Democratic and Popular Republic of Algeria
Ministry of Higher Education and Scientific Research
University of August 20, 1955, Skikda

Faculty of technology
Department of petrochemical and process engineering

Thesis presented for the degree of Master in petrochemical industries
Option: Automation in petrochemical industries

Theme:

Safety improvement using system theoretic process analysis STPA

Case study: Reactor 950-155 at CP2K-Sonatrach Skikda

By:
Maafi Israe

Supervised by:
Mechhoud El-Arkam

June 2025

Acknowledgment

With heart full of reverence, and with utmost gratitude, I bow my head before the almighty Allah, who's guidance and blessings have illuminated my path throughout this journey. Without his divine presence, this work would not have been possible.

I'm sincerely thankful to my supervisor, Mr. Mechhoud El-Arkam, for his invaluable guidance, encouragement, and insight throughout the research process. His support was instrumental in shaping this work.

I am especially thankful to my family for their love, understanding, and belief in me, even when the path seemed unclear. Your support has been my anchor.

Dedication

In the loving memory of my little angel in heaven,
forever in my heart, and always a part of everything I do.
I hope you're proud of what I become.

To the little girl who dreamed big,
who scribbled ideas in notebooks and wondered if she'd ever be enough—you made it.
Thank you for dreaming, for hoping, and for never giving up.
This is for you.

To my family and to my friends—
for the love, the strength, and the unwavering belief that carried me through,
your support made me what I am today.
It is lovely to have you in my life.

Abstract

Industrial safety is a crucial issue in high-risk fields like the petrochemical sector, where the complexity and the combination of advanced control systems, software, and human elements pose challenges to traditional risk assessment techniques. This thesis investigates the shortcomings of standard methods such as HAZOP, FMEA, and QRA, which frequently do not adequately address the dynamic interactions and systemic factors that lead to accidents in contemporary industrial settings. To overcome these limitations, the research delves into the use of System-Theoretic Process Analysis (STPA), a contemporary safety analysis approach based on systems theory. Created by Professor Nancy Leveson, STPA views safety as a control challenge rather than simply a matter of reliability. The thesis applies STPA to Reactor 950-155 at CP2K-Sonatrach Skikda, following its four primary steps and utilizing ALOHA for simulation purposes.

Key words: STPA, Risk Analysis, Hazard Identification, Control Structure, Unsafe Control Actions, Petrochemical Industry.

Résumé

La sécurité industrielle est un enjeu crucial dans les domaines à haut risque comme le secteur pétrochimique, où la complexité et la combinaison des systèmes de contrôle avancés, des logiciels et des facteurs humains représentent un défi pour les techniques traditionnelles d'évaluation des risques. Ce mémoire examine les insuffisances des méthodes standards telles que HAZOP, AMDE (Analyse des Modes de Défaillance et de leurs Effets) et AQR (Analyse Quantitative des Risques), qui ne parviennent souvent pas à traiter de manière adéquate les interactions dynamiques et les facteurs systémiques à l'origine des accidents dans les environnements industriels modernes. Pour dépasser ces limites, cette recherche explore l'utilisation de l'Analyse des Processus selon la Théorie des Systèmes (STPA), une méthode d'analyse de sécurité contemporaine fondée sur la théorie des systèmes. Développée par la Professeure Nancy Leveson, la STPA considère la sécurité comme un problème de contrôle plutôt qu'une simple question de fiabilité. Le mémoire applique la méthode STPA au reacteur 950-155 dans CP2K-Sonatrach skikda, en suivant ses quatre étapes principales et en utilisant ALOHA à des fins de simulation.

Mots-clés : STPA, Analyse des risques, Identification des dangers, Structure de contrôle, Actions de contrôle dangereuses, Industrie pétrochimique.

ملخص

تُعد السلامة الصناعية قضية أساسية في المجالات عالية الخطورة مثل قطاع البتروكيماويات، حيث تمثل التعقيدات ودمج أنظمة التحكم المتقدمة، والبرمجيات، والعوامل البشرية تحدياً كبيراً أمام تقنيات التقييم التقليدية للمخاطر. يتناول هذا البحث ، والتي غالباً ما لا تُعالج بشكل كافٍ التفاعلات QRAو FMEAو HAZOP أوجه القصور في الأساليب القياسية مثل الديناميكية والعوامل النظامية التي تؤدي إلى الحوادث في البيئات الصناعية الحديثة. لتجاوز هذه القيود، تتعمق هذه الدراسة ، وهو نهج حديث لتحليل السلامة يعتمد على نظرية النظم. وقد طورت (STPA) "في استخدام "تحليل العمليات النظمي أن السلامة هي تحدٍ في مجال التحكم وليست مجرد مسألة STPA هذا المنهج البروفيسورة نانسي ليفيسون، حيث تعتبر من خلال اتباع خطواتها Reactor 950-155 at CP2K-Sonatrach Skikdaعلى موثوقية. يطبّق هذا البحث منهجية لأغراض المحاكاة ALOHAالأربع الرئيسية، واستخدام

الكلمات المفتاحية: تحليل المخاطر، تحديد المخاطر، بنية التحكم، إجراءات تحكم غير آمنة، صناعة البتروكيماويات، STPA.

Abbreviations

ALOHA. Areal Locations of Hazardous Atmospheres

ASP. Accident Sequences Precursor

A-STPA. Automated STPA

CEI. Chemical Exposure Index

ETA. Event Tree Analysis

FEDI. Fire and Explosion Damage Index

FEI. Fire and Explosion Index

FMEA. Failure Modes and Effects Analysis, Failure Modes and Effects Analysis

FMECA. Failure Mode Effect Criticality Analysis

FTA. Fault Tree Analysis

HAZID. hazard identification

HAZOP. Hazard and Operability Study

HIRA. Hazard Identification and Ranking

IEC. International Electrotechnical Commission

ISO. International Organization for Standardization

MA. Maintenance Analysis

MOSAR. Method Organised Systematic Analysis of Risk

OHSAS. Occupational Health and Safety Assessment Series

ORA. Optimal Risk Assessment

PHA. Preliminary Hazard Analysis

PRA. Preliminary Risks Analysis

QRA. Quantitative Risk Assessment, Quantitative Risk Assessment

RBD. Reliability Block Diagram

SA. Safety Analysis

SCHAZOP. Safety Culture Hazard and Operability

SCRA. Short Cut Risk Assessment

STPA. System-Theoretic Process Analysis

TA. Task Analysis

TDI. Toxic Damage Index

UIC. Union des Industries Chimiques

WPAM. Work Process Analysis Model

Table of content

Chapter III: System theoretic process analysis

List of figures

List of tables

General introduction

General introduction

> "There are no accidents and no fatal flaws in the machines; there are only pilots with the wrong stuff ... no single factor ever killed a pilot; there was always a chain of mistakes" [1].
>
> —Tom Wolfe

Industrial safety remains a critical concern in process industries, especially within high-risk sectors such as petrochemicals. As systems grow more complex—integrating advanced control technologies, software components, and human interfaces—traditional methods of hazard identification (HAZID) and risk analysis often prove insufficient. Despite rigorous implementation of safety procedures and assessments, major industrial accidents continue to occur, highlighting the limitations of existing risk management frameworks [2].

Conventional safety analysis techniques, such as HAZOP (Hazard and Operability Study), FMEA (Failure Modes and Effects Analysis), and QRA (Quantitative Risk Assessment), have long served as the foundation for identifying potential hazards. However, these methods primarily rely on linear models and historical failure data. While effective in identifying failures at the component level, they struggle to capture the dynamic interactions, control errors, and systemic weaknesses that often underlie modern industrial accidents [3].

To address these challenges, a more comprehensive and system-oriented approach is needed—one that can account for the complexity of interactions within modern plants. System-Theoretic Process Analysis (STPA), developed by Professor Nancy Leveson at MIT, offers a powerful alternative. Unlike traditional methods that focus on failure probabilities, STPA is a relatively new safety analysis method based on system theory, which regards accidents as a control problem rather than a system failure problem. It is based on the assumption that hazards occur due to control actions not being provided when needed, or being provided when not needed. The method incorporates a more holistic view of the system compared to traditional techniques, taking into account interactions and factors both within the system but also beyond that [2]. Moreover, STPA has been argued by many publication and researches to be able to find more casual factors in a system than the conventional analysis methods [3].

General introduction

This thesis explores the use of STPA for safety improvement in **Reactor 950-155 at CP2K-Sonatrach Skikda**, through a structured and applied methodology. For this, several points have been set to achieve in order to reach the essential goal, our objectives are as follows:

- Understanding and mastery of the process with its functionality, and its components.
- Applying the four steps of the STPA study on the process (identify the accidents and hazards, Construct the control structure, Identify the unsafe control actions, determine how each Hazardous control action could occur).
- Give some recommendations.

My thesis is organized into 6 chapters:

- A general introduction.
- **Chapter I:** This chapter reviews the concept of industrial risks, with a focus on the process industry, the different risk management procedures, and the severe consequences that could be linked to it.
- **Chapter II:** This chapter examines traditional risk analysis methods such as HAZOP, FMEA, and QRA, and discusses their limitations in addressing complex system interactions.
- **Chapter III:** This chapter explains the principles and steps of the STPA method in detail.
- **Chapter IV:** Presentation of the CP2K Complex (SONATRACH – Skikda)
- **Chapter V:** Case study: application of STPA method on HDPE reactor
- A general conclusion.

Chapter I: General Overview of industrial risks

I.1. Introduction

Industrial development has traditionally been an important engine of economic growth and social advancement. Along with technological development comes an increase in hazards and accidents. All industrial activities especially the oil and gas, chemicals, pharmaceuticals, mining and nuclear energy industries involve complex processes and related hazardous materials that have the potential to create catastrophic accidents affecting people, the environment and infrastructure.

History has demonstrated the potential catastrophic impacts of industrial accidents with examples including the Bhopal disaster (India, 1984), the Seveso disaster (Italy, 1976) and the Fukushima disaster (Japan, 2011). These industrial accidents have shaped modern practices regarding safety, regulation, and risk management.

Understanding and managing the risks associated with industrial activity is an important step to reducing the likelihood of accidents and their impact.

I.2. Fundamental concepts on risk

I.2.1. Concept of risk

Risk is generally defined as the exposure of an individual or system to a hazard or an undesirable event that has a certain likelihood of occurring [Larousse, 2012]

- According to the ISO 31000 standard (2009), risk is often expressed as a combination of the consequences of an event and its likelihood;
  Risk can be defined as a quantification of a hazard, combining a measure of the occurrence of a feared event (probability or frequency) with an estimation of the severity of its consequences.
- Risk can also be defined as the "combination of the probability of occurrence of harm and the severity of that harm"

In an industrial system, risk is defined as the likelihood of an unforeseen or unfavorable event taking place within an industrial setting. This could result in various negative consequences including accidents, disruptions in production, financial setbacks, physical damage, environmental degradation, or threats to the well-being and safety of employees [4].

The previous definitions can be expressed through the following formula:

Risk (R)=Probability (P)×Gravity (G)

Where:

- **G**: Gravity of the consequences.
- **P**: Probability of occurrence.

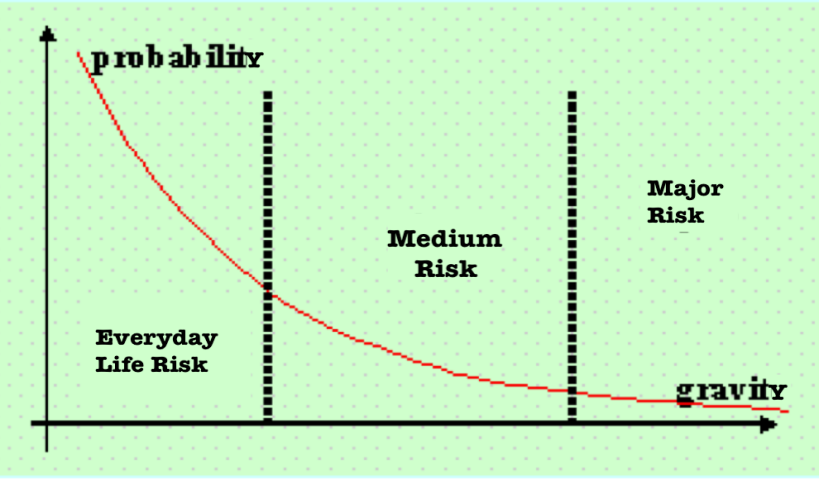


Figure I.1: Farmer Diagram (gravity – probability) [5]

I.2.2. Concept of hazard

It is important to note that various terms are used—depending on the standard or author—to describe the concept of a hazard, which can lead to confusion. Additionally, many dictionaries often equate the term "hazard" with "risk". In fact, several dictionaries treat risk as a synonym of hazard, which partly explains the confusion that can arise from this [6].

According to the IEC 61508 standard [IEC 98], a hazard is a potential threat that can cause harm to individuals, damage to property (deterioration or destruction), or harm to the environment. These hazards may directly affect people by causing physical injuries or health problems, or indirectly by damaging property or the environment [6].

The OHSAS 18001 frameworks [OHS 99] defines a hazard as a source or situation that can cause injury, health impairment, material damage, or environmental harm in the workplace—or a combination of these outcomes [6].

Hazards in the workplace can originate from many sources. General examples include substances, processes, practices, etc., that can cause harm or have a negative effect on human health or property.

Table I.2.2 below summarizes some examples of common hazards.

Workplace Hazard	**Example of Hazard**	**Example of Harm Caused**
Thing	Knife	Cut
Substance	Benzene	Leukemia
Material	Mycobacterium tuberculosis	Tuberculosis
Source of Energy	Electricity	Shock, electrocution
Condition	Wet floor	Slips, falls
Process	Welding	Metal fume fever
Practice	Hard rock mining	Silicosis
Behaviour	Bullying	Anxiety, fear, depression

Table I.1 - Examples of Hazards and Their Effects [6]

I.2.3. Concept of security

According to the ISO/IEC Guide 73:2002, safety is defined as the absence of unacceptable risk of injury or harm to people's health, either directly or indirectly, resulting from damage to equipment or the environment [7].

I.2.4. Concept of damage

All obstacles to the proper physical and psychological functioning of a human being.

The absence of circumstances likely to cause either an accident or death of personnel, or the degradation or loss of equipment or property [8].

I.2.5. Concept of accident

An unplanned and unexpected event that results in injury, illness, material damage, environmental harm, or even death. In an industrial context, accidents typically occur due to a failure in safety measures, human error, equipment malfunction, or hazardous conditions [7].

I.3. Classification of Risks

There are many criteria to classify risks. They can be classified according to their nature, origin, severity or affected area, and in order to assess risk correctly, we need to classify them properly to identify preventative and mitigation measures that can be put in place. The most noticeable classification is listed below [8]:

- **Natural Risks:**
  These are risks that originate from natural phenomena and are generally beyond human control. Examples include:
  - Earthquakes
  - Floods
  - Storms and lightning
  - Volcanic eruptions

- **Technological or Industrial Risks**:
  These arise from human activities, especially those involving complex industrial processes, energy use, or hazardous substances. This includes the following:

  - Chemical spills
  - Explosions
  - Fires
  - Equipment failures
- **Everyday life risks:** such as domestic accidents, road traffic accidents, etc.

- **Risks related to conflicts**

One of the most common classifications is to divide risks into two categories: natural risks and risks related to human activity. According to this classification, natural risks refer to events with no proven direct human cause**.**

Risks related to human activity encompass a wide range of diverse risk categories [8].

I.3.1. Industrial risk

I.3.1.1. Definition of an Industrial Risk

An industrial risk is an accidental event that occurs at an industrial site and results in serious immediate consequences for personnel, surrounding populations, property, or the environment.

Industrial risk arises from the implementation of human activities for technological purposes. t is associated with [8]:

- **The nature of the substances involved** (flammable, explosive, toxic);
- The **manufacturing processes** (depending on their state, temperature, or pressure, some products can become hazardous);
- The **facilities and equipment** (choice of machinery, materials, storage methods, etc.);
- The **human factor** (the majority of accidents occur due to negligence, lack of knowledge, or misjudgment);
- **External events** (flooding, earthquakes, accidents in neighboring industries, malicious acts, etc.).

I.3.1.2. Typology of Industrial Risks

Industrial risk is a hazardous event that can manifest in four main forms, which are:

- ✓ **Fire risk:**

A fire can occur when a substance ignites within its containment, such as in the case of a hydrocarbon tank fire, or following a loss of containment, as in a pool fire. It may be triggered by combustible solid materials or flammable liquids coming into contact with other products, a flame, or a hot spot [9].

Combustion, which is a complex chemical reaction, generates heat and flames.

For a fire to break out, three elements must be present:

- A **fuel** (combustible),
- An **oxidizer** (supporting combustion), and
- A **heat source**.

The fuel can be a solid (such as wood or paper), a liquid (like petroleum or solvents), or a gas (such as methane, propane, or butane).

The oxidizer is the substance that, when combined with the fuel, allows combustion to occur—examples include air**,** oxygen**,** or peroxides [9]**.**

✓ **Explosion risk:**

An explosion results from the ignition of an explosive mixture, a violent chemical reaction, a rapid combustion (of a gas or a cloud of dust), or a sudden decompression of a pressurized gas (such as the rupture of a compressed air cylinder). It can occur during the abrupt release of flammable vapors or gases mixed with air when in contact with an ignition source.

The shock wave generated causes overpressure, which can lead to internal injuries in the lungs and eardrums, as well as traumatic injuries [9].

✓ **Toxic Risk:**

Toxic risk typically arises from a loss of containment—for example, the rupture of a pipeline or the tearing of a storage tank—leading to the release of a toxic substance. This can involve gaseous toxic products at ambient temperature and pressure (such as ammonia) or volatile toxic substances (such as hydrochloric acid) that may escape into the atmosphere, forming a toxic cloud that spreads and dilutes in the air.

Such a cloud can also result from chemical reactions between incompatible substances during a process, often caused by a loss of process control or the accidental

introduction of an undesired material**.** Toxic risk is particularly severe for surrounding populations due to the potential for wide-scale exposure.

Inhalation of these gases can cause health effects ranging from mild irritations (such as eye or throat discomfort) to life-threatening conditions, including asphyxiation or pulmonary edema. Therefore, this type of risk is considered among the most hazardous in industrial environments [9].

- ✓ **Pollution Risk:**

The concept of pollution risk pertains to the probability and impact of harmful substances being discharged into the environment due to industrial operations. These harmful pollutants have the potential to degrade the quality of air, water, and soil, endangering ecosystems, human health, and the safety of nearby communities.

As a consequence of an industrial scenario, the pollution hazards could include:

Air pollution: consists of gases, (volatile organic compounds, sulphur dioxide and nitrogen oxides) which come from industrial operation, when combustion engines or fires and explosions are involved.

Water pollution: untreated or poorly treated industrial effluent disposed upon a water body has chemically contaminated it, having effectively destroyed the aquatic ecosystem.

Soil pollution: hazardous waste or chemical spills, which can migrate underground and destroy agricultural practices (and potentially enter the food chain).

Noise pollution and thermal pollution: can also easily be overlooked and are important nuisances to human and ecological health [10].

I.3.1.3. The Effects of Industrial Risk

Industrial risks are a form of technological risk. An industrial accident is considered major when it is both severe and unlikely to occur. Such accidents are classified based on their effects:

- ❖ **Toxic effect:** A leak of a toxic substance (such as chlorine, ammonia, phosgene, acid, etc.) in an industrial facility can cause serious injuries through inhalation, skin or eye contact, or ingestion. Potential health impacts

include acute pulmonary edema, damage to the nervous system, or chemical burns to the skin or eyes.

- **Thermal effect:** These effects are associated with the explosion or combustion of a flammable substance. They can cause burns of varying severity depending on the intensity and duration of exposure.
- **Mechanical effect:** They result from overpressure caused by a shock wave (deflagration or detonation) triggered by an explosion. The primary injuries include damage to the eardrums, lungs, and potentially other internal injuries due to the blast wave [8].

I.3.1.4. The consequences on people and property

When industrial risks materialize—such as fires, explosions, or toxic releases—they can produce both immediate and long-term consequences, on human health, property, and the environment:

- **Impact on human :**

  The primary impact of industrial accidents is on the health and safety of individuals. These impacts can manifest in various ways:

  - **Injuries and fatalities** are common outcomes of accidents like explosions, fires, and toxic releases, causing a range of harm from minor injuries to multiple deaths.

  - **Long-term health consequences** can arise from exposure to hazardous substances, even in small amounts over time, leading to chronic respiratory conditions, cancer, neurological issues, or reproductive disorders.

  - **Psychological distress** is another significant effect, with victims - including both workers and local residents - experiencing enduring mental health challenges like post-traumatic stress disorder (PTSD), anxiety, or depression in the aftermath of a major incident.

  - **Evacuation and displacement** may be necessary in situations of severe peril, requiring residents to leave their homes for extended periods, which can disrupt communities and daily routines [8].

- **Impact on property:**

Industrial accidents can also cause widespread material damage, including:

- Destruction of industrial infrastructure: Fires, explosions, or mechanical failure may damage or destroy facilities, machinery, and production equipment.
- Damage to public and private property: Shockwaves, flying debris, and secondary fires can impact neighboring buildings, roads, and utility networks.
- Economic losses: The financial cost of repairs, production stoppages, and compensation claims can be enormous. Insurance premiums may rise, and the company's reputation can suffer significantly.
- Environmental contamination leading to asset devaluation: Pollution of land or water can reduce the value of property, affect agriculture, and lead to costly clean-up operations.

In many cases, the domino effect can further aggravate consequences. For example, a fire in a chemical storage unit might lead to explosions, which in turn release toxic gases affecting populations kilometers away [8].

- **Impact on environment:**

In addition to the loss of human life and property, the environment often suffers great damage:

- Soil contamination from chemical spills impairs agricultural availability.
- Water pollution from untreated industrial wastewater discharges damages aquatic ecosystems.
- Air pollution from fires or gas releases leads to greenhouse gases or local toxicity.
- Loss of biodiversity due to disturbance or permanent changes in ecosystems [8].

I.3.2. Fire risk

The term "fire" was borrowed by the French language in the 16th century from the Latin "incendium" (blaze), derived from "incendere" (to ignite). It refers to a violent fire, a blaze that spreads to a building, a house, a forest, etc. Fire is an uncontrolled combustion reaction in time and space. [11]

For a fire to ignite, three conditions must be simultaneously present—this is commonly referred to as the "fire triangle" **Figure I.2** [12]:

- A **fuel**: a flammable substance (in solid, liquid, or gaseous form);

- An **oxidizer**: such as air, which contains oxygen;
- An **ignition source**: such as heat, an electrical spark, or a lit cigarette.

Figure I.2: Fire triangle. [12]

Starting in 1980, the fire triangle evolved into the fire tetrahedron. Indeed, a fourth essential element for combustion was identified: free radicals [13]

According to the tetrahedron of fire in **Figure I.3**, for combustion to occur, the following must be brought together [13]:

- A fuel,
- An oxidizer,
- Activation energy,
- A chemical reaction leading to the creation of free radicals.

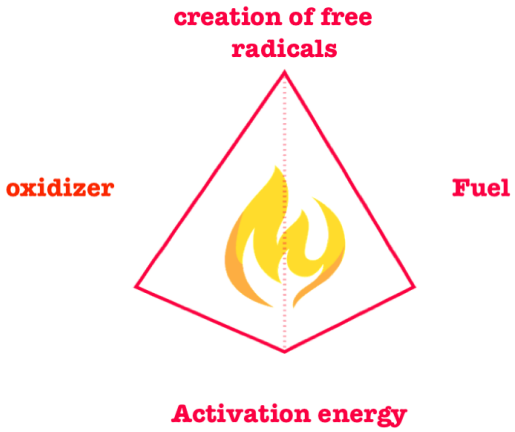


Figure I.3: The tetrahedron of fire. [13]

I.3.3. Explosion risk:

An explosion is a sudden oxidation or decomposition reaction that results in an increase in temperature, pressure, or both. It is a rapid release of energy through a high intensity combustion process.

For an explosion to occur, six conditions must be met simultaneously:

1. Ignition source
2. Suspended particles
3. Combustible materials
4. Sufficient confinement
5. Oxygen
6. Explosive range. [14].

These six conditions are generally represented in the form of the **"Explosion Hexagon." [15]**

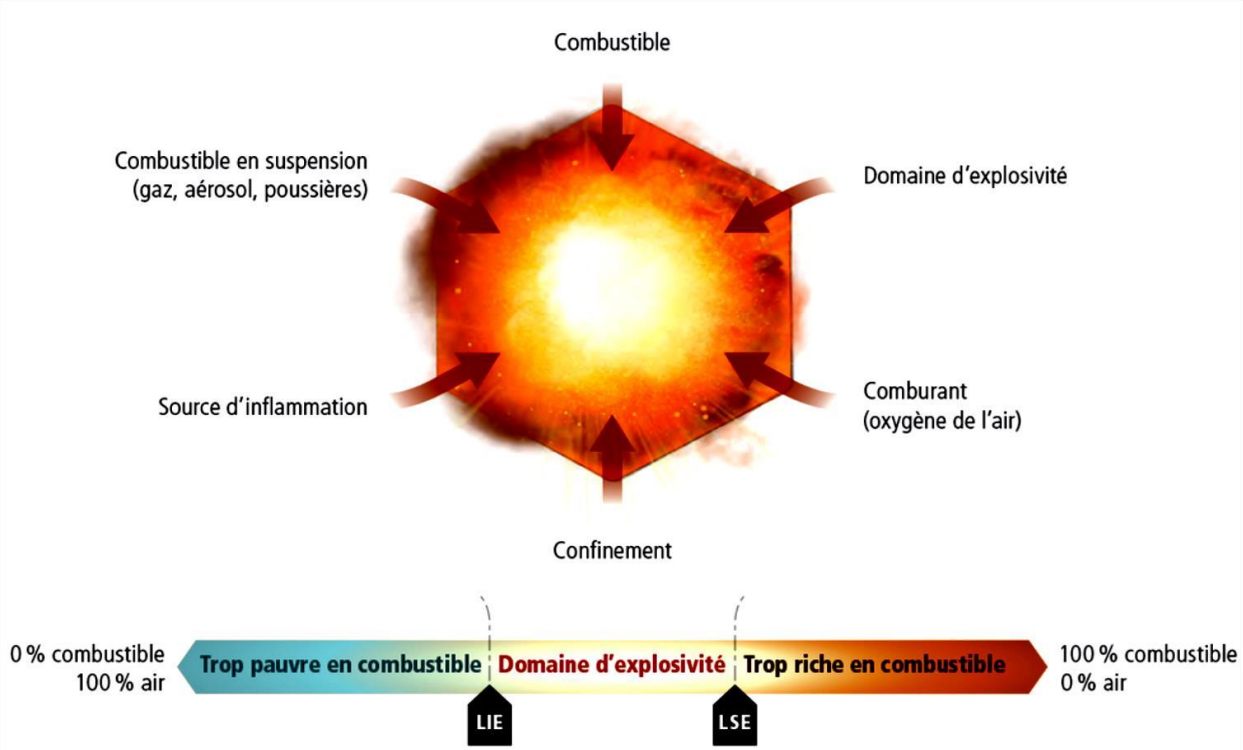


Figure I.4: The Explosion Hexagon [15].

I.3.4. Flare Fire

I.3.4.1 Description of the Phenomenon

In the industrial environment, flare fires, also known as torch fires, can occur as a result of accidental leaks of flammable fluids or intentional discharges of by-products through flare stacks [16]

Figure I.5: Flare fire. [17]

I.4. Risk Management

I.4.1. Definition of Risk Management

Risk management refers to the set of actions undertaken with the aim of reducing risks, starting from the identification and study of accidents, recognizing hazardous situations, identifying the corresponding risks, followed by their analysis, estimation, and evaluation.

Naturally, risk management does not end there, as it would be pointless without further action: the next step is to address the risks that have been assessed in order to reduce or control them. The only way to eliminate a risk entirely would be to eliminate its sources, which would mean rejecting the risk altogether [18].

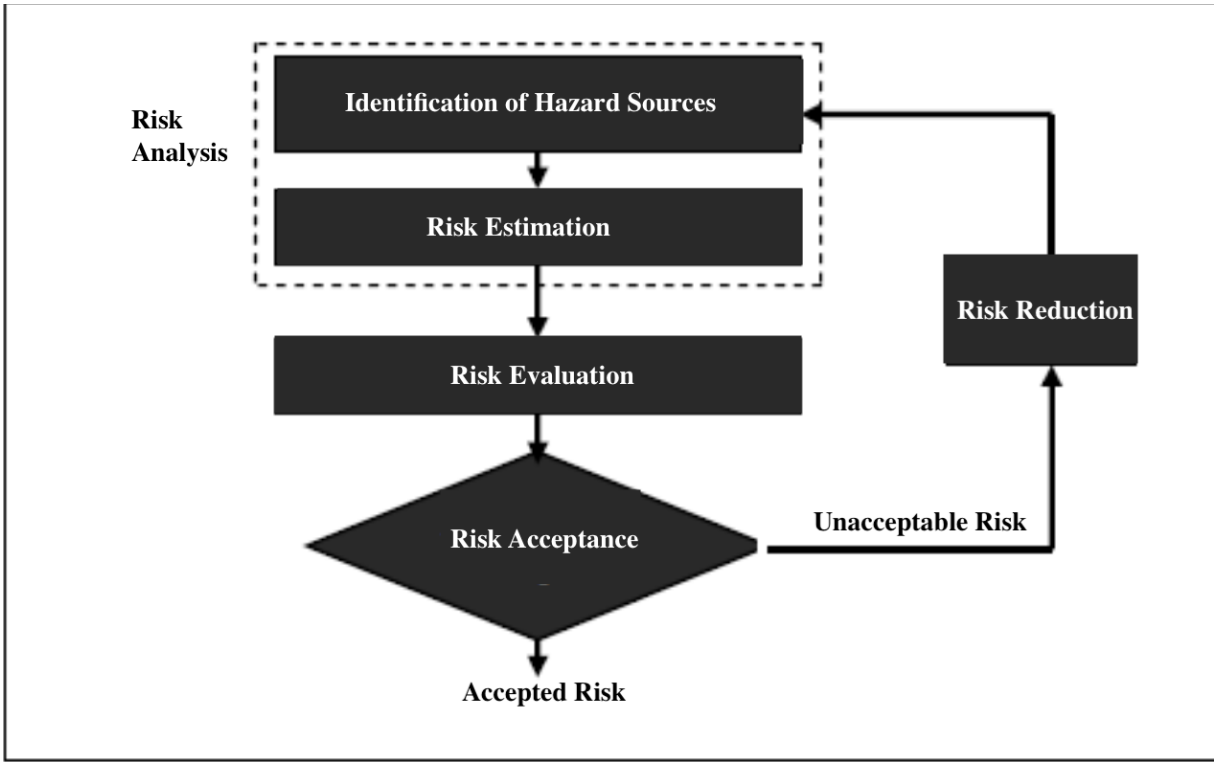


Figure I.6: Pr Risk Management Process (ISO/IEC Guide 73, 2009)

I.4.2. Steps of Risk Management

Risk management is typically structured into five key steps, each playing a crucial role in identifying, assessing, and mitigating potential dangers in industrial settings. These steps are as follows:

- Risk Analysis.
- Risk Estimation.
- Risk Evaluation.
- Risk Acceptance.
- Risk Reduction [8].

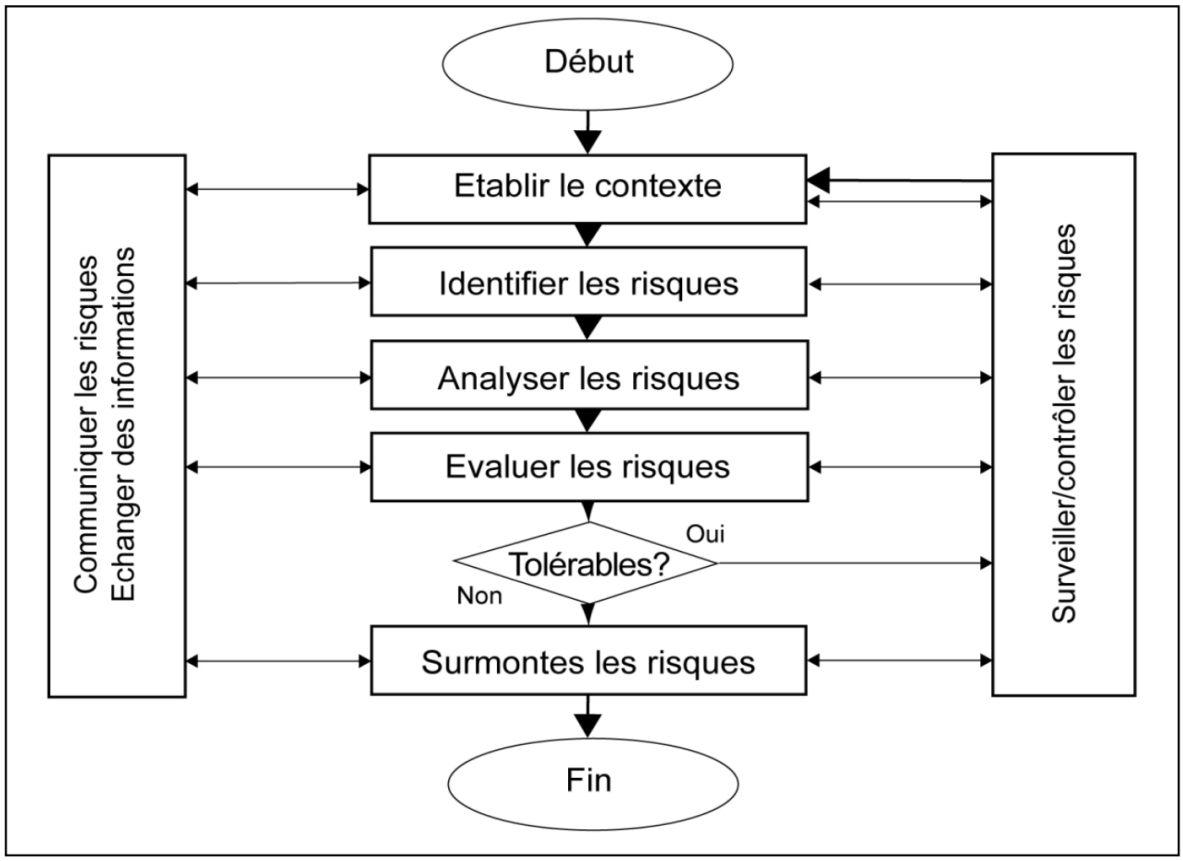


Figure I.7: Steps of Risk Management [8]

I.5. Conclusion

After considering the various aspects of industrial risks, it is evident that this subject is a pressing concern that is causing an increasing feeling of uncertainty. This situation highlights the need for ongoing and efficient contemplation. Therefore, it is essential to manage these industrial risks through suitable approaches.

Chapter II: Traditional risk Analysis Methods

II.1. Introduction

In the industrial sector, risk management is of crucial importance to ensure the safety, efficiency, and continuity of operations. Industrial systems are exposed to a multitude of potential risks, ranging from equipment failures and human errors to security incidents and environmental disruptions. Analyzing these risks not only allows for anticipation and mitigation but also transforms threats into opportunities for improvement and innovation.

Risk analysis methods are essential tools for identifying, evaluating, and mitigating potential hazards in industrial environments. These methods help decision-makers understand the nature of risks, their potential impacts, and the effectiveness of preventive measures.

There are therefore different methods with various objectives, depending on the company's needs in implementing its dynamic risk management system.

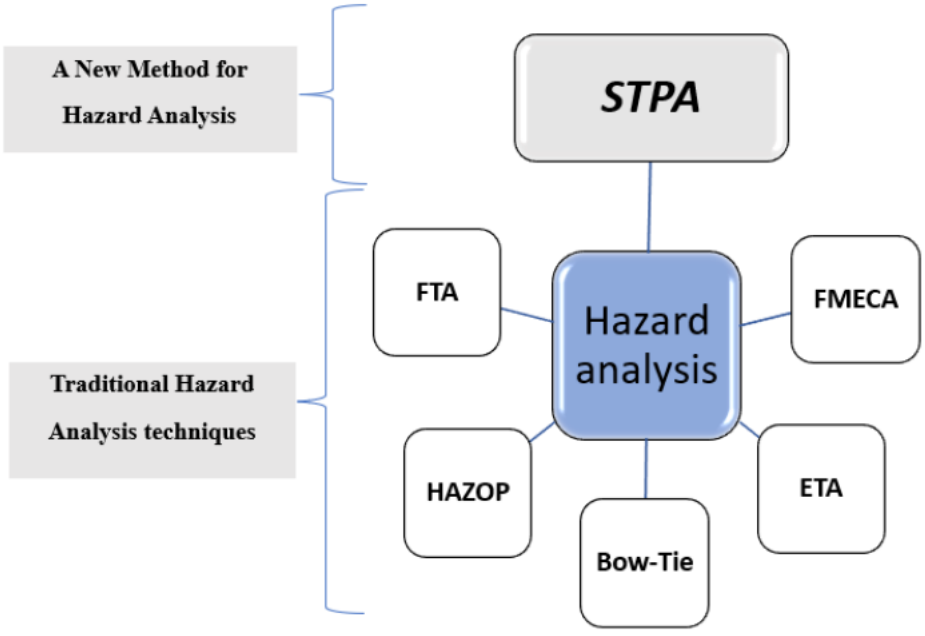


Figure II.1: Risk analysis methods

II.2. Risk analysis methods

To examine and assess the potential hazards present in different industrial facilities and locations, researchers have created risk analysis and evaluation techniques to aid in these evaluations.

These methods for risk analysis and evaluation are categorized based on various criteria. The classification of these risk analysis techniques is outlined and summarized in **Table II.1** below, as detailed in the study by J. Texier.

Table II.1: Classification of Some Risk Analysis Methods **[19]**

	Risk analysis methods			
	N°	**Qualitative**	**N°**	**Quantitative**
Determinist	1	Checklist	15	Dow's Chemical Exposure Index CEI
	2	Failure Mode Effect Analysis FMEA	16	Dow's Fire and Explosion Index FEI
	3	Hazard and Operability HAZOP	17	Fire and Explosion Damage Index FEDI
	4	Human Hazard and Operability	18	Hazard Identification and Ranking HIRA
		(Human HAZOP)	19	Methodology of domino effects analysis
	5	Optimal Hazard and Operability	20	Toxic Damage Index TDI
		(OptHAZOP)		
	6	Preliminary Risks Analysis PRA		
	7	Task Analysis TA		
	8	What if? Analysis		
Probability	9	Accident Sequences Precursor ASP	21	Event Tree Analysis ETA
	10	Delphi Technique	22	Fault Tree Analysis FTA
	11	Earthquake safety of structures and	23	Maintenance Analysis MA
		Installations in chemical industries	24	Short Cut Risk Assessment SCRA
			25	Work Process Analysis Model WPAM

Determinist & probability	12 13 14	Reliability Block Diagram RBD Safety Analysis SA Safety Culture Hazard and Operability SCHAZOP	26 27 28 29 30	Failure Mode Effect Criticality Analysis FMECA Method Organised Systematic Analysis of Risk MOSAR Optimal Risk Assessment ORA Probabilistic Safety Analysis PSA Quantitative Risk Assessment QRA

II.2.1. Preliminary Hazard Analysis (PHA)

II.2.1.1. History and Definition

Preliminary Hazard Analysis (PHA) was developed in the early 1960s within the aerospace and military sectors**.** Since then, it has been widely adopted across various other industries. In France, the "Union des Industries Chimiques" (UIC) has recommended its use since the early 1980s.

PHA is a general-purpose risk assessment method commonly applied for the identification of risks during the preliminary design phase of a facility or project. The primary objective of PHA is to identify potential hazards, evaluate their possible consequences, and establish preventive measures at an early stage of development.

One of the main advantages of PHA is that it does not require in-depth and detailed knowledge of the installation being studied. This makes it particularly suitable for early-stage projects where design details are still evolving [20].

II.2.1.2. Principles

Preliminary Risk Analysis first requires identifying the hazardous elements of the installation.

These hazardous elements most often refer to:

* Dangerous substances or preparations, whether in the form of raw materials, finished products, utilities...

* Dangerous equipment such as storage areas, reception-shipping zones, reactors, utility supplies (boiler...),
* Dangerous operations associated with the process.

-The identification of these dangerous elements depends on the type of installation studied. The APR can be implemented with or without the help of a list of typical risks or by applying the Haxo guidelines.

-It should also be noted that the identification of these elements is based on the functional description carried out prior to the implementation of the method.

-From these hazardous elements, the APR aims to identify, for a hazardous element, one or more danger situations. Within the framework of this document, a danger situation is defined as a situation which, if not controlled, can lead to the exposure of issues to one or more dangerous phenomena.

-The working group must then determine the causes and consequences of each identified danger situation and then identify the existing safety measures on the studied system. If these measures are deemed insufficient relative to the level of risk identified in the criticality grid, proposals for improvement should then be considered [20].

II.2.1.3. Procedure

The use of a summary table provides a practical tool for guiding reflection and summarizing the results of the analysis. However, risk analysis is not limited to simply filling out a table at any cost. Furthermore, this table must sometimes be adapted according to the objectives set by the working group prior to the analysis [20].

Table II.2 below is therefore provided as an example:

Table II.2: Example of a (PHA) table.

System:						Date:	
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
N°	Hazardous Element	Potential Hazard	causes	consequences	Existing Safety Measures	Recommended Actions	Observations

II.2.1.4. Advantages and Limitations

The main advantage of Preliminary Hazard Analysis (PHA) is that it allows for a relatively quick examination of hazardous situations in industrial installations. Compared to other methods, it is considered relatively economical in terms of time spent and does not require a very detailed description of the system being studied.

This advantage is naturally linked to the fact that PHA is generally implemented during the design stage of installations, where detailed information may still be limited, but early detection of risks is crucial for safety planning.

On the other hand, PHA does not allow for a detailed characterization of the sequence of events that could lead to a major accident in complex systems [20].

As its name suggests, it is primarily a preliminary analysis method designed to identify critical points that require more in-depth studies. It helps to highlight equipment or installations that may need more detailed analysis, which can be carried out using tools such as FMEA**,** HAZOP, or FTA.

However, its use alone may be considered sufficient in the case of simple installations or when the analysis team has significant experience with this type of approach.

II.2.2. Failure Modes and Effects Analysis (FMEA)

II.2.2.1. History and Application Domains

The Failure Mode and Effects Analysis (FMEA) was used for the first time in the aerospace industry during the 1960s. Its use has since become widespread in other sectors such as the chemical, petroleum, and nuclear industries.

In fact, it is primarily suited for studying failures of materials and equipment and can be applied to different technology systems (electrical, mechanical, hydraulic systems, etc.) as well as to systems combining multiple techniques [20].

II.2.2.2. Principal of FMEA

Identify potential error risks (or failure modes), evaluate their effects, and analyze their causes.

FMEA is about identifying and prioritizing potential failure modes that could occur on equipment, investigating their effects on the main functions of the equipment, and identifying their causes. For determining the criticality of failure modes, FMEA requires for each failure mode an assessment of the severity of its effects, the frequency of its occurrence, and the detectability probability. When all this information is available, different methods exist to derive a criticality value for the failure mode. If the criticality is deemed unacceptable, it is then imperative to define corrective actions to be able to address the new severity of the failure mode (if this is indeed possible), and to modify its occurrence frequency. [20].

II.2.2.3. The Steps of the FMEA Method

The method follows an eight-step approach: [20]

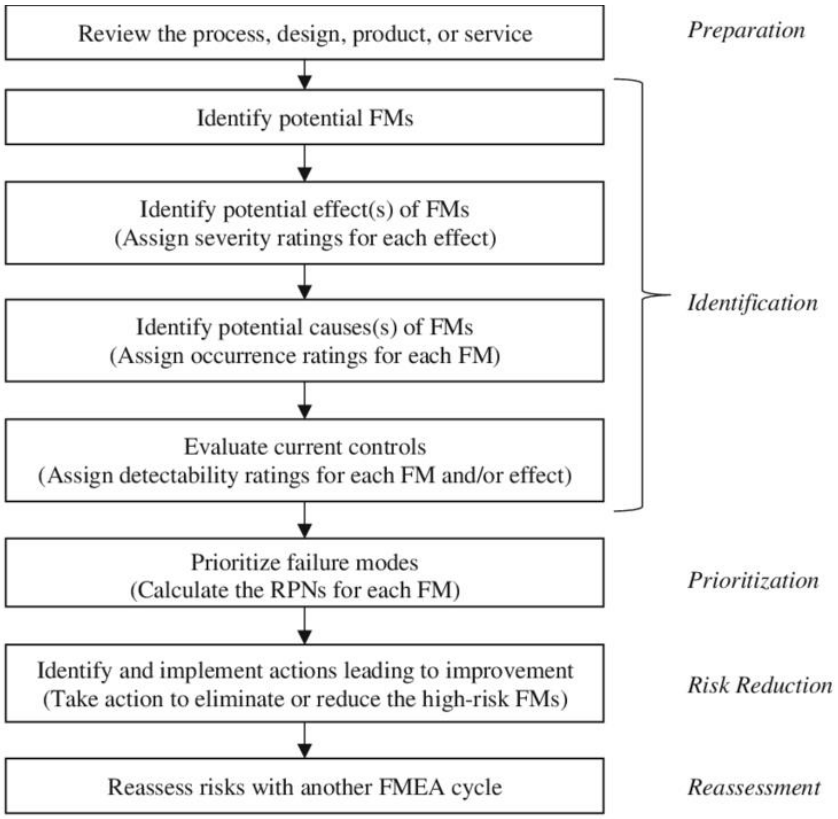


Figure II.2: The FMEA approach [20]

II.2.2.4. Advantages and Limitations

FMEA proves to be very effective when implemented for analyzing simple component failures that lead to the overall failure of the system. Due to its systematic nature and typically fine level of detail, it serves as a valuable tool for identifying potential failures and determining ways to limit their effects or prevent their occurrence.

Since it involves examining each failure mode, its causes, and its effects for the different operating states of the system, FMEA helps to identify common failure modes that could affect the studied system. Common failure modes correspond to events that, due to their nature or the dependency of certain components, simultaneously cause failure states in multiple system components. Utility losses or major external aggressions generally represent common failure modes.

In the case of particularly complex systems with a large number of components, conducting an FMEA can be very challenging and especially tedious given the substantial amount of information to process. This difficulty is further amplified when the system in question has many operating states.

Moreover, FMEA focuses on simple failures and can be effectively complemented, depending on the analysis needs, by methods dedicated to studying multiple failures, such as Fault Tree Analysis (FTA). [20].

II.2.3. The HAZOP Method (Hazard and Operability Study)

II.2.3.1. The Objective

The HAZOP method is part of an approach aimed at improving safety and processes for an existing or planned installation, with its advantages:

❖ Conducting the study within a working group bringing together various fields: safety, engineering, operations, maintenance...

❖ A systematic analysis method related to installations with fluid circuits

❖ Contributing to compliance with safety standards [9]

II.2.3.2. General Principles of the HAZOP Method

The HAZOP method is dedicated to the risk analysis of thermo-hydraulic systems for which it is crucial to control parameters such as pressure, temperature, flow rate, fluid flow, etc.

The principle of HAZOP is to associate keywords with the parameters related to the studied installation in order to identify deviations. Unlike FMEA, which focuses on failure modes, HAZOP considers potential deviations of the main parameters linked to the operation of the installation.

As a result, it is centered on the process operation, whereas FMEA is focused on the functioning of the installation's components [22].

II.2.3.3. Description of the Method

- ❖ Definition of the system to be studied
- ❖ Understanding of the system
- ❖ Specific elements of the method
- ❖ Presentation of the HAZOP table
- ❖ Analysis of malfunctions and implementation of recommendations
- ❖ When to use HAZOP?
- ❖ Application of the method on a case study [21]

II.2.3.4. Guide Words and Deviations

The guide words, associated with important parameters for the process, allow for the systematic generation of deviations to be considered. The IEC 61882 standard provides examples of guide words that are particularly commonly used [23].

I.2.3.5. Operating Parameters

The operating parameters, which may affect the safety of the installation, must be selected. Frequently, the parameters on which the analysis focuses are:

- Temperature
- Pressure
- Flow rate
- Level
- Concentration
- Viscosity
- Time
- Operations performed

The combination of these parameters with the previously defined guide words allows for the generation of deviations of these parameters. For example:

- "More" and "Temperature" = "Temperature too high."
- "Less" and "Pressure" = "Pressure too low."
- "Reverse" and "Flow rate" = "Product backflow."

– "No" and "Level" = "Empty capacity" [23].

II.2.3.6. Advantages and Limitations

HAZOP is a particularly effective tool for thermo-hydraulic systems. Like FMEA, this method is systematic and methodical. Moreover, by focusing solely on deviations of the system's operating parameters, it avoids having to consider, as FMEA does, all possible failure modes for each of the system's components.

However, in its classic version, HAZOP does not allow for the analysis of events resulting from the simultaneous combination of multiple failures.

Moreover, it is sometimes difficult to assign a guide word to a well-defined portion of the system being studied. This significantly complicates the exhaustive identification of potential causes for a deviation. Indeed, the systems being analyzed are often composed of interconnected parts, so a deviation occurring in one line or node may have consequences or, conversely, causes in a neighboring node, and vice versa. Of course, it is possible in principle to transfer the implications of a deviation from one part to another of the system. However, this task can quickly become complex.

Finally, since HAZOP addresses all types of risks, it can be particularly time-consuming to implement and may result in the generation of a large amount of information that does not pertain to major accident scenarios [20].

II.2.4. The Fault Tree Analysis Method (FTA)

II.2.4.1 Principle of the FTA

A fault tree represents, in a synthetic way, all the combinations of events that, under certain conditions, produce a given event, which is the starting point of the study. Building a fault tree is equivalent to answering the question "How can this event happen?" or "What are all the possible sequences that can lead to this event?" [24].

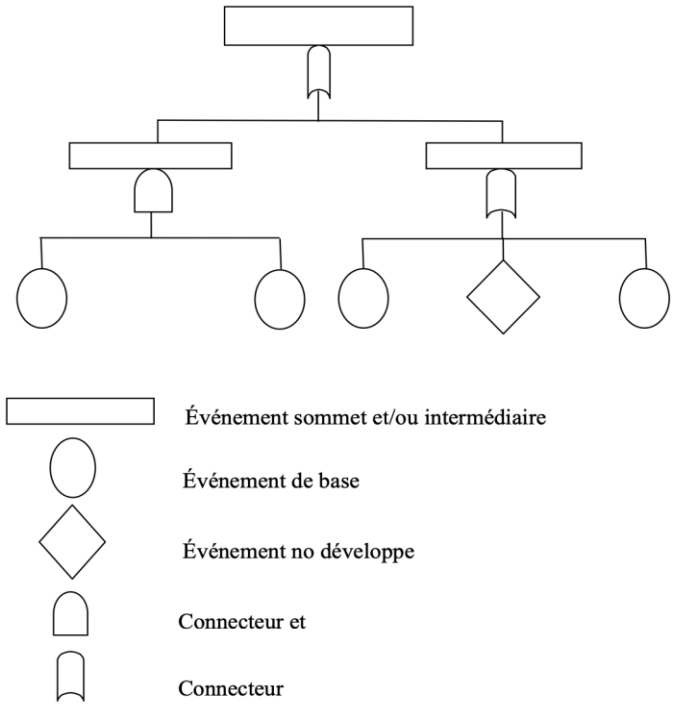


Figure II.3 Fault Tree Analysis (FTA)

II.2.4.2. Steps of the Method

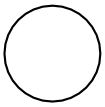
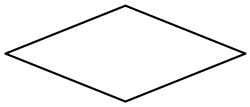
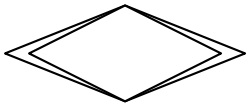
The Fault Tree Analysis (FTA) method consists of six steps:

1. Definition of the system to be studied
2. Definition of the undesirable event
3. Construction of the Fault Tree (FTA)
4. Qualitative analysis of the Fault Tree
5. Quantitative analysis of the Fault Tree:
   - Collection of quantitative data related to Basic Events (BEs)
   - Calculation of the probability of the Top Event (TE) of the Fault Tree
   - Importance analysis and uncertainty calculation
6. Analysis of results and recommendations

II.2.4.3. Characteristics of the FTA

A fault tree is generally presented from top to bottom (**Figure II.3**). The top line contains only the event for which we want to describe how it can occur. Each subsequent line breaks down the previous one, presenting the combination or combinations that could produce the event in the line above to which they are linked. These relationships are represented by logical OR or AND gates. [24]

Table II.3: Graphic Symbols for Events and Transfers **[25]**

Symbole	***Appellation***	***Signification***
	*rectangle*	*Représente un événement qui résulte de la combinaison d'événements plus élémentaires agissant à travers des portes logiques.*
	*Cercle*	*Représente un événement*
	*Losange*	*Représente un événement qui ne peut être considéré comme élémentaire mais dont les causes ne seront pas développées*
	*Double losange*	*Représente un événement dont les causes ne sont pas encore développées, mais le seront ultérieurement*
①  ② 	*Triangle*	*La partie de l'arbre qui suit le symbole ① est transféré à l'endroit indiqué par le symbole②.*
①  ② 	*Triangles inverses*	*Une partie semblable mais non identique à celle qui suit le symbole ① est transféré à l'endroit indiqué par le symbole②.*

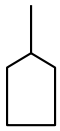
	*Maison*	*Représente un événement qui correspond à une utilisation normale du système.*

Table II.4: Graphic Symbols for Logic Gates

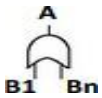
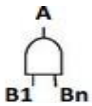
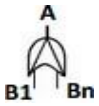
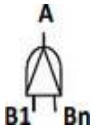
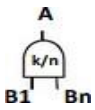
Symbole	*Appellation*	*Signification*
	**OU**	*La sortie A est gérée si au moins une des entrées B1,…, Bn existe*
	**ET**	*La sortie A est générée si toutes les entrées B1,…, Bn existe*
	**OU Exclusive**	*La sortie A est générée si une entrées et une seule Bi (i=1 à n) existe*
	**ET Prioritaire ou séquentiels**	*La sortie A est générée si toutes les entrées B1,…, Bn existent avec un ordre d'apparition donné*
	**Voteur k/n**	*La sortie A est générée si k entrées Parmi les n entrées existent*

Table II.3: Graphic Symbols for Logic Gates

II.2.4.4. The Objective of FTA

The qualitative objective is to construct a synthesis of everything that can lead to an undesired event and to evaluate the effect of a system modification, as well as to compare the consequences of measures that can be considered to reduce the occurrence of the undesired event being studied. [24]

II.2.4.6. Advantages and Limitations

The main advantage of Fault Tree Analysis is that it allows for the consideration of combinations of events that can ultimately lead to an undesired event. This capability provides a good alignment with the analysis of past accidents, which shows that major accidents often result from the conjunction of several events that, individually, would not have led to such disasters.

Furthermore, by aiming to estimate the probabilities of occurrence of events leading to the final event, it provides criteria to determine priorities for the prevention of potential accidents.

Fault Tree Analysis focuses on a specific event, and its application to an entire system can be cumbersome. In this regard, it is advisable to first implement inductive risk analysis methods. These tools allow, on one hand, the identification of the most severe events that can then be the subject of Fault Tree Analysis, and on the other hand, they help facilitate the determination of the immediate, necessary, and sufficient causes at the level of the tree's construction.

For about fifteen years, software tools have been marketed to make the application of Fault Tree Analysis easier. These tools are very useful for finding minimal cut sets, determining probabilities, and graphically presenting the results in a tree structure [20].

II.2.5. The Event Tree Analysis Method (ETA)

II.2.5.1. Description of the ETA

The event tree graphically illustrates the potential consequences of an accident resulting from an initiating event (a specific equipment failure or human error). An Event Tree Analysis (ETA) takes into account the response of safety systems and operators to the initiating event when assessing the potential consequences of the accident. The results of the ETA are accident sequences; that is, a set of failures or errors that lead to the accident.

These results describe the potential consequences in terms of event sequences (success or failure of safety functions) that follow an initiating event. Event Tree Analysis (ETA) is well-suited for studying complex processes that have multiple protection barriers or emergency procedures in place to respond to a specific initiating event [20].

The event tree is a deductive method that starts from the initiating event leading to an undesired event, considering the success or failure of safety functions, and then defining the events likely to occur downstream of the initiating event. The safety barriers and their functions must be identified and assigned failure probabilities.

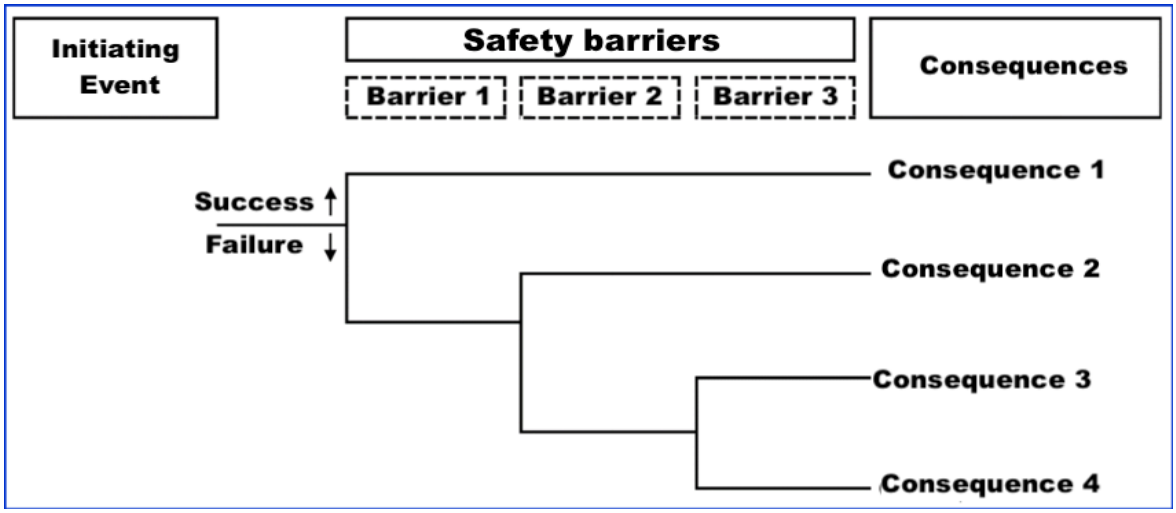


Figure II.4: Diagram of an ETA with Safety Barriers [20]

As shown in **Figure II.4,** the constructed Event Tree allows for the temporal identification of the different event sequences that may or may not lead to boundary consequences. The most dangerous paths leading to catastrophic consequences are then analyzed in detail.

II.2.5.2. The Objective of the ETA

Event trees are used to identify the various accidents that may occur in a complex system. Following the identification of individual accident sequences, the specific combinations of failures that can lead to accidents can be determined using the event tree. The event tree allows for:

- To identify all the causes and combinations of causes leading to the top event;
- To determine if each reliability characteristic of the system complies with the prescribed objective;
- To verify the assumptions made during other analyses regarding the independence of systems and the exclusion of certain failures;

- To identify the factor(s) that have the most harmful impact on a reliability characteristic, as well as the necessary modifications to improve this characteristic;
- To identify common events or common-cause failures [20].

II.2.5.3. Applications of the Event Tree

The event tree is used to identify the various events that may occur in a complex system. Following the identification of individual accident sequences, the specific combinations of failures that lead to accidents can then be determined using the fault tree [20].

II.2.5.4. Principle of the Event Tree

The Event Tree Analysis (ETA) evaluates the potential for accidents resulting from equipment failure or process disturbances (initiating event). Unlike Fault Tree Analysis (a deductive approach), ETA is an inductive reasoning method where the analyst starts with an initiating event and develops the probable sequence of events that lead to potential accidents, taking into account both the success and failure of safety barriers as the accident progresses.

Event trees provide a systematic way to record accident sequences and define the relationship between initiating events and the sequence of events that can result in accidents.

Event trees are well-suited for analyzing initiating events that could lead to a variety of consequences. An event tree highlights the initial cause of potential accidents and works from the initiating event to the final effects. Each branch of an event tree represents a separate accident sequence that, for a given initiating event, is a set of relationships between safety barriers [20].

II.2.5.5. The Advantages and Limitations

Event Tree Analysis (ETA) is a method that allows examining, starting from an initiating event, the sequence of events that may or may not lead to a potential accident. It is particularly useful for studying the architecture of existing or potential safety measures (prevention, protection, intervention) on a site. For this reason, it can also be used for post-accident analysis.

However, this method can be cumbersome to implement. Consequently, it is important to carefully define the initiating event that will be the subject of this analysis [20].

II.2.6. The Bow-Tie Method

II.2.6.1. Description of the Bow-Tie Method

A structured method consisting of listing all the hazards present in the studied installations, estimating their potential consequences, and classifying them in terms of severity/probability using an appropriate matrix. This classification allows for the identification of all scenarios with unacceptable potential consequences, for which a detailed risk analysis study will be carried out by introducing the concept of barriers.

The Bow-Tie method, used in many industrial sectors, was developed by the Shell company. It follows a tree-like approach that allows for a quick visualization of the possible causes of an accident, its consequences, and the barriers put in place. The undesired accident (in the center) can result from several possible causes, such as the loss of containment of a toxic substance, an explosion, a pipeline rupture, a runaway reaction, a breach in a tank, a substance decomposition, etc.

This tool helps illustrate the result of a detailed risk analysis (such as FMEA, HAZOP, or What-if analysis), which is more complex than a preliminary risk assessment [26].

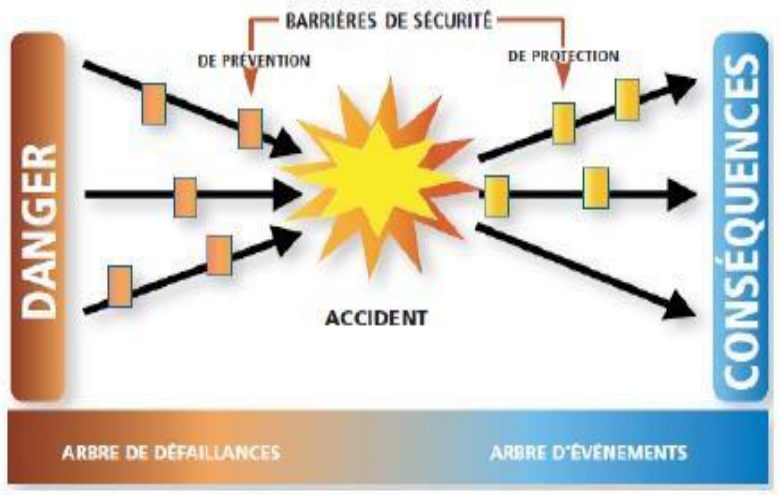


Figure II.5: Example of the Bow-Tie Method **[20]**

The left part of the bow-tie represents the identification of hazards, possible causes of the accident, and the various sequences or combinations (black arrows) that could lead to the undesired accident. Between these possible causes and the accident, so-called prevention barriers (orange rectangles) must be installed.

The right side of the node represents the possible consequences of the accident. For example, in the case of a pipeline rupture or a breach in a reservoir, it could result in the formation of a puddle or a cloud. Between this accident and the receptors, protective barriers must be installed to reduce the effects on these receptors.

So, the Bow-Tie reflects the accident scenarios that could occur and the measures taken to prevent them or reduce their likelihood, as well as those taken to reduce their consequences. This refers to prevention barriers and protection barriers.

II.2.6.1. Principle

The bow-tie is a tool that combines a failure tree and an event tree, represented in a slightly different way than described in the previous paragraphs. **Figure II.6** provides a schematic representation in the following form, where the barriers are depicted by vertical bars.

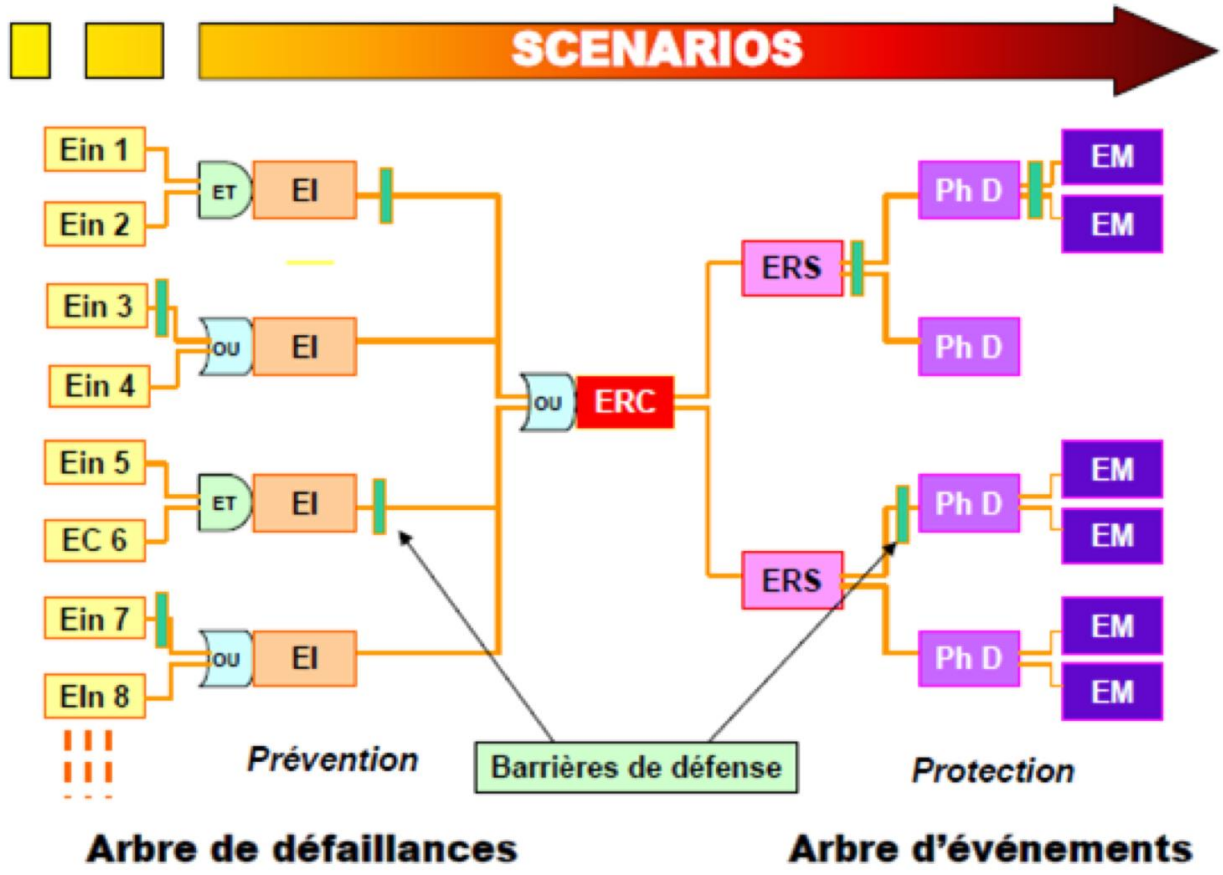


Figure II.6: Representation of accident scenarios according to the Bow-Tie model **[26]**

II.2.8.3. Advantages and Limitations [14]

The Bow-Tie node provides a concrete visualization of the accident scenarios that could occur, starting from the initial causes of the accident to the consequences at the level of the identified vulnerable elements.

As a result, this tool clearly highlights the role of safety barriers against these accident scenarios and provides a stronger demonstration of risk management control.

On the other hand, it is a tool whose implementation can be particularly time-consuming. Therefore, its use should be decided for cases that genuinely justify such a level of detail.

II.3. Conclusion

In this chapter, we explored traditional risk management methods that allow for the systematic identification of the different components of risk. Various risk situations, feared events, causes, consequences, and potential accidents are all methodically identified and presented in table form, as is the case with HAZOP, FMEA, or in a tree structure, like the Fault Tree or Event Tree.

Traditional risk analysis methods ensure the proper functioning of industrial systems and control risks; although they were proven insufficient. In our study, we focus on the application of the STPA (System-Theoretic Process Analysis) method to improve the safety in reactor reactor 950-155 at CP2K-Sonatrach Skikda.

Chapter III: System theoretic process analysis

III.1. Introduction

Currently among the various hazard analysis methods, one that is system-theoretic in nature is the System-Theoretic Process Analysis (STPA). This is a deductive (top- down) method, based on the STAMP accident model, both well-funded on Systems and Control theory rather than reliability theory.

The method targets failure of more complex systems, such as software intensive systems (systems which intensely make use of software) or socio-technical systems (systems which include human operators) [Leveson, 2004].

Even though the goal of this chapter is not to meticulously discuss the STPA method, we will briefly present it.

III.2. System Theory

Systems theory was developed to deal with modern systems. It forms the basis for system engineering, where the whole is considered to be more than the sum of the parts and top- down analysis and development is used. Systems theory deals with properties (called emergent properties) that can only be handled adequately holistically, taking into account all the technical and social aspects. These properties arise in the relationships and interactions among system components or behavioral events. That is, systems theory treats systems as a whole and not the components and events separately. In systems theory, instead of breaking systems into interacting components, systems are viewed (modeled) as a hierarchy of organizational levels. At the lowest level of road traffic, there are the individual vehicles, such as cars and trucks. At the next level, there is the design of the roads, which controls the movement of the individual vehicles and their interactions. At a higher level, one can conceive of the entire highway system including the roads but also the rules and policies imposed on the drivers of the vehicles [27].

III.3. Systems Thinking

System thinking is a term that denotes processes and ways of thinking that follow the principles of systems theory and incorporate systemic causality. Senge (1990) writes: [Systems thinking] shifts thinking from blaming a single individual or department, to recognizing that sometimes the problem or fault lies in the entire system and that everybody plays a significant role Causation becomes multi-causal. In mastering systems thinking, we give up the assumption that there must be an individual or individual agent, responsible. The feedback perspective suggests that everyone shares responsibility for problems generated in a system [28].

By applying systems thinking to safety engineering, we will be able to handle more complexity and more causal factors in safety engineering [28].

III.4. Stamp (Systems-Theoretic Accident Model and Processes)

STAMP (System-Theoretic Accident Model and Processes) is the name of the new accident causality

model based on systems theory, which provides the theoretical foundation for STPA. It expands the traditional model of causality beyond a chain of directly-related failure events or component failures to include more complex processes and unsafe interactions among system components, and it underlies STPA and other tools.

In STAMP, safety is treated as a dynamic control problem rather than a failure prevention problem.

No causes are omitted from the STAMP model, but more are included and the emphasis changes from preventing failures to enforcing constraints on system behavior.

Some advantages of using STAMP are that:

- It works on very complex systems because it works top-down rather than bottom up.
- It includes software, humans, organizations, safety culture, etc. as causal factors in accidents and other types of losses without having to treat them differently or separately.

- It allows creating more powerful tools, such as STPA, accident analysis (CAST), identification and management of leading indicators of increasing risk, organizational risk analysis, etc.

Because STAMP applies to any emergent property, STPA can be used for any system property, including cybersecurity.

The two most widely used STAMP-based tools today are STPA (System Theoretic Process Analysis) and CAST (Causal Analysis based on Systems Theory). STPA is a proactive analysis method that analyzes the potential cause of accidents during development so that hazards can be eliminated or controlled.

CAST is a retroactive analysis method that examines an accident/incident that has occurred and identifies the causal factors that were involved. This handbook concentrates on the use of STPA. future, similar handbook is planned for CAST [27].

III.5. Introduction to the STPA

III.5.1. Background and origins

In 2004, Nancy G. Leveson proposed a new model of accident causation called STAMP (Systems-Theoretic Accident Model and Processes), marking a significant departure from traditional safety engineering approaches. Unlike older models that focus primarily on failures of individual components, STAMP is grounded in system theory and views systems as dynamic entities composed of interrelated components. These components are maintained in a state of dynamic equilibrium through continuous feedback loops of information and control. This perspective is particularly useful for analyzing complex system accidents, where the interactions between components—and not just their failures—play a critical role in the emergence of unsafe conditions [29].

Under the STAMP model, safety is conceptualized as a control problem rather than solely a reliability problem. Instead of defining safety management in terms of preventing discrete component failures, it is defined as a continuous process of imposing and enforcing constraints on

system behavior. These constraints are essential for guiding system operations and adaptations in a safe direction. Accidents, therefore, are not merely the result of broken parts or isolated malfunctions. They occur when external disturbances, internal component failures, or dysfunctional interactions are not properly managed by the system's control structure. In this context, safety depends on the system's ability to adapt, respond, and maintain control under varying operational conditions.

STAMP introduces several core concepts that distinguish it from earlier models. These include constraints, control loops and process models, and hierarchical levels of control. Rather than interpreting accidents as a linear chain of events, STAMP encourages a broader systems-theoretic view where the cause of an accident lies in the absence or failure of constraints at various levels of the socio-technical system. Each level of a system imposes constraints on the level below it, and safety can be compromised if these constraints are inadequately designed, poorly enforced, or misunderstood. Therefore, system models must be structured hierarchically, incorporating control processes and constraints that operate at the interfaces between levels.

To illustrate this, Leveson presents a generalized control structure of a socio-technical system (see **Figure III.1**), in which each controller within the system must have a defined goal, the capability to influence the system, and the means to monitor its status. If any of these elements are missing or ineffective, the system becomes vulnerable to unsafe conditions. Within this framework, safety becomes an emergent property that must be proactively managed across all organizational and technical levels.

This systems-theoretic foundation laid by STAMP eventually led to the development of a practical hazard analysis technique known as STPA (Systems-Theoretic Process Analysis), which applies these principles to real-world engineering contexts. STPA builds upon the STAMP model and provides a structured method for identifying unsafe control actions, understanding causal factors, and designing more resilient systems.

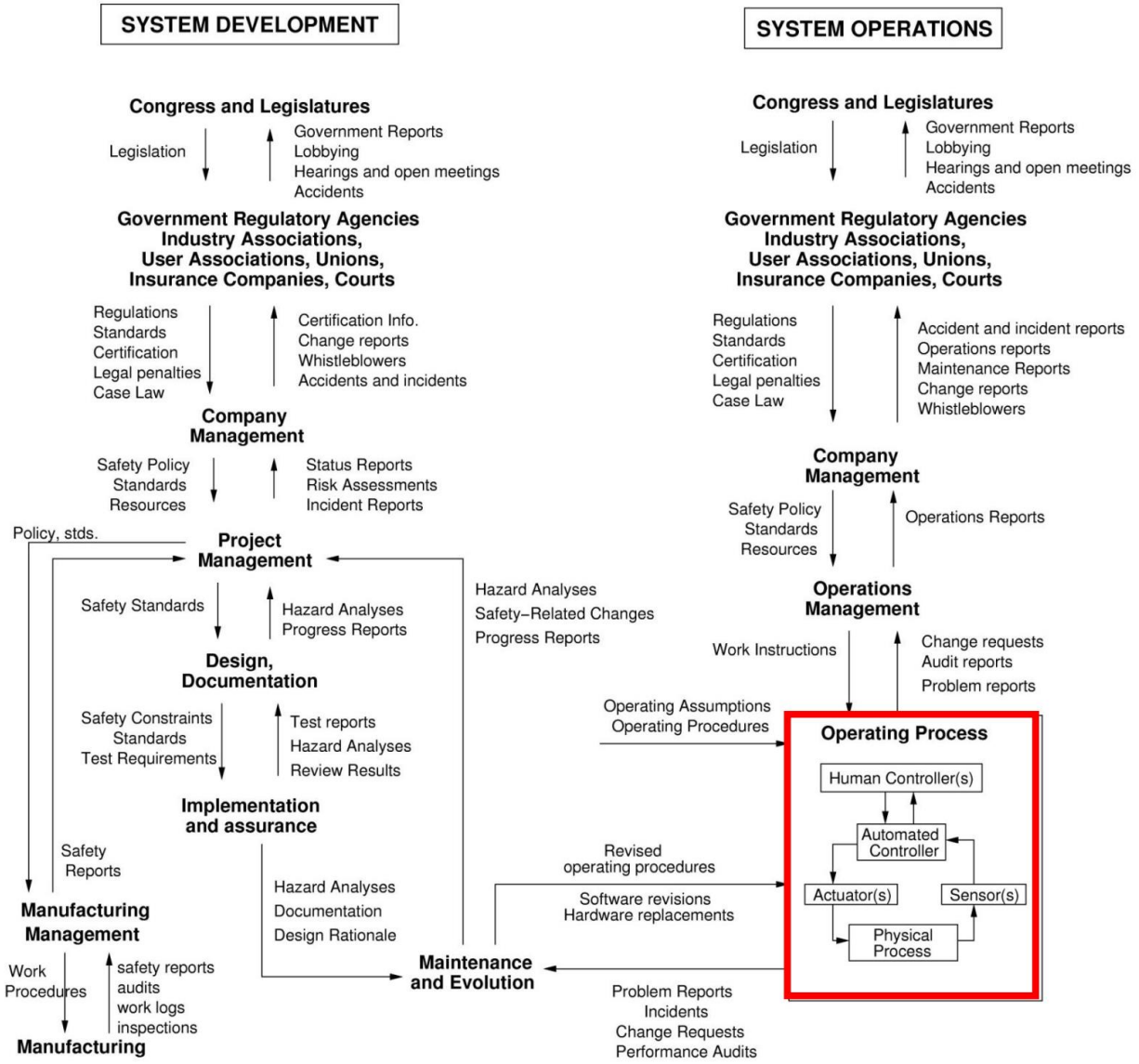


Figure III.1: General form of a model of sociotechnical control (Leveson 2012)

III.5.2. Definition of the STPA method

From the theoretical foundation provided by the STAMP model, several practical techniques have been developed to support system safety analysis. Among the most prominent of these is STPA (Systems-Theoretic Process Analysis), which is specifically designed to identify hazards in complex, software-intensive, and socio-technical systems. STPA translates the core principles of STAMP into a systematic method for hazard identification and causal analysis. Unlike traditional techniques that are based on component failures or deviations from predefined physical parameters,

STPA focuses on the control structure of the system. It examines how safety-related functions are executed through interactions and feedback between system components.

A key distinction between STPA and other conventional methods like HAZOP lies in the type of system model used for analysis. While traditional techniques often rely on physical component diagrams, STPA uses a functional control diagram. This shift reflects STPA's emphasis on the role of inadequate control in accident causation. In this view, hazards are not just the result of physical or mechanical failure, but can arise from unsafe control actions, flawed process models, or missing feedback paths. As a result, STPA facilitates a deeper understanding of system behavior, particularly in systems where software, human operators, and organizational elements play a central role in maintaining safety.

One of STPA's strengths is its flexibility—it can be applied at any stage of the system life cycle. Whether during early design, system development, manufacturing, operation, or even during system modification, STPA provides insights and documentation necessary to ensure that appropriate safety constraints are identified, specified, and enforced. This makes STPA particularly valuable in modern engineering environments where systems evolve over time and interact with dynamic operational contexts. As Leveson (2012) emphasizes, the ongoing changes in these stages require continuous assurance that safety constraints remain valid and effective throughout the system's life span [29].

III.6. Overview of STPA procedure

III.6.1. Methodology

The STPA approach has been under continuous development since emergence, and its framework can be complicated with respect to the analytical needs and constraints for practical use. According to the STPA Handbook (Leveson and Thomas, 2018), the steps in basic STPA are illustrated in **Figure III.2**.

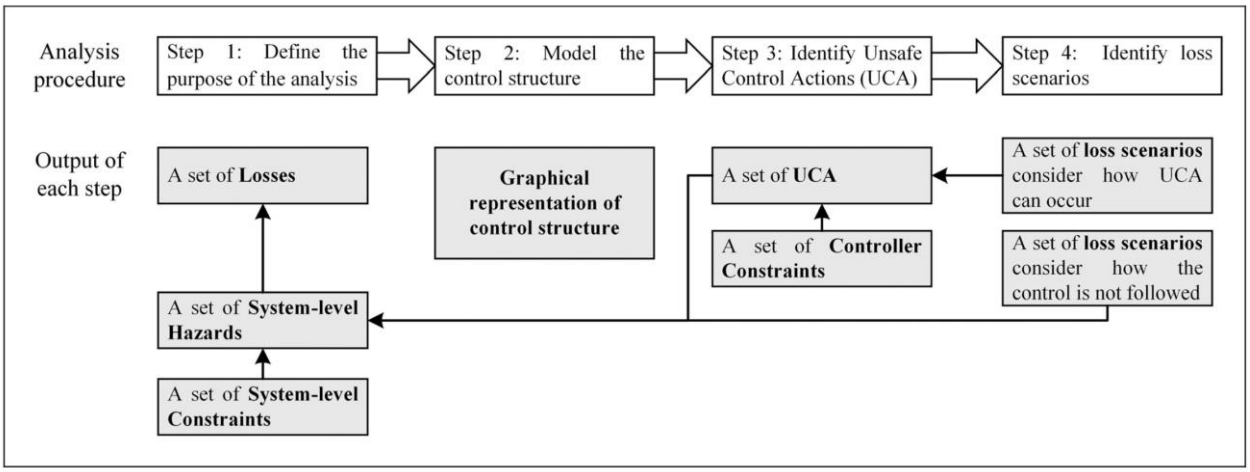


Figure III.2: Framework of STPA and its output. [30]

III.6.2. STPA steps

III.6.2.1. Step 1: Define the purpose of analysis

The first step is to define the scope of analysis by identifying the system- level consequences in the presence of any single or multiple variations in feedback control loop. The con- sequence includes the losses and associated hazards. Losses could be any type of dissatisfactory value to stakeholder when the system fails to achieve its goal and objective, and system-level hazards are a set of sys- tem states that can lead to losses together with worst- case conditions. Such broad definition of losses and hazards implies that STPA covers traditional safety issues as well as RAM issues.

Leveson, for instance, adopts a general accident definition which includes general (material) losses, as well as human injury, as follows:

"Accident is an undesired or unplanned event that results in a loss, including loss of human life or human injury, property damage, environmental pollution, mission loss, etc". [30]

III.6.2.2. Step 2: Model the control structure

The next step is to develop feedback control loops. The hierarchical control structure is composed of one or more feedback control loops and visualizes actors involved, control actions and feedback information. The objective is to have the global and complete vision about the hierarchy concern being controlled, thus supporting steps 3 and 4. An example of a feedback

control loop is illustrated in **Figure 3**; from left to right, the details are added based on the responsibilities assigned to each actor. The hierarchical control structure can be refined until the suitable granularity is reached.

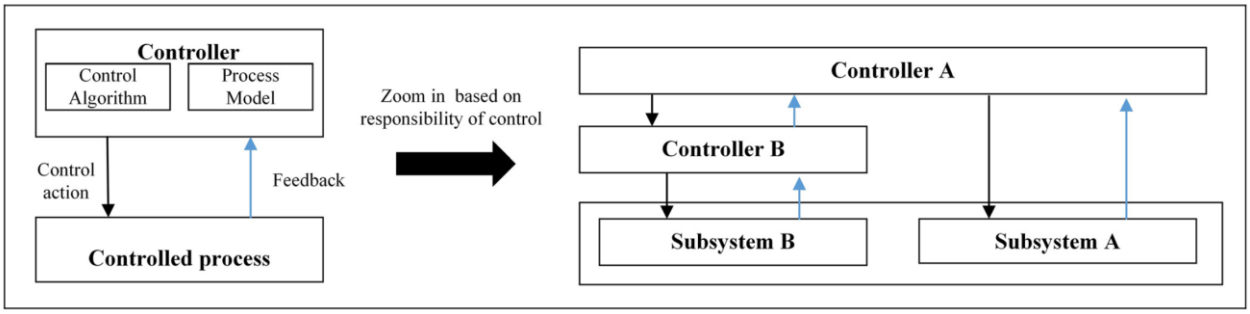


Figure III.3: Example feedback control loop. [30]

III.6.2.3. Step 3: Identify unsafe control actions

The third step relies on the structured identification of what can go wrong, using the feedback control loop and a prepared context table as basis. The output of this step is a list of unsafe control action (UCA) that in particular context results in one or more of the hazards identified in step 1. The UCAs are identified through four guide conditions taking advantage of control structure: (1) control action is not provided; (2) the UCA is provided; (3) control action is provided too late, too early or out of sequence; and (4) control action is stopped too soon or applied too long (applied only for continuous control). The constraints for controller can be defined as conditions or behaviors to prevent occurrence of UCAs (and ultimately prevent related hazards).

III.6.2.4. Step 4: Identify loss scenarios

Loss scenarios are used to describe the causal factors that lead to hazards (and ultimately to losses in worst condition).

The first type of loss scenario considers how the UCA can occur, including the causes of unsafe controller behavior and inadequate feedback.

The second type of loss scenario considers how the safe control action is not followed, including the causes of deviated control path and controlled process.

The control structure obtained through step 2 needs further refinement by including the sensors and actuator of the control loops so that analysts can examine why the feedback is not detected or wrongly detected and why the control action is not followed or improperly followed by actuators.

III.7. Purpose of STPA

All these steps involve examining parts of the control loop for each unsafe control action, to see whether the system's design or existing risk mitigation measures can be improved—or simply assessed, if the analysis is being done on an already existing design. When there are multiple controllers involved in managing the same component or safety constraint, this helps identify potential conflicts or coordination issues.

It's also important to consider how the existing controls might weaken over time and to build in safeguards accordingly. This includes:

- **Change management procedures**, to make sure safety constraints are still enforced during system updates or modifications.
- **Performance audits and operational reviews**, which help detect underlying causes of violations of safety rules or assumptions made during earlier risk assessments.
- **Incident analysis**, to trace back and understand how existing hazards may have slipped through during the system's original design. [30]

III.8. Applications of STPA

The STPA method is applicable in a variety of fields due to its structured approach to safety evaluation and risk management. Below are some significant areas where STPA proves to be especially useful [31]:

III.8.1. Aerospace

The STPA is widely used in the aerospace industry for safety analysis of aircraft systems, including avionics, autopilot systems, and ground controls. By focusing on the complex interactions between hardware and software, STPA helps identify potential errors that could

jeopardize safety at all stages of flight. This systematic approach ensures that safety measures are effectively incorporated into the design and operation of aerospace systems, ultimately improving the reliability and safety of air traffic.

III.8.2. Automotive

In the automotive industry, STPA is applied to analyze vehicle safety-critical systems, such as advanced driver-assistance systems (ADAS), automatic driving functions, and vehicle-to-vehicle communication. STPA identifies unsafe control actions and their causality, which is of prime importance while developing safer automated driving systems. By mitigating these risks, STPA ensures the overall reliability and safety of modern vehicles, avoiding accidents and making roads safer.

III.8.3. Healthcare

STPA significantly benefits the healthcare sector, particularly the safety analysis of medical equipment, hospital computer systems, and patient care procedures. By identifying risks due to device interactions, user error, and system failure, STPA enhances patient safety and care quality. With this method, healthcare organizations can anticipatively address risk before it arises, such that medical systems operate safely and without inefficiency.

III.8.4. Nuclear Power

STPA is applied in the nuclear power industry for analysis of the safety of nuclear reactor control systems, emergency responses, and human performance during operations. The method ensures that the provisions for ensuring safety are put in place to prevent accidents and minimize the effect of potential malfunctions. By analyzing interactions within complex nuclear systems, STPA guarantees the safety and reliability of nuclear power plants.

III.8.5. Chemical and Petrochemical Industries

STPA is extensively used in the petrochemical and chemical industries to evaluate chemical processes, storage terminals, and hazardous materials transportation for safety. The method

identifies unsafe control actions that can lead to chemical spills, explosions, or other hazard events. STPA promotes operational safety in these dangerous environments and avoids accidents as well as protects workers and the surrounding community.

III.8.6. Rail Transport

STPA is applied in rail transport to conduct safety analyses of train control systems, signaling systems, and man-machine interfaces. By evaluating failure points in control and communication systems, STPA enhances rail transport safety by safe guarding passengers and cargo. The process enables one to assess the hazards that will cause accidents, thereby improving the safety of rail networks.

III.8.7. Manufacturing

STPA is also beneficial to the manufacturing sector, particularly in safety analysis of automatic manufacturing lines, robots, and human-robot collaboration. With the establishment of risks in machine operation, exposure of workers, and process control, STPA facilitates safer manufacturing plants. It is a method that helps organizations apply safety interventions effectively, reduce the frequency of accidents, and improve operation performance.

III.8.8. Energy and Utilities

In the energy and utilities industry, STPA is used to conduct safety analysis of power generation systems, grid operation, and renewable energy systems. By ensuring the reliability and safety of energy systems, particularly in the integration of renewable energy sources, STPA acts to minimize energy production and distribution risks. The method is crucial to maintaining the stability and safety of energy facilities.

III.8.9. Information Technology and Cybersecurity

STPA is also used in information technology and cybersecurity, where it is used to analyze safety and security in software systems, networked systems, and critical infrastructure. It is used to determine the potential vulnerabilities in system interactions that can lead to safety events or

security breaches, thus enhancing the overall resilience of IT systems. This predictive capability is critical in safeguarding sensitive information and providing safe operation of technology-based systems.

III.8.10. Defense and Military

In the defense and military sector, STPA is employed for safety analysis of weapon systems, command and control systems, and logistics operations. By enhancing operational safety and effectiveness, STPA plays a vital role in ensuring the safety of military operations. This method helps identify potential risks in complex military systems, contributing to mission success and the protection of personnel**.**

III.8.11. Construction and Civil Engineering

Finally, in construction and civil engineering, STPA is applied to safety assessments of construction processes, equipment operation, and site management. By identifying potential hazards in construction activities, STPA improves worker safety and project outcomes. This systematic approach ensures that safety considerations are integrated into all phases of construction, reducing the risk of accidents and enhancing overall project success.

Overall, STPA's versatility makes it applicable in any domain where complex systems operate, and safety is a critical concern. By focusing on system interactions and control processes, STPA provides a robust framework for identifying and mitigating risks, ultimately enhancing safety across various industries.

III.8. Advantages and Limitations

The new insight brought by STPA is its systematic characterization of erroneous or inappropriate control actions and the associated causality. It considers all potential contributors to system losses—hardware, software, human, and organizational factors—as elements within a feedback control loop. Loss scenarios are identified when combinations of control commands, inadequate feedback, and the state of the controlled process and its environment lead to unsafe conditions.

This structured approach to hazard identification extends beyond the scope of traditional methods based largely on engineering intuition and hardware faults. In this respect, STPA is well-suited for analyzing modern subsea or industrial systems that are increasingly intelligent and software-dependent.

While STPA theoretically increases the coverage of potential hazards, it currently focuses strictly on qualitative aspects. The method lacks formal guidance on how to transition its insights into quantitative assessments. This limitation creates challenges for designers who must interpret STPA outputs and make critical decisions, such as prioritizing safety improvements or evaluating trade-offs between cost and risk reduction. Leveson (2012), the architect of STPA, has argued that quantitative analysis in this context may be questionable for two key reasons. First, it can shift attention away from important causal factors that are not statistically measurable. Second, it relies on probabilistic insights about future events for which no reliable historical data may exist. Assigning probabilities to systemic loss scenarios is inherently challenging and prone to error, even with expert input and detailed elaboration.

Nonetheless, there are compelling reasons to explore quantitative extensions to STPA. In practice, it is rarely feasible to eliminate all loss scenarios; countermeasures may degrade over time or fail under certain conditions. Studies such as those by Mahajan, and Wróbel show that applying STPA to technical systems raises the need for cost-benefit evaluations when selecting countermeasures. The lack of data for probabilistic modeling does not necessarily mean that probability-based approaches are inapplicable. Bjerga have argued for the inclusion of probabilistic reasoning in STPA as a way to better inform decisions under uncertainty, especially for risks stemming from complex systemic interactions.

In summary, the current STPA framework offers powerful capabilities in identifying and analyzing hazards across all facets of a system. However, it also leaves important tasks—such as prioritizing risks and evaluating the effectiveness of design changes—to the subjective judgment of designers. The potential benefits of quantification, particularly through mathematical modeling of control loops and system responses to disturbances, represent an important area for future

development.

III.9. Why using STAMP-STPA?

The first reason to use STAMP-STPA comes from defining safety as a control problem (vs. a failure problem). Enforcing safety constraints on system behavior allows the detect and control migration of the system to states of higher risk which finally is the main cause of most accidents. Other reasons for using STAMP methodology:

- It applies to very complex socio-technical systems.
- It includes software, human and new technology.
- It is based on systems theory and systems engineering.
- It expands the traditional model of accident causation- not just a chain of directly related failure events.

When comparing STPA features with HAZOP-SIL we can find what STPA does (and HAZOP-SIL doesn't):

- Include socio-technical analysis
- Include systemic factors
- Include all the hierarchy (from regulations to the final process): safety culture
- Fill the design operation gap: avoid higher risk states

And what STPA does not do (vs. traditional safety methods as HAZOP-SIL):

- Put the blame on you (many times an accident investigation stops when a human error is found)

- Consider only reliability and probability
- Work only in the design stage (or after changes in the plant)
- Doesn't follow chains of events

III.10. Comparison with Traditional Methods

Traditional safety analysis methods such as HAZOP (Hazard and Operability Study), FMEA (Failure Modes and Effects Analysis), and LOPA (Layer of Protection Analysis) have long been used in the petrochemical industry to identify hazards and assess risk. These methods tend to tackle component-level failures and take a linear cause-effect approach. Although they are effective and mature for structured analysis, they may overlook hazards due to complex system interactions, software failures, or human-machine interface issues. In contrast, STPA is a top-down, system-oriented approach with the emphasis on unsafe control actions and also on the conditions in which they occur. It deals with the whole control structure, including hardware, software, human behavior, and organizational factors. This allows STPA to uncover accident scenarios that need not involve any component failure but instead emerge from unexpected interactions or control logic flaws. For petrochemical plants, where human interaction and automation are tightly coupled, STPA complements traditional methods by filling analysis gaps and giving a better understanding of system behavior over a range of operating states [32].

III.11. Conclusion

In this chapter, the System-Theoretic Process Analysis (STPA) method was presented as a modern approach to hazard analysis, grounded in the STAMP model. Unlike traditional techniques that focus mainly on component failures, STPA considers the entire control structure, including software, human interaction, and organizational influences.

STPA presents a significant advancement in hazard analysis for petrochemical industry, providing a powerful framework for understanding, anticipating, and mitigating complex safety risks. This sets the stage for the subsequent chapter, where the practical implementation and results of STPA in a real petrochemical plant will be examined in detail.

Chapter IV:

Presentation of the CP2K Complex (SONATRACH – Skikda)

IV.1. SONATRACH – The Algerian Hydrocarbon Company

IV.1.1. Definition of SONATRACH

SONATRACH is the Algerian national company responsible for the exploration, production, transportation, refining, transformation, and marketing of hydrocarbons. Since its establishment in 1963, SONATRACH has rapidly expanded across the entire hydrocarbon value chain—from upstream (exploration and production) to midstream (pipeline transport and liquefaction) and downstream (refining, petrochemicals, and distribution)—to become a fully integrated oil and gas group of international statures [33].

IV.1.2. Core Activities of SONATRACH

- Exploration and Production (E&P)
- Pipeline Transportation (TRC)
- Liquefaction (LGS)
- Marketing and Sales (COM)
- Refining and Petrochemicals (RPC) [27].

IV.2. The CP2K Complex

IV.2.1. Introduction

The CP2K complex is a production unit specializing in high-density polyethylene (HDPE), with an annual production capacity of 130,000 tons, serving both local and international markets.

The facility uses the following raw materials:

- **Hexene**: imported in containers, with a storage capacity of 250 m^3
- **Ethylene**: imported
- **Isobutane**: supplied by GL1K, located nearby, with storage capacities of 2 x 265 m^3 for fresh isobutane and 170 m^3 for recycled isobutene [27].

IV.2.2. History

- **1988**: ENIP and REPSOL agree to initiate the HDPE project

- **1989** : Listed among the Algerian government's priority projects

- **March 1990** : ENIP and REPSOL sign a memorandum of understanding; POLYMED company established in December

- **1991** : Project contract signed

- **1991–1995** : Securing Spanish financing

- **1995–1996** : Engineering studies resumed; construction begins

- **1997–1998** : Civil and structural works carried out

- **March 2002** : Plant construction completed; POLYMED financial restructuring signed

- **January 16, 2004** : POLYMED plant officially launched

- **2011** : ENIP fully reintegrated into SONATRACH as the Petrochemical Division (PEC); POLYMED renamed CP2K [27].

Figure IV.1: CP2K Complex

IV.2.3. Site Location and Layout of the CP2K Complex

The CP2K complex, which includes the HDPE (High-Density Polyethylene) unit, is located within the industrial zone of Skikda. Covering an area of approximately 17 hectares (166,800 m²),

of which 10% is built-up, the complex lies along the coast, 6 kilometers east of Skikda's provincial capital, at an average elevation of about 6 meters above sea level.

Its boundaries are as follows:

- **North**: Bordered by the Mediterranean Sea
- **South**: Bordered by the main road of the industrial zone and SOMIK
- **East**: Bordered by the Intervention and Reserve Force (FIR)
- **West**: Adjacent to the CP1K complex [27].

Figure IV.2: and use of the CP2K complex [27].

Figure IV.3: Geographical position of the complex [27].

The complex is divided into four primary zones, which are:

- **Off-site Zone**: This area includes utility systems (boilers, air, nitrogen, distilled water, firewater) and auxiliary installations such as: the flare system, storage tanks for isobutane and hexene, water treatment units, and the catalyst activation station.
- **Wet Zone**: Contains the reactor, processing units, compressors, solvent purification and recovery systems.
- **Dry Zone**: Includes the extruder, blowers, silos for finished product storage, and the bagging section.
- **Building Zone**: Hosts administrative and finance offices, cafeteria and locker rooms, security and medical block, spare parts warehouse, maintenance workshop, high and low voltage substations, the control room, and the laboratory [27].

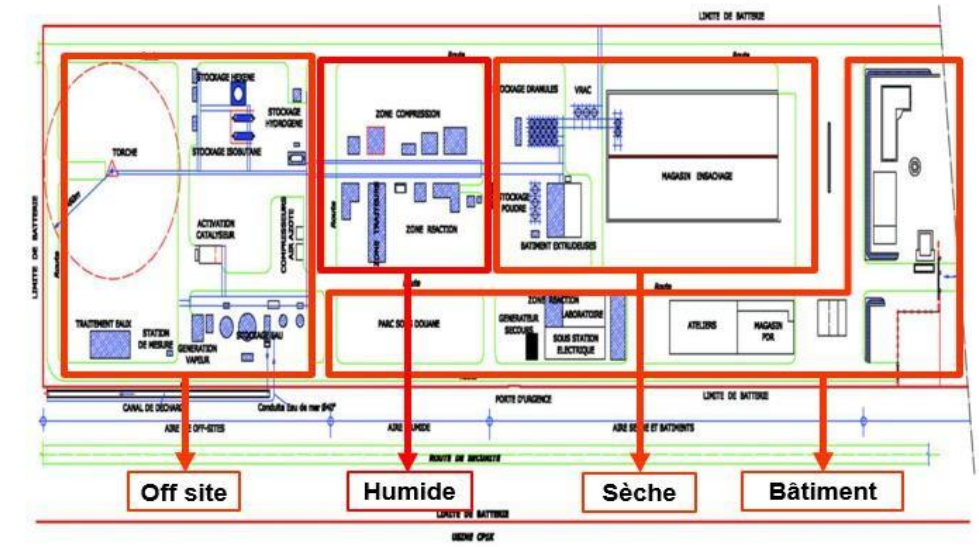


Figure IV.4: The primary zones of the complex CP2K [34]

IV.2.4. The Organization of the CP2K Complex

The complex is composed of several departments, and each department consists of multiple services.

IV.2.4.1. Production department

It includes the three zones of the complex previously mentioned (off-site zone, wet zone, and dry zone), which are grouped into two types of installations:

• Main installations of the plant: Unit for the preparation and processing of raw materials.

- Reactor where polymerization and the recovery of HDPE in powder form take place.
- Extruder that transforms the powder into pellets.
- Intermediate storage (Capacity 3500 Tons).
- Packaging unit.
- Auxiliary installations:
- Production of steam, electricity, air, etc.
- Effluent treatment.
- Storage of raw materials used and additives (Water, Hydrogen, Hexene, Isobutane).
- Finished product storage warehouse with an area of 18,000 m², i.e. a capacity of 12,000 tons.

IV.2.4.2. Technical Department

It is a very important department that works in parallel with the other departments. It consists of three services:

- **Study/Monitoring Service:** whose work focuses on studying problems that may be encountered in the different departments and making the necessary modifications. The study of new projects is also carried out within this service.
- **Inspection Service:** whose role is to validate the equipment and installations through programmed systems.
- **Laboratory Service:** whose task is to continuously analyze the raw material, the catalyst, and the final product.

IV.2.4.3. Maintenance Department

This department is responsible for the upkeep and maintenance of equipment. It consists of:

- Methods Service: divided into two sections, the planning section and the preparation section
- Mechanical Service
- Electrical Service
- Instrumentation Service

The work of this department is divided into two parts: a scheduled periodic task for each piece of equipment, and tasks carried out in response to requests made by the Production Department in case of breakdowns. In this second case, the work is first planned, then prepared, and finally sent to the concerned service, which always falls under the Maintenance Department.

IV.2.4.4. Safety Department

Like all factories, the CP2K complex has a safety department, which in turn includes two services:

- **Prevention Service**
  - To control and report any situation or procedure that violates internal regulations and legal provisions regarding safety, health, and the environment.
  - To analyze incidents and accidents.
  - To eliminate dangerous acts, specifically acts committed by a person:
    - Who is unaware of the risks to which they are exposed and/or to which they expose others.
    - Who does not develop, apply, or enforce appropriate preventive measures for these risks.
  - To eliminate dangerous situations, i.e., the defective condition of equipment, organization, or environment:
    - That creates a sufficient condition contributing to the occurrence of an accident or generating a health risk,
    - On which the direct actors have no means to act.

- **Intervention Service**

The mission of the intervention team is to respond using appropriate fixed and mobile means in the event of a fire or accident.

It also ensures the organized and planned inspection and maintenance of fixed and mobile fire-fighting equipment.

→ Mobile equipment:

- Combined foam truck (water – foam concentrate) with a capacity of 6000 and 2000 liters respectively.
- Powder truck with a capacity of 2000 kg.
- Towable powder and CO2 extinguishers: 70 units.
- Portable powder and CO2 extinguishers: 200 units.
- Medical ambulance.

Figure IV.5: Mobile equipment of the intervention service

→ Fixed equipment

The HDPE complex is equipped with:

- ❖ A fire-fighting water network (enameled looped system) that supplies fire hydrants, sprinklers, and fire hose reels (FHR). Using a jockey pump, the network is continuously maintained at a pressure of 12 kg/cm².
- ❖ A deluge system combining detection and automatic water spray extinguishing.

The HDPE complex has 13 deluge systems with manual, semi-automatic, and automatic controls. They are supplied through the fire-fighting network and distributed across all critical installations of the plant, including:

- 1 system installed at the extruder
- 1 system installed at the reactor
- 4 systems installed at the treaters
- 4 systems installed at the compressors
- 3 systems installed at the hexene and isobutane storage area

❖ Fire-fighting pumps

- Jockey pump: its role is to maintain the pressure at 12 kg/cm² in the fire-fighting water network
- Motor pumps: there are 2 electric pumps with a flow rate of 700 m³/hour at a pressure of 13 kg/cm² with an automatic start system. The two pumps are connected to the preferential electric network powered by the emergency generator.
- Diesel pump: Driven by a diesel engine with a flow rate of 1500 m³/hour at 13 bar, with both manual and automatic start systems.

IV.2.5. HDPE

IV.2.5.1. Definition of Finished Product

High-density polyethylene or HDPE (in French PEHD): is a polyolefin derived from the polymerization of ethylene, with a density ($0.95\ g/cm^3 < \rho < 0.97\ g/cm^3$) under specific temperature and pressure conditions [27].

Figure IV.6: HDPE

IV.2.5.2. Uses of HDPE

- PIPE: Grade TR 402 (Water Pipe), Grade TR 418 (Gas Pipe)
- Blow Molding: Grade HDPE 5502 (small and large bottles)
- Film: Grade HDPE TR 140 & TR 144 (General use for all types of bags)
- Injection: Grade HDPE 6080 (Pallets, crates, jerrycans, caps, cases, household items)
- griculture: Film, fishing net, irrigation pipe, crates [27]

IV.2.5.3. HDPE Grades Produced at CP2K

Given that HDPE has a wide range of applications—such as pipe manufacturing, plastic films for various uses, bottles, etc.—different grades must be produced. Therefore, the CP2K complex offers a full range of HDPE comprising nine different grades. These grades are characterized by their melt flow index and density, as shown in the following table:

Grade	Indice de fluidité (Poudre/Granulé)	La densité	L'utilisation
TR402	0.11-0.19/0.08-0.14	0.9430-0.9460	Pipe :(tube eau)
TR418			Tube gaz
TR140	0.33-0.48/0.20-0.36	0.9430-0.9480	FILM : usage général toute sacherie
TR144	0.25-0.38/0.14-0.24	0.9420-0.9470	FILM : usage général toute sacherie
5502	0.55-0.70/0.27-0.43	0.9530-0.9580	Soufflage : des bouteilles de petite et grande taille
6006L	0.80-1.15/0.47-0.73	0.9570min	Soufflage : des bouteilles de petite et grande taille
6080	7.0-10.0/6.80-9.20	0.9590-0.9650	Injection :palette,caisse,bidon ,bouchon,casier,articlrs de menage
6030	2.0-3.80/1.80-3.20	0.9590-0.9650	Injection:palette,caisse,bidon, bouchon,casier,articlrs de menage
6040	3.0-5.80/2.80-5.20	0.9590-0.9650	Injection :palette,caisse,bidon ,bouchon,casier,articlrs de menage

Table IV.3: HDPE Grades Produced by the CP2K Complex

IV.2.6. Phillips Process

The Phillips process, also known as the PF process or particle process, which is the basis for the POLYMED complex, uses a chromium-based catalyst and requires high purity of raw materials. It tolerates only trace amounts of poisons that could inhibit the catalyst's activity or affect the quality of the final product. Polymerization takes place in a loop reactor, where solid particles form in a

solvent medium. The process ends with the polymer finishing system, which includes extrusion and drying.

The result is a pellet of a specific size and quality, suitable for a wide range of applications. The main raw materials used are:

- Ethylene in gas phase, the main feedstock, supplied from CP1K located nearby, or imported (from Italy, Libya, Spain, Saudi Arabia)
- Isobutane in liquid phase, the reaction medium, supplied from GL1K, also located nearby
- Hexene in liquid phase and hydrogen in gas phase, used in small quantities
- The catalyst: chromium oxide (Cr_2O_3) [34]

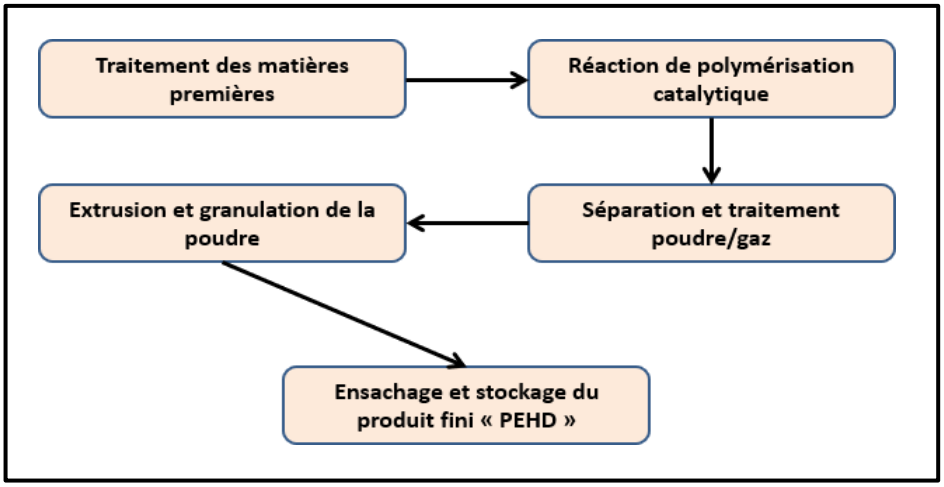


Figure IV.7: HDPE process [34]

IV.2.7. Reactor 950-155

It is a piping system with an internal diameter of 560 mm, shaped in a loop, composed of four vertical sections connected by horizontal sections. The vertical sections are equipped with insulated jackets for cooling. The reactor, with a capacity of 78.3 m^3 and a length of 304 m, is made of carbon steel.

After the raw materials are processed in the previous sections, they are sent to the reactor for feeding. Recycled isobutane, hydrogen, hexene-1, and ethylene arrive at the reactor through a main reactor feed line. The hexene and recycled isobutane are mixed in a static isobutane/hexene mixer. Hydrogen mixes with ethylene and is then added to the isobutane/hexene recycled stream coming

out of the mixer. The feed of the reactor from the different streams is adjusted based on certain variables.

The liquid inside the reactor circulates at approximately 8.6 m/s by means of a special reactor pump (it can handle the 3 phases at the same time).

Operating conditions of the polymerization reaction:

The two essential conditions in the reactor are:

- **Temperature:** varies from 93 to 110°C, depending on the grade to be produced
- **Pressure:** ranges from 42 to 44 bars

The polymerization reaction is exothermic, releasing 800 kilocalories per kilogram of polymer formed. This reaction heat is removed using the water cooling system. The reactor is equipped with six settling legs, 950-160 A/B/C/D/E/F, with pipes 2210 mm long and 27.3 mm in outside diameter, coming from one of the horizontal sections of reactor 950-155. The function of the settling leg is to concentrate the solid polymer contained in the polyethylene-isobutane mixture by decantation, before the product is discharged into flash chamber 950-161 [6].

Figure IV.8: Reactor 950-155

IV.2.8. Preparation and Treatment of Raw Materials

IV.2.8.1 ***Ethylene***

Ethylene is the main reactant in the process. It must be treated to remove certain compounds before being used in the production process.

Impurities present in ethylene—such as acetylene, oxygen, carbon monoxide, carbon dioxide, and water—are removed by treaters [36].

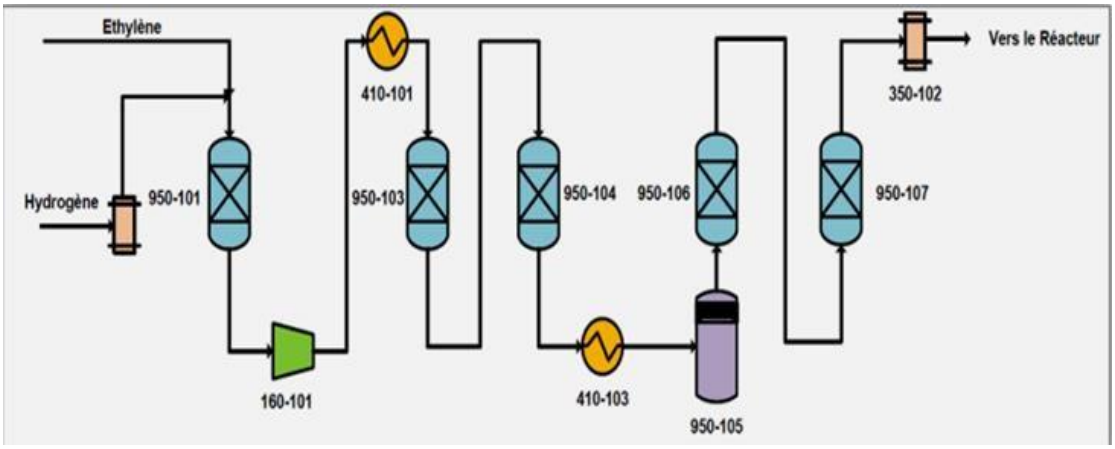


Figure IV.9: Ethylene treatment [35]

IV.2.8.2 Hexene

Hexene undergoes a process to remove water and gas absorbed in the stream. For this purpose, it is treated in a degassing column and then dried in a water removal treater, which operates by adsorbing the water using molecular sieves. [36]

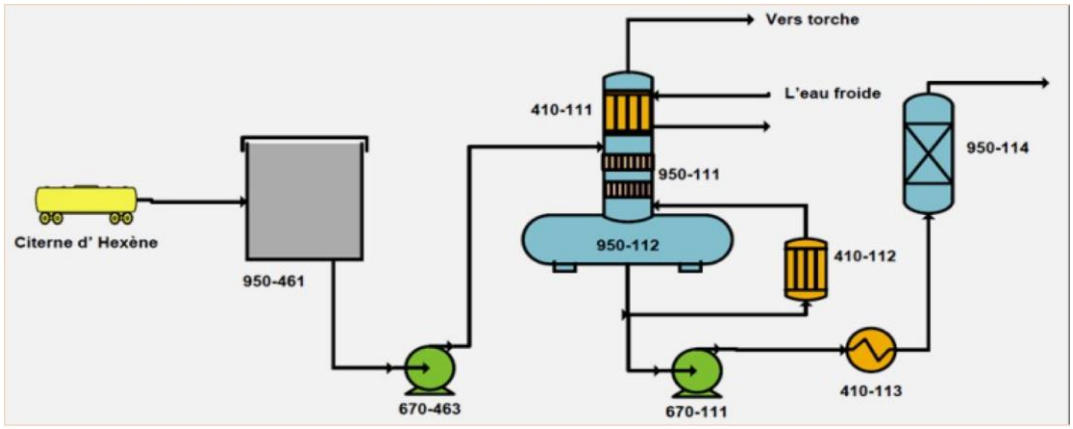


Figure IV.10: Hexene treatment [35]

IV.2.8.3 Isobutane

There are two types of isobutane: fresh isobutane and recycled isobutane:

- **Fresh Isobutane**

Fresh isobutane undergoes a process to remove water and absorbed gases in a degassing column. Then, it is dried in a water removal treater, which operates through adsorption using molecular sieves. [36]

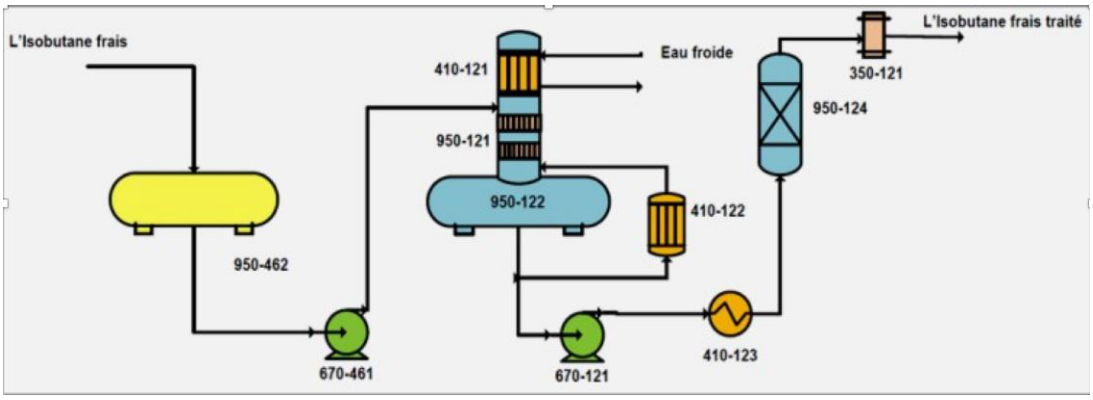


Figure IV.11: Fresh isobutane treatment [35]

- **Recycled Isobutane**

Hydrocarbon vapors exit from the top of the flash chamber and are directed to the purification and recovery system for recycled gas.

The gas is sent to a gas purification system through the recycled gas compressor. After compression, the stream enters the recycled isobutane column to separate isobutane from components such as ethylene, hexene, and other heavy products it contains.

The recycled isobutane, taken from the side extraction, is recovered and sent to the recycled isobutane storage tank. The top stream, rich in ethylene, is sent to the accumulator through the condenser of the recycling column. The non-condensable gases are fed to the ethylene vent column for separation from the isobutane. The bottom stream is sent to the dehexanization column.

100% of the isobutane and 95% of the hexene sent are recovered. The overhead vapor from this column is sent to the dehexanizer accumulator through the dehexanizer condenser. The bottom liquid, consisting of the hexene and hexane stream, is sent to the flare.

It is recovered almost entirely. It is pumped from the storage tank 950-176 to the recycled isobutane dryers 950-125 using pumps 670-172 through the cooler 410-177, where the heat

generated during pumping is eliminated. The dry and purified recycled isobutane is fed back into the reactor. [36]

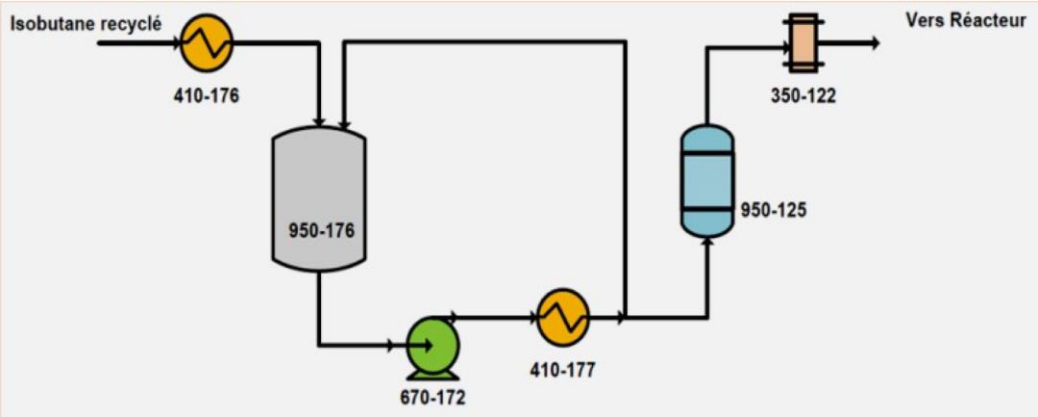


Figure IV.12: Recycled isobutane treatment [35]

Chapter V:

Study case:

Application of STPA method on the HDPE reactor

V.1. Introduction

In this chapter, we will examine the various potential accident scenarios in a polymerization reactor located at the CP2K-Skikda plant.

For this task, we chose to use the ALOHA model due to its ease of use, the ability to control multiple variables, and its free availability for simulating accident scenarios. And the A-STPA software due to its user-friendly interface, its ability to systematically manage complex systems, and its alignment with the principles of the STPA method.

Our objective with this work is to assess the effects of an accident in order to estimate safety distances and establish the necessary measures (preventive/protective) to ensure the safety of operators, equipment, and of course, the environment.

We begin first by applying the four steps of the STPA method.

V.2. The polymerization process:

The particle process is divided into a series of steps or system treatment of raw material activation and addition of the catalyst, polymerization in a reactor in the form of a loop, system of flash and drying of the polymer and purification of the recycle gas, the process ends with the finishing system of the polymer extrusion and drying thereof. The result is granulated of a certain size and of a quality suitable for a wide variety of application [33].

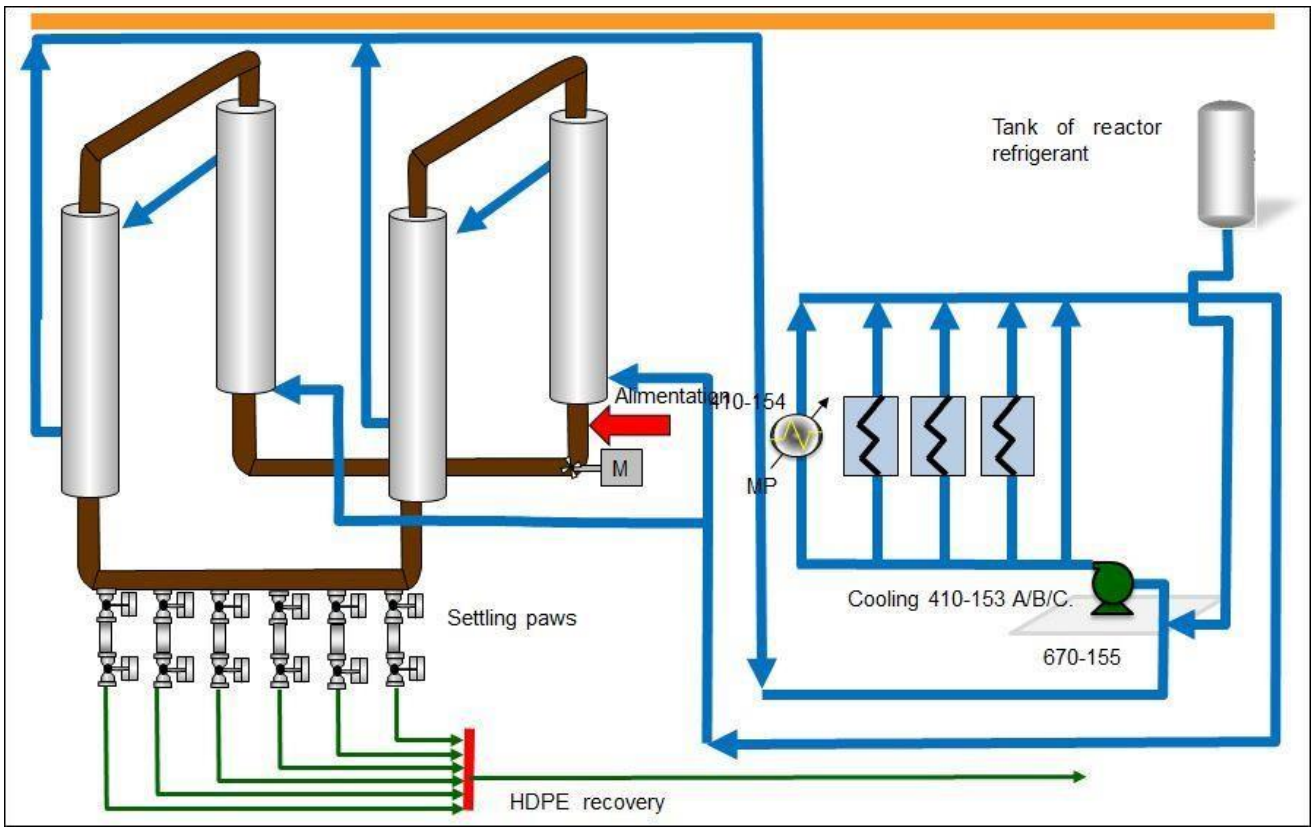


Figure V.1: The polymerization process

The reaction takes place at a temperature of 85-110C° and at a pressure of 42-44kg/cm². As the reaction is exothermic, the supply of thermal energy produced is ensured by a heat transfer fluid (cooling water) circulating in the two double jackets of the reactor [33].

The TIC17169 temperature regulator is responsible for maintaining the reactor temperature constant by acting on the external setpoint of the TIC17184 cooling temperature regulator. Note that the internal loop controlled by the TIC17184 controller is a slit-range loop [33].

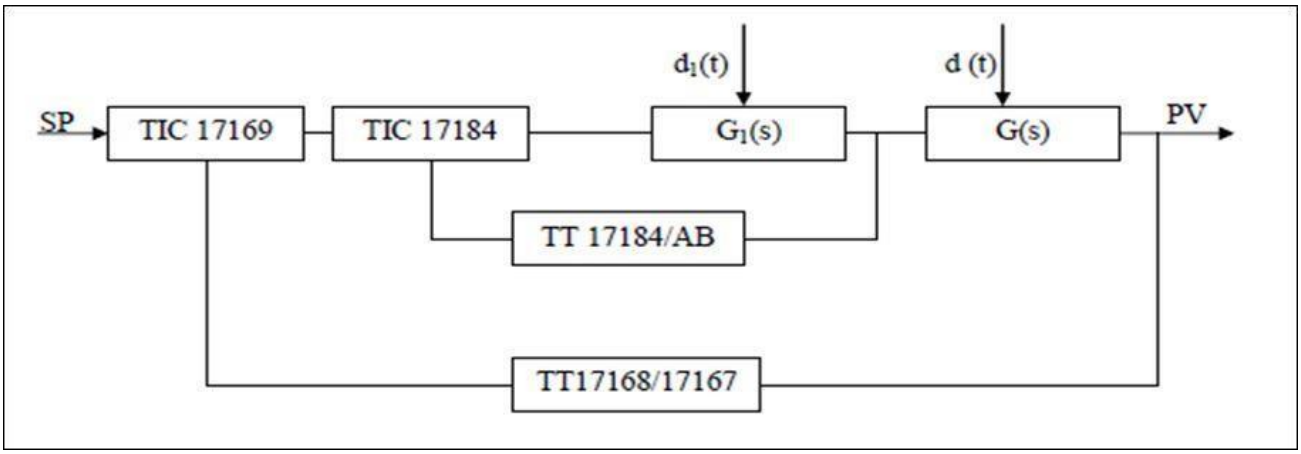


Figure V.2: Diagram of the reactor temperature loop

The objective of setting up cascade control is to make the system faster, which rapidly dampens the appearance of disturbances [33]. Where :

SP : the setpoint.

PV: the value of the process.

TIC17169: PID contoller of the external loop.

TIC17184: PID controller of the internal loop.

D1(t): the disruptive component of the inner loop.

D (t): the disruptive component of the external loop.

The principal disturbance of the temperature in the reactor is the excess of the quantity of one of the reactants in the reactor (the Ethylene, catalyzer injected etc…) which is described by the component d(t) on the one hand, and on the other hand the temperature foiling when the loop is cascaded: due to the drift of the cooling circuit described by the disturbing component d1(t) of the control cooling circuit. Generally speaking, the amount of ethylene reacted is released by the reaction, which will cause the temperature in the reactor to rise. During this temperature rise, the TIC17184 cooling temperature controller impact on the supply flow of the cooling to the hot/cold lines, by increasing the opening of the TV17184B/C/D cooling supply valves on the lines of coolers 410-153 A/B/C respectively and decrease the opening of the TV17184A/E cooling supply valve to the heater (scale sharing), including its steam line. So, it is an internal cascade control loop made up of an internal split-range loop [33].

The temperature control system is a closed circuit of treated water (water softened with chemical additives: refrigerant), this refrigerant pass through two insulated shirts with certain flow showed in DCS (FU, FV, FIC), every shirt involves two settling paws.

The temperature control of the refrigerant which regulates the reactor's temperature is done through the PID TIC-17184 controller, which commands the TV-17184B/C/D valves to lead the refrigerant to the cooling lines. It also commands the TV17184A valve to lead the refrigerant to the heating lines (vapor exchanger).

The pressure in the reactor is controlled by means of the indicator of the pressure controller PIC-16147 with indication on DCS, the reactor has two high and low pressure pressostats (PLL-PHH), integrated into the PLC.

We ensure the pressure control in the polymerization reactor by the PIC-16147 regulator which acts directly and sequentially on the 06 settling valves (06 settling paws); each paw has at the head a blocking valve and at the bottom a product discharge valve, these latter valves work alternatively with a gap of 3 seconds: in order to maintain the pressure in the stable reactor, it is to say in an interval of 42-44 bar. In certain cases of emergency or the pressure increases suddenly beyond 50 bar the controller PIC-16143 intervenes immediately on the two on-off valves called the vent valves which open leave evacuate excess pressure to atmosphere [33].

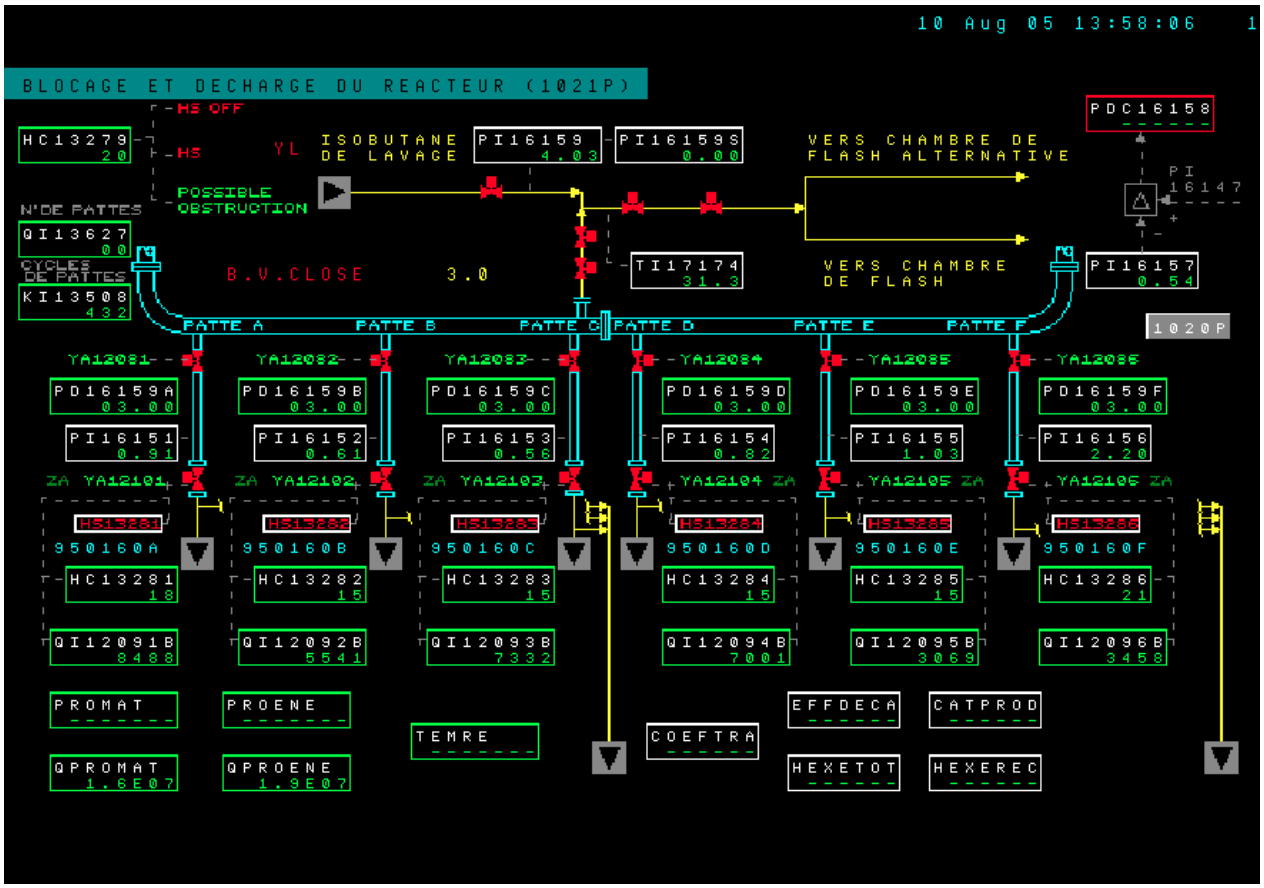


Figure V.3: A DCS view of settling paws

V.3. Application of the methodology on the reactor 950-155

In order to have more detailed safety measures it is necessary to develop a refined control structure. For this, a section of the process plant is selected and control structure is drawn to operator (**Figure V.4**)

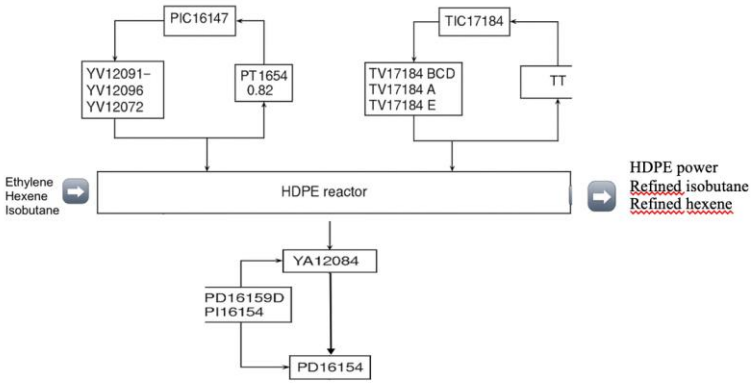


Figure IV.4: Control structure of the HDPE reactor

In our case study, we take into account changes in temperature and pressure parameters, caused by the control actions of the reactor temperature controller, the refrigerant temperature controller, heating control valves, cooling control valves, main pressure controller, emergency pressure relief controller, Discharge and block valves (settling paws) and high and low pressure pressostats

V.3.1 Application of the 4 steps of the method

Step01: Defining the purpose of the analysis

Table V.1 shows high-level system hazards and safety constraints for the Explosion scenario. The following losses are identified for the system under study:

L-1; Loss of human life or injury to people

L-2: Environmental loss

L-3: Loss or damage to asset

Then, following hazards are identified:

H-1: High Temperature in the reactor.

H-2: High Pressure in the reactor.

High-level system accident	High-level system Hazard	High-level safety constraint
Explosion	**H1:** High temperature in the reactor [L-1, L-2, L-3]	**SC 1:** The Temperature in the reactor should not exceed a specified limit. [H-1, H-2]
	H2: High pressure in the reactor [L-1, L-2, L-3]	**SC 2:** The Pressure in the reactor should not exceed a defined limit. [H-2]

Table V.1: High-level system hazards and safety constraints

In this case, the hazards can be reduced by:

TIC17169: Reactor Temperature Controller

TIC 17184: Cooling Temperature Controller

PIC-16147: Main pressure controller

PIC-16143: Emergency pressure relief controller

TV17184A/E: Heating Control Valves

TV17184B/C/D: Cooling Control Valves

YV12091–YV12096, YV12071, YV12072: Discharge and block valves (settling paws)

PT/HH and PT/LL: High and low pressure pressostats

Step02: control structure of the system

In this step, it is necessary to model the hierarchical control structure. **Figure V.5** shows the control structure of the system within the company including the process model and its variables.

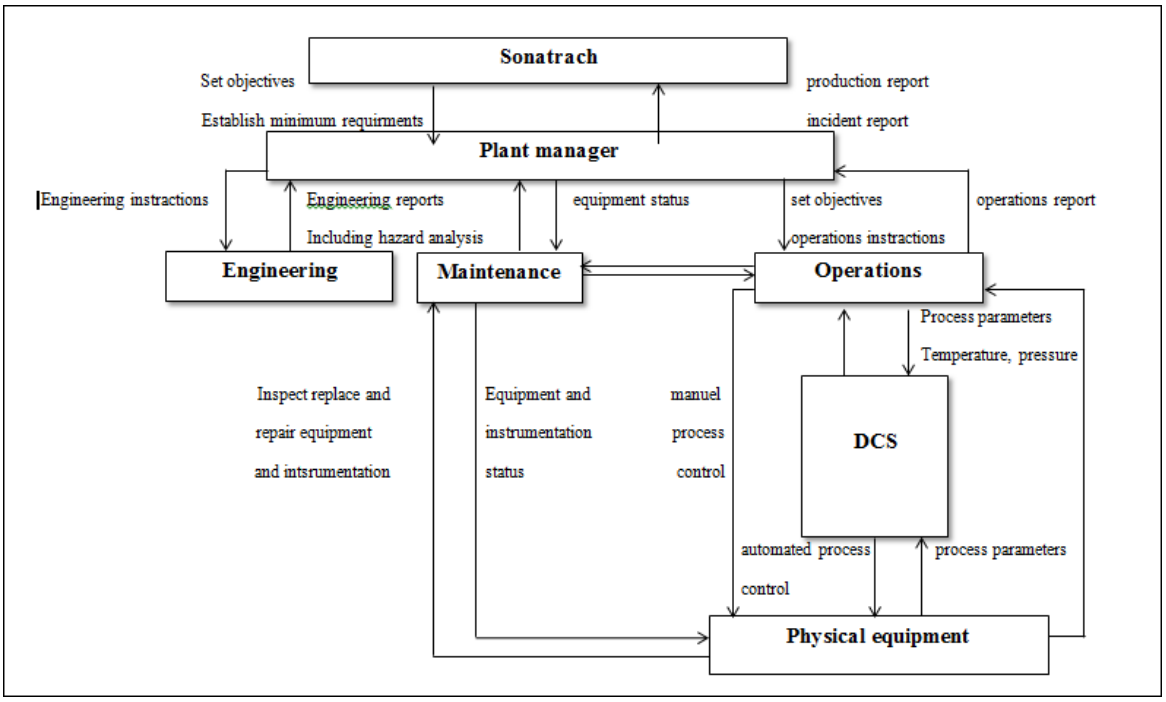


Figure V.5: General control structure of the system

Step03: Identification of Unsafe Control Actions

Once the control structure has been modeled, the next step is to identify Unsafe Control Actions (UCA). For this study, unsafe control actions up to operations and maintenance in the control structure are identified and summarized in **Table V.2**

We choose (PROVIDED, NOT PROVIDED, TOO EARLY/ TOO LATE/ OUT OF ORDER, and STOPPED TOO SOON/ APPLIED TOO LONG) as UCAs on each state.

Table V.2: Identified unsafe control actions

Control Action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long
TIC17169	**UCA-1:** TIC 17169 does not provide a control signal to TIC 17184 when reactor	**UCA-02**: TIC 17169 provides a control singal to TIC 17184 even when reactor temperature is	**UCA-03:** TIC 17169 provides a control singal to TIC 17184 too late, allowing	**UCA-04:** TIC 17169 stops adjusting the control singal too early

	temperature increases, delaying the cooling response	stable, leading to unnecessary system reaction	reactor temperature to exceed safety limits	while the reactor temperature is still above limit
TIC17184	**UCA-05** Does not control split-range valves during temperature deviation.	**UCA-06**: TIC 17184 provides control signals to the valves when no adjustment is necessary, causing overcooling or overheating	**UCA-07**: TIC 17184 sends valve control signals too late when a temperature spike is occurring	**UCA-08:** TIC17184 continues or stops controlling the valves for too long/too early, leading to ineffective temperature control
TV-17184A / E (Heating)		**UCA-9:** Open when no heating is needed		**UCA-10:** Remain open too long, causing overheating
TV-17184B / C / D (Cooling)	**UCA-11:** Do not open when cooling is needed		**UCA-12:** Open too late during a heat spike	
PIC-16147	**UCA-13:** Doesn't regulate pressure, causing instability.	**UCA-14:** Regulates unnecessarily, destabilizing system.	**UCA-15:** Acts too late after pressure rise.	**UCA-16:** Stops regulating too early or too long.

Settling Valves (YV12091–YV12096, YV12071/72)	**UCA-17:** Do not open during overpressure.	**UCA-18:** Open when not needed, causing low pressure.	**UCA-19:** Open out of sequence or late.	**UCA-20:** Stay open too long, dropping pressure.
PIC-16143	**UCA-21:** Does not open vent valves during emergency (>50 bar).	**UCA-22:** Opens vent valves during normal operation.	**UCA-23:** Activates too late.	**UCA-24:** Keeps vent open too long, wasting material.
PT/HH and PT/LL	**UCA-25:** Fail to send signal when limits are crossed.	**UCA-26:** Send false signals, triggering unnecessary actions.	**UCA-27:** Signal comes too late during real deviation.	**UCA-28:** Signal comes too late during real deviation.
Discharge Valve Actuation (YA12084 / YA12104)	**UCA-29:** Valve does not open, causing powder accumulation and potential reactor overpressure.	**UCA-30:** Valve opens when reactor pressure is unstable, causing pressure drop.	**UCA-31:** Valve opens too late in the cycle, causing overpressure.	**UCA-32:** Valve stays open longer than 3 seconds, causing a sharp pressure drop in the reactor.
Differential Pressure Monitoring (PD16159D)	**UCA-33:** Fails to detect pressure drop or blockage, allowing unsafe discharge.	**UCA-34:** Sends false signal triggering unnecessary interruption or delays.	**UCA-35:** Signal is delayed or out of sync with discharge cycle.	**UCA-36:** Signal is cut off early or held too long, confusing the control logic.
Operator responds to alarms	**UCA-37:** Operator does not respond to alarms when the reactor temperature or refrigerant pressure is		**UCA-38:** Operator responds too late to alarms, allowing the temperature or pressure to exceed	

	outside safe limits.		limits.	
Maintenance of sensors, controllers, and valves	**UCA-39**: Maintenance team does not repair or calibrate faulty temperature controllers or valves when needed.		**UCA-40**: Maintenance is performed too late, after unsafe conditions have already occurred.	

Step04: Identification of causal factors and lost scenarios

A loss scenario describes the causal factors that can lead to unsafe control actions and hazards identified in the previous step.

The obtained causal factors of the explosion accident scenarios are presented below in **Table V.3.**

Table V.3: Identified causal factors from the refined control structure

Unsafe Control Actions	**Causal Factors**
UCA-01 **UCA-05** **UCA-11** **UCA-13** **UCA-17** **UCA-21** **UCA-25** **UCA-29** **UCA-33** (Failure to	1. Mechanical valve failure (TVs, YVs) 2. Failure of instrumentation (sensors not detecting temperature/pressure correctly) 3. Incorrect transmitter readings 4. Wrong SP configuration in TICs or PICs 5. Control system software malfunction (PID algorithm issue) 6. Communication failure between TICs and final control elements

provide control action when needed)	7. Inadequate or delayed maintenance of control system 8. Controller output signal not reaching actuators.
UCA-02 **UCA-06** **UCA-09** **UCA-14** **UCA-18** **UCA-22** **UCA-26** **UCA-30** **UCA-34** (Providing action when not needed)	1. Incorrect controller logic or setpoint handling. 2. Sensor drift causing incorrect measurements. 3. Calibration error leading to false values. 4. Software bug or fault in control logic. 5. Noise/interference in communication signal. 6. Operator error during manual control override. 7. PLC misinterpretation of valid readings. 8. False differential pressure reading due to calibration drift.
UCA-03 **UCA-07** **UCA-12** **UCA-15** **UCA-19** **UCA-23** **UCA-27** **UCA-31** **UCA-35** (Control action too late, too early, or out of order)	1. Improper tuning of PID loops 2. Transmitter range or gain errors 3. Timing issues in control communication 4. Mechanical blockage or fouling (valves partially stuck) 5. Lack of preventive maintenance (dirty sensors or clogged valves) 6. Fault in sequencing logic (for paws or split-range valves) 7. Timing mismatch between discharge command and pressure status.
UCA-04 **UCA-08** **UCA-10** **UCA-20** **UCA-24** **UCA-28** **UCA-32** **UCA-36** (Control action stopped too soon or applied too long)	1. Faulty logic for deciding valve shut-off timing 2. Ambient disturbances (pressure surges, humidity, etc.) 3. Fouled or jammed valves 4. Maintenance oversight on auto-stop parameters 5. Discharge timer malfunction

UCA-39 **UCA-23** (Operator alarm response failures)	1. Alarm delay in HMI acknowledgment 2. Inaccurate alarm range for TAH17184, PAH17184 3. Inadequate training or understaffing 4. Missing alarm prioritization in HMI interface
UCA-40 (Late or no response to alarms)	1. Alarm flooding or lack of filtering 2. High workload on operators during critical moments

V.2.4 Recommendations

Finally, new safety measures are defined in the recommendation part to prevent loss scenarios that could cause the hazardous chemical explosion scenario.

Safety measures corresponding to loss scenarios are defined in **Table V.4**.

Table V.4: STPA-Derived Recommendations Based on the Refined Control Structure of the Reactor

Recommendations	
1.	Implement more preventive maintenance procedures to inspect and replace the valves (TV-17184A/B/C/D/E, YV12091–YV12096, YV12071, YV12072, vent valves) as needed.
2.	Ensure accurate configuration and validation of setpoints for all related transmitters (TT17184, PT17184, FT17184), aligning them with process safety limits and control objectives defined in the design documentation.
3.	Assess and optimize the actuation speed of the valves (TV-17184A/B/C/D/E, YV series) to ensure they open and close within acceptable time limits required for effective disturbance rejection during temperature or pressure deviations.
4.	Develop and distribute standardized operating procedures (SOPs), maintenance checklists, and valve response tuning protocols to guide operators and maintenance personnel during normal operation, troubleshooting, and system damages.
5.	Review and optimize the alarm system configuration to eliminate unnecessary alarms and ensure each alarm is relevant, properly prioritized, and actionable.

6.	Carry out alarm management practices, including configuring and monitoring alarms such as TTH17184, PAH17184, and TAH17169 to provide timely and useful information to operators about abnormal reactor and cooling conditions.
7.	Define and implement an adequate preventive maintenance and calibration program for transmitters (TT17184, FT17184, PT/LL, PT/HH), logic controllers (TIC-17169, TIC-17184, PIC-16147, PIC-16143), and final elements (TV-17184 A/B/C/D/E YV12091–YV12096) to ensure the correct operation of the temperature and pressure control loop.
8.	Audit and verify the emergency venting system (PIC-16143 and vent valves) regularly to ensure that it triggers only at the correct high-pressure limit and closes fully afterward to avoid process material loss.
9.	Validate the calibration and response range of split-range valves (TV-17184 A to E) controlled by TIC-17184, ensuring they respond accurately and proportionally across their assigned segments of the control signal range
10.	Test and validate the interlock logic associated with the reactor cooling loop to ensure automatic protective actions are taken when temperature limits are exceeded.
11.	Conduct regular functional safety assessments of the reactor temperature control loop (TIC-17169/TIC-17184) including setpoint handling, controller performance, and response of control valves to confirm compliance with industry standards and system integrity.
12.	Verify correct configuration and redundancy of pressostats (PT/HH and PT/LL), ensuring their thresholds match the protective pressure boundaries of the reactor, and that their outputs reliably reach the PLC for decision-making.
13.	Calibrate PD16159D and associated sensors periodically, and include redundancy or plausibility checks to avoid false readings that could prevent safe discharge or trigger false shutdowns.

V.4. Conclusion

In the analysis of process plant, hazards were first identified. Then controllers were evaluated to identify UCAs. The causes of UCAs and improper execution of control actions were determined to define loss scenarios. And finally, recommendations were generated to prevent, control or mitigate loss scenarios.

Analysis methods based on component failure and reliability cannot fully analyze Complex systems. The reason is that these methods do not consider the entire system and interactions between components. In that sense, systemic methods are promising and in this study STPA is applied to a process plant which is needed to be taken into consideration in risk assessment studies.

General conclusion

General conclusion

Major accidents and potential risks at the industrial level remain a critical concern, as they can severely impact system performance and safety. To address these issues, risk analysis techniques are essential to identify, evaluate, and reduce hazards within industrial processes.

This thesis presented an application of the STPA (System-Theoretic Process Analysis) methodology on the polymerization process in the CP2K unit at Sonatrach Skikda. The strength of STPA lies in its structured and systemic approach, which considers the entire sociotechnical system, including human, software, and control components.

Unlike traditional methods, STPA not only identifies unsafe situations but also offers potential solutions and safety recommendations based on the same analytical framework. This allows for a more proactive and comprehensive improvement of safety and risk management in complex industrial environments.

References

[1]. T. Wolfe, The Right Stuff. Farrar, Straus and Giroux, 1979.

[2]. Leveson, N. G. (2011). *Engineering a Safer World: Systems Thinking Applied to Safety*. MIT Press.

[3]. Leveson, N. G., & Thomas, J. (2018). STPA—A New Hazard Analysis Technique. *Safety Science*, 49(6), 818–828.

[4]. https://www.academia.edu/ _la_notion_du_risque_et_la_gestion_des_risques (page consultée le 15 avril 2025).

[5]. Farmer. F. R. (1967). Siting criteria: a new approach. Atom, chapter 128, page 152166.

[6]. Canadian center for occupational health and safety, https://www.cchst.ca/oshanswers/hsprograms/hazard_risk.html 10/05/2025

[7]. International standard ISO-IEC. (2002). Management du risque —Vocabulaire Principes directeurs pour l'utilisation dans les normes (guide). Première Edition.

[8]. Fiche DRM « le risque industriel » - DIMENC – 2014.

[9]. SayadFedoua, HamaidiWarda : Implémentation d'un système d'arrêt d'urgence du compresseur 400-K81 sur la plateforme TRICONEX / INTOUCH ; université 20 aout 1955 Skikda, 2020. la plateforme TRICONEX / INTOUCH ; université 20 aout 1955 Skikda, 2020.

[10] European Environment Agency. (2020). *Industrial pollution in Europe: Emissions, impacts and policy responses*. Publications Office of the European Union.

[11] http://www.serlienne.com/incendie.php consulter le 06/05/2025 à 18 :26.

[12]. Éric. M. (le 5 janvier 2009).les cahiers de la sécurité industrielle, risque incendie, Institut pour une Culture de Sécurité Industrielle. Foncsi, ICSI Toulouse.

https://www.jpj-executive.com/tetraedre-du-feu/ consulter le 06/05/2025 à 19 :17.

[13]. https://www.jpj-executive.com/tetraedre-du-feu/ consulter le 06/05/2025 à 20 :38.

[14]. Chebira .S.(2020). Cours. Risque incendie-explosion, Université Batna 2. Celhay.

[15] M.et Giraudo. Y. et Richard. S. (Année 2014/2015) « Facteurs de risque et prévention » Master PRNT. Université d'Aix-Marseille.

[16]. TOUAHAR. B. (2013).Modélisation et Simulation numérique pour la dispersion atmosphérique de polluant. Mémoire de fin d'étude, Université El Hadj Lakhdar- Batna.

References

[17]. Gildas. A. et Arnaud. R. et Eric .G. (Juillet 2008). Plan de prévention des risques technologiques «Caractérisation et réduction de la vulnérabilité du bâti face à un phénomène dangereux technologique thermique».

[18]. Dr Stéphane GAYET – Praticien hospitalier – Médecin infectiologue- hygiéniste, Antenne régionale de lutte contre l'infection nosocomiale (ARLIN d'Alsace) - CHRU de Strasbourg

[19]. Jérôme Tixier, Gilles Dusserre, Olivier Salvi, Didier Gaston. Review of 62 risk analysis methodologies of industrial plants. Journal of Loss Prevention in the Process Industries, Elsevier, 2002, 15 (4), pp.291-303. 10.1016/S0950-4230(02)00008-6

[20]. BennedjaiNouh, Douahi Oussama abdelghafour :Etude et analyse des risques industriels (Etude de cas) ; UNIVERSITÉ BADJI MOKHTAR- ANNABA.

[21]. Formation SF6 la Méthode HAZOP

[22]. INERIS, Outils d'analyse des risques générés par l'installation industrielle, direction des risques accidentels (DRA). 2003.

[23]. SayadFedoua, HamaidiWarda : Implémentation d'un système d'arrêt d'urgence du compresseur 400-K81 sur la plateforme TRICONEX / INTOUCH ; université 20 aout 1955 Skikda, 2020.

[24]. Jean-Pierre.D, François.F, Didier.G, Jean-Louis.G, André.L, Yves.M, Jean-Paul.P méthode danalyse des risques. Décembre 2017

[25]. Mohamed Amine. B. (01/14/19).Methodes d'analyse des Risques **«** arbres de defaillances**»**. Ecole Mohammadia d'Ingénieurs, Graduate Student.

[26]. Adel, Abd essalem Khedrougui, L'analyse et l'évaluation des risques

[27]. **Levenson Nancy**. 'STPA handbook' . March 2018

[28]. Senge 1990.p.78

[29]. Young, W., & Leveson, N. G. An integrated approach to safety and security based on systems theory. (2014).

[30]. Juntao Zhang , Hyungju Kim, Yiliu Liu and Mary Ann Lundteigen. Combining system-theoretic process analysis and availability assessment: A subsea case study. 2018.

References

[31]. Leveson, N. G. (2011). Engineering a safer world: Systems thinking applied to safety. MIT Press

[32]. Center for Chemical Process Safety. (2008). Guidelines for Hazard Evaluation Procedures.

[33]. Manuel opératoire de PHILIPS pour CP2K SKIKDA

[34]. **Levenson Nancy**. 'Engineering a safer world'. 2011

[35]. Langford, j. w. LOGISTICS: PRINCIPLES AND APPLICATIONS. MCGRAW HILL.P. 488. 1995

[36]. **Levenson Nancy**. an STPA primer version 1. August 2013