-F.** *SIL allocation of SIS by aggregation of experts' opinions*. In ESREL, Safety and Reliability Conference, Stavanger, Norvège, 2007.

[42] **Tanzi, T., Delmer, F.** *Ingénierie du risque*. Lavoisier, France, 2003.

[43] **Timo Koski, John Noble**. *Bayesian Networks: An Introduction,* 2011.

[44] **Walid Mechri**. *Évaluation de la performance des Systèmes Instrumentés de Sécurité à paramètres imprécis*. Automatique / Robotique. Université de Tunis El-Mana, 2011. Français.

[45] Arbre-Analyst. (n.d.). *Logiciel libre d'analyse d'arbres de défaillance*. Retrieved September 21, 2025, from https://www.arbre-analyste.fr/

[46] Microsoft. (2016, February 17). *MSBNx – Microsoft Bayesian Network Editor*. Microsoft Download Center.